RADISYS ENGAGE MEDIA SERVER™
Containerized Decomposed Media Server User Guide

RELEASE CD18.0.1

February 2023 **007-04984-0000**

Revision History

Publication Date	Description
November 2022	Initial release.
December 2022	Version 2.0. Updated disk space requirement in *Chapter 2, Announcement Lab, on page 136*.
February 2023	Version 3.0. Updated Appendix J, *Privacy Documentation, on page 633*.

© 2022-23 Radisys Corporation. Radisys is a registered trademark of Radisys Corporation.
All other trademarks are the properties of their respective owners.

Table of Contents

Preface **18**
About this Manual 18
What's New in this Manual 18
About Related Radisys Products 18
Technical Support 19
Notational Conventions 19

Chapter 1: Product Description **21**
Key Features 21
Containerized Decomposed Media Server in the Network 23
Composition 24
Third Party Call Control (3PCC) Architecture 25
Containerized Decomposed Media Server Redundancy 26
MRFCtrl Redundancy 26
MRFP N+k Redundancy 27
MRFP N+1 Redundancy 27
Interfaces 27
Protocol Standard Compliance 29

Chapter 2: Features **34**
Media Features 34
Encoding and Decoding 34
Multiple Codec Support 34
Transcoding 37
Silence Suppression 40
Packet Loss Concealment 42
Announcements 43
Play Audio Announcement to a Port 44
Play Video Announcement to a Port 44
Delayed Announcement 45
Variable Announcements 46
Announcement Speed Control 47
Resource Reservation for Transcode Bypass Announcements 47
CRBT Random Ring 48
Text and Icon Overlay for Video Announcements 48
RTSP Interface 49

Table of Contents

Optimal Clip Selection 50
Recordings 53
Record Audio from a Port 53
Record Video from a Port 54
Optimal Clip Recording 56
Dual-Channel Recording 56
IVR/VRU 57
DTMF 57
DTMF in Conferences 59
Automatic Speech Recognition 60
Text to Speech 61
MRCP Server 62
Concurrent Play, Record, Speech, and DTMF Collection 66
Conferencing 67
Audio Conferencing 67
Video Conferencing 74
Mute or Unmute Conference 86
Enhanced Conferencing 87
RTT Conferencing 89
Voice Quality Enhancement 91
Noisy-Line Detection 91
Noise Gating 92
Noise Reduction 93
Acoustic Echo Cancellation 94
R-factor 95
Fax 96
Fax Tone Detection 96
Fax Functionality 97
TTY and T.140 98
TTY Clamping 99
Unique CNAME Identifier 100
RTP/AVPF Feedback Message 100
RTCP-PLI 101
RTCP-FIR 101
RTCP-TMMBR/TMMBN 103

Table of Contents

RTCP-NACK 108
RTCP-TWCC 109
Keyword Detection 110
Keyword Detection on Netann Conference Port 112
Dynamic Load Modeling 114
Networking Functions 115
HTTP Caching 115
NFS Caching 116
Quality of Service 117
RTCP and SRTCP 117
HTTP Resource Server Redundancy 120
Type of Service Byte/Traffic Class 121
Sophisticated Jitter Buffer Management 122
Priority Call Management 124
ICMP Backoff 125
RTP Stream Timeout 126
NAT Traversal of RTP Packets 126
Interactive Connectivity Establishment 127
Full ICE 127
ICE Lite 129
Trickle ICE 129
RTP Media Multiplexing 129
Control Protocol Features 130
SDP Capability Negotiation 130
Call Progress Analysis 131
Beep Tone Detection 132
Containerized Decomposed Media Server Load Balance 133
Management Features 135
Single Sign-On with SAML 135
Announcement Lab 136
Performance Management Features 140
Codec High Watermark 140
Security Features 141
Secure Media 141
Secure Media for SIP 141

Table of Contents

Lawful Intercept 143
SIP over TLS 144

Chapter 3: Networking Integration 145
Network 145
Connectivity to External Network 146
Layer 2 Connectivity (Ethernet) 146
Layer 3 Connectivity (IPv4 and IPv6) 146
Location of External Devices 147
NFS Servers 147
HTTP Servers 148
DNS Servers 148
Speech Servers 148
RTSP Servers 148

Chapter 4: Security and Availability 149
Initial Access 149
User Access Control 149
Access to Management Interfaces 150
Account Access Levels (Hierarchical Permissions) 150
Web-Based Management Interface 150
SNMP Interface 151
NETCONF Interface 151
SAML Interface 152
Password Configuration 152
Configurable Password Complexity 152
Lightweight Directory Access Protocol 153
Active Directory 153
OpenLDAP 154
LDAP with TLS 154
Secure HTTP(HTTPS) for Web Access 154
Port Access Control 155
Security Logging 156
Management Activity Logging 156
MRFP N+1 Redundancy 156
Redundancy Groups 157
Redundancy Role 157

Table of Contents

Redundancy Status 158
Service Mode 158
Switchover 158
Manual Switchover 158
Automatic Switchover 158
Automatic Reboots 161

Chapter 5: License Management 162
Understanding License File 162
Initial License Management 166
Provisioned Node ID 167
Retrieving the Node ID 167
Bundle License 167
Obtaining a New License File 171
Licensing Additional RTU Packages 171
Transferring a License File 171

Chapter 6: Backup and Restore 172
Backup Operations 172
Restore Operations 173
Automated Script 173
External Server 173
Containerized Decomposed Media Server 174

Chapter 7: Web GUI Overview 176
Browser Requirements 176
Logging On 176
Screen Features 177
Status Line 178
Configuration Screen 178
Maintenance Screen 178
Fault Management Screen 179
Performance Management Screen 179
Administration Screen 179

Chapter 8: Configuration 180
Node Configuration 180
Show Instance Status 180

Table of Contents

Show Node Configuration 181
Show Audio Codec List 182
Show MRCP Configuration 182
Show Jitter Buffer Templates 183
Show NFS Configuration 183
Show SNMP Agent Configuration 184
Show SNMP Trap Destinations 184
Show Video Configuration 185
Show Video Codec List 185
Show Video Recording Configuration 185
Show VoiceXML Configuration 186
Show Conference Configuration 186
Show Fax Codec List 186
Show Call Progress Analysis Configuration 187
Show Clip Path Translation 187
Show Core Allocation 187
Show Text Codec List 188
Show Resource Server Redundancy 188
Show SNMPv3 User and Trap Destinations 188
Show Per Port Statistics Configuration 189
Show MSCML Configuration 189
Show Netconf Agent Configuration 189
Show System Security Configuration 190
Show Keyword Detection Configuration 190
Show TLS 190
Show ICE Configurations 191
Set MRFP Service Mode 191
Show CPV Layout Template Configuration 192
Configure MRCP 193
Configure SIP 197
Configure Jitter Buffer Templates 210
Configure Media ICMP 213
Configure Audio Codec List 216
Configure Audio 218
    Recording Formats 219

Table of Contents

Packetization 219
Packet Loss Concealment 220
Noise Gating 220
Audio Parameters 221
Configure Opus 227
Configure EVRC 228
Configure Silence Suppression 230
Configure NFS 231
Using NFS 231
NFS Mount Points 232
External NFS Caching 232
NFS Health Check 233
Slow NFS 234
Configure RTP 235
Symmetric RTP 236
Source Port Screening 240
Secure RTP 240
Encrypt RTCP Packets for SDES 241
RFC 2198 Redundant RTP 241
Secure RTP Key Negotiation Method 241
Configure RTP Payload 242
RTP Parameters 244
Configure RTCP 247
Configure RTCP Feedback 249
Configure RTSP 253
Configure Video 254
Configure Video Codec List 261
Configure Video Recording 265
Configure SNMP Agent 266
Add SNMP Trap Destination 268
Delete SNMP Trap Destination 270
Configure SNMPv3 User and Trap Destination 271
Delete SNMPv3 User 273
Configure Transcode Bypass 274
Configure HTTP Media and Cache 275

Table of Contents

HTTP Operating Modes 275
Cache Behavior 276
Cache Control 277
Post-processing CGI Scripts 278
HTTP Parameters 278
Configure Resource Management 281
Configure VoiceXML Parameters 287
Configure Conference 289
Large Conferences 289
Configure Fax 292
Configure Fax Codec List 294
Configure Call Progress Analysis 295
Configure Clip Path Translation 298
Configure Text 299
Configure Text Codec List 300
Configure Resource Server Redundancy 300
Configure Per Port Statistics 303
Configure EVS 309
Configure SIP Load Balancing 312
Configure MSCML 314
Configure Netconf Agent 318
Configure System Security 318
Configure CPV Layout Template 321
Configure Lawful Intercept 322
Manage Certificates 323
Configure Keyword Detection 328
Keyword Description Package File 328
Format of the model text File 328
Format of the Mode Type File 329
Add SMIL File 332
Configure TLS 333
Configure ICE 336
Media Storage Management 339
Show Audio Segment Configuration 339
Show Audio Segment Storage 339

Table of Contents

Show DRI Parameters 339
Delete Recorded Clips 340
Configure Audio Segments 340
Backup Audio Segment Configuration 342
Retrieve Audio Segment Errors 343
Configure Local Persistent Recording Path 345
Delete Local Persistent Recording Clip 346
Announcement Lab 347
Containerized Decomposed Media Server AnnLab 347
Mass Provisioning 348
Virtual File System Management 349
Audit 349
AnnLab Prerequisites 350
Configure Local Root Directory Path 352
Configure DRI Parameters 354
Add DRI Library 357
Delete DRI Library 358
List DRI Library 359
Network Management 360
Show ToS/Traffic Class 360
Configure ToS/Traffic Class 361
MRFP Redundancy 366
Show MRFP Redundancy Groups 367
Manage MRFP Redundancy Groups 367
Delete MRFP Redundancy Group 370

Chapter 9: Web GUI Maintenance 371
Web GUI Maintenance Options 371
Show Software Versions 371
Show License PortLimits 371
Show License Thresholds 372
Show Licensing 372
Show Scheduled Backup 372
Configure License Thresholds 373
Configure NodeID 373
Manage Licensing 374

Table of Contents

Provision License 375
Backup Configuration 376
Restore Configuration 378
Dump Configuration 381
Full Backup 383
Full Restore 385
Configure Scheduled Backup 388

Chapter 10: Fault Management 393
Alarms 393
About Alarms 393
Alarm Severity 393
Alarm States 393
3GPP Alarm Formats 394
Kafka Alarm Formats 394
Generic Alarm Template Formats 395
Fault Management (Alarm) Data Integration 395
Sample Fluentd Configuration File 397
Alarms Options in Web GUI 398
Events List Page 398
View Alarms 399
Show Alarms Configuration 400
Configure Alarms 401
Logs 403
About System Logging 404
System Log Severity 404
System Log Modules 405
System Log Destinations 405
Viewing System Logs 406
Protocol Logging 406
Logging Options in Web GUI 407
Show System Log Destination Configuration 407
Show System Log Severity Configuration 407
Show Protocol Log Config 408
Configure System Log Destination 408
Configure System Log Severity 409

Table of Contents

Configure Protocol Log 410
Retrieve System Log 411
Retrieve Protocol Log 413
Diagnostics 415
Show Fatal Error and Log Package Configuration 416
Retrieve Diagnostics File 416
Configure Log Package Transfer 418
Transfer Log Package 419
Delete Log Package 422

Chapter 11: Performance Management 424
About Statistics 424
Viewing Statistics 424
Statistics File in Text Format 425
General Header 426
Slot Header 426
Group Header 426
Statistics Data 427
Statistics File in XML Format 428
XML File Content 429
XML File Sample 430
Prometheus Support on Performance Management 433
Web GUI Statistics Options 464
Reset Statistics 464
Retrieve Statistics 465
Configure Statistics 468
Show High Watermarks 470
Show Statistics Configuration 470
Show Statistics History 470
Show Real-Time Statistics 471
Show Current Active Ports 472

Chapter 12: Administration Management 473
User Accounts 473
Valid User Names 474
Valid Passwords 474

Table of Contents

Access Levels (Hierarchical Permissions) 475
Management Activity Logging 476
Administration Options 477
Change Password 477
Show Authentication Configuration 477
Show Password Complexity Configuration 478
Show Users 478
Show HTTP Server Configuration 479
Show Management Activity Log Configuration 479
Show SANE Configuration 479
Configure User Authentication 480
Configure Password Parameters 487
Configure Password Complexity 488
Configure Local Provisioned Users 490
Configure Web Interface 492
Configure HTTP Server 493
Configure Management Activity Log 496
Retrieve Management Activity Log 497
Retrieve Management Activity Log (With Usernames) 499
Backup User Database 501
Restore User Database 503
Configure SANE 505
Retrieve Users 506

Chapter 13: MRFC Configuration 509
JSON File Configuration 513

Chapter 14: MNGT Tool 517
MRFCtrl Monitoring 517
MNGT Tool Commands 517
Access MNGT Tool 518
Call Interface 518
Traces Interface 518
Selection Interface 519
Call Steering 519
Stop MRFCTRL Process 519

Table of Contents

Examples 519
Directing Calls Feature 520
MRFC Configuration using MNGT Tool 520
Duration of Selection 521
Selection Termination 522
Additional Commands 522
Examples 523

Appendix A: List of Alarms 525
System Alarms 525

Appendix B: Kafka Alarm Formats 553

Appendix C: Generic Alarm Template Formats 557

Appendix D: List of Statistics 566
System Usage Group 567
Session Usage Group 567
SIP Usage Group 575
DSP Usage Group 579
Dropped UDP Packets Group 582
HTTP Media Statistics Group 583
VoiceXML Usage Group 583
CPU Core Group 584
MRFP Redundancy Groups 584
ASR/TTS Usage Group 584
Fax Usage Group 585
MRFC Stats Group 586
Disk Max Usage Group 586
MSML Usage Group 587
Statistics - Not Supported 589

Appendix E: Codecs 592
Codec Terminology and Support 592
Audio Codecs 592
Waveform or Source 592
Codec Parameters 593
Functionality 593

Table of Contents

Comfort Noise 594
DTMF 594
Packet Loss Concealment 594
Silence Suppression 595
Transcode Bypass 595
AMR 596
Supported Functionality 596
RFC 4867 Support 597
Usage Guidelines 597
AMR-WB 598
Supported Functionality 598
EVRC, EVRCB, and EVRC-NW 599
Supported Functionality 600
RFC Support 601
Operating Modes 602
Usage Guidelines 603
EVS 604
Supported Functionality 606
G.711 608
Supported Functionality 608
Usage Guidelines 609
G.722 609
Supported Functionality 610
Usage Guidelines 610
G.729 610
Supported Functionality 611
Usage Guidelines 611
Opus 612
Supported Functionality 612
Mid-call Audio Codec Change 614
H.264 614
Supported Functionality 616
RFC 6184 Support 617
VP8 617
Supported Functionality 618
H.265 618

Table of Contents

Supported Functionality 619
Mid-Call Changes on Video Port 620
T.140 621
Supported Functionality 621
TTY 622

Appendix F: IPv6 Supported Notations 623

Appendix G: Traffic on Interfaces 624

Appendix H: Automated Task 625
Containerized Decomposed Media Server Backup and Restore Script 625
External Server 625
Backup Operation 627
Restore Operation 627
Logs 628
Containerized Decomposed Media Server 628
Backup Operation 629
Restore Operation 629
Logs 629

Appendix I: Speech Adapter 630
About Speech Adapter 630
Features 631
Speech-to-Text 631
Text-to-Speech 631
Inter-working with Speech Adapter 631
Licensing Information 631
Speech Adapter Configuration on Media Server 632
Session Refresh 632

Appendix J: Privacy Documentation 633
Network Identifiers 633
User Identifiers 633
Subscriber Identifiers 634
Voice File 634
Media File 634

Preface

About this Manual

This guide provides an overview of the functions, key features, components, standards, and compliance information of the Radisys Engage Media Server™ Containerized Decomposed Media Server. It also describes how to perform operations, administration, maintenance, and provisioning (OAMP). It explains how to integrate the Containerized Decomposed Media Server into an IP network, and how to use the Web-based management interface to configure and maintain the Containerized Decomposed Media Server.

What's New in this Manual

The following features are added or updated in,

For Information on...	See in this Manual...
Release 18.0.1.0	
ME-2793—Load Balance Improvement	• *Chapter 2, Containerized Decomposed Media Server Load Balance, on page 133* • *Chapter 13, MRFC Configuration Parameters, on page 509*
ME-2809—Configurable SIP Session Refresher Role	*Chapter 8, Configure SIP, on page 197*
ME-2905—Distribution of Ports for the Licenses	• *Chapter 5, Understanding License File, on page 162* • *Chapter A, Major Alarms, on page 531* and *Minor Alarms on page 545*
ME-2807—CPU Utilization	*Chapter 8, Configure Resource Management, on page 281*
ME-2772—Container Image Size Optimization	• *Chapter 1, Composition, on page 24* • *Chapter 2, Announcement Lab, on page 136* • *Chapter 8, Announcement Lab, on page 347*

NOTE: The Containerized Decomposed Media Server provides support for iLBC codec and AI-based Noise Reduction but limited to internal Proof of Concept (PoC) and lab testing. The iLBC codec and AI-based Noise Reduction has not been verified for production deployment.

About Related Radisys Products

For information on Engage Media Server and other Radisys products, see the Radisys website at www.radisys.com.

Technical Support

Technical support is available from the Radisys Technical Assistance Center (TAC). Support is governed by the terms of your agreement with Radisys Corporation.

TAC can be reached using the following contact information:

Radisys Corporation

8900 NE Walker Rd. Suite 130.

Hillsboro, OR 97006

United States

Radisys Technical Assistance Center (TAC)

Phone:

For North America only, toll free number is +1-800-622-2235

For India only, toll free number is 000-800-100-9346

For global, the contact number is +1-604-918-6415

E-mail: tac@radisys.com

To access support for Engage Media Server from the Radisys website, go to:

http://www.radisys.com/mediaengine-support-portal

Notational Conventions

This manual uses the following conventions

BoldText	A keyword.
ItalicText	File, function, and utility names.
`MonoText`	Screen text and syntax strings.
`BoldMonoText`	A command to enter.
`ItalicMonoText`	Variable parameters.
Brackets [ ]	Command options.
Curly braces { }	A grouped list of parameters.
Vertical line |	An “OR” in the syntax. Indicates a choice of parameters.

All numbers are decimal unless otherwise stated.

PART 1: PRODUCT OVERVIEW

Chapter 1

Product Description

This chapter provides a high-level overview of the Containerized Decomposed Media Server functions, listing key features and components, and providing standards and compliance information.

Key Features

The Containerized Decomposed Media Server can be used in a broad range of applications and services, as follows:

- Decomposed architecture
- AnnLab for clip management
- Audio and multimedia announcement servers
- Call center
- Calling card and prepaid calling card
- IP Centrex or Hosted PBX
- Class 4 or Class 5 switching
- Voice, Web, and video conference
- Interactive Voice Response (IVR) or Voice Response Unit (VRU)
- Voicemail and Videomail
- Unified messaging
- Online gaming
- Transcoding
- Ringback tones
- Push-to-talk
- Lawful Intercept (LI)
- High Complexity (HC) Video
- Codec High Watermark

The Containerized Decomposed Media Server provides the following media resource functions.

- Audio codecs, including G.711 A-law, G.711 µ-law, G.722, G.729A, G.729AB, AMR, AMRWB, OPUS (NB and WB), EVS (NB, WB, and SWB), EVRC-A, EVRC-B, EVRC-NW, Telephone-event, CN (G.711 comfort noise), and RED (RFC 2198 RTP redundancy for AMR or AMR-WB only)
- Video codecs including H.264 (Mode 0 and Mode 1) and VP8
- T.140 text codec

- G.711 and T.38 fax[1] codecs
- Voice-Quality Enhancements
  - Packet Loss Concealment (PLC)
  - Acoustic Echo Cancellation (AEC)
  - Noise Reduction (NR)
  - Noise Gating (NG)
  - Noisy-Line Detection (NLD)
  - R-factor (Rating factor)
- RTCP and RTCP-XR
- Secure RTP Control Protocol (SRTCP)
- RTCP feedback messages including RTCP-PLI, RTCP-FIR, RTCP-TMMBR, and GENERIC-NACK
- Automatic transcoding between different audio and video codec types and bit rates for conferencing, port recording, announcements, and playback of audio announcements
- In-band and RFC 2833 Dual Tone Multi Frequency (DTMF) detection, collection, and generation, including optional DTMF clamping. The Containerized Decomposed Media Server also supports receiving RFC 4733 DTMF-long duration events and multiple events. The Containerized Decomposed Media Server sends out DTMF out-of-band events as per RFC 2833.
- Fixed and variable announcements
- Automatic Speech Recognition (ASR) and Text To Speech (TTS)
- Multilingual announcements (44 languages and dialects[2])
- Tones or announcements, stored inside the Containerized Decomposed Media Server or on the external Network File System (NFS), the Real Time Streaming Protocol (RTSP), Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS) servers
- Recording and playback of audio to internal Containerized Decomposed Media Server memory, NFS, and HTTP/HTTPS servers
- Rich audio mixing and conferencing capabilities suitable for simple conferencing applications, such as residential 3-way calling, to complex business conferencing applications
- Personalized audio stream mixing
- Cascade conferences to increase the number of talk-listen participants
- Flexible gain control including automatic gain control, muting, and unmuting
- HC H.264 and VP8 multimedia announcement and recording features, including announcements with HC text and icon overlay

---

1. Fax on the Containerized Decomposed Media Server is not fully qualified.
2. For information on supported Containerized Decomposed Media Server languages, refer to *Sets and Variables Interface Reference*.

- HC Video conferencing with Voice Activated Switching (VAS) or split-screen continuous presence
- Audio and audio-video media replication for lawful intercept applications
- Fax send and receive
- Call progress analysis for outgoing calls

All the footprint configuration can be performed through the Helm chart. For information on CPU, memory, DSP core, and persistent storage of each component, refer to the *Containerized Decomposed Media Server Installation Guide*.

Containerized Decomposed Media Server in the Network

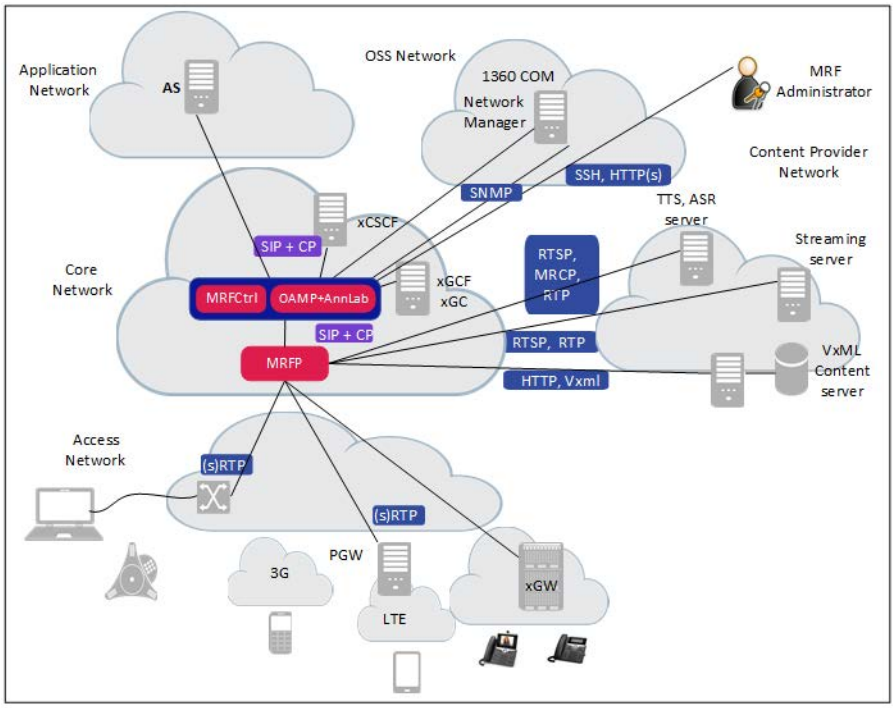
The Radisys Containerized Decomposed Media Server is a carrier-class platform designed from the outset to efficiently and cost-effectively process voice, video, and data, and to combine these into a rich, multi-service communications experience.

Containerized Decomposed Media Server is a flavor of Virtual Network Function (VNF) based Decomposed Media Server. Containerized Decomposed Media Server supports similar functionalities of Decomposed Media Server but developed as a native cloud application and is deployed on carrier-grade Kubernetes deployment. Containerized Decomposed Media Server includes MRFCtrl pod, operations, administration, maintenance, and provisioning (OAMP) pod, and multiple MRFP pods.

The Containerized Decomposed Media Server has a key role in the converged network where subscribers using multimedia enabled PCs, mobile phones, PDAs, and other terminals can communicate seamlessly with one another and with legacy devices in natural and rich multimedia interactions.

Figure 1 shows a high-level view of the network architecture that enables seamless voice and video communications and uniform access to services by all subscribers regardless of their access network and terminal capabilities.

Figure 1. Containerized Decomposed Media Server in IP Network



Composition

The following are the decomposed components (pods) of Containerized Decomposed Media Server.

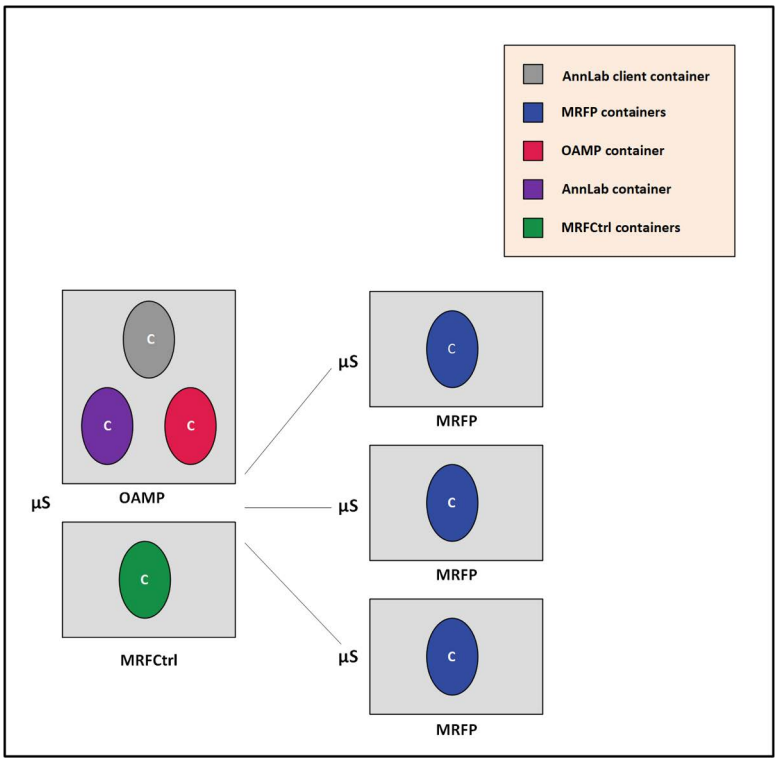
- **MRFCtrl pod.** The SIP endpoint for Containerized Decomposed Media Server and contains single container MRFCtrl.
- **OAMP pod.** This pod contains the following containers.
  - **OAMP container.** Hosts the Containerized Decomposed Media Server GUI and database for configuration. This container is also responsible for all the management activities of the deployment.
  - **AnnLab.** Hosts the AnnLab server that is responsible for clips deployment. In this document, the AnnLab refers to an AnnLab server.
  - **AnnLab Client.** Hosts the AnnLab Client that is responsible for transcoding the clips.
- **MRFP pod.** Responsible for media processing. A variable number of MRFP pods can be launched. However, Containerized Decomposed Media Server supports a maximum of 10 MRFP pods.

Hereafter in this document, the MRFC refers to OAMP and MRFCtrl pod.

NOTE: Each pod consists of a sidecar container to forward logs to Kubernetes.

Figure 2 provides the logical view of Containerized Decomposed Media Server.

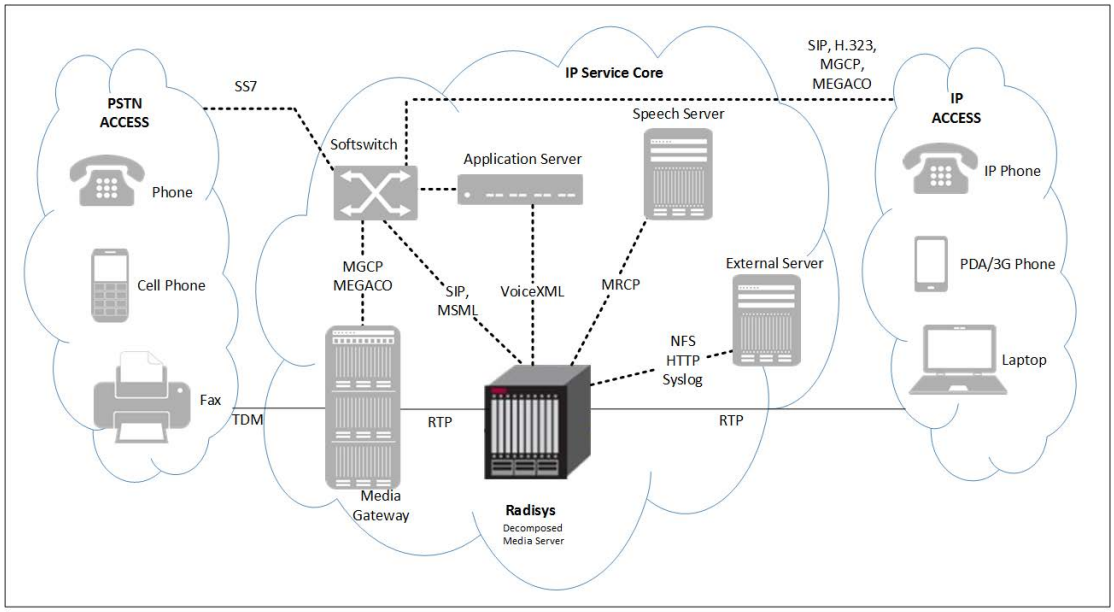
Figure 2. Logical View of Containerized Decomposed Media Server



Third Party Call Control (3PCC) Architecture

The Containerized Decomposed Media Server resides in an IP network as part of an integrated Voice over IP (VoIP) media network. Figure 3 shows the general topology of this network.

Figure 3. Containerized Decomposed Media Server as 3rd Party Call Control



The Containerized Decomposed Media Server is a slave device, which accepts commands and requests from control agents, and communicates with other key elements of the network, such as media gateways, terminals, or a combination of elements.

Containerized Decomposed Media Server Redundancy

The Containerized Decomposed Media Server offers the following redundancy features.

- 1+1 (active/standby) redundancy for MRFCs
- N+k (active/active) redundancy for MRFPs without call preservation
- N+1 (where N ≤ 5) redundancy for MRFPs with call preservation

MRFCtrl Redundancy

The MRFCtrl pod includes MRFCtrl and sidecar containers for logs. Use a keepalived daemon to maintain MRFCTRL High Availability (HA). Both the MRFCtrl pods are in *Running state* and keepalived monitors the status. Based on the state, one of the MRFCtrl have MRFCTRL VIP, and the MRFCtrl process gets started on that pod. Two MRFCtrl pod instances are launched, namely, mrfctrl-0 and mrfctrl-1. The keepalived daemon runs as the root user in both the pods.

Execute the following commands to get the state of the current pod.

```
[root@master dmrf]# kubectl exec -n <namespace> -it mrf-mrfctrl-0 -c mrfctrl cat /opt/swms/etc/status
STATE="BACKUP"
[root@master dmrf]# kubectl exec -n <namespace> -it mrf-mrfctrl-1 -c mrfctrl cat /opt/swms/etc/status
STATE="MASTER"
[root@master dmrf]#
```

MRFP N+k Redundancy

The Containerized Decomposed Media Server supports N+k (active/active) MRFP redundancy for MRFPs without call preservation. That is, N MRFP pods handle the load of N+k MRFPs when k instances are unreachable or out of service. In N+k redundancy, the optimal value is determined for N and k so that Containerized Decomposed Media Server is not overloaded when a certain number of MRFP pods (k) are not handling the calls.

MRFP N+1 Redundancy

The Containerized Decomposed Media Server supports MRFP pod redundancy with multiple redundancy groups, and each group with a maximum of N+1 (where N ≤ 5) MRFPs with call preservation for MSML, MSCML, and Netann conferences.

For more information on MRFP redundancy support, see *MRFP N+1 Redundancy on page 156*.

Interfaces

The Containerized Decomposed Media Server uses the following interfaces to communicate over the network.

- **SIP, VoiceXML, MSML, MSCML, MOML.** The Containerized Decomposed Media Server receives commands and responds to requests from control agents using open control protocols such as SIP, VoiceXML, Media Sessions Markup Language (MSML), Media Server Control Markup Language (MSCML), and Media Objects Markup Language (MOML).
- **RTP.** The Containerized Decomposed Media Server sends and receives Real Time Protocol (RTP) streams over a media network to and from RTP endpoints, where an endpoint can be an IP-capable terminal or a media gateway. This interface is used for media sessions, IVR, DTMF collection and generation, and playing media clips.
- **SRTP and SRTCP.** The Containerized Decomposed Media Server sends and receives Secure RTP (SRTP) streams over a media network to and from SRTP-capable endpoints. Secure RTP Control Protocol (SRTCP) is supported for monitoring the flow of SRTP packets.
- **RTCP, RTCP-XR, RTCP-PLI, RTCP-FIR, TMMBR/TMMBN, and Generic-NACK.** The Containerized Decomposed Media Server sends and receives RTP Control Protocol (RTCP) packets used for monitoring the flow of RTP packets. It sends Sender Report (SR), Receiver Report (RR), Source Description (SDES), and BYE packets, and receives SR, RR, and BYE packets. It also supports a number of RTCP Extended Report (RTCP-XR) statistics and RTCP

Picture Loss Indication (RTCP-PLI) messages to indicate picture loss in the media session. The Containerized Decomposed Media Server supports RTCP-FIR I-frame request capability for video sessions. Temporary Maximum Media Bit-rate Request (TMMBR) and Temporary Maximum Media Bitrate Notification (TMMBN) messages are used for dynamic video rate adaptation as required by IR.941 for terminals supporting video. Generic-NACK (RTCP-NACK) messages are used for notification and retransmission of the lost RTP video packets.

- **Web-enabled GUI.** An HTTP/HTTPS Web-based GUI allows system administrators to perform GUI configuration for the Containerized Decomposed Media Server.
- **SNMP.** All the Containerized Decomposed Media Server configurations and functions can be performed through a Simple Network Management Protocol (SNMP) interface. The Containerized Decomposed Media Server supports SNMP versions 2c and 3.
- **NFS.** The Containerized Decomposed Media Server can record media clips, and play them back, from an external NFS server.
- **HTTP/HTTPS.** The Containerized Decomposed Media Server can stream audio or audio-video clips to an external HTTP or HTTPS server and store them in a persistent file. The Containerized Decomposed Media Server can also playback audio clips using streamed mode and audio-video clips using cache mode, stored on an external HTTP or HTTPS server. The Containerized Decomposed Media Server supports HTTP or HTTPS recording for both port and conference. The Containerized Decomposed Media Server can also retrieve VoiceXML files from an HTTP or HTTPS server for processing, and return results to the server. The Containerized Decomposed Media Server includes the Server Name Indication (SNI) extension header as per RFC 6066 when communicating with the HTTPS remote server for announcement, recording, file transfer, fax-recv, and fax-send operations. For HTTP, these processes are managed by a control agent and no special configuration of Containerized Decomposed Media Server is required. Whereas, the HTTPS requires certificate configuration, see *Manage Certificates on page 323*.
- **MRCP (Version 1 and Version 2).** The Containerized Decomposed Media Server uses Media Resource Control Protocol (MRCP) to access speech resources on external servers. These resources include speech recognizers for ASR and speech synthesizers for TTS.
- **RTSP.** The Containerized Decomposed Media Server streams announcement from an RTSP server. Additionally, RTSP is supported as required by MRCP Version 1 for an ASR or TTS client device.
- **DNS.** The Containerized Decomposed Media Server uses Domain Name System (DNS) to resolve domain names for IP addresses.
- **NETCONF.** The Containerized Decomposed Media Server supports Network Configuration (NETCONF) protocol for configuration and management functions. The Containerized Decomposed Media Server supports SSH version 2 for exchanging the NETCONF message with the client. For more information on NETCONF, refer the *NETCONF Interface Reference*.

- **X3 Interface.** The Containerized Decomposed Media Server supports lawful intercept of Call Content (CC) over the X3 interface. In order to support lawful intercept of the CC, an application server named Lawful Intercept Function (LIF) is used. LIF invokes the Containerized Decomposed Media Server through the establishment of a related series of SIP dialogs.

  The sip:monitor is used as a service indicator to create pass-through dialogs and listener dialogs within the lawful intercept group. The Containerized Decomposed Media Server allows to create a maximum of five listener dialogs for each pass-through ports in a sip:monitor LI group. In mono mode, both the listener audio medias must have the same IP address and port number.

  The Containerized Decomposed Media Server supports sip:monitor service indicator for lawful intercept of the fax media type. The Containerized Decomposed Media Server supports CC interception on the image (fax) port in stereo mode. The Containerized Decomposed Media Server receives and transmits the fax packets over User Datagram Protocol Transport Layer (UDPTL), on both pass-through port and listener port. The Containerized Decomposed Media Server pass-through the fax packet from one party to another without any modification, except for modifying the IP and UDP layer to include the Containerized Decomposed Media Server IP address or port as the source, and peer party IP address or port as the destination.

  In the stereo mode, the Containerized Decomposed Media Server replicates and forwards the fax packet to LIG in two RTP streams without any modification, except for the IP and UDP layer changes to include the Containerized Decomposed Media Server IP address or port as the source, and LIG IP address or port as the destination.

  For more information refer to the *SIP Interface Reference*.

Protocol Standard Compliance

This section describes the standards supported by the Containerized Decomposed Media Server.

Table 1. Network Communications Protocol Standards

Protocol	Standard
ARP	RFC 826
DNS	• RFC 1034, RFC 1035 • RFC 3596 (IPv6)
DiffServ/ToS	RFC 2474
Ethernet	IEEE 802.3
IP Version 4 (IPv4)	RFC 791

Table 1. Network Communications Protocol Standards

Protocol	Standard
IP Version 6 (IPv6)	• RFC 2460 Internet Protocol Version 6 (IPv6) Specification • RFC 3493 (socket extension) • RFC 4291 (addressing architecture) • RFC 2464 (transmission) • RFC 4862 (auto-configuration for link-local addresses) • RFC 4861 (neighbor discovery) • RFC 4443 (ICMPv6) • RFC 1981 (MTU discovery) • RFC 3484 (default address selection) • RFC 4604 (IGMPv3) • RFC 4213 (dual-stack transition mechanism)
TCP	RFC 793 RFC 4145 (Media Control Channel Framework TCP channel)
UDP	RFC 768
TLS[a]	• RFC 2246 (TLSv1.0) • RFC 4346 (TLSv1.1) • RFC 5246 (TLSv1.2)
TLS extension	RFC 6066 (Server Name Indication)
DTLS	RFC 6347 and 4347
DTLS extension	RFC 5763 and 5764

[a] MRFP supports all the TLS versions TLSv1.0, TLSv1.1, and TLSv1.2; whereas MRFCtrl and OAMP Pod supports only the TLSv1.2 version.

Table 2. Control Protocol Standards

Protocol	Standard
MRCP	RFC 4463 Informational
MSML and MOML	RFC 5707
MSCML	RFC 5022
SDP	• RFC 3264 (Offer/Answer Model) • RFC 4566

Table 2. Control Protocol Standards

Protocol	Standard
SIP	• RFC 2543, RFC 2543bis04 • RFC 2976 (INFO Method) • RFC 3261, RFC 2543bis04 • RFC 3261 • RFC 3262 (100Rel) • RFC 3312 • RFC 3263 (locating SIP servers) • RFC 3264 • RFC 3326 (reason header) • RFC 3581 • RFC 3725 • RFC 4028 (session timer) • RFC 4092 (alternative network address types) • RFC 4240 • RFC 4412 (resource priority) • Early Media • RFC 6230 (media control channel framework)
SRGS	As specified in the W3C GRXML file format
VoiceXML 2.0	W3C Candidate Recommendation Version 2 (March 2004)
VoiceXML 2.1	W3C Recommendation 19 (June 2007)

Table 3. Management Protocol Standards

Protocol	Standard
DiffServ	RFC 2475
HTTP v1.0 HTTP v1.1	RFC 1945 RFC 2616
HTTPS	RFC 2818
NFS v3	RFC 1094
SNMP v2 plus support for community strings (SNMPv2c)	• RFC 1901–1908 • RS-232: RFC 1659 • IP: RFC 2011 • Interfaces: RFC 2233
LDAP	• RFC 4616 • RFC 2247 • RFC 2307bis • RFC 822

Table 3. Management Protocol Standards

Protocol	Standard
SNMPv3	• RFC 3411–3418 • RFC 2574 User-based Security Model (USM) • RFC 1213 MIB-II • RFC 3411 SNMP-FRAMEWORK-MIB • RFC 3412 SNMP-MPD-MIB • RFC 3413 SNMP-TARGET-MIB • RFC 3414 SNMP-USER-BASED-SM-MIB • RFC 3415 SNMP-VIEW-BASED-ACM-MIB • RFC 3416 SNMPv2-PDU
NETCONF	RFC 6241

Table 4. Media Protocol Standards

Protocol	Standard
AMR, AMR-WB	• RFC 4867 3GPP Adaptive Multi-Rate (Octet-aligned and bandwidth efficient) • 3GPP TS 26.171, 3GPP TS 26.190-26.194, 3GPP TS 26.201
RTCP-PLI	RFC 4585 (PLI only)
RTCP-FIR	RFC 5104
RTCP-TMMBR/TMMBN	RFC 5104
RTCP-NACK	RFC 4585
H.264 Mode 0 and Mode 1	• ITU H.264 Video Codec, also known as Advanced Video Codec (AVC) • RFC 6184, previously RFC 3984 • Constrained Baseline Profile Level 1.1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1
H.265	• ITU H.265 Video Codec, also known as High Efficiency Video Codec (HEVC) • RFC 7798 • Main Profile Level 1, 2, 2.1, 3, and 3.1
ITU-T E.180/Q.35	ITU-T Recommendation E.180/Q.35 (March 1998)
ITU G.711 u-law and A-law	• RFC 3551 (PCMU and PCMA) • ITU-T G.711 Appendix I
CN	• RFC 3389 (PCMU and PCMA) • ITU-T G.711 Appendix II
ITU G.722	• RFC 3551 (G.722) • ITU G.722 Appendix IV
ITU G.729 and Annexes A, B	• RFC 3551 • ITU G.729 Annexes A and B
ITU-T Q.1970 3GPP TS 29.414	BICC IP Bearer Control Protocol (IPBCP)
ITU-T T.30	ITU-T Recommendation T.30 (April 1999)
ITU-T T.38	ITU-T Recommendation T.38 (April 2007)
ITU-T V.21	ITU-T Recommendation V.21 (November 1988)
RED	RFC 2198 for AMR, AMR-WB, and T.140 (text)

Table 4. Media Protocol Standards

Protocol	Standard
RTT	• RFC 4103 (RTP payload for text conversation) • draft-ietf-avtcore-multi-party-rtt-mix-11 (RTP-mixer formatting of multiparty Real-Time Text)
RTP	• RFC 3550 • RFC 4961 • RFC 4867 • RFC 3611 (RTCP-XR)
RTSP	RFC 2326 as required for MRCP Version 1
BUNDLE (RTP Media Multiplexing)	RFC 5888
RTSP	RFC 2326 as required for MRCP Version 1
SRTP	RFC 3711
In-band DTMF Detection Standard	• EIA/TIA-464A • GR-181CORE • ITU-T Q.24
Telephone Events	RFC 4733 with some exceptions[a]
Telephone Events	RFC 2833/ RFC 4733
VP8	RFC 6386
Opus	draft-ietf-payload-rtp-opus or RFC 6716 Opus speech and audio codec
EVS	Standardized by 3GPP (3Q2014). 3GPP TS 26.441 - 3GPP TS 26.451[b]
EVRC, EVRCB, and EVRCNW EVRC0, EVRCB0, and EVRCNW0	• 3GPP2 C.S0014-A service option 3, 3GPP2 C.S0014-B service option 68, 3GPP2 C.S0014-D service option 73 • RFC 3588, RFC 5188, RFC 6884
SDP	RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams

[a] Long DTMF digits: The Containerized Decomposed Media Server detects each segment (of long digit) as new digit and the Containerized Decomposed Media Server cannot generate a digit longer than 8.19s. Multiple events in single packet: The Containerized Decomposed Media Server would detect only the first digit in a packet and ignore all subsequent digits in a packet. Transmission of state events indicated by event duration of zero: The Containerized Decomposed Media Server does not check the duration of the first packet, so it will not interpret received event as a state event. The Containerized Decomposed Media Server sends RFC 2833 events with non-zero duration in the first packet.

[b] The Containerized Decomposed Media Server does not support 3GPP TS 26.448.

Features

The Containerized Decomposed Media Server consolidates a broad range of media processing features, exposed through open standards-based control interfaces, for any IP-based communications network.

The media processing functions support multiple options and features that can be combined on the same call, or a set of calls, or in any other desired combination. The service logic in the control agent uses individual media processing functions to create applications.

The Containerized Decomposed Media Server also supports a fully-featured management interface that allows system administrators to perform OAMP (operations, administration, management, and provisioning) on the Containerized Decomposed Media Server through a Web GUI, or remotely through an SNMP or NETCONF interface.

Media Features

Encoding and Decoding

Media is transported across the network in an encoded format. Audio and video, text, and fax data use several standard encoding algorithms, from simple to highly complex. The fundamental service of the Containerized Decomposed Media Server is to provide encoding and decoding of media between different formats.

Multiple Codec Support

Table 5 lists the audio and video codecs supported by the Containerized Decomposed Media Server.

Table 5. RTP Payload Types

Payload Type ID	Encoding Name	Media Type	Clock Rate	Description
0	PCMU	Audio	8,000	G.711µ-law 64 kbps
8	PCMA	Audio	8,000	G.711 a-law 64 kbps
9	G722	Audio	8,000 or 16,000	G.722 7 kHz audio-coding within 64 kbps
13	CN[a]	Audio	8,000	RFC 3389 comfort noise
18	G729	Audio	8,000	G.729 CS-ACELP 8 kbps Includes annex A, B, and C
Dynamic 0-63 and 96–127				

Table 5. RTP Payload Types

Payload Type ID	Encoding Name	Media Type	Clock Rate	Description
	H264 (mode 0 and mode 1)[b]	Video	90,000	ITU H.264 Video Codec, also known as Advanced Video Codec (AVC) RFC 6184, previously RFC 3984 Constrained Baseline Profile Level 1,1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1
	H265	Video	90,000	ITU H.265 Video Codec, also known as High Efficiency Video Codec (HEVC) RFC 7798 Main Profile Level 1, 2, 2.1, 3, and 3.1
	AMR[c]	Audio	8,000	3GPP Adaptive Multi-Rate RFC 4867 Octet-aligned and bandwidth efficient All 7 bit rates and DTX/CNG
	AMR-WB[d]	Audio	16,000	AMR-WB media format as per RFC 4867 and RFC 3267 octet-aligned and bandwidth efficient All 8 bit rates and DTX/CNG
	Opus[e]	Audio	48,000	RFC 6716 Opus speech and audio Codec
	telephone-event[f]	Audio	8,000 or 16,000 or 48000 (opus)	RFC 2833 or RFC 4733
	RED[g]	Audio and Text	8,000 or 16,000	RFC 2198 RTP redundancy is supported for AMR and AMR-WB, and T.140
	EVRC0	Audio	8,000	3G2 Enhanced Variable Rate Codec (EVRC-A) as specified in RFC 3588.
	EVRCB0	Audio	8,000	3G2 Enhanced Variable Rate Codec B (EVRC-B) as specified in RFC 5188 and RFC 3588.
	EVRCNW0	Audio	8,000	3G2 Enhanced Variable Rate Codec NW (EVRC-NW) as specified in RFC 6884 and RFC 3588.
	T.140	Text	1,000	T.140 as defined in RFC 4103
	VP8	Video	90,000	RFC 6386
	EVS[h]	Audio	16,000	EVS audio codec as specified in 3GPP 26.445 Supports header-full format and octet aligned.

[a] The CN is currently supported only with the G.711 and G.722 codecs and the SIP control protocol. The CN is configurable in the management interface audio codec list, as with the telephone-event. The Containerized Decomposed Media Server does not send CN packet if silence suppression is disabled on the port. It can still receive and decode the CN codec only if negotiated through SDP from the far-end in case the far-end uses silence suppression. Possible codec negotiation results on the G.711 port are: G.711, or (G.711 + telephone-event), or (G.711 + CN), or (G.711 + CN + telephone-event). Possible codec negotiation results on the G.722 port are: G.722, or (G.722 + telephone-event), or (G.722 + CN), or (G.722 + CN + telephone-event).

[b] A single name is defined for H.264. There are two different operation modes supported by H.264 Mode 0 and Mode 1. These modes are mapped to two different payload formats.

[c] Although, only a single name is defined for AMR, you can configure many different operation modes using format-specific attributes. For example, AMR can be mapped to several different payload types within a media description, each with a different operation mode. The RTP payload format for AMR supports multi-channel audio content. However, the Containerized Decomposed Media Server only supports a single channel. The Containerized Decomposed Media Server supports AMR-OA, AMR-BE, AMR-OA-R, and AMR-BE-R media formats for AMR audio codec. For details on the AMR format specific attributes, refer *SIP Interface Reference*.

[d] The AMR-WB media format supports octet-align and bandwidth-efficient operation modes, with or without mode change restriction but mapped to different payload number. As with the AMR media format, the same encoding name **AMR-WB** is used for the octet-align and bandwidth efficient operation modes but is mapped to different payload number. The AMR-WB media format is only supported for the RTP port in SIP. The Containerized Decomposed Media Server supports AMR-WB-OA, AMR-WB-BE, AMR-WB-OA-R, and AMR-WB-BE-R media formats for the AMR-WB audio codec. For details on the AMR-WB format specific attributes, refer *SIP Interface Reference*.

[e] Opus supports both narrowband and wideband media formats with different payload types. The Opus media format is supported in SIP for all service contexts.

[f] The clock rate of the telephone-event must be same as the clock rate of the main audio codec. For example, if the telephone-event is enabled on the AMR port, the telephone-event clock rate should be 8000. If the telephone-event is enabled on the AMR-WB port, the telephone-event clock rate should be 16000. If the offered clock rate for telephone-event in Session Description Protocol (SDP) is different than the main audio codecs clock rate, the Containerized Decomposed Media Server ignores it and uses the main audio codec clock rate for telephone-event. The same rules applies when determining the clock rate for RED.

[g] When SIP is used as the control protocol, **RED** is only supported for sending and receiving redundant AMR payloads, if a non-zero level of RTP redundancy is enabled in the management interface.

[h] The EVS codec supports RTP ports in all service contexts for narrowband, wideband, and super wideband bandwidths. EVS-R is the restricted mode for the EVS codec.

Transcoding

Transcoding is required whenever two endpoints use different codecs, or different parameters when using the same codec. Any clip (for example, an announcement) stored in any of the supported file formats can be played to an endpoint of any other codec type using transcoding.

Transcoding is automatically applied in all audio processing functions for all supported audio codecs, unless transcode bypass is enabled through the Containerized Decomposed Media Server.

For video there is no transcode bypass configuration and the decision for bypass is taken internally. The transcode bypass setting is only used for play/record service and it controls the audio transcode bypass only. Transcoding bypass is always supported for video p2p transcoding, announcements, recordings, and VAS conferencing.

For video codecs (H.264 Mode 0 and Mode 1, and VP8), transcoding and rate matching are supported only for profile level, picture size, bit rate, and only in CP conferencing, including announcements and recordings to a CP conference.

NOTE: If the source video is from a VP8 port, the H.264 encoder cannot encode the picture size that are not in multiples of 16. However, the H.264 encoder changes the picture size to multiples of 16.

The Containerized Decomposed Media Server automatically determines video transcoding or transcoding bypass. Video transcoding bypass is managed internally in p2p call services, provided that all the parameters match. The text and icon overlay transcodes video announcements to mix text and images.

In Voice Activated Switching (VAS) conference, video switching is performed for the video component without transcoding; therefore, all VAS participants must have the same video codec/parameters.

Transcoding is Digital Signal Processor (DSP) resource-intensive and can affect capacity.

Transcode Bypass

Transcode bypass is supported on the Containerized Decomposed Media Server when the following conditions are fulfilled.

- the same codec type is present between the port and the clip
- the **mode-set** SDP attribute read from the clip is same or a subset of the **mode-set** attribute negotiated on the port
- the restrict mode (mcp=2 or mcn=1) is not requested by the far-end terminal
- the port is not in the conference
- in-band DTMF is disabled on the port

The Containerized Decomposed Media Server provides the management interface configuration to exclude the mode-change restrictions parameters (`mode-change-period=2` and/or `mode-change-neighbor=1`) from the transcode bypass decision for the AMR, AMR-WB, and EVS (AMR-WB-IO mode only) announcement ports. Following are the recommendations to be followed when the **Transcode Bypass on Restrictive Mode Change Port** parameter is enabled.

- Generate the clips in single mode. In single mode, you cannot change the mode from the clip, therefore the Containerized Decomposed Media Server ignores the `mode-change-period` and `mode-change-neighbor` settings on the port. The Containerized Decomposed Media Server plays the announcement in the transcode bypass mode if all other bypass conditions are fulfilled.
- For multiple modes in the clip, generate the clips such that the mode changes in the clip are restricted to the neighboring mode and the mode change period is restricted to the two frame-blocks.

The Containerized Decomposed Media Server ignores the codec mode change request from the far-end when the announcements are played in the transcode bypass mode.

When the **Transcode Bypass on Restrictive Mode Change Port** parameter is disabled, transcode bypass is not allowed on the AMR, AMR-WB, and EVS (AMR-WB-IO mode only) ports using the restricted mode.

The Containerized Decomposed Media Server plays the announcements in the bypass mode, regardless of the **Transcode Bypass on Restrictive Mode Change Port** configuration when the following conditions are fulfilled.

- the announcement clip does not have the mode-set parameter
- port is negotiated on all the modes
- port is not negotiated for restrictive parameters

The Containerized Decomposed Media Server plays the announcement in the bypass mode when **Transcode Bypass on Restrictive Mode Change Port** is enabled and when the following conditions are fulfilled.

- the announcement clip does not have the mode-set parameter
- port is negotiated on all the modes
- port is negotiated for restrictive parameters

Audio Support

The Containerized Decomposed Media Server transcodes an announcement before streaming it over the RTP interface. When transcoding is needed, the Containerized Decomposed Media Server decodes a compressed file, sends its audio to the Containerized Decomposed Media Server port, which then re-encodes the audio for streaming. Similarly, incoming RTP streams are transcoded before being recorded. The transcode bypass feature provides an option to bypass codecs when audio announcements or recording files use the same compression method as the port. This feature can be enabled in the management interface. When the compression method of the storage media is identical to the port codec, this feature eliminates unnecessary encoding and decoding.

For G.729, AMR, AMR-WB, G.722, and any video codec, bypassing the encoder can boost capacities and reduce the degradation of audio quality due to lossy transcoding. It also enhances G.711 performance by eliminating the use of the Voice Activity Detector (VAD) when silence suppression is enabled.

For AMR and AMR-WB, the modeset of an announcement must be within the limits negotiated for the port. This is only required if you want codec bypass to apply, otherwise the Containerized Decomposed Media Server transcodes the announcement. In recording bypassed AMR and AMR-WB, mode 8 (silence insertion descriptor (SID)) and mode 15 (No Data frames) are recorded and not replaced with silence.

NOTE: The Containerized Decomposed Media Server does not support the transcode bypass functionality for audio, if the following VQE features are enabled.

- Noise Gating
- NG Attenuation
- Noise Reduction
- Acoustic Echo Cancellation

The Containerized Decomposed Media Server supports enabling or disabling AMR and AMR-WB transcode bypass from the management interface.

It is not compatible with the use of gain, in-band DTMF detection, pre-speech and post-speech timers, and other features that require input derived from encoding or decoding the media stream. Special consideration should be given to the treatment of silence (silence suppression, comfort noise, and so on) in your application before using this feature.

Video Support

Transcode bypass is supported on the video ports, if both the caller and callee endpoints support the same video codec and video parameters. If the video bitrate is the only incompatible parameter, and if it has only a small difference; for example, not bigger than ([((video bitrate of source or sink)/64)*10]+8 kbps), the Containerized Decomposed Media Server considers the parameter to be compatible and transcoding is enabled.

This yields reasonable maximum bitrate tolerance values such as 8 kbps at (0 – 63); 68 kbps at (384 – 447); 128 kbps at (768 – 831), and so on.

Transcoding bypass is supported for the video port as long as both ends have locked down to the same video codec and video parameters.

For more information about mid-call video, see *Mid-Call Changes on Video Port on page 620*.

Silence Suppression

In RTP audio streams, packet transmission can be suppressed when it is determined that there is no useful audio to send. The Containerized Decomposed Media Server supports the following methods of silence suppression.

- **Codec-based silence suppression.** This has silence detection built directly into the codec. For instance, G.729 Annex B and AMR encoders do not generate normal voice RTP frames during silence intervals. Instead, they send a comfort noise packet at the start of a silence period that estimates the level of background noise. The SID frames are transmitted immediately upon entering silence suppression and then periodically if the character of the background noise changes. Comfort noise produces a more natural effect during silence suppression than using pure silence.
- **Non codec-based silence suppression.** This uses a silence detection algorithm or a voice activity detector (VAD) external to the codec, which detects periods of silence and suppresses the sending of normal voice RTP packets during these periods. As this method is not built into the codec, it is codec-independent and can be used for codecs that do not have built-in silence suppression. Codecs supported by the Containerized Decomposed Media Server that must use non codec-based silence suppression is G.711 and G.722. To perform non codec-based silence suppression, the VAD determines when speech is occurring. The non codec-based silence suppression algorithm sends all frames when the VAD determines that there is speech, and it stops sending during silence. This minimizes packet transmission during periods of silence and injects silence (dead calm) into the audio stream.

Table 6 shows the behavior of the Containerized Decomposed Media Server with respect to silence suppression Web GUI configuration, when there is no explicit SDP negotiation related to silence suppression and if CN payload type is not negotiated in the SDP.

Table 6. Silence Suppression when CN Payload Type is Not Negotiated with SDP

Silence Suppression Methods	When Silence Suppression is Enabled in Web GUI	When Silence Suppression is Disabled in Web GUI
Codec-based silence suppression	• Normal voice RTP frames are not sent during the silence • SID RTP frames are sent	• Normal voice RTP frames are sent during the silence • SID RTP frames are not sent
Non codec-based silence suppression	• Normal voice RTP frames are not sent during the silence • SID RTP frames are not sent	• Normal voice RTP frames are sent during the silence • SID RTP frames are not sent

For the codecs without built-in silence suppression, explicit SDP negotiation for CN payload type is mandatory to send SID RTP frames.

Table 7 shows the behavior of the Containerized Decomposed Media Server with respect to silence suppression Web GUI configuration, when there is no explicit SDP negotiation related to silence suppression and if CN payload type is negotiated in the SDP.

Table 7. Silence Suppression when CN Payload Type is Negotiated with SDP

Silence Suppression Methods	When Silence Suppression is Enabled in Web GUI	When Silence Suppression is Disabled in Web GUI
Codec-based silence suppression	Not applicable	Not applicable
Non codec-based silence suppression	• Normal voice RTP frames are not sent during the silence • SID RTP frames with CN payload type are sent	• Normal voice RTP frames are sent during the silence • SID RTP frames are not sent

When the Containerized Decomposed Media Server provides an offer in the remote SDP and if the answer contains `a=silenceSupp`, the Containerized Decomposed Media Server accepts the silence suppression as indicated in the answer (which overrides the Web GUI setting for silence suppression).

Table 8 shows the behavior when silence suppression is enabled and if CN payload type is negotiated in the SDP.

Table 8. Codecs Support Silence Suppression Negotiated in SDP and Overrides Web GUI Setting

• Codec natively supports silence suppression. • Uses payload specific parameter to indicate the use of silence suppression	• Codec natively supports silence suppression • Uses `a=silenceSupp` attribute in media description of SDP to indicate the use of silence suppression	• Codec does not natively support silence suppression. • Uses VAD of Containerized Decomposed Media Server to implement silence suppression. • Uses `a=silenceSupp` in media description of SDP to indicate the use of silence suppression	Codec does not support silence suppression
EVRC, EVRC-B, EVRC-NW, Opus, EVS, and G.729B	AMR and AMR-WB	G.711 and G.722	iLBC
• Normal voice RTP frames are not sent during the silence • SID RTP frames are sent in RTP stream	• Normal voice RTP frames are not sent during the silence • SID RTP frames are sent in RTP stream	• Normal voice RTP frames are not sent during the silence • SID RTP frames are sent in RTP stream with CN payload type identifier	SID RTP frames are not sent

The VAD is designed to detect speech signals and therefore may not reliably detect non-speech signals such as music and DTMF tones. For example, a continuous tone may be detected for about two to five seconds, after which the VAD determines that there is no signal present.

For music, the VAD may cut in and out even though the music is continuously present. For this reason, silence suppression must not be used with DTMF detection in voice band or music on hold.

Silence suppression does not apply for T.38 fax, text, and video ports.

The Containerized Decomposed Media Server supports silence suppression for receiving and sending audio when it is enabled in the management interface. Silence update frames serve as a keep-alive to prevent extended periods of silence from triggering RTP time-outs in terminals. The Opus codec supports negotiating silence suppression through **usedtx** parameter in SDP. The EVS codec supports negotiating silence suppression through **dtx** and **dtx-recv** parameter in SDP.

The Containerized Decomposed Media Server negotiates the Discontinuous Transmission (DTX) parameters used for silence suppression as described in RFC 4788: silencesupp, dtxmax, dtxmin, and hangover. In the SDP offers for EVRC, the Containerized Decomposed Media Server includes **silencesupp** attribute with the value configured for silence suppression in the management interface. The other DTX parameters are accepted in received SDP offers.

The Containerized Decomposed Media Server VAD or the built-in VAD of a codec depend on the following conditions.

- Codec has native silence suppression support.
- Remote endpoint signals support codec-based silence suppression during media negotiation.
- The Containerized Decomposed Media Server silence suppression feature is enabled.

In SIP, silence suppression is enabled and disabled on the Containerized Decomposed Media Server through the management interfaces. Specified ports can override this setting through the SDP **silenceSupp** attribute.

Enabling the Containerized Decomposed Media Server silence suppression does not mean that the Containerized Decomposed Media Server VAD is always used. When built-in VAD is available in a codec, and the endpoint signals support the same, the Containerized Decomposed Media Server uses the native VAD to detect the silence, irrespective off silence suppression configuration.

Packet Loss Concealment

Packet Loss Concealment (PLC) allows the user to enable or disable the G.711 or G.722 PLC settings through Web GUI interface. For G.722, G.729, AMR, AMR-WB, EVS, EVRC, EVRC-B, EVRC-NW, and Opus codecs, PLC is built-in and always enabled.

NOTE:

- ITU G.711 Appendix 1 packet loss concealment for G.711 codec is supported for all except transcode bypass.
- ITU G.722 Appendix IV packet loss concealment for G.722 codec is supported for all except transcode bypass.

Announcements

The Containerized Decomposed Media Server provides both audio and video announcements. The Containerized Decomposed Media Server supports playing one announcement (single announcement) or list of announcements (multi-clip announcements). Announcements can be played to a single connection or to a conference.

For more information, see the following:

- *Play Audio Announcement in a Conference on page 68*
- *Play Video Announcement to Conference on page 81*
- *Text to Speech on page 61*

When playing the single and multi-clip announcements, if **Encrypt Subscriber Data** is disabled through the management interface and if the media clip is encrypted, the Containerized Decomposed Media Server fails to play the announcement. If media clip is decrypted, the Containerized Decomposed Media Server plays the announcement.

The Containerized Decomposed Media Server supports playing announcement clips encoded in narrowband, wideband, and super wideband. In a multi-clip announcement, the Containerized Decomposed Media Server supports playing clips with different sample rates. The Containerized Decomposed Media Server supports a multi-clip announcement with a mix of audio-video and audio clips in MSML, MSCML, and VXML service contexts, where the first clip is audio-video and the second clip is audio-only. If there is a mixture of audio-video and audio-only clips in a multi-clip announcement, the Containerized Decomposed Media Server supports playing only two clips, where the first clip is audio-video and the second clip is audio-only. The Containerized Decomposed Media Server rejects the invite request, if any other combination of clips is present in a multi-clip announcement.

In the HTTP announcement, the Containerized Decomposed Media Server supports playing WAV, MP3, or MP4 clips on audio ports, even if the file does not contain the extension. The WAV file supports unsigned 8-bit PCM format, signed 16-bit and 24-bit PCM formats, or contains MP3 payloads.

In the WAV clip, the Containerized Decomposed Media Serverr ignores the unsupported and unrecognized chunks, and plays the announcement clip from the supported chunks in the VXML, MSML, Netann, and MSCML service context. The Containerized Decomposed Media Server supports this feature in internal, NFS, HTTP, and HTTPS (stream and cache mode) servers.

The Containerized Decomposed Media Server can play HTTPS announcements from the public cloud storage platform (for example, Amazon Web Services (AWS)).

This section describes the following announcement features.

Play Audio Announcement to a Port

The Containerized Decomposed Media Server has full audio announcement streaming capability and features for storing and playing audio announcements.

Audio clips used for announcements can be stored in a non-volatile memory in the Containerized Decomposed Media Server NFS, HTTP, HTTPS, or RTSP servers. These servers support WAV file, audio-only 3GP, audio-only 3G2, MP4, and audio-only QuickTime formats. Audio announcement clips use G.711, G.722, AMR, AMR-WB, EVS, EVRC, EVRCB, EVRCNW, AAC-LC (Advanced Audio Coding Low Complexity), and G.729 encoding. The support varies with protocol, server, and platform.

NOTE: Opus is not supported for an announcement container. However, you can play announcement to a Opus port by transcoding. For example, streaming and transcoding the G.711 audio stored in a WAV clip.

Each announcement request can direct the Containerized Decomposed Media Server to play a single audio clip or a list of audio clips. Where supported, an announcement request can direct the Containerized Decomposed Media Server to dynamically construct an announcement using sets (for example, using one of a set of greeting announcements in different languages) or variables (for example, telling a conference participant that the second caller is in the conference).

Audio announcements played from internal memory, streamed from an off-the-shelf NFS, HTTP, or HTTPS server can be played once, for a specified maximum duration, or repeated a specified number of times with an optional silence interval inserted between each repetition. In addition, the control agent can direct the Containerized Decomposed Media Server to begin playing at any offset from the beginning or end of the announcement. In MSML 1.1, the control agent can set and adjust the announcement volume at the beginning or during the play.

Announcements can be designated to be interruptible (bargeable) by DTMF digits or voice activity detection on an audio port. If a clip is barged, the Containerized Decomposed Media Server can report how much of the clip was played before being barged. Announcements played to a port, that is, to a single RTP session, can be barged by DTMF digits or voice activity detection; announcements played to a conference cannot be barged.

Play Video Announcement to a Port

The Containerized Decomposed Media Server provides features for storing and playing multimedia (video and audio combined) streams and clips.

Like audio-only announcements, multimedia announcements can be played from internal memory, streamed from an off-the-shelf NFS, HTTP/HTTPS, or RTSP server. They support WAV, QuickTime, 3GP, MP3, MP4, and 3G2 formats. Multimedia announcements use G.711, EVRC, EVRCB, EVRCNW, AMR, AMR-WB, or G.729 for audio encoding and H.264 Mode 0 and Mode 1, and VP8 for video encoding. The Containerized Decomposed Media Server supports audio only, video only, and audio-video over HTTP/HTTPS in cache mode. Radisys recommends to set the cache size as 1 GB when playing HTTP announcements.

Multimedia announcements can be barged by DTMF or voice activity detection, provided the media stream includes an audio channel.

Some features supported for audio announcements are not supported for video announcements. For example, multimedia announcements have the following limitations.

- Sets and variables are not supported for video, and video announcements cannot be used in conjunction with audio sets and variables.
- Multimedia clips do not support silence intervals or playing from an offset.

Announcements containing video only or video combined with audio can be played once, for a specific duration, or repeated a specified number of times. When barged by DTMF digits or voice activity detection, play time is not reported.

A multi-clip announcement must contain the same media type through the entire set of clips. For example, the Containerized Decomposed Media Server does not play a multi-clip announcement if one of the clip is video-only, another clip is audio-only, and a third clip contains both audio and video.

An audio-video announcement can be played to an audio-only or video-only port. Based on the endpoint SDP, the Containerized Decomposed Media Server automatically determines what kind of media the endpoint can accept and sends the appropriate content of the multimedia file.

Delayed Announcement

The Containerized Decomposed Media Server supports configuring the duration of silence to be played before and after streaming the audio, video, or multi-media announcement through the management interface. The pre- and post-announcement silence streaming is supported in all the service contexts and from the internal, NFS, HTTP, or HTTPS servers. The announcement can be in transcoded or transcode bypass mode.

For port announcements, the Containerized Decomposed Media Server plays the Web GUI configured duration of silence prior to streaming the first clip. The Containerized Decomposed Media Server plays the Web GUI configured duration of silence at the successful completion of the clip in a single clip announcement, at the end of the last clip in a multi-clip announcement, or at the end of last iteration in a multi-iteration announcement. Both pre- and post-announcement silence are played for the first port announcement only. For subsequent announcement requests on the same port, the pre- and post-silence are not played. When announcement barges-in or fails in-between, the Containerized Decomposed Media Server does not play the post-announcement silence. Digit collection occurs during the pre- and post-silence duration but first digit timer (FDT) is started only after completion of the pre-silence duration. Announcement are barged-in during pre- and post-silence phases. Any failure in playing pre- or post-silence fails the announcement request.

The Containerized Decomposed Media Server excludes the pre- and post-announcement silence from the total duration of the announcement played. The pre- or post-announcement duration are not considered in total play duration returned to the AS through the MSML and VxML shadow variables.

For information about configuring pre- and post-announcement silence, see *Configure Audio on page 218*.

Variable Announcements

The Containerized Decomposed Media Server supports fixed and variable announcements. For playing the variable announcements the Containerized Decomposed Media Server uses **Sets and Vars** and **Diction Rule Implementation (DRI)**.

Sets and Variables

The Containerized Decomposed Media Server supports rendering announcements dynamically from sets of clips, or by using clips referenced by variables. A set is a provisioned collection of audio clips with an associated selector type and value. The selector identifies a specific physical audio clip within the set. A variable represents a semantic concept (such as date or number), which the Containerized Decomposed Media Server uses to construct the appropriate audio segment dynamically.

The Containerized Decomposed Media Server sets and variables feature is described in detail in the *Sets and Variables Interface Reference*.

Diction Rule Implementation

The Containerized Decomposed Media Server supports Diction Rule Implementation (DRI) to play variable announcements in MSML and MSCML service contexts in addition to sets and vars. However, for a given language, only one method (sets and vars or DRI) is applicable. The DRI takes precedence over the sets and vars.

In DRI, the variable announcement grammar is specified in the DRI library for a given language and linked to the Containerized Decomposed Media Server. Each language configured in the Containerized Decomposed Media Server is associated with one DRI library. The Containerized Decomposed Media Server allows you to upload a maximum of 32 DRI libraries through the management interface, and only 16 languages are activated at any time for handling variable announcements through the DRI mechanism.

When the configured DRI library loading fails, the Containerized Decomposed Media Server raises the alarm 193 *DRI library initialization failed for languages: X*. The Containerized Decomposed Media Server fails the variable announcement calls for the failed DRI library language and does not fall-back to sets and vars for the same language.

For information on language specific configuration and variable type, refer *Sets & Vars Interface Reference*.

For information on DRI related Web GUI configurations, see *Media Storage Management on page 339*.

Announcement Speed Control

The Containerized Decomposed Media Server allows to change the audio announcement speed on the MSML port using speed-up and speed-down controls. The speed-up control allows you to listen to the audio clips at a speed faster than the original speed. The speed-down control allows you to listen to the audio clip at a speed slower than the original speed.

The speed-up and speed-down controls are supported on the audio announcements played through the internal, NFS, HTTP, or HTTPS servers. The speed-up and speed-down controls are supported in all the audio clip formats.

The speed-up control is increased in multiples of 0.2. The possible values of speed-up are 1.2, 1.4, 1.6, 1.8, and 2.0. If the speed is increased beyond 2.0, the value is discarded. The speed-down control is decreased in multiples of 0.2. The possible values of speed-down are 0.8, 0.6, and 0.4. If the speed is decreased beyond 0.4, the value is discarded. The upper limit of the speed-up and lower limit of the speed-down controls are controlled as per the management interface configuration.

The Containerized Decomposed Media Server supports speed-up or speed-down in the following options.

- Speed-up or speed-down is triggered based on the designated DTMF digit dialed by the user. The Containerized Decomposed Media Server handles the speed-up and speed-down operations without the AS intervention. The AS must configure the Containerized Decomposed Media Server with designated DTMF digit.
- The DTMF digits are reported by the Containerized Decomposed Media Server to the AS. The AS sends the MSML control command to speed-up or speed-down the announcement through a new `<dialogstart>` element.

The Containerized Decomposed Media Server supports speed-up and speed-down on both transcoded and transcode bypass audio announcements. The speed-up and speed-down operations require an announcement to be transcoded, therefore the Containerized Decomposed Media Server converts bypass announcement to a transcoded announcement on speed-up and speed-down events.

NOTE: Announcement duration reported by the Containerized Decomposed Media Server is the actual duration of the original clip being played.

For information about configuring minimum and maximum speed, see *Configure Audio on page 218*.

Resource Reservation for Transcode Bypass Announcements

The Containerized Decomposed Media Server provides a configuration parameter in the management interface to enable or disable upfront bypass transcoding resource reservation for MSML announcement service on port. When **MSML Bypass Announcement Resource Reservation** is enabled, the Containerized Decomposed Media Server performs upfront resource reservation (DSP CPU, buffers, and bandwidth) that are required for the transcode bypass announcement. The Containerized Decomposed Media Server also supports this feature in multimedia ports.

When **MSML Bypass Announcement Resource Reservation** is enabled, the Containerized Decomposed Media Server does not fail the first transcode bypass announcement request on that port. The Containerized Decomposed Media Server reserves the resources for the bypass announcement service. If any other service request comes on the port, the Containerized Decomposed Media Server releases the resources that are reserved for the announcement service.

NOTE: The Containerized Decomposed Media Server rejects the initial MSML INVITE request with 486 response, if there are insufficient resources to reserve for the transcode bypass announcement service.

If the Containerized Decomposed Media Server receives any mid-call codec change request on the port before the first service request, the Containerized Decomposed Media Server re-reserves the resource reservation for the new port codec. If the resource reservation fails for the mid-call codec, the Containerized Decomposed Media Server rejects the mid-call codec change request. The Containerized Decomposed Media Server retains the initial call bypass resources even after rejecting the mid-call codec change request.

For information about configuring MSML bypass announcement resource reservation, see *Configure SIP on page 197*.

CRBT Random Ring

Caller Ring Back Tone (CRBT) is a service for personalizing the ringback tone of a remote endpoint by choosing a specific song or audio file to play while the call is connecting, instead of the standard ringback tone. The ringback tone, offered by the service provider, is generally a clip that is of 40 to 50 seconds duration.

Using the random ring feature, you can download a much longer clip—such as a pop song—after which a 40 to 50 second segment is randomly selected as the actual ringback tone for playback.

The Containerized Decomposed Media Server allows the control agent to specify start and end offset values for the announcement, using the **start** and **end** attributes of the MSML `<play>` element, respectively.

The random ring announcement can be played to a connection or conference. Announcements must be audio-only, in WAV file format, compressed with G.711, or G.729 codecs. The clip can reside internally on the Containerized Decomposed Media Server or on an NFS server.

Text and Icon Overlay for Video Announcements

The text and icon overlay feature allows the control agent to overlay text labels and an icon image on H.264 (Mode 0 and Mode 1), and VP8 video announcements played to a port. The video announcement target must be a connection.

NOTE: VP8 cannot be natively recorded to a file, it must be transcoded to H.264.

You can specify a maximum of four text labels and one icon image per video announcement. The control agent can set the position of the label and image on the screen, the display time, and relative order of labels (from background to foreground for overlapping regions). You can customize the look of the display text using a number of optional parameters.

The underlying video announcement can be streamed either from the Containerized Decomposed Media Server itself (as with an NFS clip), from an external RTSP server (as an RTSP clip), or from an external HTTP server (as an HTTP clip using cache mode). The announcement can consist of a single clip or multiple clips, in either multimedia files or separate video and audio files. The text and icon overlay can be inserted by the control agent at any time during the announcement. When an announcement is looped (repeated), the text and icon are redisplayed at the start of all successive iterations.

The text and icon overlay feature is available for Containerized Decomposed Media Server by using SIP with MSML 1.1.

RTSP Interface

RTSP announcements can be played to a connection or an audio or video conference.

A control agent uses the RTSP URL **rtsp://** to specify an RTSP announcement. The Containerized Decomposed Media Server establishes an RTSP session with the RTSP server, receives the announcement, and streams it to the remote client. Similar to regular announcements, an RTSP announcement can be barged.

Port announcement is supported through RTSP interface. Announcements streamed from RTSP servers do not support specifying maximum duration, repetitions, offset, and MSML 1.1 volume settings. When barged by DTMF digits or voice activity detection, play time is not reported. The supported audio encoding formats are PCMU, PCMA, and AMR. This codec list is not user configurable.

The Containerized Decomposed Media Server supports the maximum packetization of 50 ms for any codec.

RTSP announcements can use audio compressed with the following formats.

- G.711 with packetization of 5, 10, 20, 30, 40, or 50 ms
- AMR that is octet-aligned/bandwidth-efficient with a bit rate between 4.75 to 12.2 kb/s and packetization of 20 or 40 ms

  NOTE: To play AMR clips from RTSP server, configure the audio jitter buffer for more than 60 ms.

For video, RFC 6184 H.264 (mode 0 and mode 1) is supported.

The control agent ensures that the video parameters (picture size, MPI, and bit rate) of the announcement are within the capabilities negotiated for the receiving terminals. The Containerized Decomposed Media Server does not verify these attributes while negotiating H.264 with the RTSP server.

Video announcement is supported through RTSP interface. As with audio-only announcements, video-only announcements streamed from an RTSP server do not support specifying maximum duration, repetitions, offset, and MSML 1.1 volume settings. The supported video encoding formats are H.264 (Mode 0 and Mode 1). This codec list is not user configurable.

RTSP servers do not signal end of stream (EOS). The Containerized Decomposed Media Server waits for a timeout period, configurable through the management interface, before terminating an RTSP announcement. The RTP packets stop streaming from an RTSP server. The RTSP server may have its own timeout period. For example, the Darwin Streaming Server Version 5.5.5 has a configurable rtp_timeout, set by default to 120 seconds, that terminates announcements if RTCP is not received from its client. As the Containerized Decomposed Media Server does not send RTCP to the server, this timeout period must be set appropriately for playing long announcements.

The RTSP announcements are supported for Containerized Decomposed Media Server using MSML 1.1.

NOTE: As required by MRCP Version 1 (RFC 2326), RTSP is also supported for an ASR or TTS client device.

The Containerized Decomposed Media Server supports H.264 video codec in the RTSP announcement. RTSP announcement is supported on all H.264 profiles. The Containerized Decomposed Media Server does not support transcoding when playing the H.264 video RTSP announcement on a port or VAS conference. But the Containerized Decomposed Media Server supports transcoding when playing the H.264 video RTSP announcement on CPV conference.

Optimal Clip Selection

In transcode bypass audio announcement, when optimal clip is enabled in the management interface, the Containerized Decomposed Media Server translates the base clip name specified in the play request to the optimal clip, based on the port codec. The Containerized Decomposed Media Server derives the optimal clip name from the base clip specified in the MSML, MSCML, VoiceXML, Netann protocol requests. The optimal clip location is supported for internal, NFS, and HTTP servers. The optimal clip selection is supported for sets and variables and multi-clip announcements as per the following conditions.

- When the port codec is AMR or AMR-WB and if more than one mode is negotiated on the port, the Containerized Decomposed Media Server plays the highest mode optimal clip. If only one mode is configured on the port, the Containerized Decomposed Media Server plays the matching mode optimal clip. If the optimal clip is not found, the Containerized Decomposed Media Server plays the base or original clip specified by the application server.

  For example, if an AMR or AMR-WB port is negotiated the mode-set from 0 to 5, the Containerized Decomposed Media Server tries the mode 5 clip first. If the mode 5 clip is not found, the Containerized Decomposed Media Server does not try with lower mode clips because it may delay the announcement.

- When the port codec is EVS (`evs-mode-switch=AMR-WB-IO`) and if more than one mode is negotiated on the port, the Containerized Decomposed Media Server plays the highest mode AMR-WB optimal clip. If only one mode is configured on the EVS port, the Containerized Decomposed Media Server plays the matching mode optimal clip. If the port codec is EVS (`evs-mode-switch=PRIMARY`), the Containerized Decomposed Media Server plays the highest bitrate and bandwidth clip.
- The Containerized Decomposed Media Server does not try to play the optimal clip if transcode bypass is disabled in the management interface.
- The Containerized Decomposed Media Server does not try to play the optimal clip when a port is in conference and transcode bypass is not allowed on the port announcement.
- The Containerized Decomposed Media Server provides the management interface configuration to exclude the mode-change restrictions parameters (`mode-change-period=2` and/or `mode-change-neighbor=1`) from the transcoding bypass decision for the AMR, AMR-WB, and EVS (AMR-WB-IO mode only) announcement ports. When the **Transcode Bypass on Restrictive Mode Change Port** parameter is disabled, transcode bypass is not allowed on the AMR, AMR-WB, and EVS (AMR-WB-IO mode only) ports using restricted mode and the Containerized Decomposed Media Server does not try to play the optimal clip. When the **Transcode Bypass on Restrictive Mode Change Port** parameter is enabled, the Containerized Decomposed Media Server plays the announcement in transcode bypass mode on the AMR, AMR-WB, and EVS (AMR-WB-IO mode only) ports using the restricted mode, if all other transcode bypass conditions are fulfilled.
- The Containerized Decomposed Media Server tries to play the optimal clip first. If the optimal clip is not found, the Containerized Decomposed Media Server plays the base clip.
- The Containerized Decomposed Media Server selects the optimal clip by searching the clip name. The optimal clip is processed for transcoding or bypass mode of announcement based on the port, clip codec, and codec parameters.
- The Containerized Decomposed Media Server does not support optimal clip selection based on port video codec. However, in a multi-media (audio-video) call, if audio-video or audio only announcement is played, the Containerized Decomposed Media Server plays an optimal clip with a clip name that is constructed using only port audio codec. When a multi-media clip is played on an audio only call, the Containerized Decomposed Media Server constructs the optimal clip using only port audio codec. The optimal clip selection is disabled for video only call.
- The Containerized Decomposed Media Server plays the optimal clip in the beginning of the announcement. The Containerized Decomposed Media Server continues to play the current clip even if the port codec changes in the mid-call.
- The Containerized Decomposed Media Server constructs the optimal clip name as per the following clip naming convention.

NOTE: The user must follow the following clip naming convention and place the optimal clips at the base location specified by the AS.

Table 9. Optimal Clip Naming Convention

Port Codecs	Optimal Clip Naming Convention
G.711a/µ-law, G.729, G.722, EVRC, EVRCNW, and EVRCB	`<BASE_CLIP_NAME>_<AUDIO_CODEC_NAME>.<EXTENSION>`
AMR and AMR-WB[a]	`<BASE_CLIP_NAME>_<AUDIO_CODEC_NAME>_<ModeN>.<EXTENSION>`
EVS (evs-mode-switch=Primary)	`<BASE_CLIP_NAME>_<AUDIO_CODEC_NAME>_<BITRATE>_<BW>.<EXTENSION>`
EVS (evs-mode-switch=AMR-WB-IO)	`<BASE_CLIP_NAME>_AMRWB_<ModeN>.<EXTENSION>`

[a] For AMR-WB codec the <AUDIO_CODEC_NAME> is AMRWB.

where,

- **`<BASE_CLIP_NAME>`**. The clip name provided by the AS in the protocol request (excluding file extension). For example, 'hello', 'welcome'.
- **`<AUDIO_CODEC_NAME>`**. Audio port codec. For example, AMR, AMR-WB, EVRC, EVRCB, EVRCNW, G.722, G.729, G.711 a-law, G.711 µ-law, and EVS.
- **`<ModeN>`**. Applicable for AMR and AMR-WB codecs only. ModeN has standard modes for the AMR and AMR-WB codec where N ranges from 0 to 8.

  For example, the clip name specified in the protocol request is **hello.3gp**. The optimal clip for AMR-WB is **hello_AMRWB_Mode0** to **hello_AMRWB_Mode8**.
- **`<BITRATE>`**. Applicable for EVS clips only. Supported values are: BR_5_9, BR_7_2, BR_8_0, BR_9_6, BR_13_2, BR_16_4, BR_24_4, BR_32_0, BR_48_0, BR_64_0, BR_96_0, and BR_128_0.
- **`<BW>`**. Applicable for EVS clips only. Supported values are: BW_NB, BW_WB, and BW_SWB.

  The BW_WB clip is selected when port is negotiated with BW_WB or BW_NB_WB. The BW_SWB clip is selected when port is negotiated with BW_SWB or BW_NB_SWB.
- **`<EXTENSION>`**. Base clip extension is ignored when received in a protocol request from the AS and the optimal clip extension is as per Table 10.

Table 10. Port Clip and Optimal Clip Extension

Port Codecs	Optimal Clip Extension
G.711a/µ-law, G.729, and G.722	.WAV
AMR, AMR-WB, and EVS	.3GP
EVRC, EVRCB, and EVRCNW	.3G2
Opus	Not applicable

For example, if the clip name in the protocol request is **welcome.wav**, the optimal clip for G.711 a-law is **welcome_G711A.wav**.

The absolute optimal clip name (exclusive of *file:/* or *nfs:/* and an inclusive of *http:/*) is supported for a maximum of 511 characters. If the optimal clip name exceeds 511 characters, the Containerized Decomposed Media Server plays the original clip and does not try for the optimal clip.

For information about configuring optimal clip selection, see *Configure Transcode Bypass on page 274*.

Recordings

The Containerized Decomposed Media Server records both audio and video announcements. Recordings can be made for a connection or a conference. For more information on recording conferences, see *Record Audio Conference on page 68* and *Record Video Conference on page 82*.

When recording is in append mode, if the existing file is already encrypted and the **Encrypt Subscriber Data** is enabled, the Containerized Decomposed Media Server appends the newly recorded content to the encrypted file. When recording is in append mode, if the existing file is already encrypted and the **Encrypt Subscriber Data** is disabled, the Containerized Decomposed Media Server fails the recording.

The Containerized Decomposed Media Server supports recording in WAV (audio-only), 3GP, and QT file formats in all service contexts and the MP4 file format with H.264 as video codec and Advanced Audio Coding Low Complexity (AAC-LC) as audio codec in the MSML service context. When the **Encrypt Subscriber Data** is enabled in the management interface, the payload and media contents are encrypted for all the supported file formats except the MP4.

This section describes the following recording features.

Record Audio from a Port

The Containerized Decomposed Media Server can record audio clips from a single port (for example, a conference participant or voice mail user) or record a full conference mix. Generally, single-port audio recordings are short clips (for example, a participant name) and are recorded during the session in real-time. These short recordings can be stored transiently in the internal memory of the Containerized Decomposed Media Server; longer recordings can be streamed to an external NFS, HTTP, or HTTPS servers.

The Containerized Decomposed Media Server supports storing of persistent recording clips on a local storage. You can configure local persistent recording path through the management interface. The clips recorded at this path are not deleted when the call is terminated and also clips are preserved across the Containerized Decomposed Media Server reboot.

The Containerized Decomposed Media Server allows you to delete the local persistent recording clips through the management interface. All the clips and sub-directories present within the configured persistent recording path are deleted. The Containerized Decomposed Media Server does not restrict access permissions for the created directories.

For information on configuring the local persistent recording path, see *Configure Local Persistent Recording Path on page 345* and for information on deleting the local persistent recording clip, see *Delete Local Persistent Recording Clip on page 346*.

Single-port audio recordings can be terminated by setting a maximum record time, or by having the control agent send an instruction to terminate the recording. Single-port audio recordings (unlike conference recordings) can also be terminated by in-band or out-of-band DTMF tones.

The DTMF clamping is supported in MSML port recording regardless of the port using in-band or out-of-band DTMF. DTMF clamp and DTMF detect can be enabled or disabled independently. The Containerized Decomposed Media Server transcodes recording when the DTMF clamp is enabled. The Containerized Decomposed Media Server supports DTMF clamping in all the supported audio codecs. However, DTMF clamp is unreliable for high-compression codecs.

These audio recording capabilities, combined with playback, provide a seamlessly integrated, cost-effective, and highly scalable audio archiving and playback system.

The Containerized Decomposed Media Server supports post-speech silence trimming on the MSML, MSCML, and VXML recording ports and MSML conference recording in 3GP and QT[1] formats. The recorded clip location can be internal, NFS, HTTP, and HTTPS servers.

Record Video from a Port

Participant video recordings are single-port video recordings. Participant video recordings are generally a short clip recorded in real-time during the session. These short recordings can be stored transiently in the internal memory of the Containerized Decomposed Media Server, whereas longer recordings can be streamed to an external NFS, HTTP, or HTTPS servers.

The Containerized Decomposed Media Server supports storing of persistent recording clips on a local storage. You can configure local persistent recording path through the management interface. The clips recorded at this path are not deleted when the call is terminated and also clips are preserved after a Containerized Decomposed Media Server reboot.

The Containerized Decomposed Media Server allows you to delete the local persistent recording clips through the management interface. All the clips and sub-directories present within the configured persistent recording path are deleted. The Containerized Decomposed Media Server does not restrict access permissions for the created directories.

For information on configuring the local persistent recording path, see *Configure Local Persistent Recording Path on page 345* and for information on deleting the local persistent recording clip, see *Delete Local Persistent Recording Clip on page 346*.

1. The .mov and .qt are the file extension used for Quick time (QT) file format.

Both the audio and video streams of a video port can be recorded to a multimedia file and can carry audio, video, or both. Files recorded by the Containerized Decomposed Media Server can be played back using QuickTime, 3GP, or MP4. QuickTime supports MOV or QT player and 3GP supports SM or VLC player, and MP4 supports VLC player. Both interleaved and non-interleaved audio and video are supported. Recording is always done as interleaved.

Single-port video recordings can be terminated by setting a maximum record time, or by having the control agent send an instruction to terminate the recording. Single-port video recordings (unlike conference recordings) can also be terminated by in-band or out-of-band DTMF tones.

These video recording capabilities, combined with playback, provide a seamlessly integrated, cost-effective, and highly scalable video archiving and playback system.

Multimedia recordings have the following limitations compared with audio recordings.

- The Containerized Decomposed Media Server does not trim pre-speech or post-speech silence from the audio component of a multimedia file. This is because the video and the audio portion of the recording must match, and there is no pre- or post-speech silence for video.
- Appending to a multimedia recording is not supported.

The Containerized Decomposed Media Server must receive an I-Frame whenever it starts to record a multimedia file. An I-Frame is a special video frame that contains complete and self-contained video data. I-Frames are generally transmitted by terminals at regular intervals. In this case, the Containerized Decomposed Media Server requests the I-Frame from the terminal using a Fast Update Request. RTCP-PLI is negotiable in SDP on port by-port basis, so it is a preferred method for I-Frame request.

NOTE: Radisys does not recommend RTP-FIR request method to invoke an I-frame.

H.323 networks support Fast Update requests; however, SIP-based networks do not uniformly implement any one Fast Update Request mechanism. For SIP networks, the Containerized Decomposed Media Server supports the Video Picture Fast Update message mechanism, draft-levin-mmusic-xml-media-control defined in RFC 5168, and the Full INTRA-frame Request (FIR) packet in RTP defined in RFC 2032. The Containerized Decomposed Media Server supports the incoming Fast Update Request.

The Containerized Decomposed Media Server stores the maximum H.264 NAL size in a Radisys custom atom for recorded clips.

To ensure backward compatibility for transcode free playback to H.264 mode 0 ports, H.264 clips that does not contain maximum NAL size atom are same as H.264 clips that has zero value for the maximum NAL size atom.

Optimal Clip Recording

When optimal clip bypass recording is enabled through the management interface, the Containerized Decomposed Media Server allows to record an audio port through forceful transcode bypass. The Containerized Decomposed Media Server overrides the clip container and codec format in the record request where optimal clip recording is possible and forces transcode bypass recording on such ports. The Containerized Decomposed Media Server records as per-clip container and codec format in the record request with transcoding, where optimal clip recording is not possible. The Containerized Decomposed Media Server performs bypass recording for internal clip, NFS, HTTP, or HTTPS recording requests.

The Containerized Decomposed Media Server generates transcode bypass recorded clips on audio ports as per Table 11.

Table 11. Port Clip and Optimal Clip Extension

Port Codecs	Optimal Clip Extension
G.711a/μ-law, G.729, and G.722	.WAV
AMR and AMR-WB	.3GP
Opus, EVS, EVRC, and EVRCB	Not applicable

The user must follow Table 9 guidelines for the optimal clip recording file naming convention. The highest configuration supported on the port is used for naming convention.

The following features are not supported when performing optimal clip recording in transcode bypass on an audio port.

- Pre-speech and post-speech timers are ignored even if pre-speech and post-speech timers are enabled for recording.
- Clamping does not work even if recording with clamping is requested.

The DTMF in-band, pass-through, and VQE VAD features are supported when they are enabled on an audio port.

When recording is requested and optimal clip recording is enabled, the Containerized Decomposed Media Server overrides the file name and generates the clips as per optimal clip recording convention with bypass recording. Optimal clip recording is ignored in multimedia recordings.

For information on configuring optimal clip recording, see *Configure Audio on page 218*.

Dual-Channel Recording

Containerized Decomposed Media Server supports both single and dual-channel recording and can be configured through the management interface. Containerized Decomposed Media Server supports recording in audio-only irrespective of whether it is an audio-only or AV conversation.

Containerized Decomposed Media Server supports encryption during dual-channel recording and can be configured through the management interface. The Containerized Decomposed Media Server can also playback the encrypted dual-channel recording.

IVR/VRU

Interactive Voice Response (IVR), or Voice Response Unit (VRU), refers to the interaction between a user and the system providing the media services. The user generally responds to menu prompts using either DTMF or voice. The system can provide a telephony service, play a clip, or voice text. Examples of IVR-based services using the Containerized Decomposed Media Server are financial information requests, call routing, and voice mail systems.

This section describes the IVR-related features.

DTMF

The Containerized Decomposed Media Server supports a wide variety of DTMF functions for both in-band and out-of-band RFC 2833 telephone-event DTMF tones. The Containerized Decomposed Media Server only supports sending out DTMF out-of-band events as per RFC 2833.

This section describes the following general DTMF functions:

- *DTMF Detection, Collection, and Generation*
- *RFC 2833 Telephone-Event Support*
- *RFC 4733 Telephone-Event Support*

The Containerized Decomposed Media Server also supports receiving DTMF as defined in RFC 4733. Accordingly long event and multiple event reception are supported. RFC 4733 represents out-of-band DTMF. For more information about the DTMF functions used in conferences, see *DTMF in Conferences on page 59*.

DTMF Detection, Collection, and Generation

The Containerized Decomposed Media Server detects, collects, and generates DTMF signals. These can be in-band audio DTMF tones or out-of-band RFC 2833/RFC 4733 (receive only) telephone-events.

DTMF collection can include a number of mechanisms supported by the control protocol/language used by the control agent, including collection grammars. For example, the control agent can use Speech Recognition Grammar Specifications (SRGSs), which are built-in language grammars dedicated to specific tasks such as digit sequences or phone numbers, or digit maps as defined by RFC 3435. The Containerized Decomposed Media Server also supports long digit detection. The MSCML supports `<playcollect>` request to collect DTMF digits.

DTMF detection is implicitly enabled on MSML port for lifetime. AS can request `<dtmf>` to collect detected DTMF but it cannot disable the DTMF detection. Since DTMF detection is an implicit service, it implies that all other AS-controlled services (for example, `<faxdetect>`, `<play>`, `<record>`) are supported concurrently with DTMF detection.

DTMF detection is implicitly enabled on the MSCML port for lifetime. AS can request `<playcollect>` to collect the detected DTMF but they cannot disable the DTMF detection. Since DTMF detection is an implicit service, it implies that all other AS-controlled services such as `<play>` is supported concurrently with DTMF detection.

In addition to collection grammars, the Containerized Decomposed Media Server supports a DTMF type-ahead buffer, as well as the following optional capabilities.

- Dynamically specified first-digit timers
- Dynamically specified inter-digit timers
- Dynamically specified extra-digit timers
- Definition of a special termination key, such as #

The way DTMF is collected depends on media negotiation by the control protocols. For example, although in-band and out-of-band DTMF methods are supported, only the method negotiated using the control protocol is used.

RFC 2833 Telephone-Event Support

The Containerized Decomposed Media Server detects and generates out-of-band DTMF (RFC 2833 telephone-events). RFC 2833 telephone-events provide greater reliability than in-band audio tones when low bit rate codecs are used (for example, G.729, AMR, EVRC).

Table 12 shows the Containerized Decomposed Media Server support for RFC 2833 (telephone-events).

Table 12. Telephone-Event Support

Event	Description	Value	Support	
			Detect	Generate
0–9	Digits 0 through 9	0–9	Yes	Yes
*	Asterisk digit	10	Yes	Yes
#	Pound sign	11	Yes	Yes
A–D	The digits A, B, C, D	12–15	No	Yes
Fax CED	The answering Group III fax machine sends a Call**ED** Terminal Identification tone of 2100 Hz.	32	Yes	No
Fax CNG	After dialing the called fax machine's telephone number (and before it answers), the calling Group III fax machine (optionally) begins sending a Calli**NG** tone consisting of an interrupted tone of 1100 Hz.	36	Yes	No

RFC 4733 Telephone-Event Support

Event numbers supported are same as in RFC 2833. Additionally, RFC 4733 telephone-events support receiving of long duration events and multiple events.

Table 13 shows the Containerized Decomposed Media Server support for RFC 4733 (telephone-events).

Table 13. Telephone-Event Support

Event	Description	Value	Support	
			Detect	Generate
0–9	Digits 0 through 9	0–9	Yes	Yes
*	Asterisk digit	10	Yes	Yes
#	Pound sign	11	Yes	Yes
A–D	The digits A, B, C, D	12–15	No	Yes

DTMF in Conferences

In conferences, the Containerized Decomposed Media Server can perform the following:

- Detect, collect, and generate DTMF tones
- Filter (clamp) DTMF tones out of the conference mix
- Allow DTMF to be passed through SIP Netann and MSML conferences

DTMF Detection, Collection, and Generation in Conferences

The Containerized Decomposed Media Server support for in-band and out-of-band DTMF signaling for conferences is identical to that for DTMF signaling during conference IVR front ends.

For more information, see *DTMF on page 57*.

DTMF Clamping

DTMF clamping filters DTMF tones out of the media stream. DTMF clamping can remove DTMF tones from the audio received from conference participants so that tones are not heard in the conference mix or recorded. Media other than DTMF tones, pass through unchanged.

In SIP, MSML, and MSCML conferences, DTMF clamping can be enabled or disabled in real-time.

DTMF Pass-Through

NOTE: DTMF clamping removes DTMF tones from the media stream, whereas DTMF pass-through regenerates and relays them to conference participants. Consequently, these two features cannot be used together.

DTMF pass-through is supported in SIP Netann and MSML conferences, for up to 125 participants (the maximum size of a conference). DTMF pass-through is not supported with the large conference feature, for conferences exceeding 125 participants. DTMF pass-through cannot be enabled on an audio participant while joining a large conference or a standard audio conference if there are already 125 send-receive participants in the conference. If the DTMF pass-through is enabled on a standard audio conference, this conference cannot be escalated to a large conference by joining more than 125 send-receive participants to the conference.

In addition, when DTMF pass-through is enabled for a SIP Netann and MSML conference ports, silence suppression is disabled regardless of what was configured for the port. The Containerized Decomposed Media Server cannot pass through simultaneous digits on multiple ports. The DTMF pass-through setting in Web GUI only controls the SIP netann and MSML conference. For RFC 4117, DTMF pass-through is always enabled regardless of the GUI setting.

For SIP Netann and MSML conferences, when pass-through is enabled (through Web GUI), it is enabled for all conference calls established on the Containerized Decomposed Media Server. For MSML conferences, the DTMF pass-through can be enabled on per-port basis.

When DTMF pass-through is disabled in SIP netann and MSML, incoming DTMF tones gets propagated to outgoing ports.

When Containerized Decomposed Media Server receives long duration DTMF events as per RFC 4733, the Containerized Decomposed Media Server suitably truncates the duration of DTMF events (RFC 2833) while sending out from corresponding output ports (1 second in case of Opus and 3 seconds in case of all other NB and WB codecs).

Automatic Speech Recognition

Automatic Speech Recognition (ASR) converts human speech to computer data. ASR is supported for VoiceXML and MSML interfaces of Containerized Decomposed Media Server by using external ASR servers.

The Containerized Decomposed Media Server interface to external ASR servers support the following standards.

- IETF MRCP Version 1 (RTSP version) and Version 2 (SIP version) as required by a client device
- RFC 2326 RTSP of April 1998 as required for MRCP Version 1 on the ASR interface
- W3C Speech Recognition Grammar Specification (SRGS) Version 1.0 syntax for representing grammar
- W3C Natural Language Semantics Markup Language (NLSML) working draft 20 for receiving ASR session results
- The Containerized Decomposed Media Server ASR feature is compatible with the Nuance Recognizer speech server (Nuance Speech Server Version NSS5.0 and Nuance Recognizer Version Nrec9.0)

The Containerized Decomposed Media Server VoiceXML and MSML interfaces send voice input that is processed by external ASR servers and return collection results to the Containerized Decomposed Media Server for interpretation.

- In VoiceXML, voice input can be enabled using the VoiceXML `<property>` element or through the Containerized Decomposed Media Server management interface

In MSML, ASR and TTS are supported on connections but not on conferences, the `<speech>` element activates grammars

By default, the Containerized Decomposed Media Server accepts DTMF input only. The Containerized Decomposed Media Server streams audio to the ASR server in G.711 µ-law or G.711 a-law, as configured through the management interface.

The Containerized Decomposed Media Server supports load balancing a pool of speech servers based on configured server capacity and number of used ports. The Containerized Decomposed Media Server does not support end pointing (detecting the end of a speech stream).

Text to Speech

Text to Speech (TTS) uses computer systems to reproduce human speech. The Containerized Decomposed Media Server VoiceXML and MSML interfaces support synthesized speech output using external TTS servers.

The Containerized Decomposed Media Server interface to external TTS servers supports the following standards.

- IETF MRCP Version 1 (RTSP version) and Version 2 (SIP version) as required by a client device
- RFC 2326 RTSP of April 1998 as required for MRCP Version 1 on the TTS interface
- W3C Speech Synthesis Markup Language (SSML) Version 1.0
- Chinese Speech Synthesis Markup Language (CSSML) for specifying TTS clips using Chinese

The Containerized Decomposed Media Server TTS is compatible with the following speech servers.

- iFLYTEK Interphonic Version 5.0 with 8k xiaoyan language package and IMS
- Nuance RealSpeak 4.5.0

The Containerized Decomposed Media Server receives SSML and text strings embedded in VoiceXML scripts or MSML dialogs and sends these to external TTS servers, which return synthesized speech. TTS servers can stream audio in G.711 µ-law or G.711 a-law, as configured through the management interface. The Containerized Decomposed Media Server supports synthesizing English and Mandarin. It also supports synthesizing of other languages supported on the external server but not included in Radisys compatibility testing. Prompt control of TTS clips is not supported.

The Containerized Decomposed Media Server supports load balancing a pool of speech servers based on configured server capacity and number of used ports.

Hindi Text-to-Speech Announcement

The Containerized Decomposed Media Server adds support for the Hindi Text-to-Speech (TTS) announcement for multimedia calls, in addition to the English TTS announcement, to provide dynamic information that is specific to the caller. The information that cannot be pre-recorded and is caller specific, such as account balance, card expiry date, location specific details, and so on, is played to the user through the TTS functionality.

The Containerized Decomposed Media Server supports playing a combination of audio or audio-video clips and Hindi TTS announcements in the same request from the Application Server (AS). When playing the text in the announcement, the Containerized Decomposed Media Server uses the current session language to play the TTS announcement. The Containerized Decomposed Media Server supports TTS announcements in male, female, and neutral voices. By default, the gender value female is selected if the same is not explicitly specified in the request from the Application Server (AS).

The Containerized Decomposed Media Server supports the `<tts>` MSML element to play a TTS announcement. The text to be played in the announcement is specified in-line in the `<tts>` element. For more information, refer to *MSML Interface Reference*.

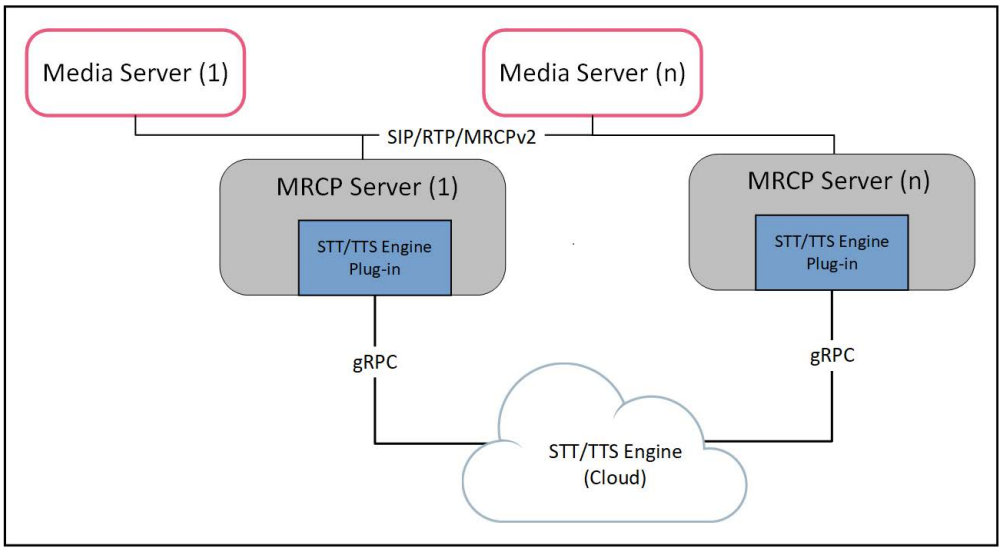
For information on configuring the **MRCP Server** and **Maximum Connection Time** through the Web GUI for TTS announcements, see *Configure MRCP on page 193*.

MRCP Server

Automatic Speech Recognition and Text-to-speech media resource capabilities are not natively present in the Decomposed Media Server. The Containerized Decomposed Media Server requires an external speech engine for these resources.

Media Resource Control Protocol (MRCP) server is the interfacing module between the Containerized Decomposed Media Server and the third party speech engine, which performs Speech-to-Text (STT) and Text-to-Speech (TTS) conversion. The MRCP server is a full-stack implementation, including SIP, SDP, MRCPv2, RTP, and RTCP stacks.

Figure 4. Containerized Decomposed Media Server - MRCP Server Networking



The MRCP server supports the following features.

- Integration with the third party speech engine
- English and Hindi language speech recognition
- English and Hindi language text-to-speech announcements

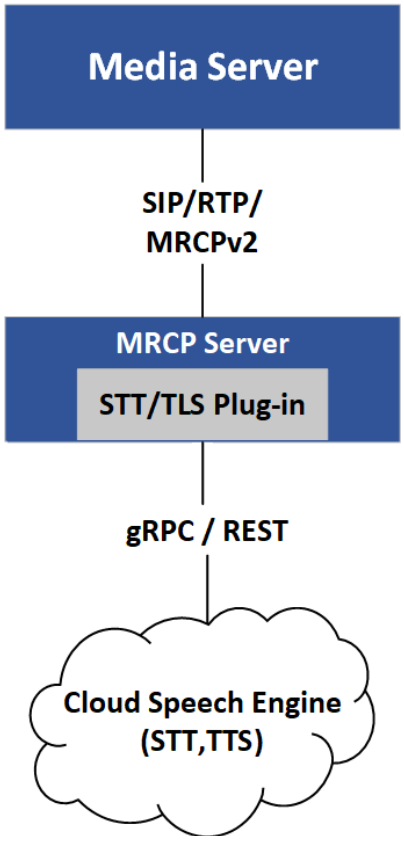
The operating system specification for the MRCP server is similar to the Containerized Decomposed Media Server. One instance of the MRCP server requires 5 vCPU, 4 GB RAM, and 30 GB hard disk.

Plug-ins

Speech recognition and TTS resources can be provided by integration with external Cloud Speech Engines. The Cloud Speech Engines provide SDK or interfaces that are required to be integrated in the MRCP server. This is called *plug-in* for a specific cloud speech resource provider. MRCP server has plug-ins for Google and Microsoft Azure. Additional plug-ins can be developed to integrate with external cloud or on-premise speech resource providers. Also, support for more languages can be extended based on the requirement.

Communication with external cloud engine is over a secured TLS connection.

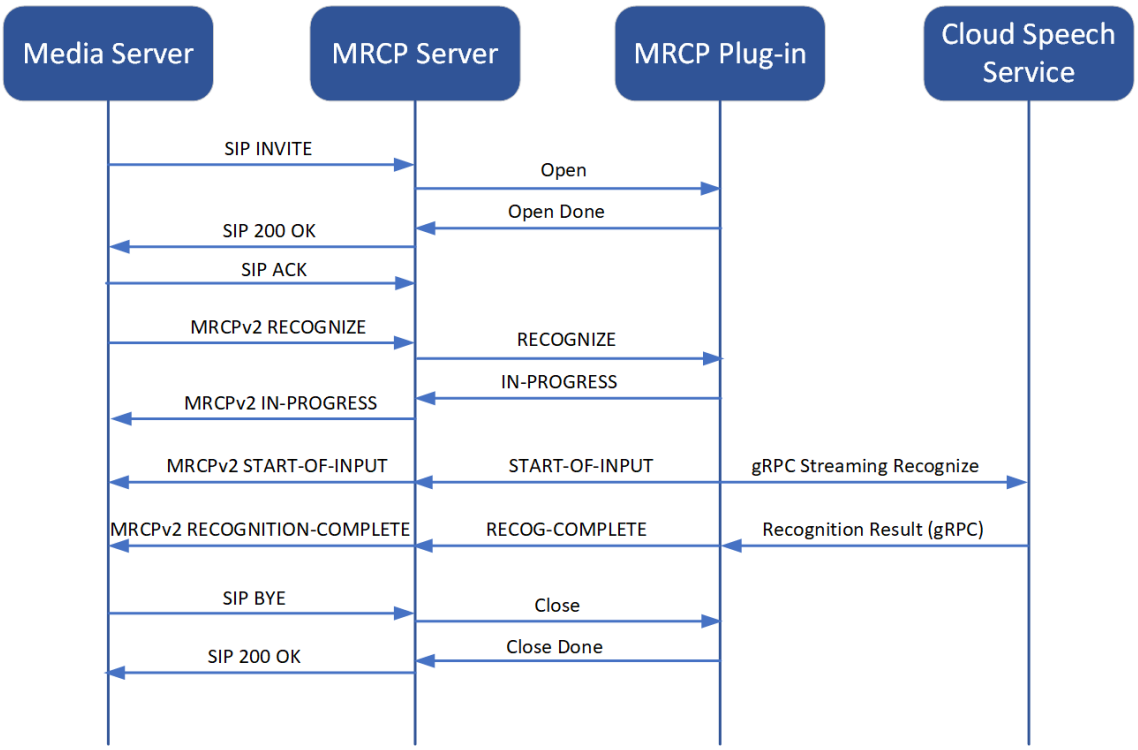
Figure 5. MRCP Server Plug-in



Speech Recognition

The Containerized Decomposed Media Server supports integration with the MRCP server using SIP or MRCPv2. The MRCPv2 is an open-source implementation of MRCP for speech recognition. The Containerized Decomposed Media Server-MRCP server interface is supported only using the PCM a/µ- law codec in RTP. If a port uses any other codec, the Containerized Decomposed Media Server transcodes to PCM a/µ-law.

Figure 6. Containerized Decomposed Media Server-MRCP Speech Recognition Call Flow

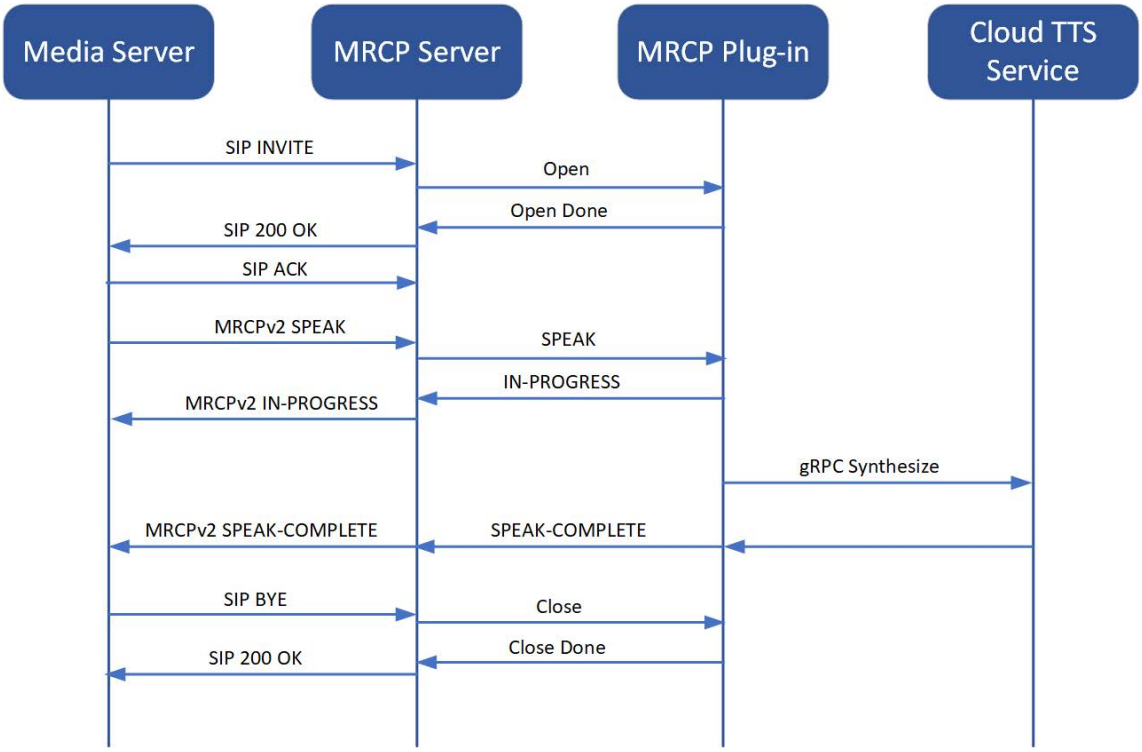


Text-to-Speech

The Containerized Decomposed Media Server supports Text-to-Speech (TTS) announcement to provide dynamic information that cannot be pre-recorded, such as account balance, card expiry date, location specific details, and so on, to the user. Variable text is synthesized into a voice clip with the help of an external TTS engine, and the synthesized clip is played to the user. Similar to pre-recorded clips, repeat playing, and barge-in based on speech and DTMF is also supported in TTS announcements.

The gender of the voice, language, and accent in which the announcement is played can be configured.

Figure 7. Containerized Decomposed Media Server-MRCP Text To Speech Call Flow

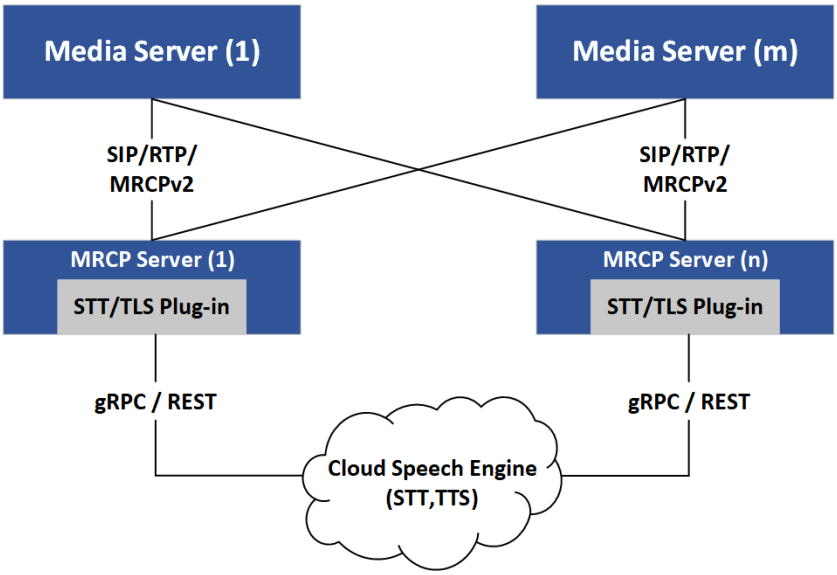


Load Balancing

The Containerized Decomposed Media Server supports multiple MRCP servers to provide High Availability (HA). Multiple Containerized Decomposed Media Server instances can have access to the same set of MRCP server instances. One Containerized Decomposed Media Server can manage a maximum of 40 MRCP servers. For each MRCP server, the number of concurrent STT and TTS resources are configured at the Containerized Decomposed Media Server.

The Containerized Decomposed Media Server acts as a load balancer for the MRCP servers and performs round-robin load distribution. The Containerized Decomposed Media Server keeps track of the availability of MRCP servers dynamically through the heartbeat mechanism. If one MRCP server goes down, the active calls of the serving server are impacted.

Figure 8. Containerized Decomposed Media Server-MRCP Load Balancing



Concurrent Play, Record, Speech, and DTMF Collection

The MSML group feature allows concurrent play, record, DTMF collection, and speech services in dialog. The `<group>` element allows parallel execution of `<play>`, `<record>`, `<speech>`, and `<dtmf>` elements. An audio clip (or a set, variable, or TTS clip) and a video clip can be played while concurrently recognizing speech using ASR, and collecting DTMF digits.

The Containerized Decomposed Media Server supports two concurrent audio only, video only, audio and video recordings, or any combination through the two `<record>` elements in the `<group>`. The attributes of each `<record>` element can be same or different except the `dest` and `id` attributes value, which is required to be unique between two `<record>` elements.

This feature reduces the number of SIP/MSML transactions and synchronizes concurrent execution for multiple MSML services. Without this feature, the control agent must initiate multiple MSML dialog instances concurrently and handle dialog events from each dialog instance independently.

The `<groupexit>` element allows events to be sent upon the termination of `<group>` element termination using either a `<send>` or `<exit>` element.

The `<group>` element does not support playing RTSP announcements.

Conferencing

Audio Conferencing

The Containerized Decomposed Media Server provides the following audio conferencing features.

N-Way Audio Mixing

A mix, or an interwork, is a collection of media sessions that are combined and redistributed in various ways, such as in a conference. The Containerized Decomposed Media Server supports standard N–1 mixing. (In N–1 mixing, conference participants does not hear themselves.)

SIP Netann conferences have a limit of 125 total participants, all of which can have send-receive media streams. For other control protocols, the Containerized Decomposed Media Server supports two-way to N-way conferencing, where n depends on the overall capacity of the Containerized Decomposed Media Server. The conference can be simple with no extra features, as in SIP Netann, or can employ any one of the features available in MSML or MSCML; such as moderation, announcements, and recording.

When large conferencing is not configured, up to 125 participants can have send-receive (that is, talk-listen) media streams; the remaining participants up to the total capacity of the Containerized Decomposed Media Server have receive-only connections.

Personalized Mixing

The Containerized Decomposed Media Server mixes audio streams so that in a conference each participant hears the same mix as the other participants. For example, in a conference with N-loudest enabled, all participants hear the loudest *N* speakers (although speakers do not hear themselves).

Personalized mixing allows each participant in a conference to select which other participants can contribute to the participant personal mix. For example, consider a conference with A, B, and C where A and B can hear everybody, but C can hear only B. The Containerized Decomposed Media Server allows the control agent to connect each participant to only the specified conference mixes. The control agent can also control whether the participant connection contributes to the conference or only listens.

This kind of mixing has many applications—for example, online gaming, call center coaching, and audio chat rooms.

Personalized mixing consumes considerable media-processing resources.

Play Audio Announcement in a Conference

When the Containerized Decomposed Media Server plays an announcement in a conference with full conference mix, so that all participants can listen to the announcement.

Unlike an audio announcement played to a conference participant, an announcement played to a conference cannot be barged by DTMF tones or voice activity detection. In all other respects, the Containerized Decomposed Media Server support for announcements played to conferences is identical to that for announcements played to a conference participant (that is, to a single port).

For more information, see *Play Audio Announcement to a Port on page 44*.

Record Audio Conference

Audio conference recordings are recordings of the full conference mix. These recordings are generally too long to be stored in the internal memory of the Containerized Decomposed Media Server and are usually streamed to an external, NFS, HTTP, or HTTPS server.

Like single-port audio recordings, audio conference recordings can be terminated by setting a maximum record time, or by having the control agent send an instruction to terminate the recording. Unlike single-port audio recordings, audio conference recordings cannot be terminated by in-band or out-of-band DTMF tones.

In MSML 1.1, multiple concurrent conference recordings, optionally with differing recording formats, are possible. For a connection, only one recording for connection audio or video is possible.

Mixing Filter

If the conference is large, mixing all the streams becomes increasingly expensive from a resource point of view.

Additionally, each participant in the conference carries some associated noise. The conference sums the audio from participating speakers together to create the conference mix; thus the background noise for the conference mix is the sum of noises of all participating speakers. In a large conference, the cumulative noise of the speakers becomes significant and can interfere with the intelligibility of the speakers. For example, increasing the number of participating speakers from two to four increases the noise by 6 dB (20log4 versus 20log2).

This feature filters the conference mix so that only the speakers with the greatest speaking energy (the N-loudest speakers) are heard by others.

The N-loudest sessions are determined by dynamically measuring the energy of each contending session. The specified number of sessions are then mixed and the resulting audio is distributed to all connected sessions. N-loudest mixing uses algorithms based on a time constant and hysteresis to ensure that brief speech pauses do not cause a currently contributing session to be switched out of the mix.

In MSML, N-loudest is configurable. In SIP RFC 4240 conferences, N-loudest is always 3. In MSML the hysteresis and time constant values are configurable.

The N-loudest speakers are considered the active speakers in the conference. The active speaker hear the N-loudest audio mix but without their own audio. If the active speaker notification is enabled, the N-loudest speaker is notified.

N-loudest behavior is slightly different in large conferences. When more than 125 talk-listen connections participate in the conference, the conference is internally cascaded. As a result, participants may hear up to N * *x* speakers, where N is the N-loudest value of the conference, and x is the number of internally cascaded conferences. In addition, it may be that the N * *x* speakers are not the absolute loudest speakers of the entire large conference.

Time Constant

The Containerized Decomposed Media Server determines which speakers are N-loudest by the measured energy of the speaker, averaged using a time constant. This time constant, which is configurable through the management interface, smooths the natural variation of energy generated in ordinary speech patterns.

For a large time constant.

- Energy measurements are smoother over time
- System is less responsive to changes in speaker activity

For a small time constant.

- System is more responsive to speaker activity
- System is more likely to switch between speakers because of natural variations in speech energy as well as when a new speaker becomes more active than an incumbent N-loudest

Hysteresis

Breaks and silences that occur naturally in speech, and measured as variations in energy, can cause frequent switching between active speakers, thus reducing the conference intelligibility. Because smoothing energies with only a time constant may not be sufficient, N-loudest is weighted (that is, biased) in favor of current (incumbent) active speakers by a hysteresis parameter.

Hysteresis applies a weighting factor to the energies of current active speakers. To become an active speaker, speaker energy must be greater than the last recorded energy of an incumbent active speaker multiplied by the configured hysteresis parameter. For example, for a hysteresis value of 10, the new speaker energy must exceed 10 times the last recorded energy of an active speaker.

This makes it more difficult for a non-active speaker to interrupt an active speaker, helping maintain a natural continuity in the conference. When hysteresis is configured appropriately for a conference, new speakers have to wait for a break in the conversation, or consciously speak loudly, to replace an active speaker.

Gain Control

The Containerized Decomposed Media Server can adjust audio gain (volume) inbound from individual conference participants and outbound to participants. The gain can be set low enough to effectively mute the audio input from a single participant, or to mute the audio output of the conference to all participants.

The control agent determines audio gain settings and directs the Containerized Decomposed Media Server to adjust gain accordingly. The Containerized Decomposed Media Server also has an automatic gain control (AGC) feature.

AGC is supported for conferences calls. When AGC is applied, the Containerized Decomposed Media Server automatically adjusts the level of a signal to a configured target level, optionally with a specified maximum amount of gain.

AGC can be applied in several scenarios as follows:

- For recording, you can set the recording level so that the speech coder optimally encodes the audio. In general, AGC must be applied to conference input rather than output.
- For conference input, the Containerized Decomposed Media Server equalizes all participant volumes to an even level, so that no one dominates the conversation and no one is too quiet.

In general, AGC should be applied to conference input rather than output. Applying AGC to conference input equalizes the speaker levels that the N-loudest algorithm acts on, which gives equal opportunity to loud and soft speakers. Also, AGC attempts to measure the background noise to determine when a user is speaking. The background noise on conference output can change rapidly, as various N-loudest users are switched in and out of the conference mix. This could mislead the AGC algorithm into falsely determining that a participant is speaking and applying AGC to the background noise.

AGC should never be applied to both conference input and output. The AGC equalization applied to input also affects conference output and therefore interferes with the decision-making ability of AGC on the output.

Active Speaker Notification

The Containerized Decomposed Media Server can send out reports about the active speakers in a conference. This feature is called active speaker notification (ASN) and is available to the Containerized Decomposed Media Server controlled by SIP or MSML. Notifications are sent when the speaker set changes, provided that a minimum reporting interval has elapsed.

The number of speakers considered active (and therefore reported) is determined by the value configured for *N* in the N-loudest feature. The *m* loudest speakers are reported in the active speaker list. In MSML, *m* is not configurable. Instead, in MSML the Containerized Decomposed Media Server automatically sets *m* equal to N, the value specified for the N-loudest speaker feature, so that the N-loudest speakers are also reported in the active speaker list.

NOTE: A change in the order of active speakers does not count as a change in the set of active speakers.

The reporting interval can be dynamically changed at any time. With ASN, you can specify a minimum threshold for a speaker to be considered actively talking.

N-loudest behavior is different in large talk-listen conferences. When more than 125 talk-listen connections participate in the conference, the conference is internally cascaded. The Containerized Decomposed Media Server combines the active speaker list from each cascaded conference and sends an aggregate ordered ASN report to the control agent.

The active speakers in the ASN report are ordered by input position for the aggregate large conference. This means that the number of speakers contained in the ASN report is greater than N for MSML. Where, N controls the number of N-loudest speakers in the conference and *m* controls the number of speakers in the ASN report for a cascaded conference.

Active Speaker Threshold

At any given time, some conference participants may be silent except for background noise. If background noise is sufficiently loud, or if the conference is sufficiently small, a silent participant could become one of the reported N-loudest speakers. You can help prevent this by setting an active speaker threshold.

The goal for setting the active speaker threshold is to ensure that all participating talk-listen participants reach the threshold while excluding background noise. The higher the active speaker threshold is set, the more likely a talk-listen participant is to be excluded from the report when they are not speaking. The lower it is set, the more likely that background noise could be reported on the active speaker participant list.

In practice, there is a substantial gap between the dBm0 levels of background noise and speech, so setting this threshold to a reasonable value still includes talk-listen participants who are truly participating, though quietly. In this case, the participant audio is added to the conference mix. You can prevent the speaker from being reported in ASN reports by configuring an active speaker threshold. If the audio energy of the participant falls below this threshold, the speaker is not reported in ASN reports even if the audio is added to the conference mix. This helps prevent a speaker from being reported unless the speaker is participating in the conference.

By default, the threshold value for active speakers is set to –96dB (silence, or none). This means that any background noise detected by the system causes even a speaker not actively participating to be included in the ASN report.

The optimal values for active speaker threshold are application-specific. As a guideline, the nominal volume for speech is generally considered to be around –20 dBm0. This means that a threshold between –40 and –70 dBm0 is reasonable. It is strongly discouraged to set the threshold to a value closer to 0 dBm0 because this gives indeterminate results.

NOTE: This threshold does not determine which speakers are included in the conference mix.

Full Mix Notification

The N-loudest filters a conference mix so that only the speakers with the greatest speaking energy (the N-loudest speakers) are heard by others. The Containerized Decomposed Media Server can send out notifications of the number of times the mix of active speakers becomes full for conferences with more than N-loudest participants.

When full-mix notification is enabled for a conference, the Containerized Decomposed Media Server counts the number of times all the allowed active speakers (N-loudest) exceed a configurable energy threshold. This can be used as an indication that the number of speakers heard in a conference mix, each of whom speaks with enough volume to be considered loud, has reached the maximum level at which the mixed output is still deemed intelligible. Additionally, the notification provides the cumulative duration for which the mix was full as well as the ongoing or total duration of the conference.

Full-mix notification is supported in MSML only. The reporting interval, as well as the threshold, are configurable (similar to ASN).

Narrowband, Wideband, and Super Wideband Audio Conference

The default audio conference sample rate is narrowband. Containerized Decomposed Media Server supports specifying the sample rates for the conferences, either narrowband (8 kHz), wideband (16 kHz), super wideband (32 kHz), or auto to enable the large-conferencing feature. By default, Containerized Decomposed Media Server uses a sample rate of 8 kHz. For higher quality audio, the conference must be wideband or super wideband and at least two of the participants must use codecs such as G.722, EVS, AMR-WB and EVC. Conference capacity is correspondingly lower for wideband codecs.

You can enable conferencing by setting a parameter through the Containerized Decomposed Media Server management interface or specifying it in the SIP Request-URI when the conference is created. The conference sample rate of an MSML conference can be set through the protocol at the time the conference is created. If no setting is specified through the protocol, the configured setting is used.

The Containerized Decomposed Media Server supports conferencing for all narrowband, wideband, and super wideband codecs. The sample rate conversion is applied as necessary, if the codec bandwidth does not match the conference bandwidth. The Containerized Decomposed Media Server supports playing announcements and recording of wideband conferences using narrowband or wideband codecs. The Containerized Decomposed Media Server supports recording wideband conferences and ports using narrowband G.711, G.722, EVC, EVRC, EVRCB, EVRCNW, and AMR.

- Narrowband ports can join a wideband conference, in which case the narrowband ports are set to the higher sample rate. This does not change the quality of the narrowband ports.
- G.722 and AMR-WB ports can also join a narrowband conference, in which case they are set to the lower sample rate. When this occurs, the bandwidth is lowered.

After one port has joined a conference, the conference sample rate cannot be changed from narrowband to wideband or wideband to narrowband.

Dynamic Sample Rate

The Containerized Decomposed Media Server allows configuring narrowband (8 kHz), wideband (16 kHz), super wideband (32 kHz), or auto sample rates for audio conference. The conference can be done through management interface or protocol signaling. If sample rate is configured as narrowband, wideband, or super wideband, the audio mixer sample rate cannot be modified throughout the conference. In auto sample rate, the Containerized Decomposed Media Server automatically sets the audio mixer sample rate based on the sample rate of the participants joining the conference.

The Containerized Decomposed Media Server dynamically upgrades or downgrades the audio mixer sample rate on each port that joins or unjoins the mixer. The Containerized Decomposed Media Server dynamically sets the conference mixer sample to the highest sample rate used by at least two senders and two receivers.

Following is an illustrative example to explain how the Containerized Decomposed Media Server upgrades the audio mixer sample rate when the participants join the conference with different sample rates in send and receive modes.

Port	Sample Rate	Audio Mixer Sample Rate	Description
Participant 1	8 kHz	8 kHz	The audio mixer sample rate is set to 8 kHz.
Participant 2	16 kHz	8 kHz	The audio mixer sample rate is not modified as there is only one 16 kHz port.
Participant 3	32 kHz	16 kHz	The audio mixer sample rate is set to 16 kHz as there is only one port with 32 kHz.
Participant 4	16 kHz	16 kHz	The audio mixer sample rate remains at 16 kHz.
Participant 5	32 kHz	32 kHz	The audio mixer sample rate is upgraded to 32kHz as there are two 32 kHz ports.

The Containerized Decomposed Media Server supports dynamic upgrade or downgrade of audio mixer sample rate in large conference (involving more than one mixer) and cascaded conferences. Inter conference links are considered for deciding the conference sample rate in cascaded and large conferences.

NOTE: If the sample rate is not specified in SIP request URI or in MSML, the Containerized Decomposed Media Server uses the default sample rate configured in the management interface.

Whisper Conference

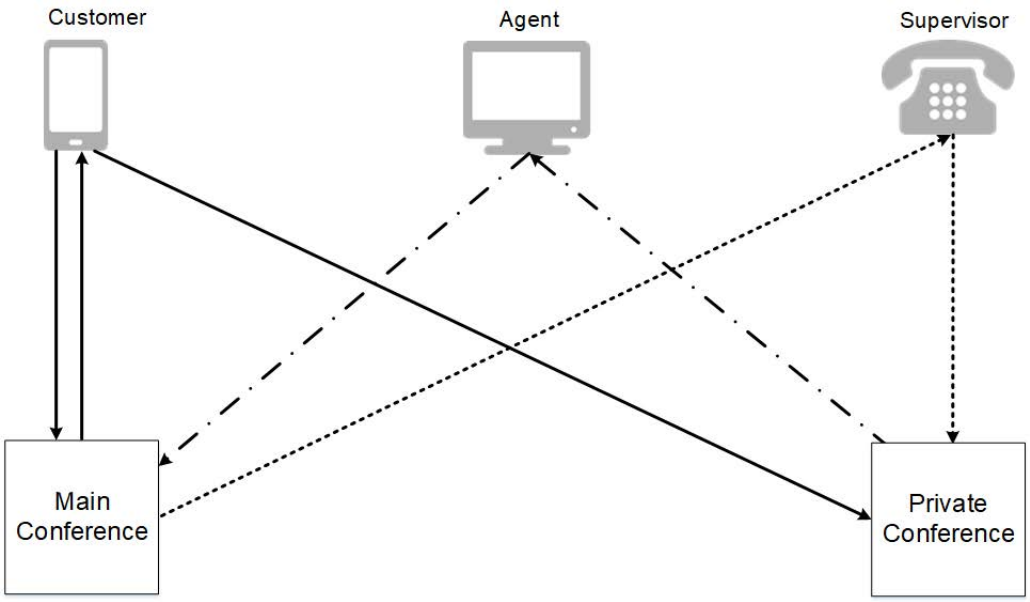
The Containerized Decomposed Media Server supports whisper conference, which enables creation of personalized mixer for three-participant audio conference through the MSCML `<configure_team>` element. Whisper conference supports silent monitoring and coaching of the participants.

The Containerized Decomposed Media Server deletes the personalized mixer when the conference terminates.

The following example describes a use case where a personalized mix is created to allow one participant to coach another participant (whisper conference) in a three member conference.

The agent interacts with the customer and receives instructions from the supervisor. The supervisor audio is fed into the personalized mix through which the agent receives the instructions. The customer interacts with the agent but cannot listen to the supervisor, however the supervisor can listen to both the agent and the customer.

Figure 9. Whisper Conference



The following section describes the call-flow to enable whisper conference on the Containerized Decomposed Media Server.

1. The supervisor joins the conference in a private mode.
2. The agent joins the conference and creates a team with supervisor as a member for the personalized mix.
3. The customer joins the conference.

Figure 9 shows the whisper conference topology after all participants have joined.

Video Conferencing

The two commonly used types of video conferencing are Voice Activated Switching (VAS), where a single video stream is shown at one time, and Continuous Presence (CP), where several video streams are shown at once on a split screen. Each type of conferencing has distinct optional features that enrich user experience.

This section describes the following video conferencing features.

VAS Video Conference

For VAS conferencing, a single participant is seen on the screen at any time. The video image switches based on who is currently speaking. But the current speaker sees the previous speaker on the screen. Video is routed from the current speaker to all the other participants. The speaker sees self or the previous speaker, based on application control. H.264 Mode 0 and Mode 1, H.265,and VP8 are the video codecs supported in a VAS conference. VAS conferencing is ideally suited for use with small-display 3G mobile phones and in cost-sensitive residential video phone applications.

A maximum of 16 participants can concurrently send-receive video streams and up to 125 participants can send-receive audio streams, as in audio conferences. VAS conferences use the system resources efficiently that enable the Containerized Decomposed Media Server to support higher capacities because video does not require encoding or decoding. VAS conferencing is suitable for smaller screens (such as mobile devices) as only one user video is displayed at a time.

Also in audio conferences, the number of participants who receive the audio mix is limited only by the overall capacity of the Containerized Decomposed Media Server. An audio-only participant can also join a VAS video conference. Although the participant neither sees nor sends video, the audio from the connection is added to the audio portion of the conference mix audio. VAS audio is encoded and decoded.

In a VAS conference, the Containerized Decomposed Media Server must receive an I-frame whenever it switches the video source. While switching the video source, the Containerized Decomposed Media Server requests the I-frame from the terminal using a Fast Update Request. I-frames are generally transmitted by terminals at regular intervals.

The Containerized Decomposed Media Server supports.

- Constrained Baseline Profile Levels 1, 1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1 for H.264 Mode 0 and Mode 1
- Main Profile Levels 1, 2, 2.1, 3, and 3.1 for H.265
- VP8 picture size QCIF, 180p, CIF, 360p, 480p (640x480 and 720x480), 720p
- Landscape and portrait orientation

H.323 networks support Fast Update Requests; however, SIP-based networks do not uniformly implement any one Fast Update Request mechanism. For SIP networks, the Containerized Decomposed Media Server supports two methods of Fast Update Requests: the Video Picture Fast Update Message mechanism defined in draft-levin-mmusic-xml-media-control, and the Full INTRA-frame Request (FIR) packet in RTP defined in RFC 2032. For VAS conferencing, the video terminal being used must support one of these methods of I-Frame requests.

An audio-only participant can also join a VAS video conference. Although the participant neither sees nor sends video, the audio from the connection is added to the audio portion of the conference mix audio. VAS audio is encoded and decoded.

N-Loudest functionality and active speaker notification are available for the audio portion of a VAS video conference.

Transcode Bypass VAS

Video codecs used in VAS conferences are not transcoded or rate-matched. Consequently, all parameters of the video stream (codec, bit rate, picture size, profile level, and minimum picture interval) must match for all the participants. Similarly, the video parameters of an announcement to a VAS conference must match those of the conference.

N-Loudest functionality and active speaker notification are available for the audio portion of a VAS video conference.

The Containerized Decomposed Media Server supports playing a multimedia announcement to a VAS conference that has an equal or lower bitrate, frame rate, and picture size than the multimedia announcement. In a VAS conference, there is some tolerance in the bandwidth comparison so that calls requesting to join the conference are not rejected for small bandwidth differences.

For example, if the bandwidth difference between port and conference is not larger than {[(video bitrate of source OR sink/64)*10]+8 kbps}, the Containerized Decomposed Media Server considers the bandwidths to be matched.

NOTE: Port video parameters must match the parameters of a VAS conference, that is, they must be identical with the exception of bandwidth (tolerance is allowed).

VAS conferences use the system resources efficiently that enable the Containerized Decomposed Media Server to support higher capacities because video does not require encoding or decoding. VAS conferencing is suitable for smaller screens (such as mobile devices) as only one user video is displayed at a time.

Transcoded VAS

When VAS transcoding is enabled through the management interface, the Containerized Decomposed Media Server performs transcoding, as required, to permit video ports with any supported codec parameters to join a VAS conference. The VAS conference announcements are supported for any video codec or parameters, and are transcoded at the conference output similar to the conference ports. The Containerized Decomposed Media Server supports VAS conference with transcoding for MSCML, MSML, and netann VAS conferences.

The existing MSML VAS conference codec parameters are ignored by the Containerized Decomposed Media Server. For netann and MSCML VAS conference, the video parameters of the first port are no longer used to restrict the codec parameters of the subsequent ports. When sending the subsequent offers for a VAS conference port (MSCML or netann), the Containerized Decomposed Media Server includes the full codec list configured in the management interface.

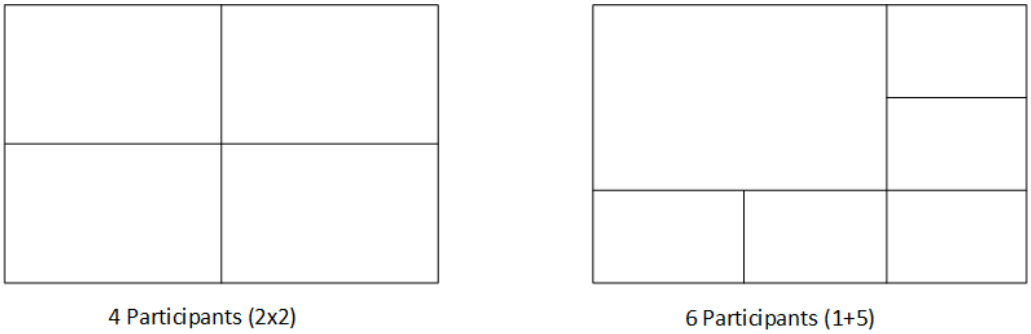
The Containerized Decomposed Media Server supports encoder sharing for transcoded VAS conferences similar to CP conference encoder sharing.

In transcoded VAS conferences, the Containerized Decomposed Media Server does not support the TMMBR, CVO, recording, RTSP streaming, and asymmetric H.264 decoding features. The mid-call video codec changes for transcoded VAS conferences are not allowed.

Continuous Presence Conference

Continuous Presence Video (CPV) conferencing continuously displays selected users on a single screen. The screen is generally split, with conference participants displayed concurrently on one screen in a multi-pane layout.

Figure 10. Quad-split and Six-split in Landscape Orientation



The Containerized Decomposed Media Server supports continuous presence conferences for the video codecs in a 2-by-2 quad-split layout, a 1+5 six-split layout, with one pane on 4/9ths of the screen, and five panes on 1/9th each, auto-split, and dynamic-hangout.

In dynamic video or auto-split layout, the Containerized Decomposed Media Server dynamically divides the root window into small regions based on the number of participants in the conference and displays the participants in those regions. As more participants join the conference, the number of regions is incremented and similarly when participants leave the conference, the number of regions is decremented.

The Containerized Decomposed Media Server supports a maximum of six participants in dynamic video layout.

Figure 11 shows the auto-split video layout for CPV conference in portrait and landscape orientation when the **Split Method In Auto Split CPV** is set to **Method1** in the *Configure Video* Web GUI page. In **Method1**, the Containerized Decomposed Media Server splits the screen vertically in portrait orientation. Similarly, the Containerized Decomposed Media Server splits the screen horizontally in landscape orientation.

Figure 11. Auto-Split Video Layout in CPV Conference—Split Method1

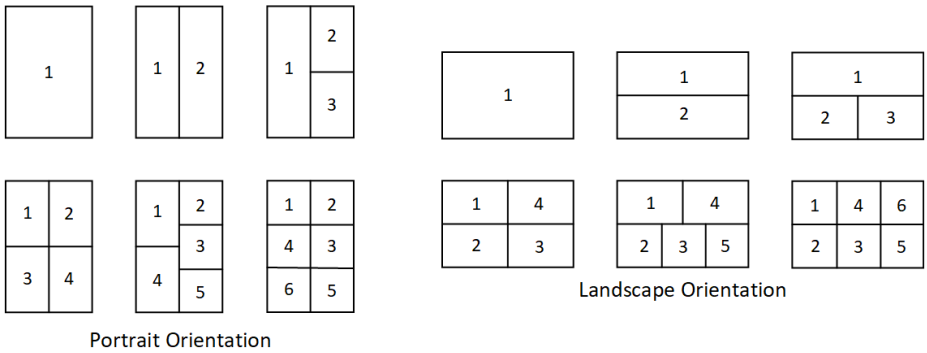
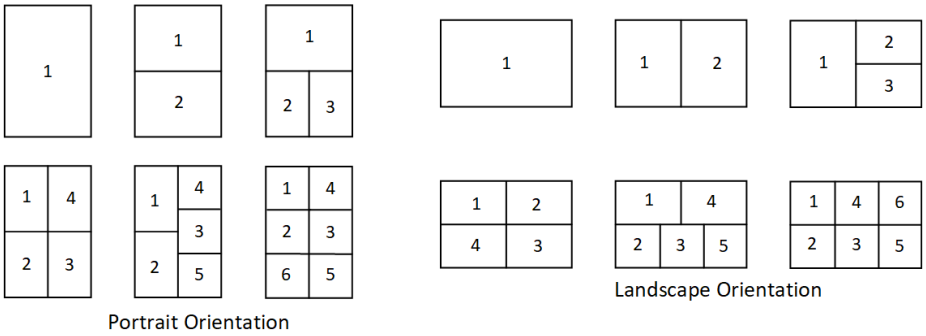


Figure 12 shows the auto-split video layout for CPV conference in portrait and landscape orientation when the **Split Method In Auto Split CPV** is set to **Method2** in the *Configure Video* Web GUI page. In **Method2**, the Containerized Decomposed Media Server splits the screen horizontally in portrait orientation. Similarly, the Containerized Decomposed Media Server splits the screen vertically in landscape orientation.

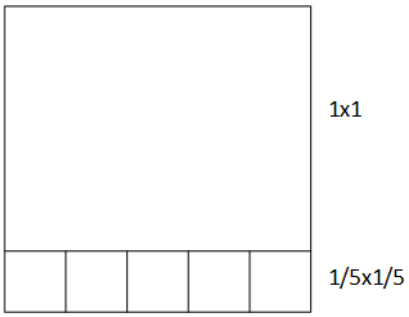
Figure 12. Auto-Split Video Layout in CPV Conference—Split Method2



When new participants join or un-join the conference, the Containerized Decomposed Media Server increases or decreases the number of regions by splitting the video layout and adjusting the region sizes dynamically. To create an auto-split CP conference using MSML, refer to *MSML Application Guide* and for information on **cvd:format** attribute, refer to *MSML Interface Reference*. For information about configuring the **Split Method In Auto Split CPV**, see *Configure Video on page 254*.

In dynamic-hangout video layout, when the first participant joins the conference, the root region is occupied by the participant. As and when the other participants join the conference, the participants are overlaid at the bottom of the root region. Figure 13 shows a sample dynamic hangout video layout in landscape orientation with six participants.

Figure 13. Dynamic-Hangout Video Layout



The Containerized Decomposed Media Server supports both landscape and portrait orientation for QCIF, CIF, 4CIF, 720p, QVGA, and VGA CP conference root picture size. An **orientation** attribute in the MSML `<root>` element specifies the orientation for CP conferencing only. The Containerized Decomposed Media Server does not support the portrait orientation picture size when playing the transcoded port announcements with an icon or text overlay.

NOTE: After the conference is created, the Containerized Decomposed Media Server does not support changing the orientation of a conference.

The Containerized Decomposed Media Server supports the CPV mixer in MSCML (advanced) conference based on the management interface configuration. The CPV mixer layout information is derived from the pre-defined layout and user-defined layout templates in the management interface.

The Containerized Decomposed Media Server supports a total of 19 pre-defined layout templates and each pre-defined layout template is identified by using a keyword.

The user-defined layout templates are based on the Synchronized Multimedia Integration Language (SMIL) and is stored in *.smil* files. The *.smil* files are provisioned through the management interface. During initialization, the Containerized Decomposed Media Server parses the SMIL files configured in the **CPV layout template** table. If any error occurs during the paring, the alarm *A configured template type value on slot X is either not found or is syntactically invalid* (alarm 179) is raised. The SMIL markup language is written in XML and is used to describe the layout and behavior of a multimedia presentation on a screen.

The Containerized Decomposed Media Server supports a maximum of six contributing video participants in the CPV conference and six layout template configuration using the management interface. When a participant joins or leaves the conference, the Containerized Decomposed Media Server determines the number of contributing participants in the video mixer and renders the corresponding CPV layout template configured in the management interface. For more information on pre-defined and user defined layout templates, refer to the *Radisys MSCML Interface Reference*.

Video announcements are scaled before being played to the conference—the announcement may use the entire screen area or just one pane of the split display. In CP conferences the Containerized Decomposed Media Server acts as a multipoint conferencing unit offering a suite of video services such as video announcement streaming, video recording, and video conferencing.

In VAS conference, if terminal requests for an I-frame, the Containerized Decomposed Media Server needs to fetch it from the source video terminal, because VAS conference is transcode-free.

In CP conferences, video is encoded by the Containerized Decomposed Media Server video encoder; consequently the Containerized Decomposed Media Server maintains a complete representation of the picture in memory. For this reason, the Containerized Decomposed Media Server does not require I-Frames from the video terminal as it does in VAS conferences and when making video recordings.

The Containerized Decomposed Media Server supports bitrate tolerance, when the connected ports to CPV conferences use encoder sharing. Ports with similar bitrates can share the same encoder with the bitrate set to the minimum of the ports that are sharing. The Containerized Decomposed Media Server provides a provision to the AS to decide whether the CPV conference participants require an encoder sharing. The encoder sharing is disabled if the mid-call CPV feature is enabled.

For information on configuring encoder sharing, see *Configure Video on page 254* and *SNMP Interface Reference*.

Also, unlike a VAS conference, video used in continuous presence conferences is transcoded and rate-matched. The picture size of a continuous presence conference can be as follows:

- QCIF, CIF, 4CIF (704x576), 720p (1280x720), QVGA (320x240), and VGA (640x480) for quad-split
- CIF, 4CIF, 720p, QVGA, and VGA for six-split
- QCIF, CIF, 4CIF, 720p, QVGA, and VGA for auto-split
- CIF, 4CIF, 720p, and VGA for dynamic-hangout

  NOTE: For 720p root picture size in dynamic-hangout, the Containerized Decomposed Media Server has a limitation on the number of HC participants less than or equal to three.

The participant picture size input (video) is automatically scaled to fit the conference. The OAMP scaling mode to crop or letterbox is used, if the aspect ratio of the incoming video stream is different from that of the root picture size. Conference output is also scaled to match the participant picture size. The profile level, bit rate and Minimum Picture Interval (MPI) of each user can also differ, and the video parameters of an announcement to a continuous presence conference need not match to those of the conference. The Containerized Decomposed Media Server supports the new VGA and QVGA pictures sizes when playing transcoded port announcements with icon or text overlay.

NOTE: VGA and QVGA have an aspect ratio of 4:3; QCIF, CIF, and 4CIF have an aspect ratio of 11:9; and 720p has an aspect ratio of 16:9.

When the participants have same codec and codec parameters, the encoder is shared among the participants. Simultaneously, if the participants have different codec and codec parameters, the Containerized Decomposed Media Server must create a distinct encoder for each participant. As video encoders consume excessive processing resources, it is most efficient to ensure that the video parameters of the conference, participants, and announcements match.

Continuous presence conferences provide a richer user experience than VAS conferences. On the whole, they are better suited to environments with larger screens such as desktop environments or broadband mobile networks.

N-Loudest functionality and active speaker notification are available for the audio portion of a continuous presence video conference, just as they are for an audio conference.

Switching between quad-split and six-split conferences is supported. Video from six-split regions 5 and 6 is dropped when switching from six-split to quad-split.

The Containerized Decomposed Media Server supports.

- Constrained Baseline Profile Levels 1, 1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1 for H.264 Mode 0 and Mode 1
- VP8 picture size QCIF, 180p, CIF, 360p, 480p (640x480 and 720x480), 720p

In a CPV conference, if the port orientation does not match the video mixer orientation, it results in cropping or letter-boxing at the terminal. This can be avoided, if port terminal always receives video from a video mixer, which has the same orientation.

When multi-mixer feature is enabled, the Containerized Decomposed Media Server creates two video mixers internally, portrait and landscape. If any port joins the conference with a different orientation than that of the original mixer, the Containerized Decomposed Media Server creates a new video mixer with matching orientation. For example, if the port joins the conference with a portrait orientation and the mixer is landscape, the Containerized Decomposed Media Server creates a video mixer with portrait orientation.

The multi-mixer feature is enabled through management interface and MSML configuration. The Containerized Decomposed Media Server supports multi-mixer feature in a CPV conference only.

The Containerized Decomposed Media Server internally creates a second CPV video mixer based on the joining ports orientation. The Containerized Decomposed Media Server supports multi-mixer CPV conference in quad-split, six-split, auto-split, and dynamic-hangout video layouts with all supported root sizes. The Containerized Decomposed Media Server supports all existing CP conference features like active or passive borders, background color, ASL, announcement, recording, and `deletewhen` attribute on multi-mixer CPV conference.

For information on the how to create an multi-mixer CP conference using MSML, refer to *MSML Application Guide* and for information on **multimixer** attribute, refer to *MSML Interface Reference*.

Play Video Announcement to Conference

The Containerized Decomposed Media Server supports playing video announcements for VAS or continuous presence video conference or to particular user port connected to a conference. In Continuous Presence Video Conference, video announcements are supported to full screen in a multi-pane layout or to a particular pane in a multi-pane layout. When required, video announcements are scaled before being played to the conference. The announcement may use the entire screen area or just one pane of the split display.

NOTE: In auto-split CPV conference, announcements are played only to the root region; region specific announcements are not supported.

The Containerized Decomposed Media Server support for playing video announcements to conferences is similar to that for playing video announcements to a port, as described in *Play Video Announcement to a Port on page 44*, with the following differences:

- Announcements to a conference cannot be barged, even when the announcement includes audio.
- Text and icon can be overlaid, as described in *Text and Icon Overlay for Video Announcements on page 48* only on announcements played to a port.
- Only announcements played to continuous presence conferences or a participant in such a conference can be transcoded for mismatching picture size, bit rate, and MPI.

In the multi-mixer feature, changes to the MSML interface are not required while playing an announcement to a CPV conference. However, for a video announcement, the Containerized Decomposed Media Server plays the announcement for the same region of both the video mixers simultaneously.

Record Video Conference

The Containerized Decomposed Media Server support conference video recording for both VAS and Continuous Presence Video Conference or from a particular user port connected to a conference. In VAS conference recording, the Containerized Decomposed Media Server must receive an I-Frame whenever it starts to record a multimedia file. In this case, the Containerized Decomposed Media Server requests the I-Frame from the terminal using a Fast Update Request.

NOTE: An I-Frame is a special video frame that contains entire, complete, and self-contained video data.

For information on different methods of requesting the I-Frame, refer *SIP Interface Reference*.

In general, the Containerized Decomposed Media Server support for recording video and multimedia conferences is the same as that for recording single-port video. However, video conference recordings are generally too long to be stored in the Containerized Decomposed Media Server internal memory; instead, they are usually streamed to an external NFS, HTTP, or HTTPS servers. The Containerized Decomposed Media Server must receive an I-Frame whenever it starts to record a multimedia file. I-Frames are generally transmitted regularly by terminals at an interval between several seconds and 30 seconds; however in some cases encoders only send an I-Frame at the beginning of a connection. In this case, the Containerized Decomposed Media Server requests the I-Frame from the terminal using a Fast Update Request.

H.323 networks support Fast Update Requests; however, SIP-based networks do not uniformly implement any one Fast Update Request mechanism. For SIP networks, the Containerized Decomposed Media Server supports the Video Picture Fast Update message mechanism defined in draft-levin-mmusic-xml-media-control, and the Full INTRA-frame Request (FIR) packet in RTCP defined in RFC 2032.

In MSML 1.1, multiple concurrent conference recordings, optionally with differing recording formats, are possible. (For a connection, only one recording per connection audio and/or video can be made.)

In a CPV multi-mixer conference video recording, the Containerized Decomposed Media Server always records from the mixer created by the AS.

VAS Conference Floor Control

The conference floor control feature enables the application server to force a specific participant’s image to be shown in a VAS conference (for example, the conference chair) to be the exclusive video source for the conference. The source of video is fixed to one participant, but the source for audio is not. The audio mix is generated in the same way as in other conferences.

Any participant in the VAS conference can be granted the floor control, as long as the participant has an input video stream to the conference. This exclusive video stream is known as the override video stream. This feature is well-suited for lecture-type scenarios, where it is inappropriate for other conference attendees to engage in dialog or speak at any time (as they can in uncontrolled VAS conferences). It can also be used in scenarios where it is important that the principal speaker is not unintentionally switched out of the mix because of applause, coughing, or other audio input.

The override video stream can be changed at any time during a conference. If the conference has no override video stream, it reverts to original VAS mode.

Floor control can be enabled or disabled at any time during a conference. This feature is supported in H.264 (mode 0 and mode 1), H.265, and VP8 VAS conferences.

Voice Activated Border

In continuous presence conferences, the Containerized Decomposed Media Server highlights the region displaying the loudest speaker's video by surrounding it with a different border. Each region in the video layout is surrounded by an active or passive border, which can differ in color and width. When enabled, the voice activated border (VAB) automatically sets the border of the loudest speaker to active, thereby visually distinguishing one region from all others to call attention to the largest speaker's video.

The VAB feature is automatically turned on for continuous presence conferences that have an audio mixer and the active border is enabled.

All speakers in the conference's audio mixer are considered even if speakers do not have a video presence. If the loudest speaker does not have a video displayed, no border is active.

The Containerized Decomposed Media Server supports this feature with a configurable switching interval and threshold, which is similar to the ASN feature.

Active Speaker in Largest Video Tile

The Containerized Decomposed Media Server supports the ASL feature in a six-split CPV conference only. In a CPV conference, when Active Speaker in the Largest Video Tile (ASL) feature is enabled, the Containerized Decomposed Media Server promotes the active speaker to the largest video tile (region1) and moves the region 1 participant to the current active speaker region.

During the conference, if other user becomes active speaker, the previous active speaker is moved to its parent region and the new active speaker is promoted to the region 1. The original participant who was there in region 1 initially is moved to the current active speaker parent region. The Containerized Decomposed Media Server does not change the display region IDs associated with the participants while switching the active speaker to the largest video tile.

The Containerized Decomposed Media Server disables ASL automatically if a six-split conference is modified to quad-split conference. The Containerized Decomposed Media Server retains the active participants with display 1 to 4 and drops the other two participants with display 5 and 6, irrespective of the current displaying region. The Containerized Decomposed Media Server displays the participants in their original regions as specified by AS.

The Containerized Decomposed Media Server switches the next active speaker to the largest video tile, if the current user in the largest video tile is disconnected from the conference or becomes a view-only participant. If there is no next loudest participant, the Containerized Decomposed Media Server randomly picks a participant and moves that participant to the largest video tile.

The Containerized Decomposed Media Server rejects the join command if a new user tries to join with the display ID of an existing participant, even if the region ID is empty because the active speaker was switched into the largest video tile. The Containerized Decomposed Media Server rejects the request, if both VAB and ASL are enabled at same time.

For more information, refer to *MSML Interface Reference* and *MSML Application Guide*.

Video Lipsync

Lipsync is defined as the delay between the audio and video signals. Lipsync error can occur at the terminal, during transmission, and within the Containerized Decomposed Media Server itself. Lipsync error can occur on the input path to the Containerized Decomposed Media Server as well as the output path. The Containerized Decomposed Media Server addresses lipsync error on the input side (except within the terminal). Lipsync error in the Containerized Decomposed Media Server is due to the differences in the audio and video jitter buffer delay. Lipsync error on the Containerized Decomposed Media Server input side is avoided by linking the audio and video jitter buffers such that they maintain the same delay as configured.

Lipsync error during the transmission path can occur because the audio and video streams may be configured with different QOS priorities. The Containerized Decomposed Media Server addresses lipsync error during transmission by adjusting either the audio or the video jitter delay to match the transmission delay. Transmission delay is computed using theRTP timestamps received in the respective audio and video RTCP Sender Report packets.

Coordination of Video Orientation

The Containerized Decomposed Media Server supports Coordination of Video Orientation (CVO) feature, which allows an endpoint or end device to indicate that the outgoing video stream is flipped, rotated, or both, and requires correction before being displayed.

For example, in a scenario where you rotate the camera and the terminal can detect but does not correct the rotation from the output. The terminal, in this scenario, indicates the Containerized Decomposed Media Server to correct the rotation.

CVO is codec independent and supported for all video codecs. In Containerized Decomposed Media Server, CVO supports 2-bit resolution as per the IR.94 and 3GPP TS 26.114 specifications. The Containerized Decomposed Media Server ignores 6-bit CVO. The Containerized Decomposed Media Server supports CVO for video ports using RTP transmission protocol and IPv4 or IPv6 internet protocol.

For information about configuring CVO ID, see *Configure Video on page 254*.

For more information on the CVO attribute, refer to *SIP Interface Reference*.

HC Video

High Complexity (HC) video provides a higher clarity video. CP conference, HC VAS, play/record, and port-to-port transcoding support HC video.

This section describes the Containerized Decomposed Media Server HC video features.

HC Ports

The Containerized Decomposed Media Server supports the H.264 (mode 0 and mode 1) codec negotiations using the Session Description Protocol (SDP) at the Constrained baseline profile levels of up to 3.1 and VP8 codec up to 720p. HC video supports profile levels 2.1, 2.2, 3, and 3.1 for H.264 (Mode 0 and Mode 1) with a maximum bandwidth of 4000 kbps and maximum of 720p resolution for VP8 with a maximum bandwidth of 2000 kbps. Selecting any of these profile levels enables the HC video on an HC port. HC video encodes and decodes the frame rate of up to 30 fps or the maximum supported by the negotiated level, whichever is lower.

When an HC port is in the session, you can modify any of the following SDP parameters:

- Video bandwidth
- Destination IP and port
- Payload
- Video picture size

If there is a difference in the image format, you can downscale and upscale the formats based on the levels. Depending on the configuration, when wider screen users are displayed in a narrow screen conference, letter boxing or scaling occurs, and the reverse is also true. For example: 720p is widescreen 16:9 and QCIF, CIF, and 4CIF are narrow screen 11:9.

For information on mid-call codec changes on HC port, refer to *Mid-Call Changes on Video Port on page 620*

HC VAS Conference

HC VAS conference is based on profile levels. Selecting a profile level 2.1 or greater for a conference enables HC video.

The bandwidth for VP8 and H.264 Mode 0 and Mode 1 is configurable using MSML 1.1. The bandwidth of all the conference in VAS must match the configured conference bandwidth (tolerance is allowed).

For more information, see *VAS Video Conference on page 75*.

HC Text and Icon Overlay

The Containerized Decomposed Media Server supports text and icon overlay with HC H.264 and VP8 ports.

For more information, see *Text and Icon Overlay for Video Announcements on page 48*.

HC Announcements and Recording

HC announcements and recording are supported for the 3GP, 3G2, MP4, and QuickTime multimedia files on the VP8 and H.264 ports.

The Containerized Decomposed Media Server supports transcoding of video port announcements when the video announcement profile level, picture size, bitrate, or framerate is incompatible with the video port. Scaling is done only when the announcement image is too large for the profile level of the video port. The picture size is reduced to the largest standard picture size supported by the Containerized Decomposed Media Server at that level.

For more information, see *Play Video Announcement to a Port on page 44* and *Record Video from a Port on page 54*.

HC Continuous Presence Conference

The Containerized Decomposed Media Server supports continuous presence conference in HC format. The input picture is dynamically scaled to fit precisely in the four-split or six-split layout in the HC video.

For more information, see *Continuous Presence Conference on page 77*.

Mute or Unmute Conference

The Containerized Decomposed Media Server supports mute or unmute of a conference using the control-leg in the MSCML conference service context. When the conference is in mute or unmute state, all participants except the host are muted or unmuted respectively. Conference mute or unmute operation does not affect the host state. By default, the first participant to join the conference is considered as the host.

For mute and unmute action, the control-leg includes the `<control>` element in the `<configure_conference>` request. The `<control>` element supports **media** and **value** attributes. The **value** attribute performs the mute and unmute action on the conference and the **media** attribute indicates the media type (audio, video, and all) on which the mute or unmute action is to be performed.

For more information on muting and unmuting the conference, refer to the *MSCML Interface Reference*.

Enhanced Conferencing

In addition to audio-specific or video-specific features, the Containerized Decomposed Media Server enhances conferencing with a number of enhanced features.

The following section describes the conferencing features.

Large Conference

In a standard conference, the number of send-receive participants is limited to 125. When large conference feature is enabled, where the number of send-receive listeners exceed 125, the Containerized Decomposed Media Server internally cascade conferences automatically, so that the maximum number of send-receive and listen-only participants is limited to the overall Containerized Decomposed Media Server capacity. No intervention on the part of the control agent is required.

The large conference feature is disabled by default, and can be enabled using the Containerized Decomposed Media Server management interface. When enabled, no explicit control is required to use it.

Internal cascading can introduce delays and latency. Enabling large conferencing usually does not affect conference announcements and recordings, wide-band conferences, personalized-mix conferences, or the audio mix in VAS conferences.

NOTE: Large conferences cannot be cascaded using the cascaded conferencing feature.

N-Loudest behavior is slightly different for large conferences. As a result of internal cascading, participants may hear up to N * x participants, where N is the number of N-loudest speakers, and x is the number of internally cascaded conferences. It can be that the N * x heard speakers are not the absolute loudest speakers in the conference.

NOTE: The large conference feature cannot be used with DTMF pass-through. Ensure that DTMF pass-through is disabled before enabling large conferencing for SIP Netann and MSML conferences.

ASN behavior also changes slightly for large conferences. The Containerized Decomposed Media Server combines the active speaker list from each cascaded conference and sends an aggregate ordered ASN report to the control agent. The active speakers in the report are ordered by input position for the aggregate large conference. This means that for a given configured value of N, the number of active speakers reported is greater than *N*.

NOTE: Full-mix notification is not supported on large conferences.

Cascaded Conference

Cascaded conferencing is a way of implementing ordinary conferences to allow them to span across geographically dispersed installations.

Each tributary conference independently performs its own N-loudest decisions. The full mixed output from each tributary conference contends as a speaker equally with the output of the others for inclusion in the main conference mix. For this reason, to maintain intelligibility, the value of N for tributary conferences must never exceed four.

NOTE: The cascaded-conferencing feature cannot cascade conferences that are using the large-conference feature.

SIP Netann conferences are cascaded manually. To implement a cascaded conference, the control agent must create and manage connections between ports in the main conference and corresponding ports in multiple tributary conferences on other Containerized Decomposed Media Server. The complete conference mix of each tributary conference is sent through the port to the main connection as a single participant. Conferences cascaded in this way can have the following issues:

- High background noise due to the large number of active talk-listen participants
- Large delay between talk-listen participants in different tributary conferences (up to three times the normal conference delay)
- Inconsistent mixes in the tributaries because talk-listen participants compete one-on-one with the main conference mix for one of the N-loudest talk slots

MSML supports internally cascaded conferences. Conferences that are internally cascaded using MSML address the issues mentioned above by supporting the following features:

- **Independent N-loudest settings.** Independent values of N for the main conference and tributary conference allow the number of participants contributing to the conference to be reduced to a much more reasonable value. It also reduces the number of participants reported in ASN events.
- **Cascaded conference port.** The enhanced implementation uses a special port on a tributary conference for connecting to the main conference mix. This port is a preferred input, so all conference participants hear the master mix.
- **RTP bypass.** The RTP port (including the codec) is bypassed when tributary conferences and the main conference reside on the same Containerized Decomposed Media Server. Bypassing the RTP processing and the codec greatly reduces the delay for inter-conference, intra–Containerized Decomposed Media Server connections. Participants who are geographically close to the main conference are able to take advantage of this reduced delay.
- **Mix override.** The mix override feature allows the Containerized Decomposed Media Server to ensure that all conference participants hear a consistent mix.
- **Conference port collocation.** A large part of conference delay is due to inter-processor delay, which occurs when a conference port is not on the processor that is hosting the conference. In a manually cascaded conference, this delay is tripled. Collocating a conference port on the conference host processor reduces the inter-processor delay to zero. Port collocation effects the greatest performance improvement for continuous presence conferences.
- **Configurable default packetization.** To reduce delays in a cascaded conference, the default packetization interval of the RTP data can be lowered.

- **Broken RTP stream timeout.** Inter-conference links, connecting tributary conferences to local mixers or the main conference, can represent many participants. When broken RTP stream timeout is enabled for a port, the Containerized Decomposed Media Server monitors received RTP packets. If no packets are received for more than the configured timeout period, the Containerized Decomposed Media Server sends an MSML event.
- **Multiple hierarchies of cascading.** To minimize delay, proximate tributaries can be joined in a local conference, the mix of which is then joined to a higher-level conference. For distant main conferences, locations with two or more tributaries avoid unnecessarily large round-trip delays. It allows two or more main mixers to be connected together.

One-Command Tear-Down

SIP Netann conferences can be destroyed only by removing conference participants one at a time. The control agent accomplishes this by issuing a SIP BYE command to each connection individually.

MSML applications can end the conference in one command. The `<destroyconference>` command deletes all connections to a conference and tears down the conference session, thereby freeing all associated resources.

Conference Audit Capability

The MSML audit package is supported for SIP and MSML 1.1 conferences. The MSML audit package allows the control agent to audit many state parameters of MSML 1.1 conferences. Auditing MSML conferences periodically can help identify and clean up orphaned resources that occur after unexpected network events.

Conference Control Channel

The Containerized Decomposed Media Server regains the control of the conference if the conference control channel is no longer available. The conference control channel can be created or modified. It can transfer the control of the conference to any other channel. After the conference control channel is changed, all the subsequent conference events are sent to the application server through the new control channel. There can be only one control channel per conference at a time.

The conference control channel is supported for MSML 1.1 conferences.

For more information, see *MSML Interface Reference.*

RTT Conferencing

Real-time text (RTT) is used for real-time text conversational sessions as per RFC 4103 (RTP payload for text conversation). The Containerized Decomposed Media Server enables the RTT text (media) in a multi-party conference using MSML RTT (T.140) ports. The Containerized Decomposed Media Server supports creating a multi-party RTT conference by allowing up to 5 RTT capable end-devices to join the conference.

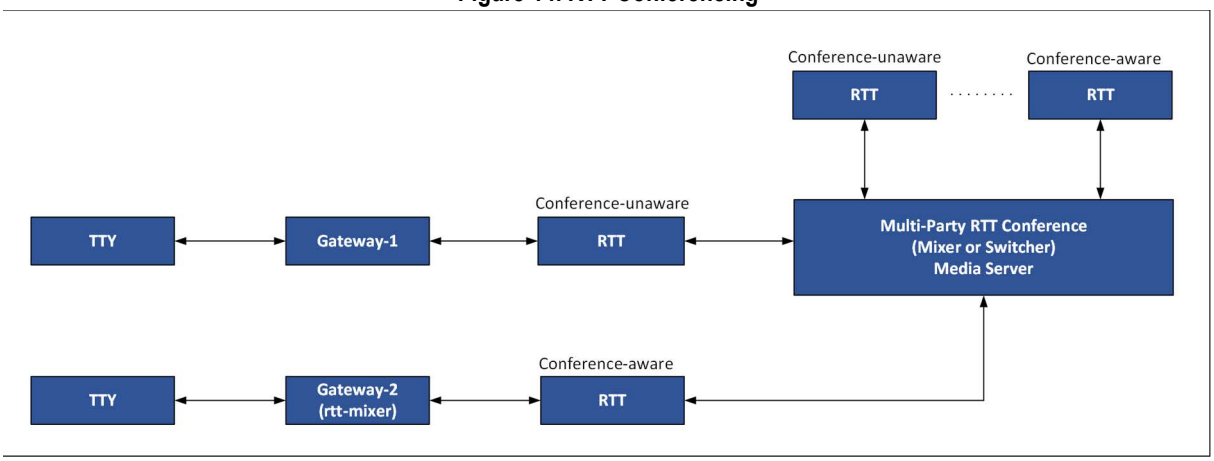
The Containerized Decomposed Media Server supports both conference-unaware and conference-aware RTT terminals to join the RTT conference. However, the Containerized Decomposed Media Server switches the active participants text messages to all other participants at any time. When multiple participants text simultaneously in a RTT conference, the Containerized Decomposed Media Server sends out the text from one active participant first, and then switch to the next active participant, and so on.

The conference-aware terminals negotiate with the SDP attribute `rtt-mixer` along with the *text* and *text/red* for RTT media whereas the conference-unaware RTT terminals negotiate the existing SDP attributes with the *text* and *text/red* for RTT media.

The current implementation of RTT conferencing refers to the *Multi-party RTT Conference IETF Specification - draft-ietf-avtcore-multi-party-rtt-mix-11 (RTP-mixer formatting of multiparty Real-Time Text)*. However, since the specification is still a draft version, the Containerized Decomposed Media Server does not implement real-time text mixing from multiple participants in RTT conference. Instead, the Containerized Decomposed Media Server implements a basic text switching method.

As per the *Multi-party RTT Conference IETF Specification*, only RTT ports can join the Text conference. If TTY devices are required to join the RTT conference, it is recommended that the TTY devices shall use the text gateway externally and convert to RTT payload before joining the RTT conference.

Figure 14. RTT Conferencing



The RTT conferencing port license is configured through the management interface per node basis. For more information on RTT conferencing license, see *License Management on page 162*.

The Containerized Decomposed Media Server supports adding <NAME> label along with the payload while switching from one active participant to another active participant in an RTT conference only for conference unaware participants. The <NAME> label information is extracted from the **NAME** attribute in the incoming RTCP-SDES packet from conference participants. In the absence of the RTCP SDES packet, the Containerized Decomposed Media Server generates the default <NAME> label. If the active participant is a conference unaware participant, the <NAME> label information is defined as User-X for conference unaware participants as SDES information is not expected on conference unaware ports. The Containerized Decomposed Media Server adds the label in the <NAME> format after the new-line character is sent towards conference-unaware participants while switching to a new active participant. The <NAME> label corresponds with the active participant.

Voice Quality Enhancement

The Containerized Decomposed Media Server supports the following features to enhance audio quality.

Table 14 summarizes the VQE features support in narrowband and wideband audio ports.

Table 14. VQE Features Support on Containerized Decomposed Media Server

VQE Features	Audio Port	
	Narrowband	Wideband
AGC	Yes	Yes
Noisy-Line Detection	Yes	Yes
Noise Gating	Yes	Yes
Noise Reduction	Yes	Yes
Acoustic Echo Cancellation	Yes	Yes
Packet Loss Concealment	Yes	Yes
R-factor	Yes, G.711 only	Yes, G.722 only
Packet PPS	Yes	Yes
Audio PPS	Yes	Yes
RTCP-XR PPS	Yes	Yes

Noisy-Line Detection

Noisy-line detection (NLD) can be applied to an audio port. When enabled, Containerized Decomposed Media Server reports to the control agent if incoming noise exceeds configured thresholds for noise on the line.

The Containerized Decomposed Media Server can detect the following noise types:

- Background noise may come from fans, machinery, traffic, crowds of people talking, and so on.
- Impulsive noise is high level noise that is generally short in duration and can be caused by packet loss, keyboard noise, lightning strikes or other electrical noise, gunfire, and so on.
- Continuous signal noise is any continuous tonal signal such as music, a continuous tone or DTMF, or someone humming or talking continuously without breaks.

- Low signal-to-noise ratio (SNR) is not really noise but a condition in which a signal is hard to distinguish from noise. For example, in a call, where the speaker is not talking loud enough to be clearly heard.

In general, the NLD algorithm relies on a user speaking to be able to distinguish the noise from the speech signal.

Each noise type has its own configuration parameter, and the type of noise detected is included in the NLD report.

The Containerized Decomposed Media Server has the following configurable parameters for using filters for noise:

- Threshold for noise power
- Sensitivity to impulsive noise
- Duration for a continuous signal to count as noise
- Threshold for SNR

If the Containerized Decomposed Media Server detects noise within the configured limits, and if subsequently the noise exceeds those limits, the line status is reported to the control agent in a noisy-line report. Line status is also reported if the type of noise exceeds limit changes. The control agent can limit the reporting to minimum time intervals.

The Containerized Decomposed Media Server supports NLD on narrowband and wideband audio ports. NLD is supported in the Containerized Decomposed Media Server MSML 1.1 interface and is enabled through that interface.

The Containerized Decomposed Media Server supports mid-call change between narrowband and wideband codecs for a port on which NLD is enabled.

Noise Gating

Noise gating (NG) is a technique, similar to squelching on two-way FM radio, that reduces perceived noise by attenuating an incoming signal when speech is not detected. This technique is especially effective in reducing the background noise in conferences during intervals when no one is speaking, which is when the accumulated background noise of all active speaker ports is most noticeable.

The Containerized Decomposed Media Server analyzes the incoming audio for speech of the port, and if it detects that none is present, applies a configurable attenuation to the port audio.

NG cannot reduce the level of the background noise during speech, but the presence of speech tends to mask background noise, making it less noticeable. NG is effective in cases where the background noise composed of N active speakers added together is high.

NG is applied to the incoming decoded audio signal just before input gain. To prevent the pops and clicks that can result from instantaneous changes in gain, the Containerized Decomposed Media Server ramps the gain up and down over an interval (non-configurable) when applying and removing the noise-gate attenuation. The rates of ramping up (attack time) and down (release time) are configurable through the management interface.

The Containerized Decomposed Media Server supports NG on narrowband and wideband audio ports. NG is a port-based feature (for audio ports only) and can be used on a conference port. By default, NG is disabled. It is enabled by setting NG attenuation to a non-zero value.

The NG attenuation value can be configured through the management interface (in all Containerized Decomposed Media Server protocol interfaces) or for each call (through the MSML interface).

The Containerized Decomposed Media Server supports mid-call change between narrowband and wideband codecs for a port on which NG is enabled.

Noise Reduction

Noise reduction (NR) is a technique for continuously removing background noise.

The Media Server supports the following noise reduction techniques.

- **Spectral subtraction-based noise reduction.** The Containerized Decomposed Media Server implements noise reduction in the spectral domain by subtracting an estimate of the background noise from the incoming audio. This estimate of the background noise, assumed additive, is derived from measurements taken during pauses in the audio signal, the presence of which is distinguished by its greater magnitude.

  NR is supported for narrowband and wideband audio ports, excluding RTP relay ports, fax ports, or the inter-conference link ports used in conference cascading. An MSML request to enable NR on a connection that does not contain a narrowband or wideband audio port is accepted, that is, the Containerized Decomposed Media Server saves the NR setting, which comes into effect when all the necessary conditions are met.
- **Artificial Intelligence (AI)-based noise reduction.** The Media Server uses Far-End-Noise-Suppression (FENS) technique together with machine learning (ML) based deep neural network analysis models to realize AI-based noise reduction.

  NOTE:

  - The Media Server supports either spectral subtraction-based noise reduction or AI-based noise reduction in any instance through a configurable and rebootable parameter.
  - The capacity of AI-based noise reduction sessions is limited.

NR and automatic NR (auto-NR) mode is enabled on narrowband and wideband ports using the Web GUI and MSML interface. NR is turned off for a connection using auto-NR when the noise on the connection drops below the configured threshold. In turning auto-NR on or off, the Containerized Decomposed Media Server uses a (non-configurable) hysteresis to prevent rapid vacillations. It can also be enabled using an MSML request for a specific port. By default, NR is disabled.

The auto-NR allows the Containerized Decomposed Media Server to monitor the noise level on a port and automatically perform noise reduction if the noise is higher than the configured threshold (assuming sufficient resources).

The Containerized Decomposed Media Server supports mid-call change between narrowband and wideband codecs for a port on which NR is enabled.

Acoustic Echo Cancellation

Acoustic Echo Cancellation (AEC) is a technique for removing echo on incoming audio. Acoustic echo is generally introduced when a terminal is operating in speaker phone mode and either does not have a built-in echo canceler or has one with poor capabilities. The AEC mechanisms on the Containerized Decomposed Media Server can remove acoustic echo.

The following terminology is used to characterize echo:

- Tail length is the length of time from the initial onset of the echo until the echo has substantially diminished (generally by 30 dB or more). A standard conference room has an echo tail of approximately 64 ms.
- Bulk delay is the time that elapses from when audio is sent until the leading edge of the echo returns, comprising round-trip network delay, acoustic delay in the echo path, and other delays in the terminal and Containerized Decomposed Media Server such as jitter, packetization, and codec delays.

  NOTE: Radisys recommends to set the jitter buffer delay for the ports that require AEC, less than half of the AEC bulk delay settings. The AEC may not detect or remove the echo if the jitter buffer delay setting has exceeded the AEC bulk delay.
- Echo Return Loss (ERL) is the difference in amplitude, in dB, between the original signal and its echo. The smaller the ERL number, the larger the echo.
- Echo Return Loss Enhancement (ERLE) is the difference in echo level, in dB, before and after echo cancellation.

AEC resources can be configured in the management interface through the number of echo monitor resources and the number of echo canceler resources option. The echo monitoring resources are shared among ports where AEC is enabled. When AEC is enabled on a port, the Containerized Decomposed Media Server performs echo monitoring on the port first. The echo monitoring resources are shared among ports where AEC is enabled. This means that at least one echo monitoring resource must be reserved when AEC is enabled; otherwise, a protocol error is returned.

The AEC is supported on both narrow band and wide band audio ports, excluding RTP relay ports, fax ports, or the inter-conference link ports used in conference cascading. The port must be a talk-listen participant.

AEC can be enabled or disabled on narrowband and wideband ports using the Web GUI and MSML interface. An MSML request to enable AEC on a connection that does not contain the narrowband and wideband audio ports or where the port is not connected to an audio conference or port to port scenario as talk-listen participant is not rejected. Instead, the Containerized Decomposed Media Server saves the AEC setting, which comes into effect when all the necessary conditions are met.

For audio ports used by talk-listen participants supported within the following limits on echo characteristics:

- **Tail length up to 64 ms.** The Containerized Decomposed Media Server does not attenuate the part of echo noise that continues beyond the supported tail length period.
- **Bulk delay up to 512 ms.** The maximum bulk delay limitation can be lowered through the management interface to reduce load and estimation time.
- **ERL of 4 dB or more.** The smaller the ERL number, the larger the echo.

The Containerized Decomposed Media Server supports mid-call change between narrowband and wideband codecs for a port with AEC is enabled.

The Containerized Decomposed Media Server monitors ports on which AEC is enabled and automatically activates and deactivates AEC as needed. Generally, only a small percentage of Containerized Decomposed Media Server ports require echo cancellation.

Resources for echo canceling can be allocated on Containerized Decomposed Media Server in one of the following ways:

- Automatically, based on lowest ERL (highest echo)
- Designated ports first, with any remaining resources distributed automatically, based on the lowest ERL (using MSML 1.1 active mode=on attribute)

The Containerized Decomposed Media Server uses the following techniques for echo cancellation:

- Non-linear processing (NLP), a technique similar to NG, removes residual echo that cannot be canceled
- Comfort noise generation (CNG) prevents audible changes in background noise level as the NLP turns on and off Comfort noise is inserted after NLP
- Anti-howling reduces the likelihood of howling. Howling occurs when echoes add constructively in an echo loop; anti-howling slightly shifts frequencies of incoming audio

The echo monitoring and echo-canceling resources are shared and the echo canceler resource is required only when the Containerized Decomposed Media Server removes the echo. Also, it can be enabled on a per-port basis by using an MSML protocol message. The MSML setting overrides the management-configured setting on a per-port basis; activation of the echo canceler resource on an AEC-enabled port is controlled by active-mode attribute in the MSML <aec> element. The echo canceler resource is also shared among ports where AEC is enabled. AEC is disabled by default and no echo monitoring and canceling resources are reserved.

R-factor

R-factor (Rating factor) is an objective measure of audio quality for audio ports. R-factor calculation is supported on the Containerized Decomposed Media Server. The value of R-factor varies from 0 to 100 for narrowband and 0 to 129 for wideband, where 0 is unintelligible and highest value is perfect. The R-factor is supported for narrowband (G.711) and wideband (G.722) on the Containerized Decomposed Media Server.

The R-Factor can be enabled on the MSML interface and applies only to R-factor supported codecs. If R-factor is enabled on an unsupported codec and there is a mid-call change to G.711/G.722 codec, the R-factor PPS gets enabled after a mid-call codec change.

The R-factor value is converted to an equivalent MOS-CQ (Mean Opinion Score-Conversational Quality). MOS-CQ value is measured on a scale from 1 to 5. Table 15 shows the correlation between R-factor and MOS-CQ scores.

Table 15. R-factor verses MOS Scores for narrowband and wideband

R-factor (narrowband)	R-factor (wideband)	MOS-CQ	User Satisfaction
90	116	4.34	Very Satisfied
80	103	4.03	Satisfied
70	90	3.60	Some Users Dissatisfied
60	77	3.10	Many Users Dissatisfied
50	64	2.58	Nearly All Users Dissatisfied

NOTE: R-factor is calculated only on input ports.

Fax

In addition to media processing on audio and video, the Containerized Decomposed Media Server provides the following fax processing capabilities.

Fax Tone Detection

The fax tone detection feature allows an application server to detect a fax tone (CNG or CED) in audio sessions for MSML and VXML protocols.

The fax tone detection is supported on both audio and multimedia connections for MSML and VXML protocols.

In MSML, the Containerized Decomposed Media Server reports the detected tone to the control agent as in DTMF detection. Unlike DTMF detection, fax detection is not enabled until the application server explicitly requests it through the `<faxdetect>` element. Fax detection is completed immediately when a single fax tone (CNG or CED) is detected, unlike DTMF detection, in which the Containerized Decomposed Media Server can collect multiple digits before detection is complete.

In VXML, the fax detection property is a Radisys extension, and is specific to the Containerized Decomposed Media Server. The com.cvd.faxdetect property enables or disables fax tone detection. The supported values are true—fax tones are detected if they occur, and a com.cvd.event.faxdetect event is thrown; false—fax tones are ignored.

In some fax over IP (FoIP) applications where the media gateway does not support fax detection, the Containerized Decomposed Media Server is used to detect fax tones from an audio session and report them to the control agent to trigger a fax session.

The Containerized Decomposed Media Server can be instructed to detect in-band and out-of-band fax tones in an audio RTP stream for all supported codecs. This feature notifies the control agent of an incoming fax call, allowing the call agent to then move the call over to a separate IP fax server (not supplied by Radisys). The call agent can also create the Fax session on the Containerized Decomposed Media Server using sip:msml service context.

NOTE: The Containerized Decomposed Media Server supports embedded fax feature in sip:msml context.

Fax Functionality

The Containerized Decomposed Media Server supports fax services in SIP using MSML. The Containerized Decomposed Media Server sends and receives RFC 3949 multi-page TIFF-F formatted faxes, in compliance with the procedures for Group 3 faxes as specified in the 1996 version of ITU-T T.30 Procedures for Document Fax Transmission in the General Switched Telephone Network.

The Containerized Decomposed Media Server sends multi-object fax using MSML interface. Multi-object fax send, facilitates a universal inbox in voice mail applications that can deliver multiple received faxes in one operation. The Containerized Decomposed Media Server allows Application Server to specify up to 15 fax objects per port in MSML interface. For more information on multi-object fax send attributes, refer *MSML Interface Reference*.

The following codecs are supported for fax:

- Voice-band fax is supported using the ITU-T G.711 codec, both a-law and µ-law.
- T.38 fax is supported according to the 1998 version of ITU-T T.38 Procedures for Real-Time Group 3 Facsimile Communication over IP Networks.

Using an MSML request, the call agent can instruct the Containerized Decomposed Media Server to create a fax port for sending or receiving a fax. Transmitted and received faxes are saved on an external NFS server in TIFF-F format. Containerized Decomposed Media Server can be requested to detect fax signals on audio ports and to notify the call agent.

When requested through MSML, the Containerized Decomposed Media Server notifies the call agent of the following fax events: start of a fax operation, completion of fax negotiation, page sent or received, completion of a fax object, and completion of a fax operation.

The Containerized Decomposed Media Server supports Error Correction Mode (ECM) as defined in T.30 for both T.38 and G.711 fax codecs. T.38 supports an additional layer of error correction with two options: packet redundancy or Forward Error Correction (FEC), the choice of which is negotiated in SDP. T.38 faxes use UDP transport layer.

To support SDP negotiation of fax parameters, the Containerized Decomposed Media Server supports **m=image** media description and T.38 fax attributes. Fax priority can be set using the ToS byte, as for audio and video. Codec preference for fax is configurable through the management interface.

The Containerized Decomposed Media Server supports PDF files in fax send and receive request. The PDF file location can be internal, NFS, or HTTP. The Containerized Decomposed Media Server converts source PDF documents in fax send request to TIFF-F before commencing the fax send operation based on the management interface configuration.

For information about setting the default resolution of TIFF images generated from the PDF files, see *Configure Fax on page 292*.

Fax Auto Switch

If you want to convert the initial call from audio or audio-video port to fax port, enable the fax auto-switch feature through the management interface.

When fax auto-switch is enabled, the Containerized Decomposed Media Server supports switching audio or audio-video to fax after receiving a fax operation (send or receive) request, and converts fax to audio or audio-video after receiving re-INVITE without an SDP offer.

For more information about the fax auto-switch, see *Configure Fax on page 292* and *SIP Interface Reference*.

TTY and T.140

TTY/TDD is an old voice band modem still used by people who are deaf or hard-of-hearing, to communicate over PSTN telephone lines. It consists of 45.45 bps 5-bit baudot codes, which are FSK-encoded according to ITU V.18, and TIA/EIA-825. The 5 bit character set contains only the upper case alphabet plus a shift key, which is used to increase the character set to support numbers, symbols, and some special characters. TTY tones can be exchanged through any Containerized Decomposed Media Server-supported audio codecs. TTY tones are found to be reliable on G.711 codec.

RFC 4103 defines the RTP payload format text/T.140 for transmitting T.140 text on a separate RTP session that is dedicated for the transmission of text. Text conversation can be used alone or in connection with other conversational facilities, such as audio and video. The RTP redundancy (RFC 2198) can be used to repeat text data transmission to lower the risk of packet loss.

The Containerized Decomposed Media Server negotiates the character transmission rates with characters per second (cps) SDP parameter between the two UEs. This avoids one UE to send characters too fast to the other UE. The Containerized Decomposed Media Server also supports interworking cases when either or both UEs do not support cps negotiation in SDP. In such cases, the Containerized Decomposed Media Server supports transmitting and receiving characters at the default maximum cps of 30.

NOTE: The maximum size of the primary payload in a T.140 RTP packet is 80 bytes.

The text/T.140 media format is enabled/disabled through the OAMP interface. By default the media format is disabled.

The Containerized Decomposed Media Server supports the following functions:

- Negotiating text/T.140 media format under sip:monitor service contexts in the AVP and AVPF profiles, only when it is enabled in Web GUI.
- Exchanging T.140 attributes through SDP in the SIP message. Adding and removing a text/T.140 session during any ongoing audio/video session via SDP negotiation under sip:tc service context.
- Transcoding between TTY and T.140 formats.
- Use TTY-TTY pass-through when neither side is a T.140 connection port.
- Connecting two T.140 ports. Supports transmission of T.140 text at the configured buffering interval. Supports a text buffer of maximum 3000 bytes for each T.140 (text) and TTY (audio) port. This buffer is used for transmission rate adaptation toward the UE and TTY terminal. The Containerized Decomposed Media Server discards incoming text while this buffer is full.

  NOTE: The buffering interval is the time during which the data is accumulated before transmitting.
- Detecting lost packets (RFC 4103 section 5.3) on T.140 ports. The RTP sequence number is used to detect the lost packet. If RTP redundancy is used, the Containerized Decomposed Media Server uses the redundant generations to compensate the lost packet.
- Reordering the text that is received out-of-order on T.140 ports. It waits for a maximum duration of 1 second for the missing packets to arrive. The Containerized Decomposed Media Server inserts a missing text marker '?' (0xEFBFBD) in the received T.140 stream for each missing text packet if the missing packet is not replaced by redundant T.140 packets. The Containerized Decomposed Media Server transcodes the missing text marker from a T.140 stream to the ' (apostrophe) character in a TTY stream.
- Enabling or disabling RFC 2198 RTP redundancy in transmitting T.140 text over RTP through the OAMP interface. By default this function is enabled with 2 levels of redundant generations. The maximum level of redundant generations is 5. To disable RTP redundancy, the level can be configured as 0.
- Configuring ToS / Traffic Class value for text media (T.140) through OAMP interface. The configured ToS byte is set in text/T.140 RTP packets' IPv4 header's ToS byte and IPv6 header's Traffic Class.

  NOTE: TTY tones are not reliably transported over highly compressed codecs like AMR, EVRC, and G.729.

TTY Clamping

The Containerized Decomposed Media Server supports TTY clamping in RTT/TTY session, based on the management interface configuration.

When **ClampingWithoutLeakageSuppression** is enabled, the Containerized Decomposed Media Server allows beginning of the TTY tone (approximately 60 ms) to pass-through. By default, TTY clamping feature is disabled.

When **ClampingWithLeakageSuppression** is enabled, the Containerized Decomposed Media Server support the following:

- 100% TTY clamping in RTT/TTY (AT-A or A-AT) session
- Adds a delay of 60 ms
- Removes all traces of the TTY tone

NOTE: The DTMF in-band tone clamping can also occur in the direction of [A] to [AT].

If a mid-call change in a RTT/TTY session disables the TTY detector on the audio port, the Containerized Decomposed Media Server forcefully disables the TTY clamping and leakage suppression on the respective audio port. Similarly, if a mid-call change in a RTT/TTY session enables the TTY detector on the audio port, the Containerized Decomposed Media Server verifies the **TTY Clamping** configuration on the management interface and configures the **TTY Clamping** feature on the respective audio port accordingly.

Unique CNAME Identifier

As per RFC 3550, RTCP SDES packet carries a persistent transport-level identifier for an RTP source called **Canonical Name** or **CNAME**. The Containerized Decomposed Media Server supports unique SSRC identifier, but uses CNAME to keep track of each participant for all the ports in an RTP session. Receivers may also require unique CNAME to associate multiple data streams from a given participant in a set of related RTP sessions. For example, to synchronize audio and video.

The Containerized Decomposed Media Server supports unique CNAME in all the SIP services.

RTP/AVPF Feedback Message

Real-time Transport Control Protocol (RTCP) based feedback message is a mechanism for solving audio and video quality issues in a timely manner. RTCP Feedback is a part of Real Time Transport Protocol/Audio Video Profile Feedback (RTP/AVPF), which is an extension to the RTP/AVP profile as defined in RFC 4585.

The Containerized Decomposed Media Server supports RTP/AVPF profile for text, audio, and video sessions. The Containerized Decomposed Media Server supports negotiating the SDP attribute **a=rtcp-fb** in the media session when RTP/AVPF profile is enabled on that media session.

The Containerized Decomposed Media Server supports the following RTCP feedback messages:

- *RTCP-PLI*
- *RTCP-FIR*
- *RTCP-TMMBR/TMMBN*
- *RTCP-NACK*
- *RTCP-TWCC*

RTCP-PLI

Real Time Control Protocol-Picture Loss Indication (RTCP-PLI) is one of the RTCP feedback messages under RTP/AVPF as defined in the RFC 4585. The RTCP-PLI is used to indicate picture loss, which triggers a new I-frame to be generated.

A user can enable or disable the RTCP-PLI message support through OAMP. By default RTCP-PLI is disabled. RTCP-PLI is applicable only for the video ports.

The Containerized Decomposed Media Server supports RTCP-PLI I-frame request capability for video sessions in the following protocols and service contexts:

- SIP netann conference (sip:conf)
- SIP/MSML (sip:msml)
- SIP/VXML (sip:dialog)

RTCP-FIR

Real-Time Transport Control Protocol-Full Intra Request (RTCP-FIR) is one of the RTCP feedback (RTCP-FB) messages under RTP/AVPF. RTCP-FIR is defined in RFC 5104.

The Containerized Decomposed Media Server supports RTCP-FIR I-frame request capability for video sessions in the following protocols and service contexts:

- SIP netann conference (sip:conf)
- SIP/MSML (sip:msml)

The Containerized Decomposed Media Server supports the following RTCP-FIR functionalities.

- RTCP-FIR can be enabled or disabled through the management interface. By default, RTCP-FIR is disabled. The changes to this field take effect immediately on the next port, without rebooting the Containerized Decomposed Media Server.
- The Containerized Decomposed Media Server negotiates RTCP-FIR through the SDP attribute **a=rtcp-fb** for video sessions that use the RTP/AVPF profile.
  - If RTCP-FIR and PLI are offered, the Containerized Decomposed Media Server includes both in the answer.
  - If the control agent offer does not include RTCP-FIR, the Containerized Decomposed Media Server does not include RTCP-FIR in the answer.
- The Containerized Decomposed Media Server offers RTCP-FIR for video sessions through the SDP attribute **a=rtcp-fb**, only if RTP/AVPF and RTCP-FIR parameters are enabled through the Web GUI.
- The Containerized Decomposed Media Server sends and receives RTCP-FIR messages for video sessions, only when the RTCP-FIR capability is negotiated in the SDP offer/answer exchange.
- RTCP-FIR is independent of the RTCP feature.
- The Containerized Decomposed Media Server receives RTCP-FIR packets at any position within a compound packet.
- The Containerized Decomposed Media Server receives RTCP packets with multiple FIR Feedback Control Information (FCI) fields, but processes only the first FCI field.

- The Containerized Decomposed Media Server processes the received RTCP-FIR packets at least once even if a duplicate sequence number is detected. The Containerized Decomposed Media Server increments the sequence number of the outgoing RTCP-FIR packet. The Containerized Decomposed Media Server uses the same sequence number when retrying a request.
- The Containerized Decomposed Media Server sends RTCP-FIR packet with a single FCI when required, without considering the RTCP bandwidth or timing rules.
- The Containerized Decomposed Media Server does not validate the SSRC fields on the received RTCP-FIR messages and sends RTCP-FIR with RTCP media source SSRC. The RTCP-FIR SSRC is set to zero initially and changes to the correct SSRC value after receiving the first RTP video packet from far-end.
- The Containerized Decomposed Media Server ignores and does not send the RTCP-FB message, if RTCP-FB is not negotiated in the SDP.
- The Containerized Decomposed Media Server uses one or many of the following methods to send I-frame request whenever needed in the service context:
  - RTCP-FIR: If negotiated on the port
  - RTCP-PLI: If negotiated on the port and RTCP-FIR is not negotiated on the port
  - SIP-INFO with the following conditions:
    - If enabled in OAMP
    - If RTCP-PLI or RTCP-FIR is not negotiated on the port
- The Containerized Decomposed Media Server receives I-frame requests from the enabled sources.
- The Containerized Decomposed Media Server supports the existing I-frame timeout and retry mechanism when creating RTCP-FIR I-frame requests.
- The Containerized Decomposed Media Server supports the I-frame throttling for RTCP-FIR I-frame requests at the encoder.

  I-frame throttling at the encoder is independent of the I-frame request source and affects the I-frame requests from RTCP-FIR, PLI, SIP-INFO, and internally generated requests from the CP.
- The Containerized Decomposed Media Server supports throttling of received RTCP-FIR I-frame requests.

  When the RTCP-FIR or PLI is processed, the processing of the subsequent RTCP-FIR or PLI packets is delayed for two seconds. If multiple RTCP-FIR or PLI packets are received within two seconds, only the last received packet is processed at the end of two seconds.
- The Containerized Decomposed Media Server generates and processes RTCP-FIR I-frame requests.
- The Containerized Decomposed Media Server models the RTP bandwidth for RTCP-FIR messages on a port, if RTCP-FIR is enabled.

RTCP-TMMBR/TMMBN

Temporary Maximum Media Bit-rate Request (TMMBR) and Temporary Maximum Media Bit-rate Notification (TMMBN) messages are used for dynamic video rate adaptation as required by IR.94[1] for terminals supporting video (as defined in RFC 5104).

The TMMBR and TMMBN are part of the RTCP-FB codec control message (ccm) group and negotiated together as RTCP-FB message **ccm tmmbr** in the SDP.

The Containerized Decomposed Media Server supports TMMBR and TMMBN capability for video sessions in the following protocols and service contexts:

- SIP netann conference (sip:conf)
- SIP/MSML (sip:msml)

The Containerized Decomposed Media Server supports the following TMMBR and TMMBN functionalities:

- The Containerized Decomposed Media Server allows the user to enable or disable TMMBR capability through the OAMP. By default, TMMBR is disabled. The changes to this field take effect immediately on the next port, without rebooting the Containerized Decomposed Media Server.
- The Containerized Decomposed Media Server negotiates TMMBR capability through the SDP attribute **a=rtcp-fb** for video sessions using the RTP/AVPF profile.
  - If TMMBR is offered, the Containerized Decomposed Media Server includes TMMBR in the answer.
  - If the control agent offer does not include TMMBR, the Containerized Decomposed Media Server does not include TMMBR in the answer.
- The Containerized Decomposed Media Server offers TMMBR capability for video sessions through the SDP attribute **a=rtcp-fb** only if RTP/AVPF and TMMBR parameters are enabled through the OAMP.
- The Containerized Decomposed Media Server sends and receives TMMBR and TMMBN messages for video sessions only when the TMMBR capability is negotiated in the SDP offer/answer exchange.
- The Containerized Decomposed Media Server receives TMMBR and TMMBN at any position within a compound packet. A compound packet contains multiple RTCP messages of different types.
- The Containerized Decomposed Media Server receives RTCP packets with multiple TMMBR or TMMBN Feedback Control Information (FCI) fields, but the Containerized Decomposed Media Server processes only the first packet.
- The Containerized Decomposed Media Server sends TMMBR and TMMBN packets with a single FCI when required, without considering the RTCP bandwidth or timing rules.

1.GSM association official document IR.94, IMS profile for conversational video service.

- The Containerized Decomposed Media Server does not validate the SSRC fields on the received TMMBR/TMMBN messages and sends TMMBR with the RTCP media source SSRC. The TMMBR SSRC is set to zero initially and changes to correct SSRC value after receiving the first RTP video packet from far-end.
- The Containerized Decomposed Media Server ignores and does not send the RTCP-FB message, if RTCP-FB is not negotiated in the SDP.
- The Containerized Decomposed Media Server calculates the Measured Overhead for the outgoing TMMBR/TMMBN packets based on the Ethernet transport. This includes overhead from Ethernet, IP, UDP, and RTP. The Containerized Decomposed Media Server ignores the Measured Overhead on the incoming TMMBR/TMMBN packets.

  NOTE: The overhead calculation differs depending on the IP type (IPv4 and IPv6).
- The TMMBR state information is part of the media state, which is not preserved after a redundancy switchover. If the port is running at a reduced bit rate before the switchover, the port reverts to the SDP negotiated rate after the switchover, till a terminal sends another TMMBR request.
- The Containerized Decomposed Media Server defines an OAMP configured parameter **TMMBR Transcode Bypass** to control the transcode bypass that must be permitted for the output video stream of the TMMBR capable ports when the Containerized Decomposed Media Server cannot change the video bit rate.
  - When **TMMBR Transcode Bypass** is enabled, the transcode bypass is permitted on TMMBR enabled ports even if the Containerized Decomposed Media Server cannot change the bit rate.
  - When **TMMBR Transcode Bypass** is disabled, the Containerized Decomposed Media Server transcodes TMMBR capable ports when it cannot change the bit rate.

  This parameter does not require a reboot to take effect and is synchronized for redundancy. For information about configuring TMMBR Transcode Bypass, see *Configure Video on page 254*.
- The Containerized Decomposed Media Server returns the TMMBN response with the SDP negotiated bit rate, if a TMMBR request for a port that is not in service is received.
- The Containerized Decomposed Media Server models the RTP bandwidth for TMMBR/TMMBN messages on a port, if TMMBR/TMMBN is enabled.
- When the Containerized Decomposed Media Server receives the mid-call bitrate change on a TMMBR port that has an encoder, the Containerized Decomposed Media Server updates the encoder bitrate to the SDP negotiated value.

Video Port Announcements

The Containerized Decomposed Media Server supports the following TMMBR/TMMBN for video port announcements for **sip:msml**:

- If the **TMMBR Transcode Bypass** is disabled in OAMP, the Containerized Decomposed Media Server includes the TMMBR capability of a port, based on the decision whether transcode bypass applies for a video port announcement. If the port is TMMBR enabled, the Containerized Decomposed Media Server does not perform transcode bypass.
- If a port receives a TMMBR request when a video announcement is in progress and is transcoded, the Containerized Decomposed Media Server adjusts the encoder bit rate on the port's output to the value in the TMMBR request and sends the TMMBN response.
- If a port receives a TMMBR request when a video announcement is in progress and transcode is bypassed, the Containerized Decomposed Media Server sends the TMMBN response using the SDP negotiated bit rate.

RTP Relay

The Containerized Decomposed Media Server supports the following TMMBR/TMMBN on video RTP relay groups:

- The Containerized Decomposed Media Server adds only video ports to a relay group that have the same TMMBR capability as the first port that was added to a relay group.
- The Containerized Decomposed Media Server relays incoming TMMBR and TMMBN messages for RTCP packets.

NOTE: The RTP relays all RTP and RTCP packets received including RTCP-FB messages, which change only the source and destination IP address and UDP port. For RTP relay, the Containerized Decomposed Media Server does not participate in the TMMBR protocol but relays the messages between the endpoints.

VAS Conference

The Containerized Decomposed Media Server supports the following TMMBR/TMMBN handling for the ports in VAS conference, either for **sip:msml** or **sip:netann**.

- The Containerized Decomposed Media Server adds a new parameter to the MSML interface when creating VAS conferences to specify TMMBR support.
- The Containerized Decomposed Media Server adds a SIP-URI parameter to specify the TMMBR capability of **sip:netann** VAS conferences during the initial invite. The SIP-URI parameter of the first port determines the TMMBR capability of the conference. The valid SIP-URI parameter values are optional and mandatory.
  - If TMMBR support is enabled for a VAS conference that is `tmmbr=mandatory`, only TMMBR enabled ports can be added to the VAS conference.
  - If TMMBR support is disabled for a VAS conference that is `tmmbr=optional`, both TMMBR and non-TMMBR ports can be added to the VAS conference.

- The TMMBR forwarding is by default supported in VAS conference with TMMBR as optional. The Containerized Decomposed Media Server enables TMMBR forwarding as long as all the ports in a TMMBR-optional VAS conference are also TMMBR-enabled ports. The Containerized Decomposed Media Server disables or suppresses the TMMBR forwarding to all the ports, if any of the ports in a TMMBR-optional VAS conference is a non-TMMBR port.
- The Containerized Decomposed Media Server operates the VAS conference at conference initial bitrate. If the conference bit rate is changed by TMMBR request and then the conference TMMBR forwarding state is changed from enable to disable and then changed back to enable state, the Containerized Decomposed Media Server retains the conference initial bitrate.
- The Containerized Decomposed Media Server responds with a TMMBN containing the SDP negotiated bit rate, when a TMMBR port in a non-TMMBR VAS conference receives a TMMBR request. The VAS conference does not forward the TMMBR bit rate request to any other TMMBR capable ports in the conference.
- The Containerized Decomposed Media Server forwards the TMMBR request with bit rate X to all participants in the VAS conference when a video port in a TMMBR enabled VAS conference receives a TMMBR request with a bit rate X lower than the minimum Y of the last agreed to TMMBR requests from all conference participants.
- The TMMBR request from a port to increase the bit rate only increases the bit rate to the minimum of the last agreed to TMMBR request from each VAS conference participant. To increase the bit rate back to the SDP negotiated value, all ports that send request to lower the bit rate must send a new request to return to their SDP bit rates.
- The Containerized Decomposed Media Server waits for all TMMBN responses from conference participants before sending the TMMBN response to the requesting port with the highest bit rate from the received TMMBN responses. If one or more ports do not respond to the TMMBR request, the Containerized Decomposed Media Server does not send a TMMBN response. The Containerized Decomposed Media Server waits up to two seconds for response to its outgoing requests and new incoming requests are delayed until the previous request is completed or the two seconds timer has expired. When there are multiple requests, the Containerized Decomposed Media Server processes only the lowest of the last request from each port and responds with TMMBN responses to each port that made a request.
- When a video port in a VAS conference receives a TMMBR request with a bitrate X higher than or equal to Y (current conference bit rate), the Containerized Decomposed Media Server does not send TMMBR requests to other senders; it responds with a TMMBN with the maximum of the last received TMMBN bit rates (Y).
- The Containerized Decomposed Media Server sends a TMMBR request to the port with the minimum of the last agreed TMMBR requests from all participants in the conference when a new video port enters a VAS conference as a sender or an existing video port becomes a sender in a VAS conference. In this case, the Containerized Decomposed Media Server does not forward the TMMBN response and does not retry its TMMBR if a TMMBN is not received.

- The Containerized Decomposed Media Server transcodes all announcements to TMMBR enabled VAS conferences when the OAMP configured **TMMBR Transcode Bypass** is disabled. If a TMMBR request is received during a VAS conference announcement, the announcement encoder changes its bit rate appropriately. When a transcoded VAS conference announcement starts, the Containerized Decomposed Media Server sets the initial encoder bit rate to the conference bit rate.
- The Containerized Decomposed Media Server permits playing a transcode bypass announcement to a TMMBR enabled VAS conference if the announcement is compatible with the VAS codec parameters and the OAMP configured **TMMBR Transcode Bypass** is enabled. Any TMMBR requests during the announcement are forwarded to all senders connected to the conference. The announcement continues to play transcode free without any change in its bit rate.
- The Containerized Decomposed Media Server continues to operate, even if the port has the lowest agreed TMMBR request and when a video port leaves a VAS conference. The TMMBR requests do not consider the port that leaves the conference.

  NOTE:

  - The mid-call bit rate changes on ports within a VAS conference are not allowed except for instances where the new bit rate is within the allowed bit rate tolerance. Changes to the conference bit rate through **sip:msml** are not allowed if there are any participants in the conference.
  - The video portion of the MSCML (advanced) conference supports the VAS conference.

Continuous Presence Conference

The Containerized Decomposed Media Server supports the following TMMBR/TMMBN for ports in a **sip:msml** CP conference:

- If the CP conference ports do not share an encoder, the Containerized Decomposed Media Server responds to the incoming TMMBR requests by setting the encoder bit rate for the port to the requested bit rate and by sending a TMMBN response with the updated bit rate.
- If the CP conference ports share an encoder, the Containerized Decomposed Media Server responds to the TMMBR requests from any port sharing the encoder. Encoder is shared by setting the bit rate to the minimum X of the last received TMMBR request from all ports, and sending the TMMBN response with the updated bit rate X (which may be lower than or equal to what was requested). If TMMBR request is not received from a port or if a port is not TMMBR enabled, the TMMBR bit rate is assumed to be the SDP negotiated bit rate.
- If a CP conference port is removed from a shared encoder, the Containerized Decomposed Media Server continues to operate at the same bit rate. TMMBR requests to the shared encoder ports do not consider the removed port.

- In a CP conference, since the bitrate of the shared encoder is the minimum of the SDP negotiated rates from all of the shared ports, the Containerized Decomposed Media Server may receive a valid TMMBR message to set the bitrate higher than the minimum SDP bitrate. If the bitrate is not TMMBR limited by any other ports, the Containerized Decomposed Media Server limits the bitrate increase to the minimum SDP bitrate and responds with a TMMBN that includes the minimum SDP bitrate value.
- If a new port is added to a shared encoder on a CP conference, the Containerized Decomposed Media Server continues to operate at the encoder bit rate and processes the TMMBR requests received from this port.

  The Containerized Decomposed Media Server permits the combination of TMMBR and non-TMMBR ports to share an encoder.

Port or Conference Record

Port or conference recording does not output video and therefore there are no changes required to support the incoming TMMBR requests. However, TMMBR can affect the quality of the video recorded from a port or a conference, as the bit rate of a port's video is lower than the initially negotiated video. For example, recording a TMMBR enabled VAS conference operating at a lower rate due to an incoming TMMBR request from one or more participants.

RTCP-NACK

Real Time Control Protocol-NACK (RTCP-NACK or Generic-NACK) is one of the RTCP feedback messages under RTP/AVPF, as defined in the RFC 4585. The Generic-NACK is used to indicate the loss of one or more RTP packets. The lost packets are identified by a packet identifier and a bit mask. RTCP-NACK is applicable only for the H.264 and VP8 video ports.

The Containerized Decomposed Media Server supports Generic-NACK capability in the following service contexts where video is supported.

- SIP netann conference (sip:conf)
- SIP/MSML (sip:msml)
- SIP/VXML (sip:dialog)
- MSCML video (sip:mscmlvideo)

The Containerized Decomposed Media Server supports the following RTCP-NACK functionalities.

- The Containerized Decomposed Media Server negotiates RTCP-NACK through the SDP attribute `a=rtcp-fb` for video sessions that use the RTP/AVPF profile.
  - If RTCP-NACK is offered, the Containerized Decomposed Media Server includes RTCP-NACK in the answer.
  - If the control agent offer does not include RTCP-NACK, the Containerized Decomposed Media Server does not include RTCP-NACK in the answer.
- The Containerized Decomposed Media Server offers RTCP-NACK for video sessions through the SDP attribute `a=rtcp-fb`, only if RTP/AVPF and RTCP-NACK parameters are enabled through the Web GUI.

- The Containerized Decomposed Media Server receives RTCP-NACK in standalone packets or at any position within a compound packet. A compound packet contains multiple RTCP messages of different types. The Containerized Decomposed Media Server always sends RTCP-NACK in a standalone packet with a single FCI. The Containerized Decomposed Media Server receives RTCP packets with multiple NACK Feedback Control Information (FCI) fields but the Containerized Decomposed Media Server processes only the first request.
- The Containerized Decomposed Media Server processes all the received RTCP-NACK packets even if the packets have a duplicate sequence number. The Containerized Decomposed Media Server increments the sequence number on the outgoing RTCP-NACK packets. The Containerized Decomposed Media Server sends an RTCP-NACK packet with a particular sequence number only once. Similar to RTCP-PLI, the Containerized Decomposed Media Server sends RTCP-NACK whenever required as per the RTCP bandwidth modifier or timing rules.
- The Containerized Decomposed Media Server receives RTCP-NACK from all sources that are enabled with Generic-NACK packet loss recovery schemes. In response, the Containerized Decomposed Media Server retransmits the requested (lost) video packets as indicated in the received RTCP-NACK message, if available in the outgoing Jitter buffer. The Containerized Decomposed Media Server generates and processes RTCP-NACK packet loss recovery through the retransmission mechanism.

RTCP-TWCC

The Containerized Decomposed Media Server supports negotiation of RTP header extension for transport-wide congestion control (TWCC) or transport-cc through the SDP in the WebRTC sessions during the video announcements and transcoded VAS conference. The Containerized Decomposed Media Server negotiates the transport-cc only on the MSML ports.

In the SDP negotiation, the Containerized Decomposed Media Server supports negotiating RTP header extension for transport-wide sequence number for video media type only when **transport-cc** is enabled through the management interface. Otherwise, the Containerized Decomposed Media Server ignores the extension header. The RTP extension header is negotiated through **a=extmap** attribute.

The format for the RTCP-FB attribute is as follows:

```
a=rtcp-fb:<PT> transport-cc
```

The Containerized Decomposed Media Server supports both extension headers for **transport-cc** and CVO at the same time through multiple extension headers.

The Containerized Decomposed Media Server force the WebRTC announcement session to be transcoded on the video port when **transport-cc** is negotiated. Mid-call changes in negotiation for **transcode-cc** shall be rejected. The Containerized Decomposed Media Server receives RTCP TWCC feedback packets from the far-end (browser) and performs video bitrate adaptation on the WebRTC announcement video port when **transport-cc** is successfully negotiated.

The Containerized Decomposed Media Server supports both the sender and receiver side TWCC in the transcoded VAS conference when **transport-cc** is enabled in the management interface on the video ports, where **transport-cc** is negotiated in SDP. If **transport-cc** is enabled in the management interface, the Containerized Decomposed Media Server forces VAS conference creation in transcoded mode, irrespective of the VAS Transcode configuration.

For information on configuring the transport-wide congestion control, see *Configure RTCP Feedback on page 249* and *SIP Interface Reference*.

Keyword Detection

The Containerized Decomposed Media Server supports keyword detection capability. The Containerized Decomposed Media Server supports detecting wakewords or commands in HotWord mode and also supports detecting DigitSet sequence based on the ASR grammar in ASR mode.

Wakeword or HotWord is a short-spoken phrase like play_music, pause_music, yes, no, and so on that the Containerized Decomposed Media Server constantly listens for, as a signal to trigger other actions. Wakeword detection is supported in the MSML and VXML service contexts. The Containerized Decomposed Media Server supports detection of DigitSet sequence, which consists of ZERO, ONE, TWO, THREE, FOUR, FIVE, SIX, SEVEN, EIGHT, NINE, OH, NOUGHT, STAR, HASH, CANCEL, and STOP. The CANCEL or STAR and STOP or HASH digits are expected to terminate the DigitSet sequence. However, other digits can also be configured to terminate the DigitSet sequence. DigitSet is supported only in the MSML service context.

When keyword detection is activated, the Containerized Decomposed Media Server looks for one or more configured keywords in the user-speech to trigger user action. The Containerized Decomposed Media Server supports a maximum of 16 distinct keywords for detection in US-English accent. In the ASR mode, the Containerized Decomposed Media Server supports detection of a maximum of 10 digits in a sequence using the DigitSet model. In the ASR mode, the Containerized Decomposed Media Server does not support detection and interpretation of words like **double** and **triple**; each digit required to be distinctly pronounced.

The Containerized Decomposed Media Server supports uploading a single keyword description package file through the SFTP in the *Configure Keyword Detection* Web GUI page. The keyword description package file contains the keyword model file, a text file containing the corresponding list of keywords, and a text file containing mode type (HotWord mode (0) and ASR mode (1)). Depending on the model file loaded, the KWD feature either works in the HotWord or ASR mode. The displayed list of keywords in the management interface corresponds to a list of keywords inside the text file. Only these configured keywords must be used in MSML and VxML sessions.

The Containerized Decomposed Media Server supports ASR mode based digit detection, collection, and reporting on the MSML ports, similar to DTMF digits. The Containerized Decomposed Media Server supports concurrent activation of ASR mode based digit detection with other services such as ASR, DTMF detection, port announcement, recording, and conference.

NOTE: The detection accuracy of keywords depends on the length of the keyword; a keyword must not be very short or too long. An ideal keyword must be of three to five syllables and with a distinct sound.

For configuration of the keywords list, see *Configure Keyword Detection on page 328*.

The Containerized Decomposed Media Server supports keyword detection on ports using G.711 a or µ-law, G.722, G.729, AMR, AMR-WB, EVRC, EVRC-B, EVRC-NW, Opus, or EVS (NB, WB, or SWB) codecs. The Containerized Decomposed Media Server supports mid-call changes on keyword detection on ports including session parameters and codecs through the SDP re-negotiation. The Containerized Decomposed Media Server supports keyword detection on audio port in multi-media sessions, IPv4 and IPv6 ports, and RTP/SRTP ports with RTCP/SRTCP enabled or disabled.

The Containerized Decomposed Media Server supports concurrent activation and switches between keyword detection and ASR using external speech server in an IVR session. The Containerized Decomposed Media Server supports enabling keyword detection and DTMF concurrently. The Containerized Decomposed Media Server supports keyword detection in conjunction with port announcement including TTS and recording services in MSML. Whereas in VXML, the Containerized Decomposed Media Server supports keyword detection in conjunction with port announcement including TTS. The Containerized Decomposed Media Server can barge the announcement (barge-in prompts) on any of the active keyword detection.

The Containerized Decomposed Media Server enables or disables AGC on keyword detection ports based on the management interface configuration. The AEC can be enabled to improve the keyword detection accuracy during the announcement and conference sessions. The Containerized Decomposed Media Server always disables NR, NG, and NLD on the keyword detection input. The Containerized Decomposed Media Server can support PLC (G.711 and G.722) on keyword detection port.

When keyword detection is enabled, the Containerized Decomposed Media Server does not remove the keyword from the user speech and does not induce any delay in forwarding the user speech.

The Containerized Decomposed Media Server supports keyword detection on narrowband, wideband, super wideband, and dynamic sample rate audio mixers. The Containerized Decomposed Media Server supports MSML, and MSCML audio conference redundancy switchover with call preservation. The Containerized Decomposed Media Server supports keyword detection in conjunction with fax tone detection, CPA on the port, DTMF pass-through, and DTMF clamping on the port joined to the conference. When keyword detection is enabled on the port and conference, the keyword detection license is consumed.

For more information on keyword detection through MSML and VXML, refer to the *MSML Interface Reference* and *VXML Interface Reference*.

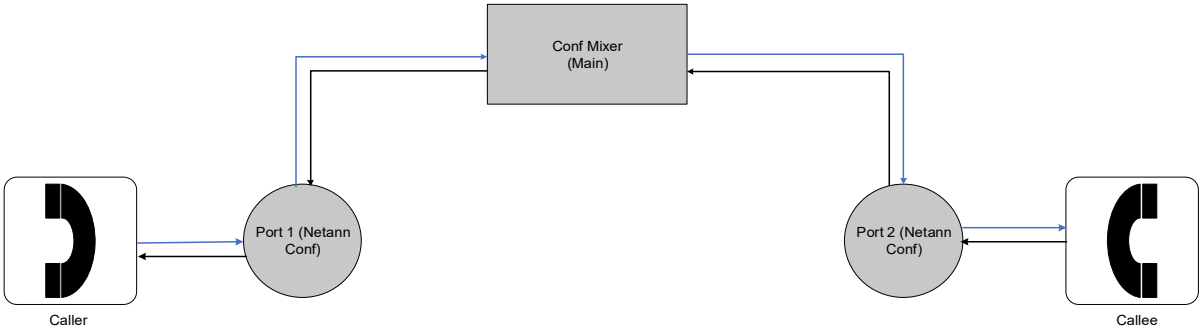
Keyword Detection on Netann Conference Port

The Containerized Decomposed Media Server enables keyword detection on first two ports of Netann conference using a VXML port and modified topology. In a Netann conference, keyword detection is enabled through an optional Request-URI parameter—`enable-kwd`, of the initial INVITE.

The `enable-kwd` parameter in the INVITE Request-URI support the **caller** and **callee** values. The first user joining the conference is known as the **caller** and the second user joining the conference is known as the **callee**. In keyword detection, the Containerized Decomposed Media Server supports caller or callee port, but not both. For information on request-URI to enable keyword detection for the caller, refer to the *SIP Interface Reference*.

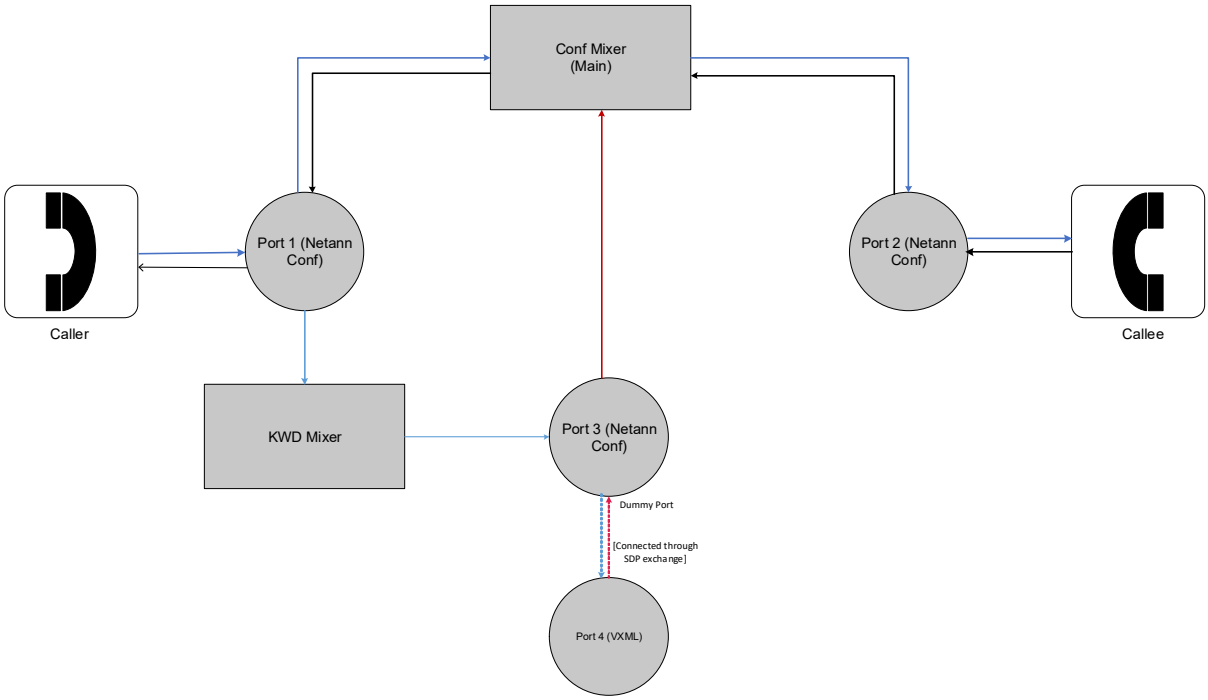
Figure 15 describes the Netann conference topology after the caller and callee join the conference.

Figure 15. Topology after Caller and Callee Join the Netann Conference



The `enable-kwd` parameter creates a dummy keyword detection port in the Netann conference. After receiving the `enable-kwd` parameter in the INVITE Request-URI of the `sip:conf` service context, the Containerized Decomposed Media Server modifies the topology as shown in Figure 16.

Figure 16. Topology after Keyword Detection Dummy Port Joined the Netann Conference



In Figure 16, the participating ports in the Netann conference are as follows:

- **Port 1.** Port for caller
- **Port 2.** Port for callee
- **Port 3.** Dummy port used for enabling keyword detection for the caller
- **Port 4.** VXML port used for keyword detection and announcement

The modified topology describes the Containerized Decomposed Media Server behavior for keyword detection in a Netann conference.

1. The control agent sends an initial SIP INVITE request (`sip:conf`) to join caller A to the conference. The Containerized Decomposed Media Server internally creates a **Conf** mixer and joins caller A to the conference.
2. The control agent sends the SIP INVITE request to join callee B to the conference. To view the Netann conference topology, see *Figure 15*.
3. The application server sends the SIP INVITE to join the dummy port C to the conference. The SIP INVITE request for dummy port C includes an optional parameter `enable-kwd` in the request URI. For example, `enable-kwd=caller`.
4. The Containerized Decomposed Media Server modifies the topology after receiving the SIP INVITE for dummy port C. To view the modified Netann conference topology, see *Figure 16*.
5. The VXML announcement played from port 4 (where keyword detection occurs) is provided into the **Conf** mixer. The **Conf** mixer plays the announcement so that both caller A and callee B can listen to the announcement.
6. The control agent joins port 4 with dummy port C at the SDP level.

The Containerized Decomposed Media Server supports redundancy switchover for the conference topology. The Containerized Decomposed Media Server does not support redundancy switchover for VXML dialog service context. Therefore, the keyword detection session is not preserved over switchovers. However, the Netann conference is preserved across switchovers, so that the users can continue to talk without any interruption.

NOTE: The Containerized Decomposed Media Server rejects the INVITE request,

- if the caller or callee has left the conference or did not join the conference and the `enable-kwd` request is received.
- if insufficient DSP resources are available for the conference.

Dynamic Load Modeling

The Containerized Decomposed Media Server supports the Dynamic Load Modeling feature. When the Dynamic Load Modeling parameter is enabled through the OAMP adapter, the Containerized Decomposed Media Server models the load based on the feedback received from the current actual CPU usage. The Containerized Decomposed Media Server supports this feature only for audio use cases.

The Dynamic Load Modeling feature can be configured through the OAMP adapter using the CLI commands and is a rebootable parameter. By default, the Dynamic Load Modeling feature is disabled.

- Execute the following commands to enable this feature on
  - MNGT/OAMP pod

    ```
    /opt/swms/bin/oampadapter -s -o 1.1.1.35.20 -t bool -v true -d
    ```
  - MRFP pod; here, MRFP pod is instance number 3

    ```
    /opt/swms/bin/oampadapter -s -o 1.1.3.35.20 -t bool -v true -d
    ```
- Execute the following command to disable this feature on
  - MNGT/OAMP pod

    ```
    /opt/swms/bin/oampadapter -s -o 1.1.1.35.20 -t bool -v false -d
    ```
  - MRFP pod; here, MRFP pod is instance number 3

    ```
    /opt/swms/bin/oampadapter -s -o 1.1.3.35.20 -t bool -v false -d
    ```

The Dynamic Load Modeling feature behaviour is as follows:

- If Dynamic Load Modeling is enabled,
  - the Containerized Decomposed Media Server models the load based on the feedback received from the current actual CPU usage. When the **ht_core_enable** parameter is enabled, this feature assumes that the hyperthreading is enabled on the platform, and 50% of the CPU clock resource is available for each logical DSP core.
  - the Containerized Decomposed Media Server allows to configure the maximum audio and video load threshold configurations to 100% and adapt the modeled load to the actual load about 10 minutes after the start of steady state.
- If Dynamic Load Modeling is disabled, the Containerized Decomposed Media Server models the load statically.

NOTE: Specific platforms like KVM or OpenStack may steal or lose cycles to other VMs since there is no specific configuration to reserve CPU clock cycles on such platforms. It is recommended to disable the **ht_core_enable** parameter on such platforms when the base machine is not sufficiently loaded.

Networking Functions

This section describes the network features.

HTTP Caching

The Containerized Decomposed Media Server supports the following modes of operation for the HTTP media:

- **Streamed mode.** The Containerized Decomposed Media Server streams clips directly from external HTTP or HTTPS servers at clip play speed. There is at least one HTTP connection per announcement. For example, if the Containerized Decomposed Media Server is concurrently playing a five-minute clip to 100 connections, all 100 HTTP connections are kept open for five minutes. The Containerized Decomposed Media Server supports WAV, MP3, and MP4 container file formats in streamed mode.
- **Cached mode.** The Containerized Decomposed Media Server caches media clips and streams clips to connections from the internal cache. The Containerized Decomposed Media Server retrieves a clip from the external HTTP or HTTPS server when the clip is not cached or if it must be revalidated. This allows the Containerized Decomposed Media Server to retrieve the clips at near-line speed. HTTP connections remain open only during clip retrieval. When the cache is full, the Containerized Decomposed Media Server applies a Least Recently Used algorithm to replace stale clips. The Containerized Decomposed Media Server supports WAV, MP3, MP4, 3GP, 3G2, AMR, and AWB container file formats in cached mode.

HTTP media caching reduces the burden on the external HTTP or HTTPS server. In addition, cached clips are retrieved much faster than streamed clips. HTTP media caching can significantly increase capacity for applications where media streaming is a critical operation.

The Containerized Decomposed Media Server supports playing chunked streams in the HTTP and HTTPS announcements for mp3 and wav files. The Containerized Decomposed Media Server reads the chunk-size field from the chunk data and decodes the chunk packets. The Containerized Decomposed Media Server considers the end of chunked encoding only after receiving the chunk size as zero.

Primary uses of HTTP caching are:

- Playing multiple short clips in sequence, where each clip represents a word or a phrase from a sentence
- Playing long clips when the media or file server is close to capacity
- Using HTTP for audio prompting for Voicemail applications written in VoiceXML
- Call-parking and music on hold, which can require five or six (2 to 5 MB) files to be cached

HTTP caching is enabled through the management interface. It can be used on Containerized Decomposed Media Servers in conjunction with an NFS external cache; both features can be used simultaneously.

NFS Caching

The Containerized Decomposed Media Server can cache clips played from an external NFS server to enhance performance of applications such as announcement servers. The effect of caching on performance depends on the number of clips used, clip sizes, usage pattern, and so on.

Primary uses of NFS caching are:

- Playing multiple short clips in sequence, where each clip represents a word or a phrase from a sentence
- Playing long clips when the file server is close to capacity
- Call-parking and music on hold, which can require five or six (2 to 5 MB) files to be cached

The Containerized Decomposed Media Server caches announcement files streamed from external NFS servers (version 2 or version 3). If the cache memory is temporarily insufficient (when caching a clip would exceed available memory space, shared with internal clips) or for files that are particularly large, the Containerized Decomposed Media Server continues playing announcements directly from the NFS server without caching.

NFS caching is enabled through the management interface. It can be used on Containerized Decomposed Media Servers in conjunction with HTTP caching; both features being used simultaneously.

NOTE: The Containerized Decomposed Media Server immediately rejects NFS recording, announcement, and fax send and receive requests if the,

- NFS server is unavailable
- mount operational mode of the NFS mount point is disabled
- mount is unsuccessful

However, if the NFS request is received prior to detecting the NFS server unavailability, the request fails after NFS file operations (file opening, reading, and writing) time-out.

Quality of Service

The Quality of Service (QoS) is an important consideration in all networks that support time-sensitive media such as voice and video. The Containerized Decomposed Media Server provides the following mechanisms to enable the deployment of networks with high QoS demands.

RTCP and SRTCP

The Real Time Control Protocol (RTCP) monitors the flow of Real Time Protocol (RTP) packets. The Containerized Decomposed Media Server supports RTCP packets for video and audio ports with the exception of RTCP-XR, which is supported only for audio ports.

RTCP relay is supported for IPv4 and IPv6 ports. The IP version of all ports in a relay group must be same. Secure RTCP (SRTCP) is not supported in RTCP relay. RTCP is supported for audio and video streams.

The RTCP packets are relayed on relay ports if RTCP is enabled through the management interface. On the relay ports, the Web GUI RTCP settings such as transmission internal, RTCP Bye Packet Processing, and RTCP XR VOIP Metrics Reset Internal are not applicable.

The Containerized Decomposed Media Server sends Sender Report (SR), Receiver Report (RR), Source Description (SDES), and BYE packets, and receives SR, RR, and BYE packets as defined in RFC 3550. It ignores received SDES or APP packets. The Containerized Decomposed Media Server responds to a received RTCP BYE packet by sending a BYE on a SIP call leg, delete speech server port, or delete RTSP port.

The Containerized Decomposed Media Server uses the next highest User Datagram Protocol (UDP) port number for sending and receiving RTCP packets associated with a video RTP stream. It also supports RTCP video RTP streams from a RTSP server, as it does for audio.

The Containerized Decomposed Media Server supports the mid-call key change call flow on the SRTCP and Secure RTP (SRTP) port for a new custom profile value in the SIP custom profile. This is to ensure that the behavior of Containerized Decomposed Media Server remains unchanged whether it uses SRTP port or another custom profile. You can achieve this behavior by setting the SIP custom profile to six in the management interface.

RTCP is used for out-of-band statistics and control information for RTP streams. SRTCP is used in the same way for SRTP streams.

The Containerized Decomposed Media Server sends and receives SRTCP on video ports (similar to that of audio ports), when RTCP is enabled through the management interface on connections using SRTP. Only encrypted and authenticated SRTCP is supported using the encryption parameters configured for the SRTP stream.

The Containerized Decomposed Media Server uses the following existing management interfaces:

- RTCP configuration (audio and video RTCP)
- RTCP reporting interval configuration (audio and video RTCP)
- RTCP BYE configuration (audio and video RTCP)
- RTCP-XR VOIP Metrics Reset Interval

For more information about the new SIP custom profile, see *Configure SIP on page 197* *and SIP Interface Reference*.

RTCP Timeout

The Containerized Decomposed Media Server monitors the RTCP messages to determine the endpoint link aliveness. If no RTCP messages are received within the configured time interval, the Containerized Decomposed Media Server cleans up the call leg by sending a SIP BYE with return code 503 (service unavailable) with a message “RTCP Timeout on media port” in the **Reason** header. The associated response code in the **Reason** header specifies the control agent that the requested service did not complete normally.

The Containerized Decomposed Media Server supports the RTCP Timeout with the following:

- All SIP service contexts
- Audio (including G.711 fax) port
- Video port

The Containerized Decomposed Media Server does not support the following RTCP Timeout for any of the following:

- T.38 Fax does not use RTP
- RTP media streams to ASR/TTS servers
- RTP media streams to RTSP servers

During call setup, if the application server puts audio or video media on hold by setting the far-end address to zero (0.0.0.0), the Containerized Decomposed Media Server disables RTCP timeout on the audio or video port even if RTCP timeout is enabled. During mid-call, if application server changes the audio or video far-end address from zero (0.0.0.0) to non-zero, the Containerized Decomposed Media Server enables RTCP timeout on the audio or video port, if RTCP timeout was enabled during port creation.

In case of a multimedia connection, when the RTCP timeout occurs on an audio port, an audio port is deleted and the call continues. The call is deleted when a video port is deleted due to RTCP timeout or other reasons.

The Containerized Decomposed Media Server supports RTCP Timeout when SRTCP is used.The SRTP is enabled in the OAMP and negotiated through SIP or SDES. RTCP-PLI packets are counted along with RTCP packets by the RTCP Timeout algorithm.

The RTCP Timeout value is configured through the Web GUI and SNMP Interface, by default RTCP Timeout is disabled. The RTCP Timeout configuration is ignored for non-supported port types. Changes in the RTCP Timeout applies only to new calls. RTCP packets are sent or received at all times when RTCP is enabled on a port. However, the Containerized Decomposed Media Server RTCP Timeout configuration takes “RTCP packets being received to Containerized Decomposed Media Server” is considered for this feature. If you are using dynamic NAT translation timeouts in the network, ensure that the configured RTCP intervals are short enough, so that RTCP messages to or from the Containerized Decomposed Media Server do not get dropped.

For information on RTCP Timeout configuration, see *Configure RTCP on page 247* and *Radisys SNMP Interface Reference*.

RTCP Bandwidth Modifier (b=RR/RS)

As recommended by RFC 3556, the RTCP bandwidth modifier b=RS and b=RR specifies the RTCP bandwidth for sender and receiver respectively. This allows some applications to specify the RTCP bandwidth independently of the session bandwidth. The Containerized Decomposed Media Server uses “RS” and “RR” to control RTCP timeout monitoring and to stop sending RTCP packets when both are set to zero.

The Containerized Decomposed Media Server supports the RTCP bandwidth modifier b=RR/RS for audio and video ports for all SIP service contexts. The Containerized Decomposed Media Server allocates RTCP bandwidth based on the negotiated b=RR/RS value. If b=RR/RS is not negotiated and RTCP is enabled in OAMP, the Containerized Decomposed Media Server allocates 5 percentage of the RTP session bandwidth. The Containerized Decomposed Media Server calculates the RTCP transmission interval based on the allocated RTCP bandwidth and size of the outgoing RTCP SR/RR report for SIP control protocol.

For all other SIP service contexts, the Containerized Decomposed Media Server supports negotiating the b=RR/RS in SDP offer/answer model by allocating the RTCP bandwidth based on the SDP b=RR/RS negotiation and by calculating the RTCP transmission interval based on the allocated RTCP bandwidth.

The RTCP bandwidth modifiers b=RS and b=RR can be specified at the session-level or media-level in SDP. When specified in SDP session-level, the total RTCP bandwidth is shared by all the media. When specified in SDP media-level, the total RTCP bandwidth is allocated for that specific media only. When it is specified in the session level and media-level, media-level value is used for that media session.

RTP-RTCP Multiplex

The Containerized Decomposed Media Server multiplexes the outgoing and incoming RTP and RTCP packets when the RTP-RTCP multiplexing is negotiated on that port.

The Containerized Decomposed Media Server includes the `a=rtcp-mux` attribute in the SDP offer when the **RTCP** and **RTP-RTCP Multiplexing** parameters are enabled in the management interface. The Containerized Decomposed Media Server enables RTP-RTCP Multiplexing on the port, if the SDP answer includes the `a=rtcp-mux` attribute.

The Containerized Decomposed Media Server supports RTP-RTCP multiplexing on SDES/RTCP port, and all the supported RTP profiles.

For information on configuring the RTP-RTCP Multiplexing, see *Configure RTCP on page 247* and *SIP Interface Reference*.

HTTP Resource Server Redundancy

The Containerized Decomposed Media Server supports HTTP Resource Server (RS) Redundancy for HTTP clips (announcements and file transfer) and to fetch the VXML document. The Containerized Decomposed Media Server supports RS Load balancing mode in the RS Redundancy feature.

When RS load balancing mode is disabled, the RS has one primary and one secondary host instance for redundancy. The two instances have identical inventory. When requesting a service, such as to play an HTTP clip (announcement or file transfer) and to fetch VXML document, the domain name or IP address of the RS is specified in a request that is sent to the Containerized Decomposed Media Server. The Containerized Decomposed Media Server periodically performs a health check on the two RS instances and selects the instance that is alive to serve the request.

When RS load balancing mode is enabled, the Containerized Decomposed Media Server allows configuring a maximum of four server addresses for a given FQDN through the management interface. The Containerized Decomposed Media Server distributes the HTTP fetch requests in the round-robin method for clips (announcement and file transfer) and VXML document among the active servers. The Containerized Decomposed Media Server periodically performs a health check on the configured server addresses and load balances to serve the HTTP fetch request among the active servers.

The Containerized Decomposed Media Server supports a maximum of five resource servers.

For information on Resource Server Redundancy configuration, see *Configure Resource Server Redundancy on page 300*.

Type of Service Byte/Traffic Class

You can use Quality of Service (QoS) features to specify network behavior for packet forwarding, traffic classification, and traffic conditioning such as metering, policing, and shaping.

The Containerized Decomposed Media Server does not make any QoS packet forwarding. But it can set appropriate service type parameters in outgoing IP headers based on the requested QoS type. The service type parameter in IPv4 headers is Type of Service (ToS) byte. The service type parameter in IPv6 headers is Traffic Class.

The traffic class includes the following types:

- Management
- Control
- Audio
- Video
- HTTP media
- Fax
- Emergency Telecommunications Service (ETS) prioritized calls
- Wireless Priority Service (WPS) prioritized calls
- Text media
- MSRP media

For media traffic, the Containerized Decomposed Media Server supports rewriting the entire ToS/Traffic Class byte. This is consistent with setting RFC 791 3-bit IP precedence, RFC 1349 4-bit ToS values, or setting 6-bit RFC 2474 DiffServe Code Point (DSCP) values. For non-media traffic, the Containerized Decomposed Media Server supports setting 6-bit RFC 2474 DiffServe Code Point (DSCP) values of the ToS/Traffic Class byte. To provide maximum flexibility in QoS deployments, the QoS semantics values are not validated against any particular semantic. The Containerized Decomposed Media Server sets the default ToS value (0x00) for egress NFS traffic associated with port or conference announcement.

The Containerized Decomposed Media Server uses the **Default UDP Control** value for DSCP while resolving DNS query over UDP, on both IPv4 and IPv6 address types. Similarly, the Containerized Decomposed Media Server uses the **Default TCP Control** value for DSCP while resolving DNS query over TCP on both IPv4 and IPv6 address types.

For SIP messages in priority calls over UDP, the Containerized Decomposed Media Server uses the values for DSCP as per namespace (ets and wps) in the `Resource-Priority` header, and in the non-priority calls over UDP, the Containerized Decomposed Media Server uses the **Default UDP Control** value for DSCP. However, the Containerized Decomposed Media Server uses **Default TCP Control** value for DSCP in SIP messages regardless of priority or non-priority call.

The Containerized Decomposed Media Server sets the ToS value for egress HTTP traffic associated with conference announcement or recording service based on configured **Default HTTP Media** value.

NOTE: To set **DscpValue** on MRFCtrl pod, configure **sipproxysubsystem.ini** manually in ***/opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini***.

The Containerized Decomposed Media Server supports the following DSCP modes for the Lawful Intercept (LI) service media packets.

- **static.** The Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured DSCP value through the management interfaces.
- **dynamic.** The Containerized Decomposed Media Server sends the DSCP value in the outgoing media packet whatever is received in the incoming media packets.

The following are the RTP and RTCP functionalities of DSCP in LI media packets.

- For pass-through RTP and RTCP media in
  - dynamic DSCP mode, the Containerized Decomposed Media Server sends the DSCP value in the outgoing media packet whatever is received in the incoming media packets.
  - static DSCP mode, the Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured media DSCP value through the management interfaces.
- In listener RTP media in
  - dynamic DSCP mode, the Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured audio DSCP value through the management interfaces.
  - static DSCP mode, the Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured media DSCP value through the management interfaces.
- The following are the exceptions in listener media.
  - For listener, the Containerized Decomposed Media Server does not support RTCP media.

For audio mono mode, the Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured audio DSCP value through the management interfaces, irrespective of the dynamic or static.

Sophisticated Jitter Buffer Management

Sophisticated jitter buffer management enables the deployment of networks with high QoS demands.

Audio Jitter Buffer

The audio jitter buffer facilitates proper reconstruction of the received RTP audio in the Containerized Decomposed Media Server. The jitter buffer is a first-in-first-out (FIFO) buffer that is indexed by a time slot. The jitter buffer algorithm is designed to compensate for silence suppression, clock differences between the transmitting device and the Containerized Decomposed Media Server, and large variances in jitter.

When audio is received, it is placed in the jitter buffer at the appropriate location. The Containerized Decomposed Media Server plays out the current frame of audio within the jitter buffer every 10 milliseconds and removes the frame from the buffer. It fills the buffer with enough data so that the jitter in received audio packets does not affect their audio play. Also, packets received out of order (a form of jitter) can be reordered so that they do not affect the play out of the audio.

The average amount of data within the buffer is referred to as the average jitter position. The average jitter position is initially set to half of the total size of the maximum jitter, which is also the total size of the jitter buffer. The jitter buffer is filled initially by not removing data from the buffer or by incrementing the current timestamp until the time slot at the middle of the buffer contains audio.

Because the jitter buffer size is configurable, carefully set the maximum jitter buffer size so that delays are minimized and the jitter buffer can handle the jitter in the media stream.

Automatic Audio Jitter Buffer

The Containerized Decomposed Media Server provides a robust automatic audio jitter buffer, which minimizes the delays in the jitter buffer relative to jitter of the incoming media stream. This algorithm estimates the jitter and adjusts the desired average jitter position accordingly. This feature can be enabled or disabled through the management interface.

The automatic jitter buffer algorithm is best at minimizing the delay when the incoming media stream has a relatively stable jitter pattern. However, if the jitter of the media stream is continuously changing, it is better to use a large fixed-sized jitter buffer. When using the automatic jitter buffer, a change in the average jitter amplitude degrades audio quality until the jitter buffer automatically adjusts. Therefore, the jitter buffer has been adjusted based on estimated jitter, to minimize the delay, if the jitter increases, some packets are lost and cannot be placed in the jitter buffer.

For most applications, the benefit of robust dejittering outweighs its corresponding increased delay, generally in the order of tens of milliseconds. For applications for which preventing even small delays is critical, use the aggressive operational mode of the automatic audio jitter buffer, which reduces audio delay to the minimum. This mode should be used only in networks with low jitter. Operational mode is configurable through the management interface. By default, aggressive mode is disabled.

Video Jitter Buffer

The video jitter buffer is similar to the (non-automatic) audio jitter buffer except that video rather than audio frames are stored in the timeslots. A major difference from audio is that video frames are fragmented and each video timeslot is used as a placeholder to accumulate the fragments of a video frame as it arrives.

Video frames do not need to be fully received before they are processed. In fact, some terminals perform bandwidth shaping by spreading the sending of large frames over many frame periods. Frames are released from the jitter buffer after the configured video jitter buffer delay, whether or not they are completely received. This is called partial sending.

The jitter buffer supports reassembly of only one video frame at a time. Arrival of a new frame terminates the reassembly of older frames. Out-of-sequence packets cause severe degradation to the video performance; these packets correction is supported for a maximum of five sequence numbers. Because the Containerized Decomposed Media Server does not actually decode the video, packet loss concealment for video is not possible. Video jitter buffer implementation is fixed at 80 ms and the Web GUI setting is ignored.

Priority Call Management

The Containerized Decomposed Media Server supports SIP-based priority management as defined in RFC 4412 and ATIS PTSC-2006-016. RFC 4412 defines the `Resource-Priority` and `Accept-Resource-Priority` SIP headers. PTSC-2006-016 defines procedures and capabilities for supporting Emergency Telecommunications Service (ETS) between IP-based service provider networks and Wireless Priority Service (WPS). The Containerized Decomposed Media Server supports configuring SIP-based priority management using the management interface and is disabled by default. **SIP Priority Queuing**

The Containerized Decomposed Media Server supports the priority queuing mechanism of RFC 4412 for initial INVITEs with the `Resource-Priority` header specifying the ets or wps namespace. The Containerized Decomposed Media Server propagates this header in subsequent requests and responses, excluding 401 and 407 as per PTSC-2006-016. Under call overload conditions, the Containerized Decomposed Media Server provides a single queue for ets and wps priorities and imposes a waiting time (configurable) limit on queued calls. The Containerized Decomposed Media Server does not support pre-emption.

The Containerized Decomposed Media Server supports the `Accept-Resource-Priority` header, enumerating priorities ets and wps namespace to be included in its 200 and 417 response. A `Supported:` header with the `resource-priority` option tag is included in the Containerized Decomposed Media Server 200 response to a SIP OPTIONS request. The `Accept-Resource-Priority` header is included in the Containerized Decomposed Media Server 417 response to a SIP INVITE request that contains the `resource-priority` option tag in its `Require` header and does not specify a supported priority namespace.

For UDP transport, the Containerized Decomposed Media Server supports setting appropriate ToS values, provisioned per ets and wps namespace priority, for the SIP control and RTP media egress traffic associated with the `Resource-Priority` header. For TCP transport, the Containerized Decomposed Media Server does not set the QoS value for outgoing SIP packets for priority calls based on the priority level indicated in the `Resource-Priority` header of the INVITE request. The QoS value is same as **Default Control** value and not the value configured in priority namespace in the management interface.

The Containerized Decomposed Media Server uses the default ToS value for control and media packets as per the management configuration when generating SIP messages for priority calls for ets and wps namespace.

In call overload scenario, the MRFP behavior is as follows:

- The MRFP de-registers with MRFCtrl when **Priority Management** settings is disabled, or when **Priority Management** settings is enabled and **SIP Priority Call Mgmt Method** is set to **Enhanced.**
- The MRFP does not de-register with MRFCtrl when **Priority Management** setting in enabled and **SIP Priority Call Mgmt Method** is set to **Basic**.

In service overload scenario, the MRFP de-registers with MRFCtrl.

ICMP Backoff

The Containerized Decomposed Media Server can receive Internet Control Message Protocol (ICMP) messages related to problems with transmission of RTP streams at any time such as Destination Unreachable for ICMPv4/v6 or Packet Too Big for ICMPv6.

Table 12 shows the Containerized Decomposed Media Server support for ICMP Destination Unreachable codes as defined in RFC 792.

Table 16. Containerized Decomposed Media Server Support for ICMP Destination Unreachable Codes

Destination Unreachable ICMP Code	Support	
	Receive	Transmit
Net Unreachable	Supported	Not Supported
Host Unreachable	Supported	Not Supported
Protocol Unreachable	Supported	Not Supported
Port Unreachable	Supported	Supported
Fragmentation Needed and DF Set	Supported	Not Supported
Source Route Failed	Supported	Not Supported

When the Containerized Decomposed Media Server receives an ICMP Destination Unreachable message for ICMPv6, a Packet Too Big message, it executes a backoff procedure, to allow for the possibility that the UDP port is slow to initialize, or that a router is temporarily unavailable, but will soon recover. This is based on the received message, which indicates that the port does not exist, is no longer reachable, or that it is larger than the MTU for the path. The Containerized Decomposed Media Server stops sending media for an interval, which lengthens with each subsequent received message. The RTP stream is stopped permanently after the nth backoff where n is the configured number of retries.

Other types of ICMP messages can be received during backoff periods. For example, when roundtrip delays are larger than the packetization interval or when video sent in bursts causes a burst of returned ICMP messages.

RTP Stream Timeout

The MSML interface can detect and report the loss of incoming RTP packets on a port. When the RTP stream timeout feature is enabled for a port, the Containerized Decomposed Media Server monitors the received RTP packets. If no packets are received within the configured timeout period, the Containerized Decomposed Media Server sends an MSML event.

The timeout period for a port can be changed mid-call. This can be done before or after the expiration of a previously set period.

NAT Traversal of RTP Packets

Network Address Translation (NAT) maps an entire subnet network (the private subnet) on to a second subnet (the public subnet) that has fewer IP addresses than the private subnet. NAT translates the IP addresses and port numbers of packets that pass through it by mapping the private local addresses and port numbers to a smaller range of IP addresses and port numbers on the public subnet.

Because the local IP address and port number negotiated by an end terminal located on the private network are only valid behind the NAT, they cannot be used by the Containerized Decomposed Media Server to send RTP packets to the end terminal. To allow a device on the public network to determine the equivalent public destination address and port number of the private device, one solution is to inspect the source address and port number on incoming RTP packets after they are translated by the NAT. This solution is called symmetric RTP.

If symmetric RTP is enabled in the management interface, the Containerized Decomposed Media Server uses the source address and port number of incoming RTP packets as the destination for outgoing RTP packets. If symmetric RTP is disabled, the Containerized Decomposed Media Server uses the address and port number as negotiated through SDP as the destination for outgoing RTP packets.

For symmetric RTP to work, the end terminal must be configured to send RTP traffic. The end terminal does not receive any RTP packets from the Containerized Decomposed Media Server until it has sent at least one RTP packet and the packet passes successfully through the network to the Containerized Decomposed Media Server. If the end terminal is configured for receive-only operation, or if its RTP packets are suppressed due to silence suppression, the Containerized Decomposed Media Server does not send any RTP packets.

To avoid delays in sending to terminals that are not located behind a NAT and with symmetric RTP enabled, the Containerized Decomposed Media Server starts sending to the address and port as negotiated through SDP. If the end terminal is not located behind a NAT, the source address of the incoming RTP packets matches the SDP information and no change takes place. If the end terminal is located behind a NAT, the Containerized Decomposed Media Server initially sends to the wrong destination. These packets may be simply ignored by the network or they may attract ICMP Destination Unreachable messages, in which case the Containerized Decomposed Media Server begins its normal ICMP back-off procedure. The arrival of the first incoming RTP packet with a source IP address that does not match the one negotiated by SDP causes the Containerized Decomposed Media Server to start sending to the new address.

The Containerized Decomposed Media Server checks the source IP address for changes any time it synchronizes to the timestamps of the incoming stream. This occurs on receipt of the first RTP packet. It also occurs after receiving three consecutive RTP packets with a timestamp outside of the jitter buffer range. The Containerized Decomposed Media Server assumes that the source IP address does not change for RTP packets that arrive within the jitter buffer range.

Interactive Connectivity Establishment

The Interactive Connectivity Establishment (ICE) functionality interworks with different end-points as a solution for the Network Address Translator (NAT) traversal issues for Voice over IP (VoIP) applications. The presence of NAT in a VoIP network creates an issue in communication between the endpoints. The NATs assign private IP addresses to their endpoints behind the NAT and provide private-public address mapping when the endpoints communicate outside the NAT.

The ICE technique in NAT traversal for UDP-based multimedia sessions are established with the offer/answer model. ICE solves NAT issues for the media streams. ICE uses the Session Traversal Utilities for NAT (STUN) protocol and its extension, Traversal Using Relay NAT (TURN) protocol, and can be used by any protocol utilizing the offer/answer model. For example, SIP.

STUN. STUN protocol enables a device to discover its public IP address.

TURN. TURN protocol enables a server to relay data packets between the devices.

The Containerized Decomposed Media Server supports ICE Lite, Full ICE, and Trickle ICE to communicate its public IP address and connect to other devices.

NOTE: The Containerized Decomposed Media Server supports ICE on the MSML and **sip:conf** service context.

Full ICE

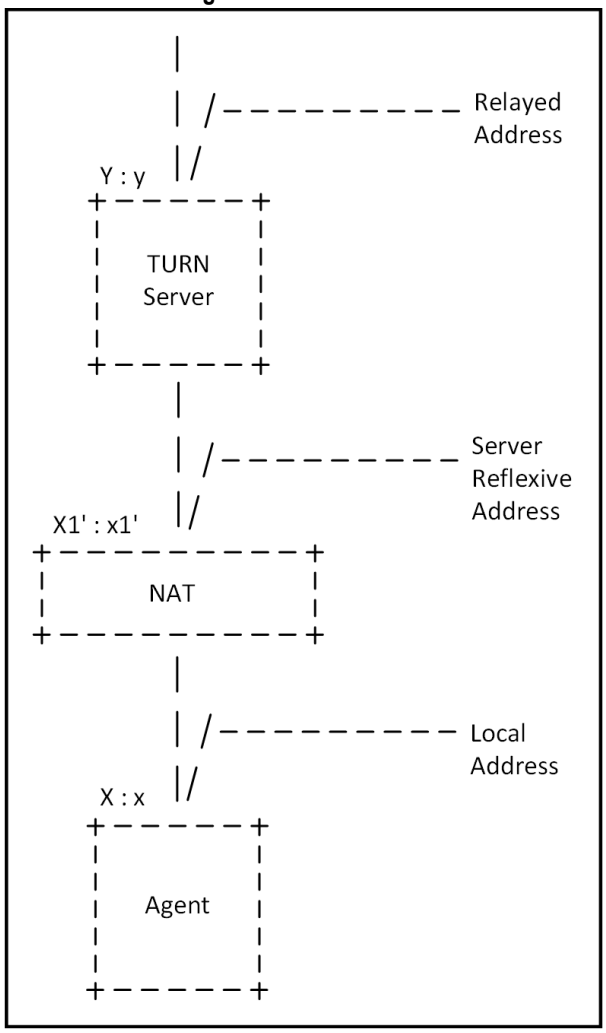
Full ICE is a full implementation of ICE. The Full ICE implementation in Containerized Decomposed Media Server adheres to the following ICE processing phases in a sequential manner.

- **Gathering the candidate addresses.** The endpoints supporting the ICE determine whether they are behind the NATs or not. The endpoint sends the STUN binding request and the STUN server replies with the IP address. If the endpoint is behind the NAT, the address is visible to the STUN server, which is different than the endpoints local host address. If the TURN server is present, both the endpoints can communicate using the TURN server.

  There are three types of candidates.

  - **Host Candidate.** A candidate is obtained by binding to a specific port from an IP address on the host.
  - **Server Reflexive Candidate.** A candidate whose IP address and port are binding allocated by a NAT for an agent when it sends a packet through the NAT to a server.
  - **Relayed Candidate.** A candidate is obtained by sending a TURN allocate request from a host candidate to a TURN server.

Figure 17. Full ICE



- **Sorting of the candidates.** After the agent has gathered its candidates, it assigns each candidate with a priority value and sorts the candidates from high priority to low priority. The priority algorithms are designed to prefer direct routes over indirect routes, which has multiple media relays and NATs.
- **Offering and answering.** After the ICE candidates are gathered and sorted, the calling agent includes them in the SDP offer for each media. If the called party also supports ICE, the called party performs the same gathering of the candidate, sorting the candidate, and encodes them in the SDP answer.
- **Connectivity checks.** After the SDP offer/answer exchange, each agent has a complete list of both its candidates and peer's candidates, resulting in CANDIDATE PAIRS.

  Each agent schedules a series of connectivity CHECKS to find out which CANDIDATE PAIRS are feasible. ICE checks are performed in a specific sequence, starting from high-priority CANDIDATE PAIRS to the lower-priority CANDIDATE PAIRS. The ICE assigns one of the agents role as CONTROLLING AGENT and the other role as CONTROLLED AGENT. The CONTROLLING AGENT nominates the CANDIDATE PAIRS that is used for the media and the same is flagged in the STUN request.

ICE Lite

The ICE-Lite is a minimal version of the ICE specification, intended for servers running on a public IP address. ICE-Lite is easy to deploy and requires the Containerized Decomposed Media Server to answer only the incoming STUN binding requests.

The ICE-Lite procedure starts with the offerer discovering all the IP ports where it is reachable. These are known as local candidates. A host candidate is obtained by binding to a specific port from an IP address on the host. The Containerized Decomposed Media Server supports only the host candidate for any media stream.

After completion of the SDP offer/answer exchange, the far-end acts as an ICE controlling agent and performs connectivity checks between the candidate pairs (from the local candidate to the remote candidate) by sending STUN messages. The Containerized Decomposed Media Server acts as a **controlled agent** and responds to the STUN requests. Based on the connectivity check result, the **controlling agent** selects a candidate pair (includes candidate and peer's candidate) to exchange the media.

Trickle ICE

Trickle ICE is an extension of Full ICE. Trickle ICE enables the ICE agents to send and receive the candidates incrementally rather than waiting to exchange a complete candidate list. The ICE agents can begin the connectivity checks while they are still gathering the candidates, by incrementally exchanging the candidates over time instead of all at once. This considerably accelerates the process of establishing a communication session.

NOTE: The Containerized Decomposed Media Server currently supports only Half Trickle ICE implementation and does not support incremental exchange of the candidates with the peer. However, the Trickle ICE related SDP parameters are supported.

For more information, see *Configure SIP on page 197* and *Configure ICE on page 336* on page 250.

RTP Media Multiplexing

The Containerized Decomposed Media Server supports RTP media multiplexing, also known as BUNDLE, an SDP grouping framework extension defined in RFC 5888. BUNDLE defines using one single transport, referred to as BUNDLE transport (**address:port**), for audio and video media flows for a call. The SDP offerer and the answerer negotiate a single BUNDLE **address:port** and the set of BUNDLE attributes that applies to all the `m=` sections within a BUNDLE group. All RTP-based bundled media streams within a given BUNDLE belong to a single RTP session. The BUNDLE framework is backward compatible; that is, when a given endpoint does not understand BUNDLE, both offerer and answerer can use a separate **address:port** for each `m=` line. This feature is applicable only in the MSML and `sip:conf` service contexts.

The Containerized Decomposed Media Server allows you to enable or disable **RTP Media Multiplexing** through the management interface. The Containerized Decomposed Media Server allows you to configure the **Media ID** through the management interface. The **Media ID** value is negotiated through the SDP offer/answer and is set in the RTP extension header for Bundle support in Containerized Decomposed Media Server offer call flow.

For information on the configurations, see *Configure RTP on page 235* and *SIP Interface Reference*.

Control Protocol Features

SDP Capability Negotiation

The SDP capability negotiation framework is defined in RFC 5939, and it extends the SDP offer answer exchange procedure defined in RFC 3264 with capability negotiation parameters and associated offer/answer procedures. The SDP capability negotiation framework provides support for indicating capabilities and their associated potential configurations, and negotiate the use of those potential configurations as actual configurations. It also defines how to provide attributes and transport protocols as capabilities and negotiate them using the framework.

The SDPCapNeg feature works when the Containerized Decomposed Media Server is an offerer and SDPCapNeg is enabled along with RTP/AVPF through OAMP. The Containerized Decomposed Media Server supports SDPCapNeg feature as answerer even if SDPCapNeg is disabled and an offerer contains the SDPCapNeg.

The Containerized Decomposed Media Server supports SDPCapNeg mechanism in the following service contexts.

- sip:annc
- sip:conf
- sip:tc
- sip:dialog
- sip:msml
- sip:monitor

NOTE: The Containerized Decomposed Media Server supports SDPCapNeg for audio ports in mono mode and ignores in stereo mode.

For more information on SDP Capability Negotiation, refer to SIP Interface Reference. For information about setting up and configuring SDP Capability Negotiation, see *Configure SIP on page 197*.

Call Progress Analysis

The call progress analysis (CPA) feature, when enabled allows the Containerized Decomposed Media Server to detect and forward call progress events to the control agent and Containerized Decomposed Media Server generates the notification if requested.

CPA is often used for IP Contact Center (IPCC) out-bound dialing applications to accurately and rapidly interpret events occurring after a call is sent or originated. The Containerized Decomposed Media Server monitors the RTP audio and informs the control agent of the call progress.

CPA consists of the following components:

- Call progress tone detection (CPTD)
- Call progress voice activity detection (CPVAD)
- Call progress answering machine detection (CPAMD)

CPA is supported only on the Containerized Decomposed Media Server SIP/MSML 1.1 interface. To use CPA, the SIP control agent sets up an Containerized Decomposed Media Server port with CPA enabled before initiating call setup with the far-end terminal. Subsequently, the Containerized Decomposed Media Server detects and forwards call progress events to the control agent in SIP INFO messages.

The Containerized Decomposed Media Server supports detection of the following call progress tones as defined by the ITU E.180/Q.35 Technical Characteristics of Tones for the Telephone Service, ITU T.30 Real Time Fax Termination, and ITU V.21 standard:

- Ringback
- Busy
- Reorder (Fast-Busy or Congestion)
- Dial Tone
- Special Information Tone (SIT)
- Modem/fax called station identification (CED)
- V.21 flag (to identify fax vs. modem answer)

The Containerized Decomposed Media Server can detect in band call progress tones using any of its supported audio codecs. Although any audio codec can be used, G.711 a-law or G.711 µ-law is recommended for reliable tone detection. RFC 2833 out-of-band call progress tones are not supported.

Tones vary considerably in frequencies and timing from country to country, and this can give varying results. The Containerized Decomposed Media Server default values for CPA settings detect CPA events in most countries.

CPA can be used in IP based call center out-bound call services. The AS assigns a port on the Containerized Decomposed Media Server with CPA attribute enabled before initiating a call setup to the far-end terminal. The Containerized Decomposed Media Server detects and forwards the call progress events to the AS using SIP INFO messages. As part of the call progress analysis, the Answering Machine Detection (AMD) identifies the contact as either a real person or an answering machine. This identification involves audio energy detection

followed by a period of silence. This approach has many challenges such as human answering too long, accurate speech detection, and background noise that can lead to an incorrect identification. The Containerized Decomposed Media Server provides configurable CPA attribute parameters such as `SilenceLong`, `SilenceShort`, `SilenceTime`, `SilenceLevel`, and `GreetingTime`, so that the AS can customize its logic for answering machine detection. Based on these two attribute values, the Containerized Decomposed Media Server generates two events —`CP_VOICE_END` and `CP_GREETING`, which allows the AS to distinguish between a real person and an answering machine.

The Containerized Decomposed Media Server defines 13 new attributes along with the "template" attribute in an MSML `<cpa>` request on per call basis. These attributes allow the user to configure the thresholds and parameters of the call progress events that the Containerized Decomposed Media Server generates.

- When neither the *"template"* attribute nor the 13 new attributes are present in the MSML `<cpa>` element, the Containerized Decomposed Media Server accepts the request and applies the CPA settings as per the default template *"0"*.
- When the *"template"* attribute and any newly defined attributes are present in the `<cpa>` element, the Containerized Decomposed Media Server overrides the threshold and parameters values defined in the template with the values of the newly defined attributes.
- When only *"template"* attributes are present in the `<cpa>` element, the Containerized Decomposed Media Server applies the CPA settings as per the user-defined CPA template configured through the management interface.
- When one or more of the newly defined attributes are present in the MSML `<cpa>` element and *"template"* attribute is not included, the Containerized Decomposed Media Server overrides the threshold and parameters values defined in the default template *"0"* with the values of the newly defined attributes.

For information on call progress analysis, refer to the *Radisys MSML Interface Reference*.

Beep Tone Detection

Beep tone is a single frequency pure tone of any length configured by the answering machine manufacturer. Some answering machines may have custom tones as their Answering Machine Detection tones. The Containerized Decomposed Media Server supports single frequency beep tone detection.

The Beep tone detection feature allows the Containerized Decomposed Media Server to detect beep tones at the end of the answering machine message and reports the same to the AS on successful detection. The user can leave a pre-recorded message at the end of the greeting and use the beep tone as an indicator that the greeting has been ended.

The Containerized Decomposed Media Server starts the answering machine Beep tone detection on a call session where the CPA is negotiated at the beginning of the call.

The Beep tone can be enabled in a CPA session in Containerized Decomposed Media Server through the MSML service. The Containerized Decomposed Media Server provides following optional attributes in the `<CPA>` element.

- **am-beep-bitlist.** Specifies the classes of beep tones to be detected and represented as a bit-field. A bit-value 1 enables the detection of the respective class of beep tone; and a bit-value 0 disables the beep tone detection. When the `am-beep-bitlist` attribute is absent, the Containerized Decomposed Media Server considers it disabled by default.

  In the scenario, the classes of Beep tones to be enabled is not known specifically, the recommendation is to enable all the classes of Beep tones for detection with the value 14,384 ms.
- **am-beep-time-out.** Specifies the time out interval (in ms) for detection of answering machine beep tones after the start of a CPA session. The recommended timeout value is 33,000 ms.

The Containerized Decomposed Media Server keeps the answering machine Beep tone detection ON until the following conditions are fulfilled.

- An answering machine Beep tone is detected.
- Beep time-out is detected.

The Containerized Decomposed Media Server disables the Beep tone detection based on the following conditions.

- Beep tone is detected successfully.
- Beep time-out is detected.
- Call progress analysis is terminated internally due to any internal CPA event.
- CPA `<dialogend>` through MSML.
- Termination of the call.

NOTE:

- The detection accuracy of answering machine Beep tone is affected by the lossy compression schemes. The reliability of Beep tone detection is better with non-lossy compression schemes such as G.711 and G.722.
- The Containerized Decomposed Media Server detects the beep tones greater than or equal to -40 dB in amplitude.

For information on `<cpa>` element attributes, refer to the *Radisys MSML Interface Reference*.

Containerized Decomposed Media Server Load Balance

The Containerized Decomposed Media Server supports both Round-Robin and Dynamic-Feedback load balancing methods for selecting MRFP where initial invite request is forwarded. For this feature to function, load balancing method must be set to same value in both MRFP and MRFCtrl. You can configure the load balancing method on MRFP through the management interface, see *Configure SIP Load Balancing on page 312* and MRFCtrl through the configuration (*mrfctrl.cfg*) file, see *MRFC Configuration on page 509*.

When the Dynamic-Feedback method is configured, MRFPs report their current resource utilization to MRFCtrl at regular intervals through the `SIP-REGISTER` request of the *kpiInfo* service context. MRFP reports the following resource utilization.

- Average CP CPU utilization
- Average modelled audio DSP utilization
- Average actual audio DSP utilization
- Memory utilization
- Media interface bandwidth utilization

For more information on the `SIP-REGISTER` request, refer to the *SIP Interface Reference*.

MRFCtrl evaluates the resource utilization for each MRFP and re-bucketizes based on the current resource utilization information reported by each MRFP. Following are the bucketization criteria for an MRFP in a bucket.

- **bucket1.** MRFPs are in bucket1, if the resource utilization of all the monitored resources of an MRFP is below the **Slab1** threshold value (by default, the value is 40%).
- **bucket2.** MRFPs are in bucket2, if the resource utilization of all the monitored resources of an MRFP is above the **Slab1** threshold value (by default, the value is 40%) and below the **Slab2** threshold value (by default, the value is 60%).
- **bucket3.** MRFPs are in bucket3, if the resource utilization of all the monitored resources of an MRFP is above the **Slab2** threshold value (by default, the value is 60%) and below the **Slab3** threshold value (by default, the value is 80%).
- **bucket4.** MRFPs are in bucket4, if the resource utilization of all the monitored resources of an MRFP is above the **Slab3** threshold value (by default, the value is 80%).

NOTE: Slab values are the maximum threshold levels of the buckets in a configuration file (*mrfctrl.cfg*) on MRFCtrl. The administrator configures these slab values in the *mrfctrl.cfg* file. Any changes to the threshold level requires a reboot to take effect. For more information on how to configure the slab value, see *MRFC Configuration on page 509*.

MRFCtrl routes the new calls to one of the MRFPs as per the following guidelines.

- For any bucket, the MRFCtrl routes the calls in the Round-Robin method.
- MRFCtrl routes the new calls to one of the MRFPs as per the following guidelines.
  - If bucket1 is not empty, the MRFCtrl routes the new call to one of the MRFPs in bucket1.
  - If bucket1 is empty, the MRFCtrl routes the new call to one of the MRFPs in bucket2.
  - If bucket2 is empty, the MRFCtrl routes the new call to one of the MRFPs in bucket3.
  - If bucket3 is empty, the MRFCtrl routes the new call to one of the MRFPs in bucket4.
- In a given bucket, MRFCtrl maintains a list of registered MRFPs. MRFPs are added to the list in the order in which SIP-REGISTER requests are received from the MRFPs. The MRFCtrl routes new incoming calls to the next MRFP instance in the list. If MRFCtrl reaches the end of the list, the MRFCtrl picks the first MRFP instance from the list in the bucket. For example, instances P7, P5, and P2 belong to bucket 1, are registered with MRFCtrl in same

order, and MRFCtrl has routed the previous call to P5, the MRFCtrl routes the next call to P2. If P2 has moved into bucket 2 before the next call is presented, the MRFCtrl routes the next call to P7.

The de-registered MRFPs are not considered for bucketization and call routing.

The **Round-Robin** load balancing method is recommended when the deployment has similar complex codec ports to obtain the even distribution of Media resources across multiple MRFPs. The **Dynamic-Feedback** load balancing method is recommended when the deployment has a combination of different complex codecs ports, to obtain the even distribution of Media resource across multiple MRFPs.

Management Features

Single Sign-On with SAML

The Containerized Decomposed Media Server Web GUI supports user authentication using Security Assertion Markup Language (SAML) 2.0 standards to provide single sign-on (SSO) functionalities, in addition to the user authentication. The Containerized Decomposed Media Server Web GUI passes the SAML artifact through the SAMLart URL parameter.

Figure 18. SAML Architecture

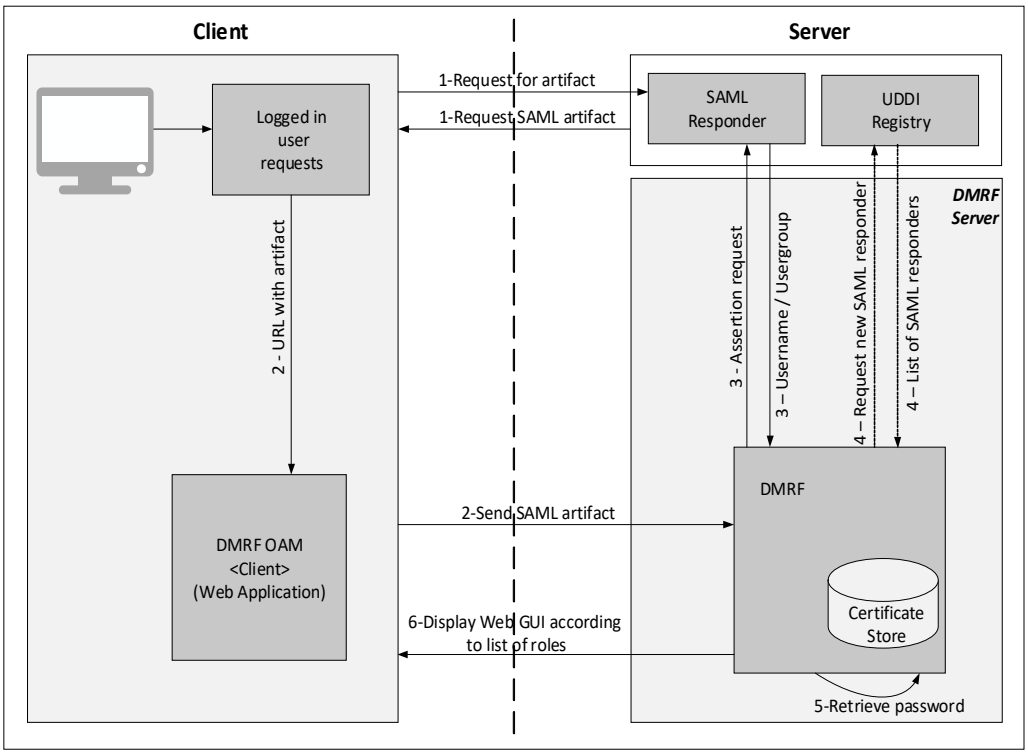


Figure 18 shows the SAML architecture. The call flow is a follows:

1. The SSO portal sends a request to the SAML responder including user information and how the user is authenticated. In response, the SAML responder returns an artifact (a short encoded string) on the complete user authentication data. The SAML responder URL is directly encoded in the artifact.
2. The user is directed to the Web GUI home page with the SAML artifact passed through the URL parameter **SAMLart**. The following is an example URL for the Web GUI home page with a SAML artifact.

   ```
   https://<Containerized Decomposed Media Server's management
   address>/ms.cgi?SAMLart=AAJe80priKjVhOLT%2F3gzwv4iys85QWh0dHBzOi8vc2FuZTUtZGV2L
   nZoLmVuZy52endjb3JwLmNvbS9zZXJ2aWNlcy9zZXJ2aWNlcy9TQU1MUmVzcG9uZGVy
   ```
3. The Web GUI extracts the SAML responder URL from the artifact and sends the assertion request regarding the arriving user. The SAML responder returns the assertion containing the user's credentials (name, role, and so on).
4. The Web GUI requests a list of alternative SAML responder URLs from the UDDI registry, if the previously extracted SAML responder URL is unreachable. Repeat Step 3 using the listed URLs in succession until a valid responder is found.
5. The Containerized Decomposed Media Server does not verify the password corresponding to the user group.
6. The user logs on to the Web GUI. The Web GUI displays the page according to list of roles.

The Containerized Decomposed Media Server allows the user to login though the SAML interface even when a user is deactivated due to password expiry or failed direct login attempt. The Containerized Decomposed Media Server does not allow the user to login through the SAML interface if the user is disabled or locked. The Containerized Decomposed Media Server does not prompt for password change on the first login, when the user logs in through the SAML interface and the password complexity is configured as complex.

NOTE: The SAML user must be provisioned locally on the Containerized Decomposed Media Server for successful authentication.

For more information about the SAML interface, refer to the *Radisys Special Interfaces Reference*.

Announcement Lab

Containerized Decomposed Media Server supports AnnLab for media clip provisioning and transcoding. AnnLab is an environment to manage the internal media server announcement clips on the Containerized Decomposed Media Server. It provides the following functionality.

- Upload clips from any source such as CD-ROM, disk
- Upload different clips to MRFPs
- Transcode the clips in advance to avoid transcoding while playing an announcement

- MRFP synchronizes the clips from the AnnLab container and generates the transcoded clips for the configured list of codecs. The Containerized Decomposed Media Server generates the transcoded clips in only G.711, AMR, AMR-WB, G.722, G.729, and EVS codecs.
- AnnLab supports uploading clips in *wav, qt*, mp3, *mov*, *3gp*, *3g2*, *amr*, and *awb* announcement file extensions.
- When optimal clip selection is enabled and an announcement is played on the EVS (AMR-WB-IO Mode) port, the Containerized Decomposed Media Server selects playing the clip in the following sequence.
  - EVS (AMR-WB-IO Mode) clip with corresponding mode of EVS (AMR-WB-IO Mode) port
  - AMR-WB clip with corresponding mode of AMR-WB port
  - Base clip
- AnnLab generates transcoded clips in *wav and 3gp* formats. The Containerized Decomposed Media Server generates the transcoded clips as per the optimal clip selection naming convention, see Table 9. The transcoded clips for each codec must follow the extension specified in Table 10. When the AnnLab client fails to generate the transcoded clip from the original clip, the Containerized Decomposed Media Server raises an alarm 201 *AnnLab transcoding failure alarm for: Clipname-X, Hostname-Y*.

  For information on the AnnLab transcoding alarm Web GUI configurations, see *Configure Alarms*.
- AnnLab does not generate the transcoding clips for video-only and multimedia clips.

Table 17 lists the media type used by AnnLab for each codecs file.

Table 17. AnnLab Supported Codec and File Extensions

Input Codecs	Input File Extension	Media Type in AnnLab	Output Codecs
Transcoding			
PCMA and PCMU	wav	audio/g.711	PCMU, PCMA, AMR, AMR-WB, EVS, G.722, and G.729
PCM	wav	audio/pcm	
G.722	wav	audio/g.722	
G.729	wav	audio/g.729	
AMR	amr	audio/amr	
AMR-WB	awb	audio/awb	
AMR, AMR-WB, and EVS	3gp	video/3gp	
MP3 files	mp3	audio/mp3	
Transcode Bypass			
EVRC, EVRC-B, EVRC-NW, and H.264	3g2	video/3g2	EVRC, EVRC-B, EVRC-NW, and H.264
H.264	3gp	video/3gp	H.264
	qt	video/qt	
	mov	video/mov	

These codecs can be configured in the JSON file. To change the transcoder options, see *JSON File Configuration on page 513*.

- Transcoding time and disk space requirement.
  - AnnLab requires approximately 40 seconds to transcode a 10 second WAV clip completely and generate about 58 transcoded optimal clips on MRFP.
  - The AnnLab client container generates the transcoded clips in the OAMP pod. These transcoded clips are stored in the AnnLab client PVC, which is mounted on AnnLab client container for all the MRFPs.
  - The Containerized Decomposed Media Server requires additional AnnLab client PVC to store the generated transcoded clips. For example,
    - AnnLab consumes approximately 2.1 MB of memory for offline transcoding of 1 WAV, MP3, or 3GP audio clip of 10 seconds.
    - For 1000 uploaded WAV, MP3, or 3GP clips each of 10 seconds, AnnLab consumes approximately 2 GB of disk space for storing the generated offline transcoded clips.
    - AnnLab consumes approximately 25 GB of disk space for offline transcoding of 12,500 WAV, MP3, or 3GP audio clips, each of 10 seconds.
      NOTE: An additional 3 GB ephimeral storage is required, if the **isSecretRepoEnabled** parameter is set to true in the *values.yaml* file.
    - If the AnnLab client PVC is created with 25 GB, so 12,500 clips each of 10 seconds can be loaded on the Containerized Decomposed Media Server.
    - For 5 seconds audio clip (WAV, MP3, or 3GP), 1 clip, 1000 clips, and 12,500 clips consumes approximately 1.2 MB, 1.2 GB, and 15 GB of disk space, respectively.
    - For 60 seconds audio clip (WAV, MP3, or 3GP), 1 clip, 1000 clips, and 1,750 clips consumes 14 MB, 14 GB, and 24.5 GB of space, respectively.
    - For the provisioning of 12,500 clips (total 2 Gi size), which includes audio and video clips, 3 Gi AnnLab-PVC, and 5 Gi OAMP-PVC (total 21 Gi) are required. This calculation depends on the clip count and clip size.
    - Minimum of 1 Mi AnnLab-PVC, AnnLab Client-PVC, and 15 Mi OAMP-PVC storage size is required for Containerized Decomposed Media Server deployment when there is no AnnLab clip provisioning.
  - Transcoding clips are not generated on the MRFC. The MRFC requires double the space of the input clips size to store the clip on MRFC. For example, on MRFC,
    - If the input file is 100 KB, you need approximately 200 KB of space for storing the clip.
    - For 5 seconds audio clip (WAV, MP3, or 3GP), 1 clip, 1000 clips, and 12,500 clips consumes approximately 160 KB, 160 MB, and 2 GB of space, respectively.
    - For 10 seconds audio clip (WAV, MP3, or 3GP), 1 clip, 1000 clips, 12,500 clips consumes 160 KB, 160 MB, and 2 GB of space, respectively.
    - For 60 seconds audio clip (WAV, MP3, or 3GP), 1 clip, 1000 clips, and 1,750 clips consumes 1.1 MB, 1 GB, and 1.9 GB of space, respectively.
  - For video clips, AnnLab does not generate the transcoding clips. The MRFC or MRFP requires double the space of input clips size. For example, if the input file is 500 KB, approximately 1 MB of space is needed on the MRFC or MRFP for storing the clip.

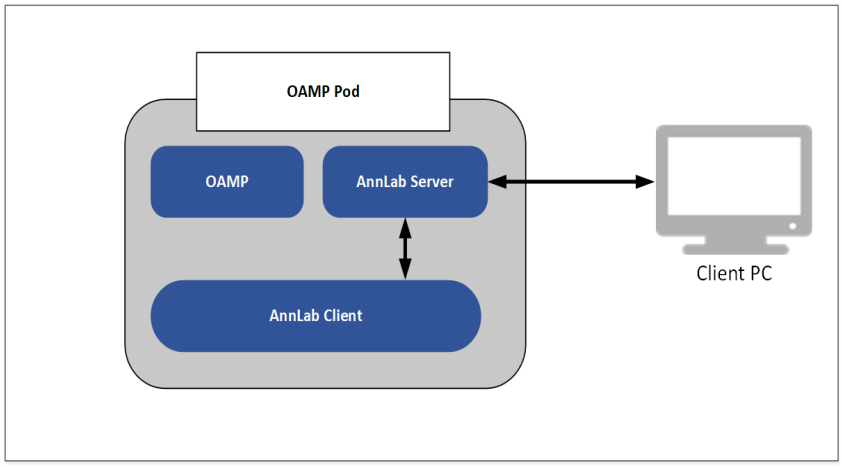
- Maximum of 12,500 clip uploads are supported using the AnnLab. Bulk clip upload, backup, and restores are supported with a maximum of 12,500 clips.
- You need to use NFS or HTTP for clips storage if the number of clips crosses the recommended memory specification.

However, the Containerized Decomposed Media Server provides a configuration JSON file (txConfig.json) on AnnLab container, at */opt/swms/cfg/modules/txConfig.json*. Changes in this configuration file are synchronized automatically with each MRFP after restart. The *txConfig.json* file is modified to select the list of desired generated clips. The specific sections of the codec formats in the JSON file can be removed or modified to reduce offline transcoding time and disk space requirements.

As shown in Figure 19, the AnnLab component has two modules.

- **AnnLab server.** This module runs as a container within the OAMP pod. The user is connected to the AnnLab server using the management interface floating IP. It provides the Web GUI and REST API access for the user to load the clips onto the OAMP PVC storage. When the user provisions the clip, the AnnLab server uploads the clip to the PVC storage. The AnnLab server creates and manages the clusters, Virtual File System (VFS), folders, and clips, and manages bulk upload, clip play, and audit functionalities.
- **AnnLab client.** This module runs on the AnnLab client container within the OAMP pod. During the start-up, it syncs the provisioned clips from the AnnLab server to the AnnLab client PVC. This AnnLab PVC is mounted on all MRFP pods. Any change in the provisioned clips is updated in the AnnLab client container.

Figure 19. AnnLab Module



NOTE:

- Currently, all the MRFPs are grouped under a single cluster. They share the same set of clips.
- The AnnLab server and client configuration parameters and transcoding codecs are present in the respective *.cfg* files. These configuration parameters and transcoding codecs are configured to the default values and included in the package. The Containerized Decomposed Media Server does not support configuring or accessing these configuration values through the management interface.

For more information announcement lab configurations, see *Announcement Lab on page 347*.

Performance Management Features

Codec High Watermark

The Codec High Watermark feature enables you to track maximum codec usage.

The Containerized Decomposed Media Server supports the following for codec high watermark:

- Sets all high watermarks to zero for a new installation
- Uses the following algorithm to calculate the high watermark:
  - The watermark for a licensed entity (for example, a codec) is determined by adding the maximum licenses in use over the Containerized Decomposed Media Server
  - If the total value is greater than the previously saved, the saved value is updated with a new value

  NOTE: The high watermark value increases when there is an increase in resource usage.
- Calculates the high watermarks for every 10 seconds
- Preserves the high watermark values across the Containerized Decomposed Media Server reboots or upgrades
- Preserves the high watermark values across database backup or restore operations
- Provides read-only access to the high watermark values for each codec from the Web GUI and SNMP interface
- Tracks the high watermark for the following licensed entities that are available on the Containerized Decomposed Media Server.

Table 18. Codec High Watermark for Containerized Decomposed Media Server

High Watermark Licensed entities	Containerized Decomposed Media Server
G.711 codec (PCMU and PCMA)	Yes
G.722 codec	Yes
G.729 codec	Yes
AMR-NB codec (OA and BE)	Yes
AMR-WB codec (OA and BE)	Yes

Table 18. Codec High Watermark for Containerized Decomposed Media Server

High Watermark Licensed entities	Containerized Decomposed Media Server
EVRC codec	Yes
EVRC-B codec	Yes
EVRC-NW codec	Yes
EVS codec	Yes
H.264 codec (Mode 0 and Mode1)	Yes
VP8 codec	Yes
H.265 codec	Yes
Opus-NB codec	Yes
Opus-WB codec	Yes
PLC	Yes
Noise Reduction	Yes
T.140 codec	Yes
Keyword Detection (KWD)	Yes

For information about setting up and configuring Codec High Watermark, see *Show High Watermarks on page 470* and *SNMP Interface Reference*.

Security Features

Secure Media

The Containerized Decomposed Media Server implementation of secure media depends on control protocol and platform.

Secure Media for SIP

The SIP interface supports SRTP for secure media traffic for secure SIP communications with call agents.

The Containerized Decomposed Media Server supports the following security standards:

- RFC 3711 The Secure Real-time Transport Protocol (SRTP) from March 2004
- RFC 4568 SDP Security Descriptions for Media Streams
- RFC 6347 and 4347 for Datagram Transport Layer Security for DTLS handshake
- RFC 5763 and 5764 for DTLS extension

RFC 3711 provides confidentiality, message authentication, and replay protection for RTP traffic. RFC 4568 defines a cryptographic attribute for SDP that configures security for media streams. RFC 2401 protects traffic at the IP layer.

The Containerized Decomposed Media Server SIP interface supports SRTP for all media types except T.38 fax. However, SRTP cannot be used for the following RTP streams:

- Audio from external speech servers
- Audio for media replication (for example, as used in lawful intercept)
- RFC 4117 transcoding audio

SDES

The SDES, a key management protocol for SRTP, is a signaling plane key exchange scheme that enables the media sender to specify the distinct session keys and related security parameters (such as the key lifetime, the key index and the cryptographic algorithms) used to protect the media stream, through a SDP attribute **a=crypto**.

The Containerized Decomposed Media Server supports an SRTP replay protection with a window size of at least 64. Master Key Identifier (MKI) in SRTP is not supported and should not be sent to the Containerized Decomposed Media Server.

The Containerized Decomposed Media Server SIP interface supports sending and receiving the SDP **a=crypto** attribute. The attribute is always present when the Containerized Decomposed Media Server offers SRTP and must be present for the Containerized Decomposed Media Server to accept an SRTP offer.

The Containerized Decomposed Media Server supports the following values for crypto parameters:

- crypto-suite: **AES_CM_128_HMAC_SHA1_80** and **AES_256_CM_HMAC_SHA1_80**

  NOTE: The default encryption and authentication algorithm is **AES_CM_128_HMAC_SHA1_80**.
- key-params: **key** and **salt**

For more information, refer to the *SIP Interface Reference*.

Datagram Transport Layer Security

Datagram Transport Layer Security (DTLS) protocol is also known as TLS over datagram transport. DTLS provides authentication, data integrity, and confidentiality for communications between the two end-points over UDP. DTLS has additional capabilities such as sequence number and retransmission.

The Containerized Decomposed Media Server supports DTLS for SRTP/SRTCP streams only over a media network.

The end-point sends an **INVITE** request with fingerprint SDP attribute to establish DTLS based media sessions. The fingerprint SDP attribute has an encrypted digital certificate for the calling endpoint (Containerized Decomposed Media Server). The Containerized Decomposed Media Server validates the certificates received in the DTLS handshake against the finger print received in the SDP offer. The Containerized Decomposed Media Server performs a DTLS handshake between the local and far-end RTP and RTCP ports independently. The DTLS handshake can be initiated from either end-point based on the `setup` SDP attribute.

The DTLS protocol exchanges the security keys between the participating end-points using the SDP media path. Both the end-points send the X.509 certificate through either self-signed or a trusted third party. The public keys in a certificate are used for encryption by the sender and are exchanged through the DTLS. The private keys in a certificate are used for decrypting the RTP packets. The private keys are stored locally and never exchanged.

For more information, see *Configure RTP on page 235* and *SIP Interface Reference*.

Lawful Intercept

The Containerized Decomposed Media Server supports lawful intercept of the Call Content (CC) and delivers the intercepted content to the Lawful Intercept Gateway (LIG) over the X3 interface. To support lawful intercept of CC, Lawful Intercept Function (LIF) application server invokes the Containerized Decomposed Media Server by establishing a series of SIP dialogs between LIF and Containerized Decomposed Media Server.

Following are the purposes of the SIP dialogs.

- **To establish a *pass-through* path for each of the media streams involved in the user SIP session.** This enables the Containerized Decomposed Media Server to forward packets from one user involved in the user SIP session to the other. These pass-through paths are established for both directions of a user SIP session. The establishment of the pass-through paths require two SIP dialogs between the LIF and the Containerized Decomposed Media Server.
- **To establish a *replicated* (listener) media stream.** The Containerized Decomposed Media Server duplicates the media streams associated with the *pass-through* paths and forwards the duplicated paths to ports specified by the LIF. These ports initially correspond to a lawful intercept delivery function. The LIF establishes a SIP dialog for each direction of the user SIP session.

Containerized Decomposed Media Server supports the following interception modes.

- **Stereo mode.** In this mode, the Containerized Decomposed Media Server delivers the received and transmitted streams from the intercepted port, in two separate RTP streams to the LIG.
- **Mono mode.** In this mode, the Containerized Decomposed Media Server mixes the received and transmitted streams from the intercepted port, and delivers in a single RTP stream to the LIG.

  For more information, refer *SIP Interface Reference* and see *Configure Lawful Intercept on page 322*.

SIP over TLS

The Containerized Decomposed Media Server adds support for SIP over TLS as a transport protocol to establish a trust with the external SIP servers or trusted domains. The TLS protocol provides endpoint authentication using one-way or mutual authentication.

In one way authentication, the client authenticates the server; whereas in mutual or two-way authentication, both the server and client use certificates to authenticate each other. In the two way authentication, the client or server issue a certificate for authentication and a public key for encryption or decryption. After the sender is verified, the receiver sends its certificate to the sender for verification. SIP signaling starts after verification.

The MRFP supports all the TLS versions TLSv1.0, TLSv1.1, and TLSv1.2, whereas MRFCtrl and OAMP Pod supports only TLSv1.2 version. The Containerized Decomposed Media Server supports end-to-end TLS using transport =TLS in the Request-URI. When SIP over TLS is enabled through the management interface, the Containerized Decomposed Media Server listens on the SIP-TLS port for incoming connection requests.

For more information on SIP over TLS, see *Configure SIP on page 197*, *Configure TLS on page 333*, *and SIP Interface Reference*.

Networking Integration

This chapter is designed to help you integrate the Containerized Decomposed Media Server into your existing IP network in a cloud environment.

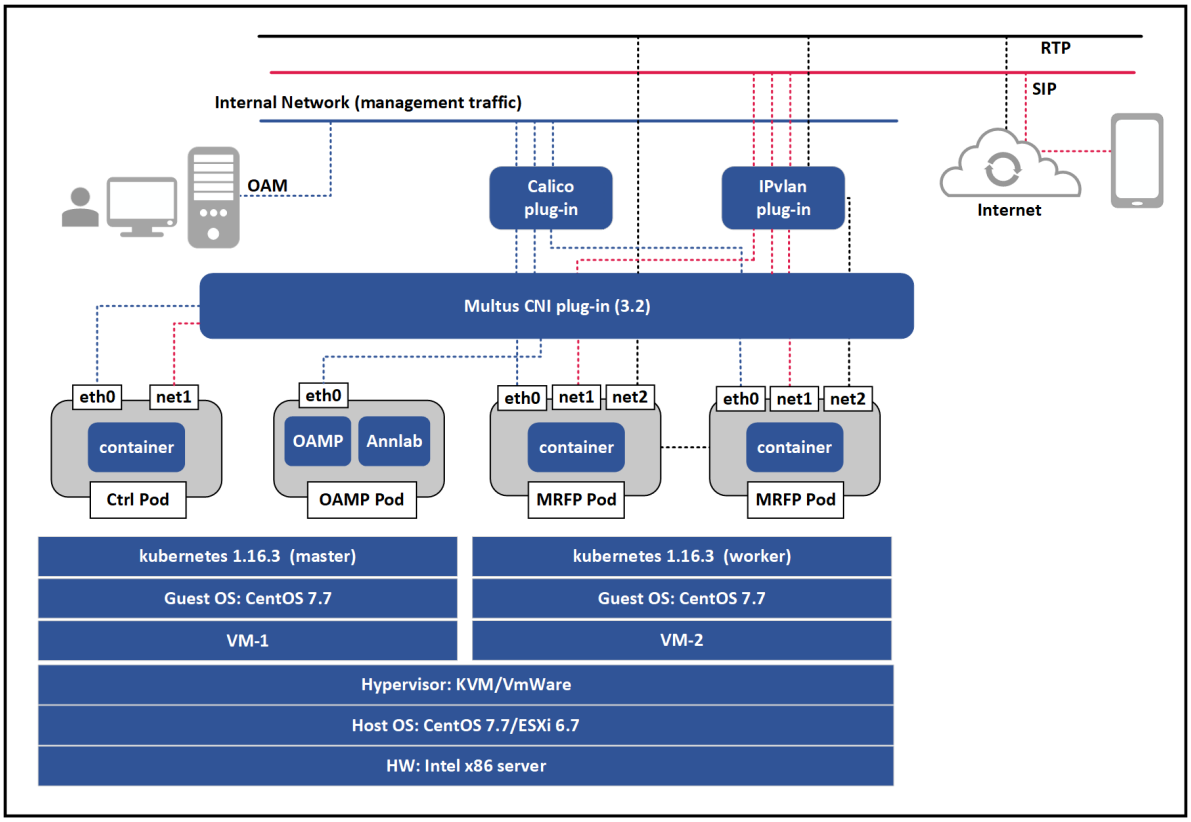
Network

The Containerized Decomposed Media Server requires the following network for deployment.

- **Management network.** This network is provided by calico. In each pod, it is represented by eth0.
- **Control network.** MRFCtrl pod and all MRFP pod requires a control network, which is provided by IPvlan plug-in over Multus. In MRFCtrl and MRFP pod, it is represented by net1.
- **Media network.** MRFP pod requires a media network, which is provided by IPvlan plug-in over Multus. In MRFP pod, it is represented by net2.

Figure 20. provides network topology of Containerized Decomposed Media Server.

Figure 20. Logical View of Containerized Decomposed Media Server Network Architecture



Connectivity to External Network

The Containerized Decomposed Media Server uses flat network topology for control and media interfaces to the provider (external) network directly without using the NAT. The management services (Web GUI and SNMP) hosted on management network (Calico) is accessible through node port service of Kubernetes.

For more information, refer to the *Containerized Decomposed Media Server Installation Guide*.

Layer 2 Connectivity (Ethernet)

The Containerized Decomposed Media Server requires full duplex Ethernet connections and must be connected to devices capable of full duplex communication. Connecting to half duplex devices may lead to traffic collisions, packet loss, and other traffic problems.

This means that you must connect the Containerized Decomposed Media Server infrastructure network adapters (used for IPVlan or Calico) to a switch, and not a hub. If you need to sniff the network traffic, you must use the port mirroring facility of the switch. They must be auto-negotiate, or they must both be set to the same speed.

Layer 3 Connectivity (IPv4 and IPv6)

The Containerized Decomposed Media Server is a multi-homed node: it can have multiple IP addresses assigned to multiple physical interfaces connected to different networks. The Containerized Decomposed Media Server supports IPv4 and IPv6 for control, media, and management interface.

For more information, refer to the *Containerized Decomposed Media Server Installation Guide*.

In the network examples given in this chapter, IPv4 addresses are typically shown. IPv6 addresses can be used as well.

For more information about IPv6, see *Appendix F, IPv6 Supported Notations, on page 623*.

Location of External Devices

All remote devices must be reachable using the configurable routes. In locating other devices, the main consideration is maintaining the Containerized Decomposed Media Server performance.

NFS Servers

The Containerized Decomposed Media Server routes NFS traffic based on the destination location.

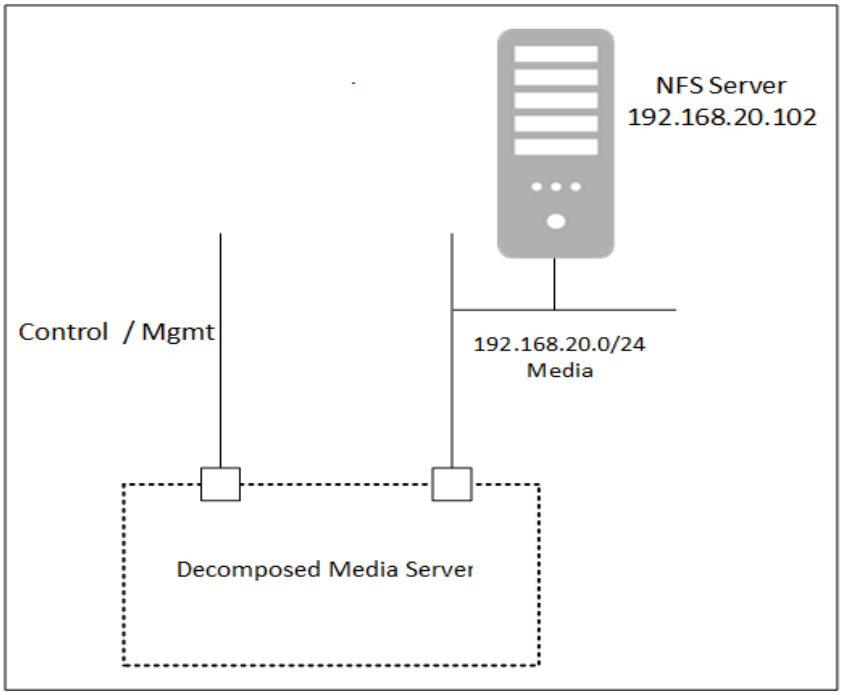
- When the server is on a local subnet, traffic is routed through the interface connected to that subnet.
- When the server is on a remote subnet, traffic routing is based on user-configured routes.

It is recommended that you directly connect the NFS server to the Ethernet port, as shown in Figure 21. In general, when using NFS servers with the Containerized Decomposed Media Server, all the effort must be made to reduce network latency.

It is recommended that you use an Ethernet port configured for media traffic. Routing NFS traffic through a control or management port may cause overload conditions.

The NFS server must be set up to inter-operate with the Containerized Decomposed Media Server. For information, refer to the *Radisys Special Interfaces Reference*.

Figure 21. Location of NFS Servers



HTTP Servers

The Containerized Decomposed Media Server uses IP routing rules plus any configured routes to route traffic to and from HTTP servers.

It is recommended that these devices be directly connected to the Containerized Decomposed Media Server. In general, every effort must be made to reduce latency for HTTP servers. It is also recommended that you use an Ethernet port configured for media traffic. Routing HTTP streams through a control/management port may cause overload conditions.

The HTTP server must be set up to interoperate with the Containerized Decomposed Media Server. For information, refer *Radisys Special Interfaces Reference*.

DNS Servers

The Containerized Decomposed Media Server uses Kubernetes DNS servers to resolve domain names to IP addresses. DNS service must be available for Containerized Decomposed Media Server to function correctly.

NOTE: To resolve DNS entry on MRFCtrl, configure **sipproxysubsystem.ini** manually in ***/opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini***.

Speech Servers

When media and control are on separate networks, speech servers should preferably use separate interfaces for control and media. They must either reside locally or be reachable using the configured routes.

RTSP Servers

RTSP servers must be on the media network. They must either reside locally or be reachable using configured routes.

Chapter 4

Security and Availability

The Containerized Decomposed Media Server security features help prevent access by non-authorized individuals and back-door entries through insecure ports.

Initial Access

The Containerized Decomposed Media Server supports the following features to control user access to the system. For a new installation, the following features apply.

- **Encrypted, configurable webadmin user ID and password.** A user ID and password are required to access the Web-based management interface. The system ships with a default user ID and password, which you can change using the management interface. This user ID has Level-1 access level and administrator privileges for the Containerized Decomposed Media Server.
- **swmsuser account.** The swmsuser is a CLI user.
- **Configurable idle session timeout.** The Containerized Decomposed Media Server sets a limit on how long a Web GUI session can remain idle. When this interval expires, the session is closed and the user is logged off. The default idle timeout is 15 minutes. You can change this interval using the Web GUI.
- **Configurable SNMP community string.** The SNMP community string provides basic security against spurious SNMP requests. The system ships with a default community string. You can change the default community string. This can be configured using the management interface.
- **GUI access.** The GUI is accessible through node port. For more details, refer to *Containerized Decomposed Media Server Installation Guide*.
- **Login to individual pods.** CLI login with root user can be done through `kubectl` command. For command details, refer to *Containerized Decomposed Media Server Installation Guide*.

User Access Control

The Containerized Decomposed Media Server controls user account access to configuration and data through its support of hierarchical permissions.

Access to Management Interfaces

Table 19 shows the different account types the Containerized Decomposed Media Server supports and access each has to its management interfaces.

Table 19. User Account Access to Interfaces

Account Type	SAML	NETCONF	Management-Interface Access	
			Web	SNMP
Operating System User: **webadmin** for Web GUI/SAML **snmpadmin** for SNMP **swmsadmin** for NETCONF (default password = convedia)	Y	Y (OAMP Pod)	Y (OAMP pod only)	Y (OAMP pod only)
Operating System User: root (Password is not set)	N	N	N	N
SNMP User	N	N	N	Y (OAMP pod only)
Locally Provisioned User	Y	N	Y (OAMP pod only)	N
NETCONF Users	N	Y (OAMP Pod)	N	N
LDAP Users	N	N	Y	N

NOTE: The system (Containerized Decomposed Media Server) local users and local groups with the same name must not be created in the LDAP server.

Account Access Levels (Hierarchical Permissions)

The Containerized Decomposed Media Server supports creating hierarchical accounts such that not every user is permitted the full range of configurations and actions that can be performed on the system. For example, you can allow some users read-only configuration data that other users are allowed to configure.

Support for hierarchical permissions differ for the following management interfaces and types of accounts:

- The Web-based management interface supports hierarchical permissions based on the defined access levels.
- The SNMP interface supports SNMPv3 user management.
- The NETCONF interface supports configuring common settings for all NETCONF clients through the management interface.

Web-Based Management Interface

For the Web-based management interface, you can set hierarchical permissions based on four pre-defined access levels: 1, 2, 3, and 4, with level 1 having the highest access. User accounts configured for any one of these access levels can perform only actions permitted to that level.

The Containerized Decomposed Media Server supports assigning an access level to locally provisioned user accounts. The operating system's Admin user account always retains the highest-level access.

Level 1 access can perform actions that may be restricted for accounts with lower access levels. An account with access level *n* is permitted all the actions of lower access accounts, that is, an account with access level 2 can perform all actions requiring access level 2, 3, and 4.

Table 20 shows the access level required for an account to be permitted to perform the different actions available to the Containerized Decomposed Media Server Web-based management interface.

Table 20. Permissions for Each Access Level

Permitted Action	Minimum Access Level
All (full read and write permissions for all configurations)	1
• Read and configure users • Configure password aging • Retrieve the management activity log	1 1 1
• Change configuration data • Backup and restore actions • AnnLab (announcement clip management)	2 2 2
• Reset statistics • Retrieve log packages • Acknowledge alarms	3 3 3
• Read configuration data • Change account password • Retrieve a reduced version of the management activity log	4 4 4

SNMP Interface

The Containerized Decomposed Media Server supports remote user management over SNMP. Typically this is done using an SNMPv3-capable MIB browser or management suite. New user accounts are created by cloning a factory-configured template and then applying View-based Access Control Model (VACM) views to the newly created account.

For more information about configuring access levels for SNMP users, refer the *SNMP Interface Reference*.

NETCONF Interface

The Containerized Decomposed Media Server supports NETCONF protocol for configuration and management functions. The `swmsadmin` user can perform NETCONF operations.

NOTE:

- If a LDAP authentication is enabled, you cannot create the NETCONF users and groups with the same name as that of the LDAP user and group respectively.
- If a LDAP authentication is disabled, you must not create the NETCONF users and groups with the same name as that of the LDAP user and group respectively.

For more information on configuring NETCONF operations, refer the *NETCONF Interface Reference*.

SAML Interface

The Containerized Decomposed Media Server Web GUI supports user authentication using SAML 2.0 standards to provide SSO functionalities. Only `swmsadmin` and `locally provisioned users` can access Web GUI through the SAML.

For more information, refer the *Special Interfaces Reference*.

Password Configuration

The Containerized Decomposed Media Server supports a number of policies designed to enhance password security.

Configurable Password Complexity

The Containerized Decomposed Media Server enforces rules on users of locally provisioned accounts when configuring passwords through its management interface. Two sets of such password rules are supported: basic and complex. Once one of these sets is configured for the Containerized Decomposed Media Server, all new passwords must meet that level of complexity to be accepted as valid for the account.

For Web users.

- **Basic Passwords.**
  - Passwords must be between 6 and 64 alphanumeric characters in length excluding a NULL terminator.
  - Passwords can include printable ASCII characters 0x20 through 0x7E.
  - Passwords are case-sensitive.
- **Complex Passwords.**
  - Passwords must be between 8 and 64 alphanumeric characters.
  - Passwords can include printable ASCII characters 0x20 through 0x7E, with the exception of 0x22 (“) and 0x27 (‘). Passwords must contain at least one alphabetic character (a–z, A–Z), one a numeric character (0–9), and one a special character (example, an underscore, “_”).
  - Password must not contain the account username.
  - Passwords are case-sensitive.

NOTE: The same user names under locally provisioned users, and OS user can have different passwords.

Lightweight Directory Access Protocol

The Containerized Decomposed Media Server supports Lightweight Directory Access Protocol (LDAP) user authentication for login. The LDAP directory service is a centralized database to manage the LDAP user accounts information.

LDAP is based on a client-server model where the Containerized Decomposed Media Server acts as an LDAP client to the LDAP server. LDAP provides the directory service, and the Containerized Decomposed Media Server uses the directory service to authenticate the LDAP users. LDAP server stores the users, groups, and password information to access the Containerized Decomposed Media Server. LDAP authentication is supported only for SSH, Web GUI, and NETCONF users. LDAP user authentication is configured through the Web GUI.

If the LDAP packet source routing to the management interface is not performed manually, it takes the default route.

To login to the Web GUI or SSH as an LDAP user, the Containerized Decomposed Media Server restricts the length of the username to 20 characters and the length of the password to 64 characters. The allowed set of characters for the LDAP username is.

- Uppercase alphabetic characters (A-Z)
- Lowercase alphabetic characters (a-z)
- Numeric characters (0-9)
- Special characters, period (0X2E), hyphen (0X2D), and underscore (0X5F)

NOTE:

- Do not begin the username with a special character.
- Do not end the username with a period.

The Containerized Decomposed Media Server supports the following LDAP server types.

- **Active Directory (AD).** The AD is customized for the Microsoft product suite.
- **OpenLDAP.** The OpenLDAP server.

Active Directory

During the LDAP user creation in the Active Directory (AD) server,

- If the **First name**, **Full name**, and **User logon name** of the LDAP user are created with the same value, the **User ID Attribute** supported value is **CN**, **givenName**, **sAMAccountName**, **displayName**, or **name**. If the **First name**, **Full name**, and **User logon name** of the LDAP user are created with different values, the **User ID Attribute** supported value is **sAMAccountName**.
- LDAP username and the group name must be **User Logon Name (pre-Windows 2000)** and **Group Name (pre-Windows 2000)**, respectively.

OpenLDAP

During the LDAP user creation in the OpenLDAP server,

- If the **CN**, **givenName**, and **uid** are created with the same value, the **UserID Attribute** supported value is **CN** or **uid**. If the **CN**, **givenName**, and **uid** are created with different values, the **UserID Attribute** supported value is **uid**.
- The OpenLDAP user schema must contain **posixAccount**, **shadowAccount**, **inetOrgPerson**, **organizationalPerson**, and **person** objectclasses.
- Multiple LDAP usernames must not be created with the same **uid** attribute.

During the LDAP group creation in the OpenLDAP server,

- The LDAP group schema must contain the **posixGroup** objectClass.
- When the Containerized Decomposed Media Server configures the **Group Member Attribute** as a **member** in the Web GUI, the LDAP user primary group is considered.

NOTE:

- The **memberOf** overlay must be configured in the OpenLDAP server.
- The Containerized Decomposed Media Server uses the **memberOf**, **memberUid**, or **member** attribute of the users to identify the user entries in the groups.

LDAP with TLS

The following TLS information is applicable for LDAP users.

- LDAP supports TLS 1.0, TLS 1.1, and TLS 1.2 versions. The default version is TLS 1.2.
- For LDAP to function, ensure that the DNS is configured appropriately.
- Ensure that the manage certificates, and TLS configurations are performed before configuring the LDAP user. For more information on configuration, see *Manage Certificates on page 323*, and *Configure TLS on page 333*.

For more information on configuring the LDAP information, see *Configure User Authentication on page 480* and *Special Interface Reference*.

Secure HTTP(HTTPS) for Web Access

The Containerized Decomposed Media Server supports a secure HTTP over SSL (HTTPS) connection for the Web-based management interface. HTTPS enhances security through the following means:

- **Protecting the transferred data from eavesdropping.** To protect the data, the server encrypts it using a private key unique to the server. The server's public key is used to decrypt the data.
- **Verifying the server identity.** To verify the server identity, a trusted certificate authority (CA) digitally signs the server certificate (or if third-party verification is not required, the server administrator self-signs it).

The Containerized Decomposed Media Server supports both pre-installed key and certificate and the provisioning of a key and certificate.

Port Access Control

The Containerized Decomposed Media Server supports the following features to control port access:

- **Limited access to secure syslog debugging.** Access to system logs is available through SSH, which is protected by the management user ID and password.
- **Limited access to TCP/UDP services.** TCP/UDP services are not required for the operation of the Containerized Decomposed Media Server and are disabled for security.

Table 21 lists the TCP/UDP ports that the application opens for inbound traffic.

Table 21. TCP/UDP Ports Used for Inbound Traffic

Port	Protocol	Service	Description
22	TCP	SSH	Provides SSH access. Can be disabled through the management interface.
80, 1443	TCP	HTTP/HTTPS server	Provides Web GUI access. Configurable through Apache.
1161	UDP	SNMP agent	Provides SNMP access. The Containerized Decomposed Media Server can configure this port.
1830	TCP	NETCONF	Default NETCONF port.
5060	UDP/TCP	SIP	SIP control port. The Containerized Decomposed Media Server can configure this port.
5061	TLS	SIP-TLS	SIP control port. The Containerized Decomposed Media Server can configure this port. This port is enabled only when SIP over TLS is enabled through the management interface.
9989	TCP	SIP	Media control channel TCP port. The Containerized Decomposed Media Server can configure this port.
65535	UDP	SIP	SIP debug port. Disabled by default.
1011 to 1014	UDP/TCP	NFS	Provide NFS service.
1025 to 1028	TCP	HTTP	For HTTP file transfer after recording.
8081 and 8443	TCP	HTTP/HTTPS server	Provides Web GUI access for AnnLab.
7776 to 7777 and 7787	TCP	Redundancy	For Containerized Decomposed Media Server redundancy. Used in OAMP pod and MRFP.
9000	UDP		
8192 to 8192 +(min of (1024,X) * number of DSP cores) -1	UDP	RTP/RTCP	RTP streams. End port can be configured at runtime in Web GUI. Maximum allowed value is 1024, depending on the end port. X=(endport-startport+1)/Number of DSP media processing cores.
8192+(min of (1024,X) * number of DSP cores) to 65534	TCP/UDP	Miscellaneous	Ephemeral port range. Dynamically used ports for NFS and other services. Maximum allowed value is 1024, depending on the end port. X=(endport-startport+1)/Number of DSP media processing cores.

Security Logging

The Containerized Decomposed Media Server supports log files that can aid security.

Management Activity Logging

Management activities generate log messages at different severities. Log severities of events are predefined. However, you can configure the level of detail that is reported in log messages by specifying the level of severity that is reported. The lower the level of severity specified, the more detail is captured in the logs.

When you specify a severity to report, the system reports all log messages of that severity and higher. For example, if you specify a severity of information, the system reports all Notice and Information log messages.

The default level of severity for all management activities is None (that is, management activities are not logged).

MRFP N+1 Redundancy

The Containerized Decomposed Media Server supports MRFP redundancy with multiple redundancy groups and each group with a maximum of N+1 (where N ≤ 5) MRFPs with call preservation for MSML, MSCML, and Netann conferences.

Following terminologies are used to explain MRFP redundancy.

- *Redundancy Groups*
- *Redundancy Role*
- *Redundancy Status*
- *Service Mode*
- *Switchover*
- *Automatic Reboots*

Faults and switchover activities are reported in the element management system and through the SNMP traps.

For information on configuring MRFP redundancy, see *MRFP Redundancy on page 366*.

NOTE:

- You must enter media and control IP addresses in the Containerized Decomposed Media Server *values.yaml* file for all the 20 MRFP instances.
- When instance 3 is not part of the redundancy group, the errors raised for rebootable parameters on the other instances are not displayed the Web GUI.
- For MRFP, the license needs to be applied manually to configure the auto redundancy group where the zero touch is not supported.

Redundancy Groups

The MRFP redundancy is managed using redundancy groups. Two or more MRFPs with common configuration items are added to a redundancy group. The Containerized Decomposed Media Server supports up to six redundancy groups. The redundancy status of an instance is indicated in the management interface.

A Containerized Decomposed Media Server can contain a mix of redundant and non-redundant MRFPs.

An MRFP can be added to a redundancy group using the management interface if:

- It is out of service.
- The redundancy group does not have the maximum number of instances.

The first instance added to a redundancy group is designated as the standby MRFP. If a standby MRFP is taken out of service and any active MRFP is rebooted, the rebooted active MRFP becomes standby.

Instances can be removed from a redundancy group using the management interface. To remove a faulted instance from a redundancy group, make the instance out of service through the management interface. The instance can be added and taken out of service while in the redundancy group.

A redundancy group can be deleted using the management interface. When you delete a redundancy group, the standby instance of the group is automatically restarted.

Redundancy Role

Every MRFP instance has the following redundancy role.

- **Standalone.** The instance does not belong to a redundancy group.
- **Active.** The instance belongs to a redundancy group, in which it is actively performing services.
- **Standby.** The instance belongs to a redundancy group and acts as a standby for the active instances in its group.

Only one instance in a redundancy group can have the role of standby. In general, the redundancy group always has a standby instance as long as there is at least one in-service instance in the group. The Containerized Decomposed Media Server determines the role of instances during a startup. An instance is assigned a standby if:

- There was no instance in the standby role before reboot, or
- The instance was in standby role before the reboot and no other instance has assumed the standby role.

If there was no standby instance before a reboot, the first instance to reboot assumes the standby role.

Redundancy Status

Every MRFP instance in a redundancy group has the following redundancy status.

- Online
- Offline
- Faulted

Service Mode

Every MRFP instance has a service mode:

- In service
- Out of service

A redundancy group can have both in-service and out-of-service instances. Out-of-service instances do not have any redundancy role or redundancy status.

Switchover

The Containerized Decomposed Media Server supports both manual (user-initiated) switchover and automatic switchover based on two diagnostic mechanisms: heartbeat polling and detection of designated alarm conditions. In either case, switchover is non-revertive; after a failed MRFP recovers, it remains in its new role rather than reverting to its old role.

NOTE: After an MRFP switchover, the hostname is swapped only at the management interface level and not at CLI.

Manual Switchover

Switchover can be initiated manually if there is a standby-online MRFP in the redundancy group. When switchover occurs, the active reboots and there is a loss of redundancy for a period of time.

Switchover can also be manually initiated when there is a standby-offline instance in the redundancy group, but in this case, not all the information may be synchronized.

Automatic Switchover

Switchover from an active MRFP to the standby is automatically initiated when the Containerized Decomposed Media Server detects that the standby must resume service for one of the active instances in the group.

Automatic switchover from an active instance to the standby is based on heartbeat polling or designated alarm detection:

- The Containerized Decomposed Media Server periodically polls all the active MRFP in a redundancy group. If an instance fails to respond to the heartbeat in a timely manner, the Containerized Decomposed Media Server initiates a switchover.

- Alarm-based switchover occurs when all the following conditions are met.
  - An alarm is generated on an active instance in a redundancy group.
  - The alarm is designated as one that can trigger a switchover.
  - There is an Online-Standby instance in the redundancy group.

Table 22 lists the alarms that can initiate an MRFP switchover. The capacity of an alarm to cause switchover is not user-configurable.

Table 22. Alarms Causing MRFP Switchover

Alarm ID	Alarm Name
16	Unidentified Reboot
17	Watchdog Reboot
18	Exception Reboot
19	User-Initiated Reboot
47	Overload Reboot
84	MRFP Heartbeat Failure
86	User-Initiated Switchover
97	Soft Watchdog Timeout Detected Alarm
98	SWT Limit Exceeded Alarm

Some special cases of automatic switchover may require user intervention. For example, an active instance is gracefully taken out of service. If, during the delay, the instance experiences a fault, the standby takes over from the faulted instance. The formerly active instance then becomes the standby and immediately goes out of service. In this case, the redundancy group has no standby instance. Should this occur, take one of the active instances out of service and bring it into service again. The system automatically designates the instance as the new standby.

After Switchover

After the switchover is initiated, the following takes place:

- Within 4 seconds from the first loss of conference of RTP traffic on the formerly active MRFP, the newly active MRFP restores RTP traffic to all conferences (This assumes that the standby instance was online and available when switchover was initiated).
- After switchover, the new standby instance reboots, synchronizes state with the other instances in the redundancy group, and reaches a standby-online state. During this interval, assuming all instances are functioning (that is, assuming that there are no new switchover alarms and no heartbeat failures); MRFP loses redundancy for approximately four minutes without load and a maximum of six minutes with load.

  NOTE: After switchover, the Containerized Decomposed Media Server sends a session refresh re-INVITE using a random offset timer (that is, it is not half of the negotiated value).

Table 23 lists the states that are restored.

Table 23. States Restored after MRFP Switchover

Restored	Comment
MSML conferences	The newly active instance attempts to restore MSML conferences, MSML conference recordings, and all the SIP call legs related to the MSML conference and MSML recording conference (for example, conference participants, conference control leg, conference recording control leg) after a switchover. This includes: • Connections in conferences. • The SIP call leg used to create the conference. • The SIP call leg used to start a conference recording. • The SIP session timers are refreshed. • The Containerized Decomposed Media Server notifies the control agent using the MSML `msml.conf.restart` event. • The Containerized Decomposed Media Server requests clients using media control channel framework to create a new TCP connection using the same dialog identifier (cfw-id) on the new instance. There may be special cases, (when the Containerized Decomposed Media Server is operating at or near full capacity, and where the capacity of the MRFP depends on the order in which services are requested) in which the newly active MRFP cannot recreate a service. If this occurs, the Containerized Decomposed Media Server generates an error message to the syslog.
RFC 4117 Transcoding	RFC 4117 transcoding services are restored to all ports that are connected using the sip:tc service context.
MSCML conferences	The newly active instance attempts to restore MSCML conferences, MSCML conference recordings, and all the SIP call legs related to an MSCML conference and MSCML recording conference (for example, conference participants, conference control leg) after a switchover. This includes: • Connections in conferences. • The SIP call leg used to create the conference. • The SIP session timers are refreshed. There may be special cases, (when the Containerized Decomposed Media Server is operating at or near capacity, and where the capacity of the MRFP depends on the order in which services are requested) that the newly active MRFP cannot recreate a service. If this occurs, the Containerized Decomposed Media Server generates an error message to syslog.
Video conferences	The Containerized Decomposed Media Server initiates I-Frame requests for all appropriate participants in video conferences. VAS speaker sees previous; I-Frame request for the current speaker. For the current speaker, there is no video (same as, at the start of a conference).
Control IP addresses	The Containerized Decomposed Media Server uses the same control IP addresses that were in use before the reboot and the control agents need not be reconfigured.
RTCP CNAME	The Containerized Decomposed Media Server preserves CNAME during an MRFP switchover.

If a failed instance recovers, its new role is:

- **Standby.** if there is no other standby instance in the redundancy group
- **Active.** if there is already a standby instance in the redundancy group

After switchover on a SIP-controlled system, the previously standby MRFP restores all conference-related SIP calls (connections and control channels).

Table 24 lists the states that are not restored.

Table 24. Non-Restored States

Restored	Comment
Non-conference SIP calls	The newly active MRFP sends a BYE for all non-conference related SIP call legs.
Audio recordings to HTTP	Audio recordings to an HTTP or HTTPS server are restarted, overwriting the existing recording. The current length of the recording is set to 0.
Internal recordings	Internal recordings are lost.
Announcements	Announcements in progress are not restored.
ICMP	ICMP backoff state is not maintained.
NAT Traversal	NAT Traversal state is not maintained.
Statistics	The standby instance does not take over the statistics of the failed instance.
RTP stream values	The Containerized Decomposed Media Server uses new values for the following fields in each RTP stream following a switchover: • SSRC • Sequence number: The Containerized Decomposed Media Server starts from a new random value • Timestamp: The Containerized Decomposed Media Server starts from a new random value
AMR codec values	AMR values for mode set, period, and neighbor can be updated through the RTP stream. These updates are not replicated, and the Containerized Decomposed Media Server reverts to values negotiated through SDP.
ASN reporting	The Containerized Decomposed Media Server restarts ASN reporting, independent of any reports from the previously active instance. This means that an ASN report could be repeated (this would be a new message without any change of active speaker). ***NOTE:*** The first ASN reported after the switchover is unreliable to decide the number of active speakers. It is suggested to consider the subsequent ASN reports.
VAS floor control	Conference floor control for voice activated switching video conference is not restored.

Automatic Reboots

The Containerized Decomposed Media Server automatically reboots an MRFP under the following conditions.

- The instance transitions from active to standby.
- The instance transitions from Standby-Online to Standby-Faulted.
- The instance experiences a heartbeat failure.

Chapter 5

License Management

This chapter explains the Containerized Decomposed Media Server license file and license management.

Understanding License File

The license key defines the port-limit per MRFP. It also defines time-limit, and maximum number of MRFPs. For example, if port limit is 100 and number of MRFP is set to 10 in the license file, the user is allowed to create a Containerized Decomposed Media Server instance with up to 10 X MRFPs each MRFP supporting 100 ports. The customer pays for the license of 100x10 = 1000 ports.

The Containerized Decomposed Media Server uses a Node Locked License file and only runs on a single platform for which a license file is installed. The license file permits the use of a predetermined set of features on this platform; for example, a certain number of audio ports, video ports, text ports, and specific codecs.

The Containerized Decomposed Media Server uses a license file at MRFCtrl pod, where the license limits are maintained and monitored at this central location. The MRFP reports the license usage to the MRFCtrl pod at regular intervals. Based on the license usage received from all the MRFPs, the MRFCtrl pod calculates the overall license usage across the MRFPs. The MRFCtrl pod responds with the current license limit to the MRFPs.

The features and ports supported on the Containerized Decomposed Media Server that require license are as follows:

- G.711 audio port (PCMU and PCMA)
- G.729 audio port
- G.722 audio port
- AMR-NB audio port (OA and BE)
- AMR-WB audio port (OA and BE)
- Opus audio port (NB and WB)
- EVS audio port (NB, WB, and SWB)
- EVRC, EVRC-B, and EVRC-NW audio ports (NB and WB)
- H.264 non-HC video port
- H.264 HC video port
- VP8 non-HC port
- VP8 HC port
- PLC (G.711 and G.722 audio ports with PLC enabled)
- Noise Reduction
- R-factor
- Acoustic Echo Cancellation

- Noise Gating
- Noisy-Line Detection
- G.711 fax port
- T.38 fax port
- T.140 text port
- Keyword Detection (port and conference)
- External Speech Sessions
- RTT conferencing port

The **External Speech Sessions** license is applicable for ASR and TTS. When ASR or TTS call is established, the **External Speech Sessions** license is consumed. When this license is exhausted, the Containerized Decomposed Media Server rejects the new ASR or TTS session creation with external speech servers.

NOTE: The Containerized Decomposed Media Server supports bundle license feature in license file for each of the audio ports supported on the Containerized Decomposed Media Server. For information on bundle license, see *Bundle License*.

The Containerized Decomposed Media Server locks down the most preferred codec from the offered list for which the required license and resources are available. If the most preferred codec license is unavailable, the Containerized Decomposed Media Server accepts the next preferred codec from the offered list for which the required license and resources are available.

For all the codec features, as long as the port is created, regardless of whether transcoding is enabled, the corresponding codec license is required. But for port-to-port transcoding call, if the transcoding is bypassed, codec license is not required. Usually, an encoder and a decoder of a port uses the same setting, therefore only one codec license is required for each port. When asymmetric H.264 codec feature is enabled, the encoder and decoder of a port may use different profile level settings (for example, if decoder is HC level while encoder is non-HC level), then only one HC codec license is required for this port.

For the scenario, where the Containerized Decomposed Media Server reserves one port with multiple codecs before making an offer, all the codecs in the offer requires a license. After a codec is locked down, the port license of the non-selected codecs are released.

The creation of the number of ports enabled with VQE features such as NG, NR, PLC, and NLD is limited by the VQE feature license. The actual limit for audio port enabled with VQE feature is lesser than the codec license and VQE feature license. If the actual Containerized Decomposed Media Server capacity is lower than the port license, then you cannot create more ports than the actual Containerized Decomposed Media Server capacity even though the port license is still available.

The VQE features such as AEC, NR, NG, PLC, and R-Factor are enabled through the management interface or through an INVITE Request-URI parameter during audio port creation. The VQE feature is considered as **mandatory** when it is requested through an INVITE Request-URI parameter and considered as **optional** when it is enabled through the management interface. The Containerized Decomposed Media Server selects an audio codec from the list only if the codec license and VQE features are available. The Containerized Decomposed Media Server reserves the resources for the next codec from the list and does not reserve the resources again for the same codec with optional VQE features disabled.

The Containerized Decomposed Media Server accepts the call and disables the VQE features, for which VQE license is unavailable but port license is available. It is supported only if the VQE features are enabled through the management interface. The VQE port settings are preserved on redundancy switchover. If the VQE feature is disabled on the port due to license issue, the Containerized Decomposed Media Server logs a warning message in syslog. The Containerized Decomposed Media Server tracks the number of times a VQE license is exhausted, using the statistics in the Web GUI.

The Containerized Decomposed Media Server rejects the call if the codec or VQE license is exhausted and if the VQE feature is explicitly requested in the INVITE or MSML command. The Containerized Decomposed Media Server rejects the incoming MSML request to enable keyword detection when keyword detection license is exhausted.

The Containerized Decomposed Media Server supports the following license functionalities for mid-call change.

- The Containerized Decomposed Media Server does not acquire the license for the VQE features (NR and NG), if license is not acquired for the port earlier, during mid-call change on a audio port.
- The Containerized Decomposed Media Server attempts to acquire PLC and R-factor license when the port codec changes from non-G.711 or non-G.722 to G.711 or G.722 respectively through a mid-call change.
- The Containerized Decomposed Media Server attempts to acquire PLC and R-factor license when the port codec changes from G.711 or G.722 to G.722 or G.711 respectively through a mid-call change.
- The Containerized Decomposed Media Server releases the PLC or R-factor license, if PLC or R-factor is enabled on a G.711 or G.722 port and the codec changes to non-G.711 or non-G.722 respectively after a mid-call change.
- The Containerized Decomposed Media Server does not attempt to acquire PLC or R-factor license during a mid-call change, if the port is G.711 or G.722, PLC or R-factor license is not acquired, and the mid-call change does not change the codec.
- The AEC licenses are acquired only on the Containerized Decomposed Media Server start-up and not attempted during port creation or mid-call change on per-port basis.
- Unlike other VQEs, the NLD is enabled explicitly through MSML INFO and not during port creation or mid-call change.
- The mid-call offer can add any new media streams independent of the existing media stream changes.

The AEC license limits the number of AEC echo canceller resources, which can be reserved on Containerized Decomposed Media Server through the OAMP. AEC echo canceller resources are pre-allocated during the start-up and are never freed. If the OAMP configuration has exceeded the port limit defined in the license file for AEC, the alarm *AEC provisioning exceeds maximum capacity* is triggered and AEC echo canceller resources are not allocated.

The NR license is used to monitor the NR resources (including active auto-NR ports) on the Containerized Decomposed Media Server. The NR license limits the total number of narrowband and wideband ports with NR active. Similarly, NLD license is used to monitor the NLD resources on the Containerized Decomposed Media Server. The NLD license limits the total number of narrowband and wideband ports with NLD enabled.

The PLC license is used to monitor the G.722 PLC resources on the Containerized Decomposed Media Server using the existing G.711 PLC. The existing PLC license limits the total number of G.711 and G.722 PLC ports enabled. The Containerized Decomposed Media Server tracks the total number of G.711 and G.722 PLC enabled ports using the statistics in OAMP. The R-factor is added to monitor the R-factor resources on the Containerized Decomposed Media Server. The R-factor license limits the total number of active ports on R-factor regardless of the codec type.

The HC video is supported in H.264 and VP8 codec. The H.264 port at level 1.0 to 2.0 is non-HC video port and H.264 port at level 2.1 or above is HC video port. The VP8 port with frame size of 99, 225, 396, 900, 1200, and 1350 MB is non-HC video port and VP8 port with frame size of 3600 MB is HC video port.

The non-HC video port license is used for creating non-HC video port only, but the HC video port license can be used to create either non-HC or HC video port. For example, if HC video port limit is 50 and non-HC video port limit is 30 in the license file, then you must be able to create up to 50 HC video port or 80 non-HC video port. When offering H.264 video codec at HC level, the Containerized Decomposed Media Server acquires only the H.264 HC video port license. When the answer is received and if the H.264 codec is downgraded to non-HC level, the Containerized Decomposed Media Server switches to non-HC video port license if available. If non-HC video port license is not available, the Containerized Decomposed Media Server continues to use the HC video port license.

In a multi-media initial call setup during control agent or Containerized Decomposed Media Server offer, the Containerized Decomposed Media Server establishes audio only call if the video licenses are unavailable. Similarly, the Containerized Decomposed Media Server establishes video only call if the audio licenses are unavailable.

For more information on Containerized Decomposed Media Server behavior while handling initial offer in different service contexts, refer to the *SIP Interface Reference*.

The Containerized Decomposed Media Server does not consume port license beyond the call setup duration on audio and video ports in port-to-port transcoding, when transcode bypass is used in both the directions. This is applicable for p2p ports created using **sip:tc** service context. If transcode bypass is applicable only in one direction, the Containerized Decomposed Media Server consumes licenses for both caller and callee. The Containerized Decomposed Media Server reserves the port license until the call setup between the caller and callee is complete, whether the session is transcoded or transcode free.

NOTE: In video mid-call changes, the Containerized Decomposed Media Server deletes the current port and re-creates the new port. The port license is consumed at the time of port re-creation and is released, if the session is transcode free. If there is no port license for port re-creation, the mid-call change is rejected.

The Containerized Decomposed Media Server releases port licenses when changing session from transcoding to bypass-transcoding due to mid-call changes. The port license is consumed if transcode bypass session, changes to transcoded during mid-call change. If no license is available, the mid-call change is rejected. The Containerized Decomposed Media Server releases the port license for T.140 text ports pass-through created using **sip:tc**.

NOTE: T.140 text pass-through can be created using initial INVITE, mid-call re-INVITE, or UPDATE request.

The RTT conferencing port license is provisioned per node basis. The supported values are 0 and unlimited. The node license value 0 means the Media Server does not allow to create any RTT conferencing ports. The node license value unlimited means the Media Server can allocate unlimited port license for the RTT conferencing ports.

The Containerized Decomposed Media Server does not increment the codec high watermark statistics for transcode bypass sessions established without using license.

NOTE: License expires as per UTC time zone irrespective of your system time zone settings.

For example, if you are in the time zone of GMT-11, license expires 11 hours before the actual system time.

Initial License Management

The Containerized Decomposed Media Server uses a Node Locked License file, which means that the Containerized Decomposed Media Server only runs on a single platform for which a license has been installed. The license file permits the use of a predetermined set of features on this platform; for example, a certain number of audio ports, video ports, and specific codecs.

You can provision the license using user provisioned Node ID or system generated Node ID.

Provisioned Node ID

Node ID is not linked to the universally unique identifier (UUID) or any run-time variable on the instance. Before instantiating the Containerized Decomposed Media Server, user requests the Node ID, number of MRFPs with the port limit, and the corresponding license key from Radisys. The user modifies the heat template with the Radisys provisioned Node ID and license key information. The Node ID is provided through values.yaml during instantiation of the Containerized Decomposed Media Server. Node ID can also be provided through the Web GUI.

For information on editing the values.yaml and deploying the Containerized Decomposed Media Server, refer to *Containerized Decomposed Media Server Installation Guide*.

Retrieving the Node ID

The Node ID on your platform is available through the Containerized Decomposed Media Server management interfaces.

To retrieve the Node ID through the management interface:

To retrieve the Node ID through the management interface, the Containerized Decomposed Media Server must be running.

1. Launch the Containerized Decomposed Media Server Web GUI without the provisioned Node ID.
2. Obtain the system generated OAMP Node ID, click **Maintenance** > **Show Licensing**.

Bundle License

The bundle license feature allows bundling of one or more companion codecs in one license. When a bundle license is acquired, the codec applied on the port can be any of the codecs that were ordered as part of the bundle. For a given codec, the Containerized Decomposed Media Server acquires a base license when creating the audio port; the Containerized Decomposed Media Server acquires a bundle license only if base licenses are unavailable. The Containerized Decomposed Media Server does not create audio port with the given codec if the base license or bundle licenses are unavailable.

Following terminologies are used to explain this feature.

- **Base license.** The individual feature license is not shared with other features.
- **Sub-limit.** Sub-limit is the individual codec limit in the bundle license.
- **Bundle license limit.** The maximum of all the sub-limit within a license file.

The maximum number of audio ports allowed on the Containerized Decomposed Media Server is a sum of all the base licenses and the bundle license limit.

Bundle license is supported only for the following audio codec licenses.

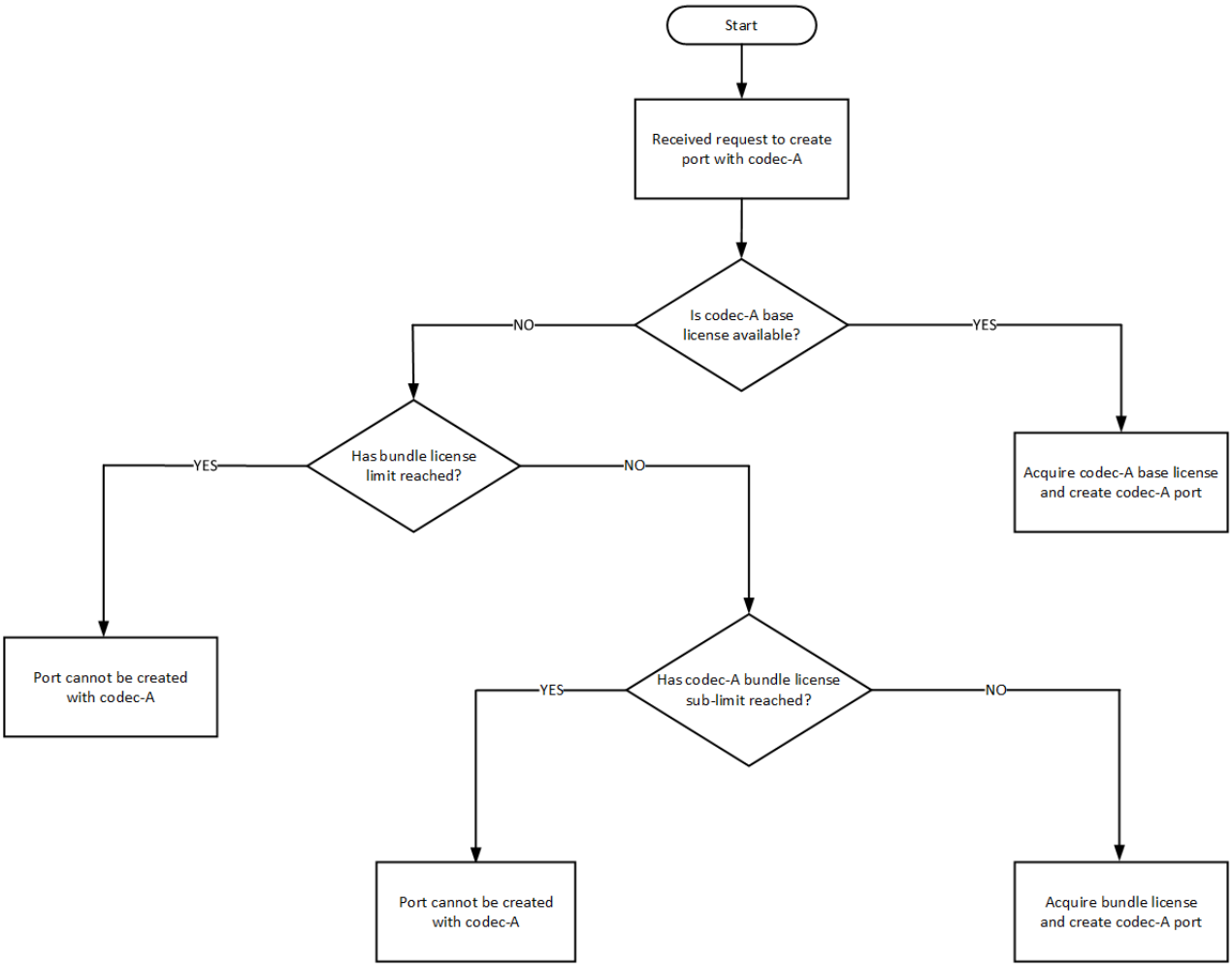
- G.711
- G.729

- G.722
- AMR-NB
- AMR-WB
- Opus
- EVS
- EVRC
- EVRCB
- EVRCNW

When creating a port for a given audio codec, the Containerized Decomposed Media Server acquires the available base license. If base licenses are unavailable, the Containerized Decomposed Media Server verifies whether a bundle license is available for the codec (because a bundle license can be acquired for any of the codecs that are part of the bundle). Bundle license limit, sub-limit for a given codec, and the current port usage for the given codec are considered to determine whether bundle licenses are available for the codec.

Figure 22 provides the bundle license flow when creating a port for a given audio codec.

Figure 22. Bundle License Flow



Bundle license behavior is explained using the following examples.

Example 1: Bundle license limit is same as the sub-limit for all the codecs

User has ordered 100 base licenses for AMR-WB codec and 50 bundle licenses for AMR-WB, G.711, and EVS codecs.

Feature Name	Block-limit
AMR-WB audio port	100
AMR-WB audio port Bundle	50
G.711 audio port Bundle	50
EVS audio port Bundle	50

Here, the Containerized Decomposed Media Server can create a maximum of 150 ports. The 100 base licenses for AMR-WB codec can create only AMR-WB ports. The bundle license limit is 50; a maximum of 50 ports can be created with a mix of AMR-WB, G.711, and EVS. The sub-limit for the individual codecs (AMR-WB, G.711, and EVS) is same as the bundle license limit (50).

Example 2: Bundle license limit with different sub-limits

User has ordered 100 base licenses for AMR-WB codec, 50 base licenses for G.711 codec, and 100 bundle license limit with a sub-limit of 100 for AMR-WB, 50 for EVS, and 30 for Opus.

Feature Name	Block-limit
AMR-WB audio port	100
G.711 audio port	50
AMR-WB audio port Bundle	100
EVS audio port Bundle	50
Opus audio port Bundle	30

The Containerized Decomposed Media Server can create a maximum of 250 ports. 100 AMR-WB base licenses allow to create 100 AMR-WB ports. Similarly, 50 G.711 base licenses allow to create 50 G.711 ports. The bundle license limit is 100; a maximum of 100 more ports can be created with a mix of AMR-WB, Opus, and EVS. Out of the 100, a maximum of 30 can be Opus, a maximum of 50 can be EVS, and a maximum of 100 can be AMR-WB.

For the CA offer call-flow, the Containerized Decomposed Media Server acquires the base license for the associated codec when creating an audio port or when modifying an existing port during the mid-call. If base license is unavailable, the Containerized Decomposed Media Server acquires the available bundle license for the codec.

The Containerized Decomposed Media Server uses the sum of the base licenses and bundle licenses for a given codec to determine the port limit warning and port limit block threshold levels. The Containerized Decomposed Media Server raises the alarm 156 *Port limit warning for Y feature*, if the current license usage for a given codec has crossed the port limit warning. Similarly, the Containerized Decomposed Media Server raises the alarm 157 *Port limit hit for Y feature*, if the current license usage for a given codec has crossed the port limit block threshold levels.

Bundle licenses are common pool of licenses associated with all the codecs in the bundle. Therefore, available bundle license for a given codec-A can reduce when a port with a different codec-B consumes the bundle license. As a result, the alarm 156 *Port limit warning for Y feature* and alarm 157 *Port limit hit for Y feature* for codec-A can be raised even though ports are not being created for codec-A.

When an audio port is deleted, the Containerized Decomposed Media Server releases the base license for the codec if the current port usage for the codec is lower than or equal to the base license limit. The Containerized Decomposed Media Server releases the bundle license, if the usage of the codec is higher than the base limit but lower than or equal to the bundle sub-limit for the codec.

Obtaining a New License File

After the Containerized Decomposed Media Server is installed, it is activated but remains out of service until the license file is validated.

When requesting a new license file, submit the following information to your sales representative and OrgMSBUcms_purchase_orders@radisys.com:

- Purchase order
- License file type: New license file
- Customer information: Company, contact name, phone number, and address
- Node ID on the platform

Licensing Additional RTU Packages

To add additional Right to Use (RTU) packages, you need to purchase new licenses. To purchase a new license file, follow the instructions in *Obtaining a New License File*.

Transferring a License File

After deployment, if the license file is lost and the Containerized Decomposed Media Server has to be redeployed, you need to *replace the license file*.

It is possible to store the license file to PVC volume, which allow the Containerized Decomposed Media Server to be redeployed any number of times using the same initial PVC volume. For more details about zero touch deployment, refer to the *Containerized Decomposed Media Server Installation Guide*.

When requesting a replacement license file, submit the following information:

- License file type: Replacement license file
- Customer information: Company, contact name, phone number, and address
- Node ID on the new platform
- Node ID on the old platform or the initial purchase order number

  NOTE: Send this information to your sales representatives or field application engineers to tac@radisys.com.

Following are the alarms related to license features:

- The node license key is invalid
- License will expire in X days
- License expired
- Port limit warning for Y feature
- Port limit hit for Y feature

For more information on alarms, refer to *Appendix A, List of Alarms, on page 525*. For information on setting up and configuring license information refer to *Chapter 9, Web GUI Maintenance, on page 371*.

Backup and Restore

The Containerized Decomposed Media Server backup and restore operations can be configured through the Web GUI or triggered through the SNMP interface.

Backup Operations

The following are the different types of backup operations in the Containerized Decomposed Media Server.

- **Backup Configuration.** Allows you to backup the configuration of the entire Containerized Decomposed Media Server to a file on a file server. For more information see *Backup Configuration on page 376*.
- **Full Backup.** Allows you to backup all configurable elements (backup_config.ms) of the Containerized Decomposed Media Server through the management interface including audio segment configuration file, provisioned license file, and AnnLab configurations. However, the full backup configuration does not backup the web user database. The full backup operation includes output of the backup configuration. For more information see *Full Backup on page 383*.
- **Backup User Database.** Allows you to backup the locally provisioned Containerized Decomposed Media Server users and their configuration by saving the user database to a file server. For more information see *Backup User Database on page 501*.
- **Backup Audio Segment Configuration.** Allows you to backup the audio segment configuration to a file on a file server. For more information see *Backup Audio Segment Configuration on page 342*.
- **Configure Scheduled Backup.** Allows you to configure the Containerized Decomposed Media Server to perform scheduled backup operations. For more information see *Configure Scheduled Backup on page 388*.

NOTE:

- All the above backup operations can be scheduled through the *Configure Scheduled Backup* Web GUI page.
- All the sensitive information like backup_config.ms, license, annlab-db, cert, file_transfer_keys, and userDB.enc are encrypted during the backup operation.

Restore Operations

The following are the different types of restore operations in the Containerized Decomposed Media Server.

- **Restore Configuration.** Allows you to restore the entire configurations of the Containerized Decomposed Media Server from a backup stored on a file server. For more information see *Restore Configuration on page 378*.
- **Full Restore.** Allows you to restore all configurable elements of the Containerized Decomposed Media Server through the management interface, audio segment configuration file, license file, and AnnLab clips and database. For more information see *Full Restore on page 385*.
- **Restore User Database.** Allows you to restore the user database from a file server. For more information see *Restore User Database on page 503*.

NOTE: All the Containerized Decomposed Media Server backup and restore operations can also be configured through the SNMP interface. For more information, refer the *SNMP Interface Reference*.

Automated Script

The Containerized Decomposed Media Server backup and restore operations can be triggered through an automated script provided with the release package. This allows you to perform the automatic backup or restore operations using the SNMP interface.

External Server

The **`mrfBackupRestore.sh`** script allows the user to perform the automatic backup and restore operations on an external server using the SNMP interface.

- Execute **mrfbackuprestore.sh** script on the remote server by providing the remote FTP server path.

  ```
  ./mrfbackuprestore_v1.sh -c mrf_01_v1.cfg
  ```

- By executing the above script from the outside worker node, the backup/restore cannot be taken inside the worker node */weboam/<backup_dir>/.*

NOTE:

- The OAMP pod to access the FTP server from outside is not allowed.
- The `mrf_01_v1.cfg` file can be used to configure the backup and restore parameters.

Containerized Decomposed Media Server

The **`mrfbackuprestore_v1.sh`** script allows the user to perform the automatic backup and restore operations on the Containerized Decomposed Media Server using the SNMP interface.

For more information, see *Containerized Decomposed Media Server Backup and Restore Script on page 625*.

By providing the remote FTP server path

- Execute **mrfbackuprestore.sh** script on the worker node by providing the remote FTP server path. The backup must be uploaded to the remote server.

  ```
  ./mrfbackuprestore_v1.sh -c mrf_01_v1.cfg
  ```

By providing the local server path

- Execute **mrfbackuprestore.sh** script on the worker node by providing the local */weboam/<backup_dir>/* path. The backup must be uploaded to the PVC */weboam/< backup_dir >/* path.

  ```
  ./mrfbackuprestore_v1.sh -c mrf_01_v1.cfg
  ```

NOTE:

- For the FTP server, always provide the FTP IP address.
- Executing the **mrfbackuprestore.sh** script on the worker node prompts the username and password.
- The `mrf_01_v1.cfg` file can be used to configure the backup and restore parameters.

PART 2: OPERATIONS

Chapter 7

Web GUI Overview

This chapter provides an introduction to the Web GUI management interface.

Browser Requirements

The Web GUI is an HTTP-based interface for performing Web GUI configuration on the Containerized Decomposed Media Server. This management interface can run using a supported Web browser on any workstation connected to the Containerized Decomposed Media Server management network. The Web GUI must be accessed through the Containerized Decomposed Media Server management port. You cannot access the Web GUI through the control port. Containerized Decomposed Media Server supports Internet Explorer version 11 browser.

The Web browser must be Javascript-enabled.

To view the Web GUI, the monitor must be set to a resolution of 1024 x 768 or greater.

Logging On

You can open only 10 administrative user sessions at one time. By default, idle login sessions timeout is 15 minutes if there is no activity. You can change the timeout interval.

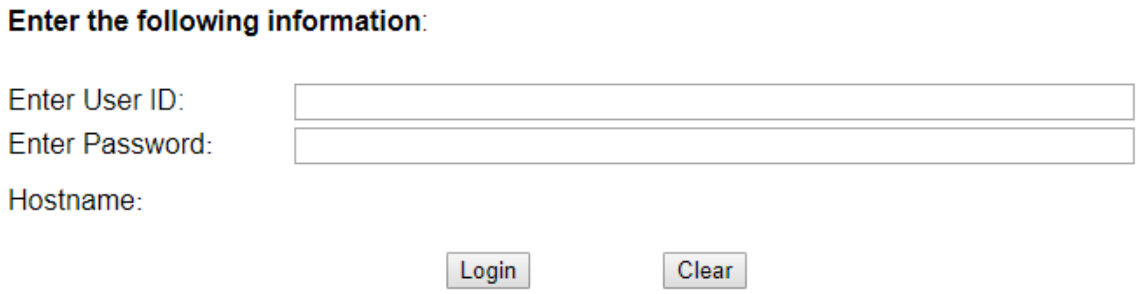
For information about configuring the Web GUI timeout interval, see *Administration Management on page 473*.

To log on to the Web-based management interface:

1. In your browser, enter the hostname or IP address in URL format, as follows:
   - For unsecure HTTP use
     http://<AnyKubernetesHostIp>:<NodePortHttp>/swms
   - For HTTP over SSL (HTTPS) use
     https://<AnyKubernetesHostIp>:<NodePortHttps>/swms

   The Administrator Login screen appears. The title bar of your Web browser displays **SWMS:**`<hostname>`, where SWMS signifies the Containerized Decomposed Media Server and `<hostname>` gives the OAMP pod name.

2. On the Login screen, enter the user ID and password. The default ID is `webadmin`, and the password is `convedia`.



3. Click **Login**. After your user information is authenticated, you are logged on to the initial screen, the Fault Management screen, which opens on the Alarms Summary page.

Screen Features

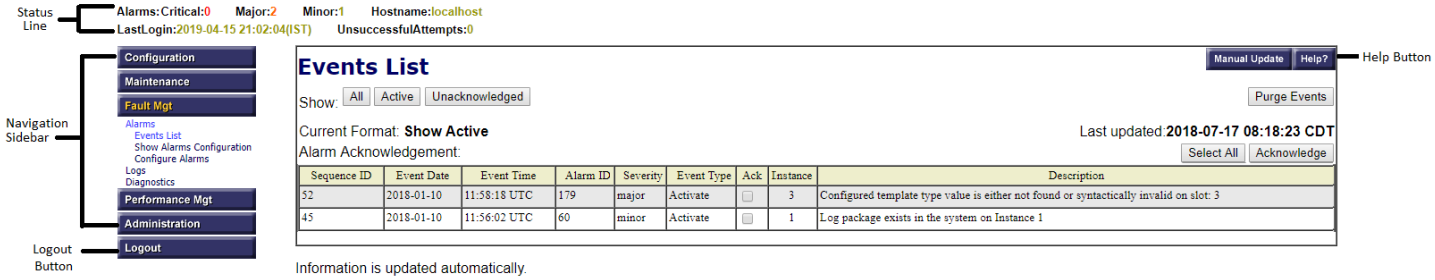
The Web GUI consists of following main screens:

- Configuration
- Maintenance
- Fault Management
- Performance Management
- Administration

These screens are accessible through navigation buttons in a navigation sidebar that appears on each screen. In addition to the buttons for the main screens, a Logout button and a Help button appear on each screen.

At the top of each screen, the Status Line displays. Independent of the screen displayed, the browser-title bar (the top part of your browser) displays the hostname configured for the instance and alarm information:

This information is helpful when multiple Containerized Decomposed Media Servers are accessed.



Status Line

The Status Line appears at the top of each Web GUI screen, just below the screen title. The Status Line provides a quick summary of the operational status of the Containerized Decomposed Media Server.

The Alarms section of the Status Line summarizes the number of critical, major, and minor alarms active on the system and the hostname.

The status line displays the **LastLogin** and **UnsuccessfulAttempts** information for the logged in user on all the Web GUI pages.

LastLogin displays the date and time when the user last logged in to the Web GUI, in YYYY-MM-DD HH:MM:SS time zone format. On the first login for a newly created user, the status line displays the **FirstLogin** string on all the Web GUI pages. For the migrated users from the earlier releases, on first login, the status line displays **NA** string on all the Web GUI pages.

UnsuccessfulAttempts displays the number of unsuccessful login attempts by the user. The number of unsuccessful attempts between two successful login is displayed. The Containerized Decomposed Media Server does not update the **LastLogin** and **UnsuccessfulAttempts** information on the existing login window automatically when the same user is logged in to another window.

Configuration Screen

From the Configuration screen, you can:

- Configure global settings for the Containerized Decomposed Media Server
- Manage media storage
- Manage network settings
- Manage MRFP redundancy

For more information about configuration, see *Chapter 8, Configuration, on page 180*.

Maintenance Screen

From the Maintenance screen, you can view software version details, manage software, manage licensing, restart or shut down the Containerized Decomposed Media Server, or back up configuration and restore system configuration.

For more information about maintenance, see *Chapter 9, Web GUI Maintenance, on page 371*.

Fault Management Screen

From the Fault Management screen, you can work with system alarms, system and protocol log messages, and internal diagnostic files.

For more information about Alarms, logs, and diagnostics, see *Chapter 10, Fault Management, on page 393*. System alarms are listed in *Appendix A, List of Alarms, on page 525*.

Performance Management Screen

From the Performance Management screen, you can retrieve and reset statistics that help you monitor the performance of your system. You can also display statistics at 5, 15, or 30 minute interval for the past 72 hours, or display a history and snapshot of statistics in real time.

For more information about performance management, see *Chapter 11, Performance Management, on page 424*.

The statistics generated by the Containerized Decomposed Media Server are listed in *Appendix D, List of Statistics, on page 566*.

Administration Screen

From the Administration screen, you can change user account information, configure management logs, advisory feature, and customize the GUI idle timeout interval.

For more information about administration management, see *Chapter 12, Administration Management, on page 473*.

Configuration

This chapter explains configuration options available through the Web GUI.

NOTE:

- Do not leave IP addresses fields blank. If you want to leave an IP address unconfigured, enter the value **0.0.0.0**.
- In configurations settings through the Web GUI, some parameters take effect immediately. Parameters marked with * require reboot or reset to take effect.
- If the **Instance Number** field is not present for a GUI page, the configuration for that page is reflected on all the instances in the Containerized Decomposed Media Server.
- For MRFC (OAMP and MRFCtrl) configuration, see *MRFC Configuration on page 509*.
- Login to the pod through the **`kubectl`** command and execute the following command to restart the OAMP or MRFP process.

  `#/opt/swms/bin/swms_service_restart.sh`
- Login to the pod through the **`kubectl`** command and execute the following command to restart the MRFCtrl process.

  `#/opt/swms/bin/mrfctrl_service_restart.sh`
- If the management interface is configured with IPv6 address type and the Containerized Decomposed Media Server pods cannot reach the servers outside the cluster due to local IPv6 address, the file transfer operations do not work for the server outside the Kubernetes cluster due to reachability issues.

Node Configuration

The Node Configuration option allows you to configure most of the Containerized Decomposed Media Server operational settings.

Show Instance Status

The Show Instance Status page displays MRFC1 (denotes OAMP pod) and MRFP instance status.

To view instance status:

1. Click **Configuration** > **Node Configuration** > **Show Instance Status**.

   The Show Instance Status page displays.
2. Click **Execute**.

   Instance status displays in the **Output Messages:** box.

Show Node Configuration

The Show Node Configuration page displays configuration information for the Containerized Decomposed Media Server.

The information shown includes:

- SIP parameters (set on the *Configure SIP*)
- Jitter buffer settings (set on the *Configure Jitter Buffer Templates*)
- ICMP back-off settings (set on the *Configure Media ICMP*)
- Audio recording format and VAD sensitivity settings (set on the *Configure Audio*)
- Opus settings (set on the *Configure Opus*)
- Silence suppression settings (set on the *Configure Silence Suppression*)
- Symmetric RTP, secure RTP, encrypt RTCP packets for SDES, RTP redundancy, port source screening configuration, RTP payload value, RTP media multiplexing, and media ID (set on the *Configure RTP*)
- RTCP settings (set on the *Configure RTCP*)
- RTSP settings (set on the *Configure RTSP*)
- RTCP Feedback and RTCP Feedback Message settings (set on the *Configure RTCP Feedback*)
- Default packetization interval settings (set on the *Configure Audio*)
- Packet loss concealment settings for G.711 and G.722 (set on the *Configure Audio*)
- Noise gating (set on the *Configure Audio*)
- Acoustic Echo Cancellation (set on the *Configure Audio*)
- Noise Reduction settings (set on the *Configure Audio*)
- Audio/Video resource allocation settings (set on the *Configure Resource Management*)
- Service mode and operational state (set on the *Set MRFP Service Mode*)
- HTTP mode and caching, post processing CGI script, chunked transfer encoding, and HTTP response wait duration (set on the *Configure HTTP Media and Cache*)
- Fax settings (set on the *Configure Fax*)
- Resource Server Configuration (set on the *Configure Resource Server Redundancy*)
- T.140 number Buffer Interval (set on the *Configure Text*)
- Persistent Clip Path (set on the *Configure Local Persistent Recording Path*)
- EVS settings (set on the *Configure EVS*)
- Transcode bypass and optimal clip selection settings (set on the *Configure Transcode Bypass*)
- EVRC settings (set on the *Configure EVRC*)
- Pre-Announcement Silence Duration and Post-Announcement Silence Duration settings (set on the *Configure Audio*)
- Maximum and minimum announcement speed settings (set on the *Configure Audio*)
- Lawful Interception settings (set on the *Configure Lawful Intercept*)

- TTY Clamping settings (set on the *Configure Audio*)
- Load balancing method settings (set on the *Configure SIP Load Balancing*)
- Optimal clip recording settings (set on the *Configure Audio*)
- ASR VAD (VAD Controlled ASR, ASR End Of Speech Detection Timeout, and VAD Noise Threshold) information settings (set on the *Configure Audio*)

To view the Containerized Decomposed Media Server configuration information:

1. Click **Configuration** > **Node Configuration** > **Show Node Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays configuration information.

Show Audio Codec List

The Show Audio Codec List page displays the audio codecs that are supported on the Containerized Decomposed Media Server, and the order of preference in which the codecs are offered during 3PCC codec negotiation for SIP calls.

NOTE: This audio codec list is for 3PCC codec negotiation.

To view supported audio codecs:

1. Click **Configuration** > **Node Configuration** > **Show Audio Codec List**.

   The Show Audio Codec List page displays.
2. Click **Execute**.

The **Output Messages:** box displays a list of supported audio codecs, in order of preference. If the codec list has not yet been configured, the order of codecs follow the default ordering.

The information shown on this page is set on the *Configure Audio Codec List*.

Show MRCP Configuration

The Show MRCP page displays the configured characteristics for connections between the Containerized Decomposed Media Server and MRCP servers.

The Containerized Decomposed Media Server supports connections with a maximum of 40 servers. These can be automatic speech recognition (ASR) or text-to-speech (TTS) servers.

To view MRCP configuration:

1. Click **Configuration** > **Node Configuration** > **Show MRCP**.

   The Show MRCP Configuration page displays.
2. Select the **Server number.** If you want to view information for all MRCP servers, select **all**.
3. Click **Execute**.

   MRCP configuration information displays in the **Output Messages:** box.

To change the MRCP configuration, see *Configure MRCP on page 193*.

Show Jitter Buffer Templates

The Show Jitter Buffer Templates page enables you to view the parameters set in the jitter buffer templates. Information shown on this page is set using the Configure Jitter Buffer Templates page.

The Containerized Decomposed Media Server supports up to 10 templates.

To view jitter buffer template settings:

1. Click **Configuration** > **Node Configuration** > **Show Jitter Buffer Templates**.

   The Show Jitter Buffer Templates page displays.
2. Select the **Template number**. If you want to view information for all Jitter Buffer Templates, select all.
3. Click **Execute**.

   Jitter buffer template information displays in the **Output Messages:** box.

To change the jitter buffer settings, see *Configure Jitter Buffer Templates on page 210*.

Show NFS Configuration

The Show NFS page enables you to view information defined for external NFS servers.

The following NFS information is shown.

- NFS operational mode
- Health check information
- NFS server unavailable attempts
- External NFS cache is enabled or disabled
- Slow NFS Throttling Interval (minutes)

For enabled mount points the following information is shown.

- The IP address (or hostname) of the external NFS server where this mount point is located
- The path to the exported directory
- The read and write request sizes
- The NFS version
- The NFS transport protocol

To view NFS configuration:

1. Click **Configuration** > **Node Configuration** > **Show NFS Configuration**.

   The Show NFS Configuration page displays.
2. Select the **Mount number** you are interested in. If you want to view information for all mount points, select **all**.
3. Click **Execute**.

   The NFS configuration information for the specified mount points displays in the **Output Messages:** box.

The information shown on this page is set on the *Configure NFS on page 231*.

Show SNMP Agent Configuration

The Show SNMP Agent Configuration page displays the SNMPv2c community string, SNMPv3 parameters, and SNMP agent listening port, and SNMP manager IP address configured for the SNMP agent residing on the Containerized Decomposed Media Server.

To view the SNMP agent information:

1. Click **Configuration** > **Node Configuration** > **Show SNMP Agent Configuration**.

   The Show SNMP Agent Configuration page displays.
2. Click **Execute**.

   The SNMP agent configuration information displays in the **Output Messages:** box.

To change the SNMP agent configuration, see *Configure SNMP Agent on page 266*.

Show SNMP Trap Destinations

The Show SNMP Trap Destinations page displays all the destinations configured for SNMP traps. For each configured destination, the information displayed includes the IP address or hostname of the destination, the UDP port where the host is listening for SNMP traps, and the trap community name.

To view the SNMP trap destinations:

1. Click **Configuration** > **Node Configuration** > **Show SNMP Trap Destinations.**

   The Show SNMP Trap Destinations page displays.
2. Click **Execute**.

   The SNMP trap destination information displays in the **Output Messages:** box.

Show Video Configuration

The Show Video Configuration page displays video configuration settings such as maximum transmission unit, drop percentage of encoder frame rate, scaling method, timeout value of I-Frame, maximum retries request for the I-Frame, picture size settings, default H.264 profile level ID, codec for asymmetric H.264, and so on.

To show video configuration:

1. Click **Configuration** > **Node Configuration** > **Show Video Configuration**.

   The Show Video Configuration page displays.
2. Click **Execute**.

   The specified video configuration information displays in the **Output Messages:** box.

   The information shown on this page is set on the *Configure Video on page 254*.

Show Video Codec List

The Show Video Codec List page displays the video codecs that are supported for the Containerized Decomposed Media Server, the order of preference in which the codecs are offered during codec negotiation, and the other parameters supported by the video codec.

To view the supported video codecs list:

1. Click **Configuration** > **Node Configuration** > **Show Video Codec List**.

   The Show Video Codec List page displays.
2. Click **Execute**.

   The list of supported video codecs displays in the **Output Messages:** box, in order of preference.

To change the video codec list, see *Configure Video Codec List on page 261*.

Show Video Recording Configuration

The Show Video Recording Configuration page displays the configuration settings for video recording, such as the initial I-frame timeout, default bitrate for CIF and QCIF, default MPI, and default picture size.

To view video recording configuration:

1. Click **Configuration** > **Node Configuration** > **Show Video Recording Configuration**.

   The Show Video Recording Configuration page displays.
2. Click **Execute**.

   The video recording configuration information settings are displayed in the **Output Messages:** box.

To change the video recording configuration, see *Configure Video Recording on page 265*.

Show VoiceXML Configuration

The Show VoiceXML Configuration page displays configuration of the characteristics for SIP/VoiceXML dialogs.

To view VoiceXML configuration:

1. Click **Configuration** > **Node Configuration** > **Show VoiceXML Configuration**.

   The Show VoiceXML Configuration page displays.
2. Click **Execute**.

   VoiceXML configuration displays in the **Output Messages:** box.

To change the VoiceXML configuration, see *Configure VoiceXML Parameters on page 287*.

Show Conference Configuration

The Show Conference Configuration page displays the settings configured for conferences.

To view conference configuration:

1. Click **Configuration** > **Node Configuration** > **Show Conference Configuration**.

   The Show Conference Configuration page displays.
2. Click **Execute**.

   The conference configuration displays in the **Output Messages:** box.

To change the conference configuration, see *Configure Conference on page 289*.

Show Fax Codec List

The Show Fax Codec List page displays the supported fax codecs in the order of preference that they are offered during codec negotiation.

The following table shows the default ordering of fax formats in the fax codec list.

Table 25. Default Ordering of the Fax Codec List

Name	Description	Order
T.38	T.38 fax	1
PCMU	G.711 µ-law	2
PCMA	G.711 a-law	3

To view fax codec configuration:

1. Click **Configuration** > **Node Configuration** > **Show Fax Codec List**.

   The Show Fax Codec List page displays.
2. Click **Execute**.

   Fax codec configuration information displays in the **Output Messages:** box.

To change the fax codec list, see *Configure Fax Codec List on page 294*.

Show Call Progress Analysis Configuration

The Show Call Progress Analysis Configuration page displays the call progress analysis (CPA) settings for all of the three CPA templates stored on the Containerized Decomposed Media Server.

To view call progress analysis template settings:

1. Click **Configuration** > **Node Configuration** > **Show Call Progress Analysis Configuration**. The Show Call Progress Analysis Configuration page displays.
2. Click **Execute**.

   The call progress analysis template information for all three templates (the default template, template 1, and template 2) is displayed in the **Output Messages:** box.

To change the CPA settings, see *Configure Call Progress Analysis on page 295*.

Show Clip Path Translation

The Show Clip Path Translation page displays the mappings that have been specified between file path formats supported by a control agent and file path formats supported by the Containerized Decomposed Media Server.

To view configured clip path translations:

1. Click **Configuration** > **Node Configuration** > **Show Clip Path Translation**.

   The Show Clip Path Translation page displays.
2. Click **Execute**.

   Clip path translation information displays in the **Output Messages:** box.

To change the clip path translations, see *Configure Clip Path Translation on page 298*.

Show Core Allocation

The Show Core Allocation page displays the CPU core allocations for the instance. The information shown on this page is detected for the platform.

To view core allocation:

1. Click **Configuration** > **Node Configuration** > **Show Core Allocation**.

   The Show Core Allocation page displays.
2. Select the **Instance number** from the drop-down list.

   The default value is **all**.
3. Click **Execute**.

   The core allocation information displays in the **Output Messages:** box.

Show Text Codec List

The show text codec list page displays the text codecs supported on the Containerized Decomposed Media Server and the order of preference in which the codecs are offered during codec negotiation.

To view Text Codec List:

1. Click **Configuration** > **Node Configuration** > **Show Text Codec List**.
2. Click **Execute**.

The codec list information displays in the **Output Messages:** box.

Show Resource Server Redundancy

The Show Resource Server (RS) Redundancy page enables you to view the configured resource servers.

To view the configured resource servers:

1. Click **Configuration** > **Node Configuration** > **Show Resource Server Redundancy**.

   The Show Resource Server Redundancy page displays.
2. Select the **Resource Server** from the drop-down list. The default value is **all**.

   NOTE: Select **all** from the Resource Server drop-down list to view all the configured resource servers.
3. Click **Execute**.

   The configured resource server information displays in the **Output Messages:** box.

To change the Resource Server configuration, see *Configure Resource Server Redundancy on page 300*.

Show SNMPv3 User and Trap Destinations

The Show SNMPv3 User and Trap Destinations page displays the configured SNMPv3 users and trap destinations details.

To view the SNMPv3 user and trap destinations:

1. Click **Configuration** > **Node Configuration** > **Show SNMP v3 User and Trap Destinations.**

   The Show SNMPv3 User and Trap Destinations page displays.
2. Click **Execute**.

   The SNMPv3 user and trap destinations information displays in the **Output Messages:** box.

Show Per Port Statistics Configuration

The Show Per Port Statistics Configuration page enables you to view the configured per-port statistics settings for 3PCC services.

To view the configured per-port statistics settings:

1. Click **Configuration** > **Node Configuration** > **Show Per Port Statistics Configuration**.

   The Show Per Port Statistics Configuration page displays.
2. Click **Execute**.

   The configured per-port statistics information displays in the **Output Messages:** box.

Show MSCML Configuration

You can view which all MSCML parameters are configured on the Containerized Decomposed Media Server. The information shown on this page is set on the Configure MSCML page.

To view the MSCML information:

1. Click **Configuration** > **Node Configuration** > **Show MSCML Configuration**.

   The Show MSCML Configuration page displays.
2. Click **Execute**.

   The MSCML information is displayed in the **Output Messages:** box.

Show Netconf Agent Configuration

The Show Netconf Agent Configuration page displays the NETCONF agent configuration for the NETCONF session. The information displayed on this page is set on the Configure Netconf Agent page.

To view the NETCONF agent information:

1. Click **Configuration** > **Node Configuration** > **Show Netconf Agent Configuration**.

   The Show Netconf Agent Configuration page displays.
2. Click **Execute**.

   The NETCONF agent information is displayed in the **Output Messages:** box.

Show System Security Configuration

The Show System Security Configuration page displays the system security configuration. The information displayed on this page is set on the Configure System Security page.

To view the system security information:

1. Click **Configuration** > **Node Configuration** > **Show System Security Configuration**.

   The Show System Security Configuration page displays.
2. Click **Execute**.

   The system security information is displayed in the **Output Messages:** box.

Show Keyword Detection Configuration

The Show Keyword Detection Configuration page displays the keyword list, uploaded model file, mode type, and configured Automatic Gain Control (AGC) information on the Containerized Decomposed Media Server.

The information displayed on this page is set on the *Configure Keyword Detection* page.

To view the keyword detection information:

1. Click **Configuration** > **Node Configuration** > **Show Keyword Detection Configuration**.

   The Show Keyword Detection Configuration page displays.
2. Click **Execute**.

   The configured keywords and AGC information is displayed in the **Output Messages:** box.

Show TLS

The Show TLS page displays the configured Transport Layout Security (TLS) information.

The information shown on this page is set on the *Configure TLS* page.

To view TLS Configuration information:

1. Click **Configuration** > **Node Configuration** > **Show TLS**.

   The Show TLS page displays.
2. Click **Execute**.

   The Output Messages: box displays the configured TLS information.

Show ICE Configurations

The Show ICE page display the Interactive Connectivity Establishment (ICE) Information.

To view ICE information:

1. Click **Configuration** > **Node Configuration** > **Show ICE Configurations**.

   The Show ICE page displays.
2. Click **Execute**.

   The **Output Messages:** box displays the ICE information.

Set MRFP Service Mode

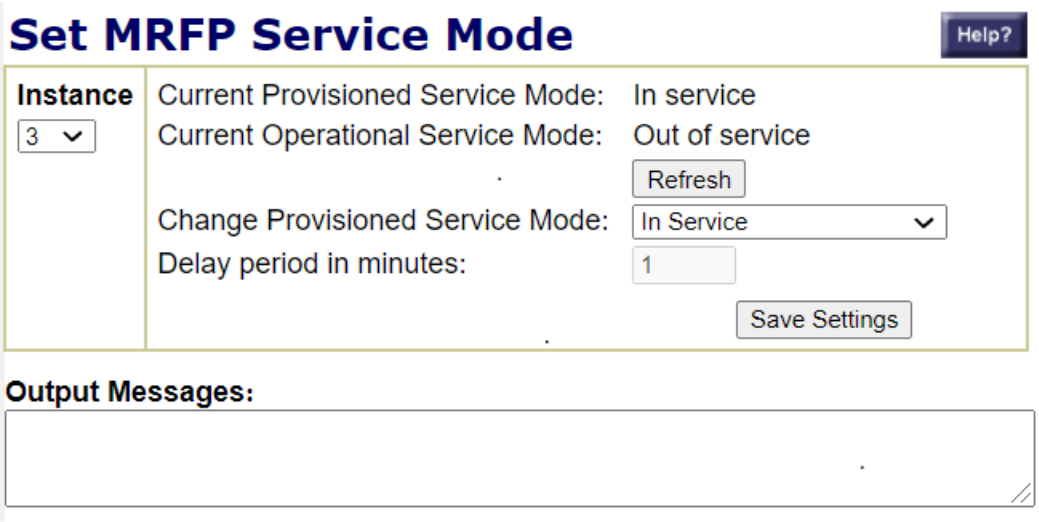
The Set MRFP Service Mode page allows you to set the status of an MRFP.

You can put an MRFP in service or take it out of service. Taking a instance out of service makes it unavailable for provisioning services.

To set the MRFP service mode:

1. Click **Configuration** > **Node Configuration** > **Set MRFP Service Mode**.

   The Set MRFP Service Mode page displays.



2. Select the **Instance Number** to set the service mode.

   NOTE: Warning message is displayed when the selected MRFP instance in a redundancy group.
3. Click **Refresh** to display the current service mode information.

4. In the **Change Provisioned Service Mode** list, choose the mode type. If you are taking the instance out of service, choose one of the following:
   - **Normal.** Takes the instance out of service only after it is no longer busy.
   - **Forced.** Takes the instance out of service immediately, whether or not there are active services provisioned on it. This may affect service on the instance.
   - **Delayed.** Takes the instance out of service after a delay that you specify. You can specify a delay between 1 and 720 minutes.
     - If the instance is not busy, it is taken out of service immediately.
     - If the instance is busy, then no new ports are created on the instance during the delay interval, and existing ports are allowed to finish naturally until the delay period expires.
     - When the delay period expires, any remaining active ports are closed and the instance is taken out of service.
5. Select **Yes** for the warning message to enable **Save Settings**, else select **No**. By default it is set to **No**.
6. Click **Save Settings**.

   The changes take effect immediately. A confirmation message displays in the **Output Messages:** box.
7. Click **Refresh** to display the current service mode information.

Show CPV Layout Template Configuration

The Show CPV Layout Template Configuration page displays the template types configured for the Continuous Presence Video (CPV) layout. The information displayed on this page is set on the *Configure CPV Layout Template on page 321*.

To view the CPV layout template configuration information:

1. Click **Configuration** > **Node Configuration** > **Show CPV Layout Template Configuration**.

   The Show CPV Layout Template Configuration page displays.
2. Click **Execute**.

   The CPV Layout Template Type Configuration information is displayed in the **Output Messages:** box.

Configure MRCP

The Configure MRCP page enables you to specify how the Containerized Decomposed Media Server handles connections with MRCP servers.

The following table shows MRCP values that can be configured.

Table 26. Configurable MRCP Information

Value	Description
Server	Mandatory. Selects an MRCP server to configure. The supported value range is 1 to 40. Changes to this field take effect immediately.
MRCP Version	Optional. The version of the MRCP protocol to be supported for all servers connecting to the Containerized Decomposed Media Server. The supported values are: • **MRCP v1**. MRCP v.1 is used. • **MRCP v2**. MRCP v.2 is used. The default value is MRCP v1. To change the MRCP version, you must first disable all servers. Before enabling the servers again, you must reboot the Containerized Decomposed Media Server (or change the MRCP version). The Containerized Decomposed Media Server does not allow you to enable servers if the configured version for MRCP is different from the run-time version. Changes to this field require a MRFP restart to take effect.
Request Timeout	Optional. The time, in seconds, that the Containerized Decomposed Media Server waits for a reply to an MRCP request. If a response is not received before the timeout expires, the MRCP server is considered as down. The supported value range is 1 to 30. The default value is 5. Changes to this field take effect immediately.
Disable All Servers	Optional. Disables all the servers. If this field is unchecked, but a specific server has an operational mode of disabled, the server remains disabled.
Set Speech Server Properties From Protocol	Optional. Specifies whether the Containerized Decomposed Media Server sends MRCP headers to override the external speech server's ASR and/or TTS properties, such as confidence threshold, fetch timeouts, and so on. • If this field is checked, the Containerized Decomposed Media Server constructs an MRCP header based on a number of properties, which can be set as VoiceXML properties but are not configurable in MSML. • If this field is unchecked, ASR and TTS property settings are determined by external speech server configuration. By default, this field is checked. Changes to this field take effect immediately.

Table 26. Configurable MRCP Information

Value	Description
Include Start-Input-Timer	Includes or excludes the `Start-Input-Timers` header in the RECOGNIZE request sent to the MRCP v.2 server. This is applicable only for VXML context. • If this field is checked, the Containerized Decomposed Media Server includes the `Start-Input-Timers` header in the RECOGNIZE request. • If this field is unchecked, the Containerized Decomposed Media Server excludes the `Start-Input-Timers` header in the RECOGNIZE request. ***NOTE:*** If the **Set Speech Server Properties from Protocol** field is checked, it overrides the **Include Start-Input-Timer** settings and includes the `Start-Input-Timers` header in the RECOGNIZE request. By default, this field is unchecked. Changes to this field take effect immediately.
Start-Input-Timer Value	Allows to configure the value of the `Start-Input-Timers` header in the MRCP v.2 RECOGNIZE request. This is applicable only for VXML context. The supported values are: • **True.** The value of the `Start-Input-Timers` header is set to **true** in the RECOGNIZE request. • **False.** The value of the `Start-Input-Timers` header is set to **false** in the RECOGNIZE request. The default value is False. Changes to this field take effect immediately.
MRCP Max Connection Time(sec)	Allows to configure the maximum connection time, in seconds, for the MRCP server. The supported value range is from 60 to 3600. The default value is 0. ***NOTE:*** This field is applicable only for MRCP v2. This field is disabled when the **MRCP Version** is set to MRCP v1. Changes to this field require a MRFP restart to take effect.
Server Operational Mode	Optional. Enables or disables the server being configured. The supported values are: • **Enabled.** The server is operationally enabled. • **Disabled.** The server is operationally disabled. ***NOTE:*** If the **Disable All Servers** is unchecked and this field is set to Disabled, the server remains disabled. The default value is Disabled. Changes to this field take effect immediately.
Server Name	Optional. A name associated with this server, maximum of 32 characters. Any references specifically to this server within protocol scripts, such as a VoiceXML script, must use this name. By default, the server is assigned the name MRPC_Server_X, where X is the number of the server being configured. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.

Table 26. Configurable MRCP Information

Value	Description
Server URI	Mandatory. The URI that control traffic must use to connect with the server. When the IP address or host name of the server is required, it is extracted from this URI. The URI may be up to 512 characters. Unsupported characters are "<>". ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.
Server Port	Optional. The TCP port used for sending MRCP traffic to the server. The supported value range is 554 or 1024 to 65535. For MRCP v2, this field is ignored and the port information is extracted from the URI. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.
Server Type	Mandatory. Specifies the type of MRCP server. The supported values are: • **ASR.** The server is an automatic speech recognition (ASR) server. • **TTS.** The server is a text-to-speech (TTS) server. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.
Server Language[a]	Optional. Specifies the languages supported by the server, maximum of 1024 characters. If this field is not configured, the MRCP server supports all the languages for backward compatibility reasons. Each MRCP server supports up to 32 languages. The language names can be delimited using the semi-colon (;) character. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.
Offered Codec	Optional. Specifies the codec offered to the external server during codec negotiation. The supported values are: • **pcmu**. G.711 μ-law is offered. • **pcma**. G.711 a-law is offered. The default is pcmu. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.
Server Capacity	The number of connections that is supported by the server. This value is used by the load balancing algorithm to determine which servers are operating closer to capacity. The supported value range is 0 to 9999, where 0 means unlimited capacity. The default value is 100. ***NOTE:*** This field is disabled when the **Server Operational Mode** is enabled. Changes to this field take effect immediately.

[a] The session is connected to the In-Network engine if the English-US language is configured. If both the In-Network and cloud engine are present, the Google engine is considered a universal engine; thus, all requests for any other language are directed to the Google engine. If other languages (for example, Chinese, French, or so on) are configured in the Azure engine, the request to the Media Server for Chinese and French translation ends in the Azure engine. When the In-network and Azure engine licenses are completed, further license requests are terminated in the Google engine.

You can view the information set on this page on the *Show MRCP Configuration on page 182*.

There are a number of properties that are activated as part of support for voice-based grammars. These property values are passed to the specified ASR speech recognizer when a grammar is activated through the equivalent MRCP header field. If a value is not specified, default values are used for these properties.

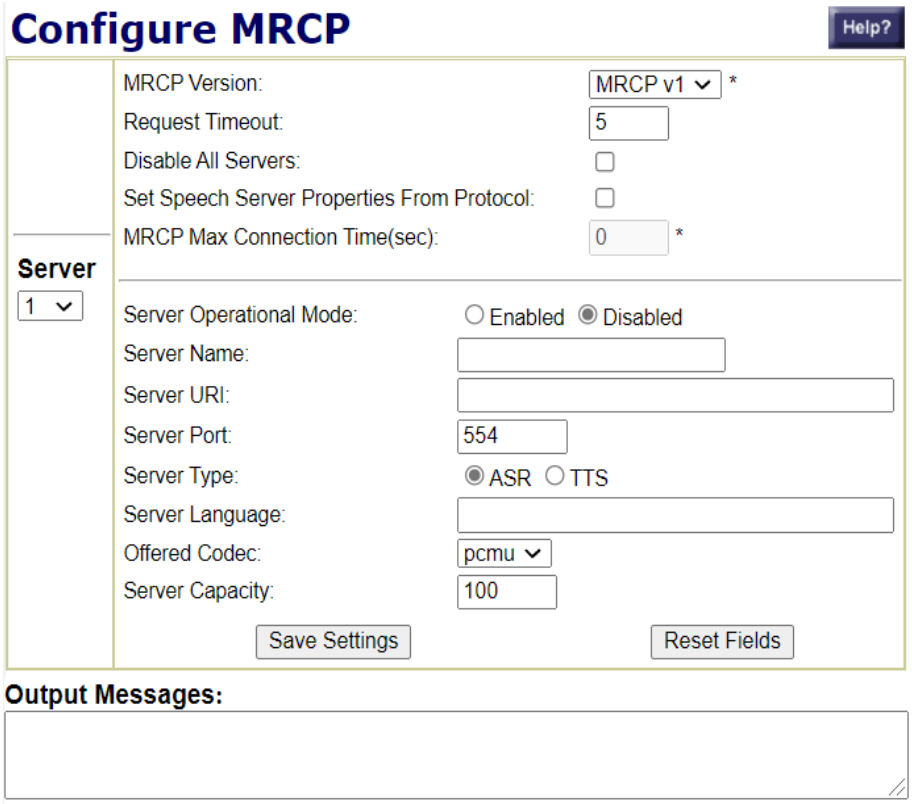
These values can be configured on the external speech server. Alternatively, the Containerized Decomposed Media Server can be configured to set these values through the control protocol by configuring the Containerized Decomposed Media Server through the management interface. If VoiceXML is the control protocol, these values are set through the MRCP speech recognizer properties. If MSML is the control protocol, the default value listed for the property is set.

For information on the MRCP speech recognizer properties, refer to *VXML Interface Reference*.

To configure MRCP:

1. Click **Configuration** > **Node Configuration** > **Configure MRCP**.

   The Configure MRCP page displays.



2. Select the MRCP server to configure.
3. Enter the other MRCP information described in the table above.
4. Click **Save Settings**.

   Changes to MRCP version require a restart to take effect. Other changes take effect immediately.

   Confirmation message displays in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

In addition to requiring a restart, changing the MRCP version number requires that all speech servers be disabled before making the change. The Containerized Decomposed Media Server must be restarted before the speech servers can be enabled again.

NOTE: When you change the **Server Operational Mode** from disabled to enabled, the MRCP server can take a maximum of two minutes to update the correct server status.

To change MRCP version:

1. Disable all speech servers.
2. Change the MRCP version setting, as well as any other setting changes (such as server URI, if necessary).
3. Restart MRFC and MRFP.
4. Enable the speech servers.
5. Click **Save Settings**.

Configure SIP

The Configure SIP page enables you to configure control protocol settings for the Containerized Decomposed Media Server controlled by SIP.

In SIP communication, sessions are initiated by the control agent, and addressing information is included as part of the initial SIP messages. The control agent addressing information must be configured on the Containerized Decomposed Media Server when SIP is the control protocol.

The following table shows the information you can configure when SIP is the control protocol.

Table 27. SIP Information Required

Value	Description
Node SIP Port	Optional. The SIP receive control port, on which the MRFP is listening for SIP messages. The value range is from 1 through 65535. The default value is 5060. The SIP transmit control port is dynamic, and is derived from the SIP INVITE message. The initial default for the transmit port is also 5060. Changes to this field require a MRFP restart to take effect.
Minimum Session Expiration Time	Optional. When SIP Session Timer enables negotiating session expiration, this value, in minutes, is used as the MRFP default for the Min-SE header. The Min-SE header indicates the minimum session interval the MRFP accepts. The value range is from 1 through 600. The default value is 600. Changes to this field take effect immediately.
Session Expiration Time	Optional. When SIP Session Timer enables negotiating session expiration, this value, in minutes, is used as the MRFP default for the Session-Expires header. The Session-Expires header establishes the session interval. A session that has not received a refresh request, halfway through the interval, expires at the end of the interval. Sessions for which no interval is negotiated persist indefinitely till the caller hangs up. The value range is from 1 through 600. The default value is 600. Changes to this field take effect immediately.
SIP Session Timer	Optional. Enables or disables the SIP session timer. The supported values are: • **Enabled**. Enable SIP session timer. • **Disabled.** Disable SIP session timer. The default value is Enabled. Changes to this field take effect immediately.

SIP Custom Profile	Optional. Enables or disables specific SIP messaging behavior. The supported values are:
	• **None.** No customization. Retains the Containerized Decomposed Media Server previous behavior.
	• **Custom 1.** Changes the Containerized Decomposed Media Server behavior as follows:
	  • The Containerized Decomposed Media Server returns a 404 response for failed announcements not involving early-media.
	  • The Containerized Decomposed Media Server returns a 404 response rather than 400, 488, or 606 responses when invalid or unacceptable SDP is received.
	  • The Containerized Decomposed Media Server returns a 501 response for a service context error.
	  • The Containerized Decomposed Media Server returns a 486 response, when the Containerized Decomposed Media Server does not have sufficient port license to handle the request.

Table 27. SIP Information Required

Value	Description

	• **Custom 2.** Changes the Containerized Decomposed Media Server behavior as follows:
	  • The Containerized Decomposed Media Server includes the **c= line** at the session level of SDP.
	  • When offering G.711 fax, the Containerized Decomposed Media Server always includes **a=Fax** in the SDP offer. When answering G.711 fax, the Containerized Decomposed Media Server includes either a=Fax or a=Modem in the SDP answer.
	  • Default **ptime** for G.711 fax is 20 ms.
	  • SDP parsing is case-insensitive.
	• **Custom 3.** Changes the Containerized Decomposed Media Server behavior as follows.
	  • When an unknown service identifier is received in the SIP INVITE request, the Containerized Decomposed Media Server returns error code 488.
	• **Custom 6.** Changes the Containerized Decomposed Media Server behavior as follows.
	  • When receiving a mid-call change request on an active SRTP port to put a call on hold (0.0.0.0), the Containerized Decomposed Media Server sets the local IP address (IPv4 and IPv6) to zero and puts the SRTP port on-hold; ignores incoming and outgoing SRTP packet. If RTCP is enabled, the paired SRTCP port is put on hold.
	  • When receiving a mid-call change request (to resume a call with non zero (0.0.0.0) IP address) on an on-hold SRTP port, the Containerized Decomposed Media Server restores the original local IP address (IPv4 and IPv6) and re-activates the SRTP port. If RTCP feature is enabled, the paired SRTCP port is re-activated. Reactivating the port resets the crypto context from the beginning.
	  • The Containerized Decomposed Media Server does not send re-INVITE to complete the lock down procedure in B2BUA when SIP Custom 6 is configured. It is used to disable the re-INVITE lock down procedure in B2BUA.
	  • The Custom 6 profile is not applicable for Containerized Decomposed Media Server.
	• **Custom 7.** None
	The default value is None.
	Changes to this field require a MRFP restart to take effect.

Table 27. SIP Information Required

Value	Description

	• **Custom 8.** Changes the Containerized Decomposed Media Server behavior as follows.
	  • For the initial MSCML `<configure_conference>` request that is included in the SIP-INVITE request of the control call-leg, the Containerized Decomposed Media Server generates the MSCML response in a separate SIP-INFO message after the INVITE transaction is completed. The response body remains same.
	  • For the initial MSCML `<configure_leg>` request that is included in the SIP-INVITE request of participant call-leg, the Containerized Decomposed Media Server generates the MSCML response in a separate SIP-INFO message after the INVITE transaction is completed. The response body remains same.
	  • The supported value range of **delay** parameter in the SIP Standards Profile **Profile 1** is from 0 to 99999 milliseconds. Now, the same value is extended to the **Default** profile.
	NOTE:
	• After Containerized Decomposed Media Server downgrade, the **Custom 8** profile becomes the default profile.
	• When the **Custom 8** profile is configured, MRFP restart is required and the MNGT switchover needs to be performed.
	The default value is None.

SIP Standards Profile	Optional. Assists the MRFP to comply with one of the SIP standards. The supported values are:
	• **Default.** Retains the MRFP previous behavior.
	• **Profile 1.** Changes the MRFP behavior as follows:
	  • The MRFP initial VoiceXML document retrieval behavior is modified, and the MRFP returns a 404 response code for failed VoiceXML document fetch.
	  • The MRFP returns a 503 response for unavailable resource.
	  • The SIP Request-URI **delay** parameter is measured in units of milliseconds (instead of 100-milliseconds increments) and can be set to up to 99999 milliseconds.
	The default value is Default.
	Changes to this field require a MRFP restart to take effect.

Precondition Call Flow Profile	Optional. Allows you to configure precondition call flow profiles. The supported values are: • **Default.** The Containerized Decomposed Media Server SIP behavior is similar to previous implementations. The Containerized Decomposed Media Server always sends 183 (session progress) response for an initial INVITE, regardless whether the remote precondition condition is met in the initial INVITE request. • **Profile 1.** The Containerized Decomposed Media Server sends 200 OK response as per 3GPP TS24.930 instead of 183 response for an initial INVITE, if remote precondition is already met in an INVITE request. The default value is Default. ***NOTE:*** Precondition is only applicable in MSML, VXML, and MSCML contexts.

Table 27. SIP Information Required

Value	Description
SIP Message Serialization	Enables serialization of SIP messages. The supported values are: • **Enabled.** The MRFP serializes multiple SIP messages and does not send the new SIP messages till previous messages on the same SIP dialog are received (that is, the final response is received). • **Disabled.** The MRFP sends multiple SIP messages concurrently. By default, this option is Disabled. Changes to this field require a MRFP restart to take effect.
RFC 4317 Call Flow Support	Mandatory. Enables or disables the SIP RFC 4317 Call Flow Support. The supported values are: • **Enabled.** The SIP RFC 4317 Call Flow Support is enabled. When enabled, the MRFP includes multiple codecs in the SDP answer based on the resource availability and expects re-INVITE / UPDATE offer for codec lock-down in point to point transcoding using **sip:tc** service context. • **Disabled.** The SIP RFC 4317 Call Flow Support is disabled. When disabled, the MRFP locks down the codec on initial INVITE offer in point to point transcoding using **sip:tc** service context. The default is Disabled. The changes to this field take effect immediately on the next **sip:tc** call without restarting the MRFP. ***NOTE:*** Only the call flow of RFC 4317 (section 2.2) is supported.
MSML Version Number	Optional. Specifies the MRFP which version of Media Sessions Markup Language (MSML) to use. The supported value is v1.1. Changes to this field require a MRFP restart to take effect.
MSML Announcement Override	Optional. Enables or disables overriding MSML announcements. When enabled, after receiving an MSML request to play a new announcement, the MRFP stops the currently playing announcement and plays the new announcement. The supported values are: • **Enabled.** Currently playing announcement is stopped, new announcement is played. • **Disabled.** Currently playing announcement continues uninterrupted, new announcement is rejected. The default is Enabled. Changes to this field take effect immediately.
MSML Single Clip Variable (date and time) Announcement	Enables or disables MSML single clip variable (date and time) announcement. The supported values are: • **Enabled.** The MRFP supports single clip announcement for day (1-31), hour (0-23), and minute (0-59). • **Disabled.** The MRFP does not support single clip announcement and uses multi clips for playing date or time variables. The default is Disabled. Changes to this field take effect immediately.

Table 27. SIP Information Required

Value	Description
Netann DTMF Pass-through	Enables or disables DTMF pass-through in the SIP Netann conference. When DTMF pass-through is enabled, the Containerized Decomposed Media Server collects and relays the DTMF tones 0 through 9, *, #, and A through D. The Containerized Decomposed Media Server collects the DTMF digits from the conference member and relays to the other members of the conference. DTMF pass-through is supported for a maximum of 125 participants (the maximum conference size in SIP Netann conferences). Pass-through is supported in conferences where participants use a mix of in-band and out-of-band DTMF tones. Pass-through of CNG signals (fax tone) is not supported. By default, DTMF pass-through is disabled and the Containerized Decomposed Media Server clamps in-band DTMF in SIP Netann conferences. When pass-through is enabled, it is enabled for all the conference calls established on the device. Changes to this field take effect immediately for any new conferences or new ports joining the existing conferences. Existing ports in existing conferences do not have any impact.
Msml DTMF Pass-through	Enables or disables DTMF pass-through in the MSML conference. When DTMF pass-through is enabled, the Containerized Decomposed Media Server collects and relays the DTMF tones 0 through 9, *, #, and A through D. The Containerized Decomposed Media Server collects the DTMF digits from the conference member and relays to the other members of the conference. DTMF pass-through is supported for a maximum of 125 participants. Pass-through is supported in conferences where participants use a mix of in-band and out-of-band DTMF tones. Pass-through of CNG signals (fax tone) is not supported. By default, DTMF pass-through is disabled. When pass-through is enabled, it is enabled for all the conference calls established on the device. ***NOTE:*** When DTMF pass-through is enabled through the Web GUI, it overwrites the DTMF clamping settings. Changes to this field take effect immediately for any new conferences or new ports joining the existing conferences. Existing ports in existing conferences do not have any impact.
Priority Management	Optional. Enables or disables SIP-based priority management. The supported values are: • **Enabled.** Enables SIP-based priority management. • **Disabled.** Disables SIP-based priority management. The default value is Disabled. Changes to this field require a MRFP restart to take effect.
Priority Queue Max Waiting Time	Optional. Defines how long, in seconds, a SIP priority call can remain in the queue before it is timed out. The range of values is 5 through 120. The default is 15. Changes to this field take effect immediately.
Timer T1	Optional. The estimated round trip, in milliseconds, used for the initial transaction retransmit interval. Range is from 100 through o 5000. The default is 500. Changes to this field take effect immediately.

Table 27. SIP Information Required

Value	Description
Timer T2	Optional. The maximum retransmit interval, in milliseconds, used for non-INVITE requests and responses to INVITEs. Range is from 1000 through 10,000. The default is 4000. Changes to this field take effect immediately.
Timer T4	Optional. The maximum duration, in milliseconds, that a message remains in the network. Range is from 1000 through 10,000. The default is 5000. Changes to this field take effect immediately.
Preferred IP Type for Media Sessions in MS Initiated SDP Offers	Optional. Sets the preferred IP type, either IP version 4 or IP version 6, for media sessions where the Containerized Decomposed Media Server initiates an SDP offer. The supported values are: • **IPv4.** IP version 4 • **IPv6.** IP version 6 The default value is IPv4. Changes to this field take effect immediately.
Media Control Channel TCP Port Number	This field is not supported on the Containerized Decomposed Media Server.
Preferred SDP “a=rtcp-xr” syntax	The supported SDP syntax in the Containerized Decomposed Media Server SDP for rtcp-xr are. • a**=rtcp-xr** The Containerized Decomposed Media Server sends **a=rtcp-xr** in the SDP without colon. • **a=rtcp-xr:** The Containerized Decomposed Media Server sends **a =rtcp-xr** in the SDP with colon. The default is a=rtcp-xr.
RTP mode ("sendrecv") as per RFC 6337	Optional. The supported values are: • **Enabled.** The Containerized Decomposed Media Server sets the RTP media direction attribute to sendrecv, in a 200 OK SDP offer in response to re-INVITE without SDP. • **Disabled.** The Containerized Decomposed Media Server sends the last negotiated RTP media direction. The default is Disabled. Changes to this field take effect immediately.
SDP Capability Negotiation Feature	Enables or disables SDP Capability Negotiation when the Containerized Decomposed Media Server acts as an offerer. The supported values are: • **Enabled.** Enables SDP Capability Negotiation when the Containerized Decomposed Media Server acts as offerer. • **Disabled.** Disables SDP Capability Negotiation when the Containerized Decomposed Media Server acts as offerer. The default is Enabled. ***NOTE:*** The Containerized Decomposed Media Server does not depend on this OAMP parameter when acting as answerer.

Table 27. SIP Information Required

Value	Description
SDP Capability Negotiation Re-offer	Enables or disables SDP Capability Negotiation Re-offer when the Containerized Decomposed Media Server acts as an offerer. The supported values are: • **Enabled.** Enables SDP Capability Negotiation Re-offer when the Containerized Decomposed Media Server acts as offerer. • **Disabled.** Disables SDP Capability Negotiation Re-offer when the Containerized Decomposed Media Server acts as offerer. The default is Disabled. ***NOTE:*** • The SDP Capability Negotiation Re-offer is non-configurable if SDP Capability Negotiation Feature is disabled. • As per RFC 5939, the Containerized Decomposed Media Server offerer using SDPCapNeg in the initial SDP offer receives an answer which accepts the potential configuration and the Containerized Decomposed Media Server initiates a re-offer containing the potential configuration as the actual configuration.
Full Capabilities in Mid Call offer	Enables or disables full capabilities in a mid-call offer. The supported values are: • **Enabled.** When re-INVITE without SDP is received for a port, the Containerized Decomposed Media Server sends the full capabilities in a mid-call Offer in 200 OK. • **Disabled.** The Containerized Decomposed Media Server continues to send the current port setting in 200 OK. The default value is Enabled. The changes to this field take effect on the next call and the settings for the existing calls are preserved during switchover.
Sip Locale Interpretation Method	Allows you to configure the interpretation method of the **locale** parameter while forming the clip path through management interface. This is applicable in SIP netann service context. The supported values are: • **Default.** For a file with the format file*://<path>/<fname>.wav* with *locale=<language-tag>*, the interpretation is /<provisioned>/<language-tag>/<path>/<fname>.wav • **Method 1.** For a file with the format file*://<path>/<fname>.wav* with *locale=<language-tag>*, the interpretation is /<provisioned>/<path>/<language-tag>/<fname>.wav The default value is Default. Changes to this field take effect immediately.
Default Locale	Allows the Containerized Decomposed Media Server to use the default locale when the user does not specify the locale in the request. The default locale is applicable for Netann announcements and all the MSCML prompt requests. The supported length is 128 characters. The default value is empty. Changes to this field take effect immediately.

Table 27. SIP Information Required

Value	Description
Contact Feature Tag	Enables or disables the Contact Feature Tag. The supported values are: • **Enabled.** If the initial INTIVE request from the far-end includes audio and video media feature tags in the `Contact` header, the Containerized Decomposed Media Server mirrors the corresponding media feature tags in the non-100 provisional and 2XX final response. • **Disabled.** The Containerized Decomposed Media Server ignores the audio and video media tags in the `Contact` header of the incoming INVITE request and does not include media tags in the subsequent in-dialog requests or responses. The default value is Disabled. Changes to this field take effect on the next call.
SIP over TLS	Enables or disables the Transport Layer Security (TLS) for SIP calls. The supported values are: • **Enabled.** The Containerized Decomposed Media Server listens on the SIP-TLS port for incoming connection requests. The Containerized Decomposed Media Server supports end-to-end TLS using transport =TLS in the Request-URI. • **Disabled.** The Containerized Decomposed Media Server does not send the SIP request using TLS. The default value is Disabled. Changes to this field require MRFP restart to take effect. ***NOTE:*** The Containerized Decomposed Media Server does not support this feature for the ASR or TTS interfaces.
SIP-TLS Port	Port number used for SIP-TLS. The range is 1 to 65535. The default value is 5061. ***NOTE:*** The Containerized Decomposed Media Server does not allow you to assign the same port number for **Node SIP Port** and **SIP-TLS Port** through the management interfaces. Changes to this field require MRFP restart to take effect.
SIP-TLS Mutual Authentication	Enables or disables the SIP-TLS mutual authentication. The supported values are: • **Enabled.** When acting as a TLS server during a TLS handshake, the Containerized Decomposed Media Server sends a certificate request and authenticates the client. • **Disabled.** When acting as a TLS server during a TLS handshake, the Containerized Decomposed Media Server does not send a certificate request to the client. The default value is Enabled. Changes to this field require MRFP restart to take effect. ***NOTE:*** When acting as TLS client, the Containerized Decomposed Media Server accepts the certificate request from the TLS server regardless of the SIP-TLS Mutual Authentication configuration.

Table 27. SIP Information Required

Value	Description
SIP Priority Call Mgmt Method	Allows to configure the priority call management method. The supported values are: • **Basic.** In this method, the Containerized Decomposed Media Server handles the priority calls in an overload situation using the priority queuing algorithm. The Containerized Decomposed Media Server adds the incoming ets and wps priority calls to this queue if there are insufficient resources to handle the additional calls. • **Enhanced.** In this method, the Containerized Decomposed Media Server handles calls using call shedding algorithm. The wps namespace is optional and the Containerized Decomposed Media Server rejects the calls if only the wps namespace is present in the Resource Priority Header (RPH) Resource Priority Header (RPH). The default value is Basic. •
	Changes to this field require a MRFP restart to take effect.
SIP Response to sent-by Parameter of via Header	This field is not supported on the Containerized Decomposed Media Server.
Include b=AS in SDP Audio Media Description	Includes or excludes b=AS in the audio media description of the outgoing SDP. The supported values are: • **Enabled.** The Containerized Decomposed Media Server includes b=AS in the audio media description of the outgoing SDP. • **Disabled.** The Containerized Decomposed Media Server excludes b=AS in the audio media description of the outgoing SDP. The default value is Enabled. ***NOTE:*** This field is applicable only for MSML audio. Changes to this field take effect immediately.
Peer Authentication	Enables or disables peer authentication through IP validation, while establishing the SSL connection. The supported values are: • Enabled • Disabled The default value is Disabled. ***NOTE:*** • The **SIP-TLS Mutual Authentication** must be enabled to perform peer authentication when the Containerized Decomposed Media Server acts as client or server for the TLS connection. • When **SIP-TLS Mutual Authentication** is disabled and the Containerized Decomposed Media Server acts as a server for the TLS connection, the Containerized Decomposed Media Server does not query the client certificate and peer authentication cannot be performed. Therefore, the Containerized Decomposed Media Server skips the peer authentication. • When **SIP-TLS Mutual Authentication** is disabled and the Containerized Decomposed Media Server acts as a server for the TLS connection, the Containerized Decomposed Media Server performs peer authentication. Changes to this field require MRFP reboot to take effect.

Table 27. SIP Information Required

Value	Description
IPV4 Validation List	Allows to configure a list of IPv4 addresses that are verified at the server to authenticate the client certificates. The IPv4 addresses are represented as comma-separated values. When the Containerized Decomposed Media Server acts as a server for SSL connection, the Containerized Decomposed Media Server allows connection request only from the configured IP validation list. When the Containerized Decomposed Media Server acts as a client, the Containerized Decomposed Media Server is aware of the destination IP address and therefore validates the IP address received in the SSL certificate with the destination IP address. The default value is ' '. ***NOTE:*** This field can be configured only when **Peer Authentication** is enabled. Changes to this field require MRFP restart to take effect.
IPV6 Validation List	Allows to configure a list of IPv6 addresses that are verified at the server to authenticate the client certificates. The IPv6 addresses are represented as comma-separated values. When the Containerized Decomposed Media Server acts as a server for SSL connection, the Containerized Decomposed Media Server allows connection request only from the configured IP validation list. When the Containerized Decomposed Media Server acts as a client, the Containerized Decomposed Media Server is aware of the destination IP address and therefore validates the IP address received in the SSL certificate with the destination IP address. The default value is ' '. ***NOTE:*** This field can be configured only when **Peer Authentication** is enabled. Changes to this field require MRFP restart to take effect.
MSML Bypass Announcement Resource Reservation	Enables or disables upfront transcode bypass announcement resource reservation on MSML ports. The supported values are: • **Enabled.** The Containerized Decomposed Media Server performs upfront resource reservation (DSP CPU, buffers, and bandwidth) that are required for the transcode bypass announcement. • **Disabled.** The Containerized Decomposed Media Server does not perform any upfront resource reservation. The default value is Disabled. Changes to this field take effect on the next MSML INVITE request.
Add Connection Address In Session Level	Includes or excludes c=line at the session-level attribute in the SDP negotiation. The supported values are: • **Enabled.** For the SDP negotiation, the Containerized Decomposed Media Server includes c=line only at the session-level attribute. • **Disabled.** For the SDP negotiation, the Containerized Decomposed Media Server sends c=line only at the media-level attribute. The default value is Disabled. Changes to this field take effect immediately.

Table 27. SIP Information Required

Value	Description
Include fax tone events in SDP	Includes or excludes fax tone events in SDP for the telephone-event. The supported values are: • **Enabled.** The Containerized Decomposed Media Server includes the fax tones event types for CED (32) and CNG (36), along with DTMF (0-15) event types in the SDP **a=fmtp** attribute in the telephone-event of the outgoing SDP. • **Disabled.** The Containerized Decomposed Media Server includes only DTMF (0-15) event types in the SDP **a=fmtp** attribute in the telephone-event of the outgoing SDP. The default value is Enabled. ***NOTE:*** When this parameter is disabled, the Containerized Decomposed Media Server disables the out-of-band fax tone detection. Changes to this field take effect on the next SDP offer/answer.
SIP Session Refresher	Indicates the session refresher role when the initiator does not include a session **refresher** parameter in the `Session-Expires` header. • **Enabled.** The Containerized Decomposed Media Server acts as a session refresher by including **refresher=uas** in the `Session-Expires` header of the response and refreshes the session. • **Disabled.** The Containerized Decomposed Media Server requests the far-end to act as a session refresher by including **refresher=uac** in the `Session-Expires` header of the response. The default value is Enabled. ***NOTE:*** This field is configured only when **SIP Session Timer** is enabled. Changes to this field take effect immediately.
Include fmtp parameter for declined text line	Enables or disables the FMTP parameter for the declined text line. • **Enabled.** The Containerized Decomposed Media Server adds the FMTP parameter to the declined text line. • **Disabled.** The Containerized Decomposed Media Server does not add the FMTP parameter to the declined text line. The default value is Disabled. Changes to this field take effect immediately.

To configure SIP:

1. Click **Configuration** > **Node Configuration** > **Configure SIP**.

   The Configure SIP page displays.

Configure SIP

Help?

Node SIP Port:	5060 *
Minimum Session Expiration Time:	600 Minute(s)
Session Expiration Time:	600 Minute(s)
SIP Session Timer:	(●) Enabled ( ) Disabled
SIP Custom Profile:	None *
SIP Standards Profile:	Default *
Precondition Call Flow Profile:	Default
SIP Message Serialization:	( ) Enabled (●) Disabled *
RFC 4317 Call Flow Support:	( ) Enabled (●) Disabled
MSML Version Number:	v1.1 *
MSML Announcement Override:	( ) Enabled (●) Disabled
MSML Single Clip Variable (date and time) Announcement:	( ) Enabled (●) Disabled
Netann DTMF Pass-through:	( ) Enabled (●) Disabled
Msml DTMF Pass-through:	( ) Enabled (●) Disabled
Priority Management:	( ) Enabled (●) Disabled *
Priority Queue Max Waiting Time:	15 Seconds
Timer T1:	500 Milliseconds
Timer T2:	4000 Milliseconds
Timer T4:	5000 Milliseconds
Preferred IP Type for Media Sessions in MS Initiated SDP Offers:	IPv4
Media Control Channel TCP Port Number:	9989 *
Preferred SDP "a=rtcp-xr" syntax:	a=rtcp-xr
RTP mode ("sendrecv") as per RFC 6337:	( ) Enabled (●) Disabled
SDP Capability Negotiation Feature:	(●) Enabled ( ) Disabled
SDP Capability Negotiation Re-offer:	( ) Enabled (●) Disabled
Full Capabilities in Mid Call offer:	(●) Enabled ( ) Disabled
Sip Locale Interpretation Method:	Default
Default Locale:	
Contact Feature Tag:	( ) Enabled (●) Disabled
SIP over TLS:	( ) Enabled (●) Disabled *
SIP-TLS Port:	5061 *
SIP-TLS Mutual Authentication:	(●) Enabled ( ) Disabled *
SIP Priority Call Mgmt Method:	Basic *
SIP Response to sent-by Parameter of via Header:	( ) Enabled (●) Disabled
Include b=AS in SDP Audio Media Description:	(●) Enabled ( ) Disabled
Peer Authentication:	( ) Enabled (●) Disabled *
IPV4 Validation List:	*
IPV6 Validation List:	*
Include both IPv4 and IPv6 for Media Sessions in MS Initiated SDP Offers:	(●) Enabled ( ) Disabled
MSML Bypass Announcement Resource Reservation:	( ) Enabled (●) Disabled
Add Connection Address In Session Level:	( ) Enabled (●) Disabled
Include fax tone events in SDP:	(●) Enabled ( ) Disabled
SIP Session Refresher:	(●) Enabled ( ) Disabled
Include fmtp parameter for declined text line:	( ) Enabled (●) Disabled

Save Settings Reset Fields

Output Messages:

2. Configure the SIP setting information as described in the above table.

3. Click **Save Settings**.

   The MRFP must be restarted for specific fields to take effect as mentioned in the table above.

   Confirmation message displays in the **Output Messages:** box.

4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Jitter Buffer Templates

The Configure Jitter Buffer Templates page enables you to set parameters for the jitter buffer.

You can view Information set on this page on the *Show Jitter Buffer Templates on page 183*.

The following table shows the jitter buffer templates information you can configure.

Table 28. Jitter Buffer Templates Information Required

Value	Description
Template number	Specifies the index number of the jitter buffer template to be used. The supported value range is from 1 to 10. The default (Template 0) is used when no jitter template is specified. The default is always used for RTSP and speech-server ports.
Jitter Buffer Size (10 - 500 ms)	Sets the size of the jitter buffer. This is used to account for discrepancies in the inter-arrival time of packets in a media stream. The jitter buffer must be set to at least twice the packetization period of the far-end device. For example, if the MRFP is receiving RTP packets from a VoIP gateway or a number of SIP phones with a maximum packetization period of 20 ms, the jitter buffer must be configured to at least 40 ms. It may be that you are unable to determine the maximum packetization period of far-end devices. In this case, you can either enable the automatic jitter buffer, or set the jitter buffer size to maximum. Out-of-band DTMF detection (RFC 2833 telephone-events) is not affected by this setting. RFC 2833/RFC 4733 packets bypass the MRFP jitter buffer and are passed directly through to the DSPs. The supported value range is from 10 to 500. The default value is 40. Changes to this field take effect immediately.
Automatic Jitter Buffer	Enables or disables the automatic jitter buffer packets. The automatic jitter buffer dynamically reduces end-to-end delay at peak periods in the network. When the automatic jitter buffer is enabled, the system uses the configured jitter buffer size as the maximum buffer size. Out-of-band DTMF detection (RFC 2833 telephone-events) is not affected by this setting. RFC 2833/RFC 4733 packets bypass the Containerized Decomposed Media Server jitter buffer and are passed directly through to the DSPs. The default value is disabled. Changes to this field take effect immediately.

Table 28. Jitter Buffer Templates Information Required

Value	Description
Jitter Buffer Operational Mode	Sets the operational mode of the automatic jitter buffer. In applications where reducing delay is imperative, the MRFP **aggressive** operational mode minimizes delay in its jitter buffer. This mode is suitable only in environments with small network jitter and clock skew. Typically the jitter buffer is set to **safe** mode. The jitter buffer in **aggressive** operational mode reduces the risk of dropping packets during surges in network jitter by functioning similarly to its **safe** operational mode for the duration of the surge. Once the surge subsides, the jitter buffer again operates as is typical for **aggressive** operational mode in a low-jitter network. A short hysteresis period in responding to a surge's leading and lagging edges prevents excessive switching between this safe-like and typical **aggressive** functioning. (At no point does the configured operational mode change—this switch to functioning similarly to **safe** operational mode is internal to the MRFP **aggressive** operational mode.) While functioning similarly to **safe** operational mode, during surge periods, delay through the Containerized Decomposed Media Server jitter buffer increases by 5 ms. Supported values are: • **safe.** Jitter buffer minimum delay adapted to typical networks. • **aggressive.** Jitter buffer delay is minimized. The default value is safe. Changes to this field take effect immediately.
Jitter Buffer Initial Delay (0 - 500 ms)	Sets the initial delay in milliseconds automatic jitter buffer. This value cannot exceed the value of Jitter Buffer Size or be smaller than the value of Jitter Buffer Minimum Delay. The supported value range is from 0 to 500. The default value is 40. Changes to this field take effect immediately.
Jitter Buffer Minimum Delay (0 - 500 ms)	Sets the minimum delay in milliseconds automatic jitter buffer. This value cannot exceed the value of Jitter Buffer Size. The supported value range is from 0 to 500. The default value is 0. Changes to this field take effect immediately.
Jitter Estimate Decay Time Constant (150 - 60000 ms)	Sets a time constant, in milliseconds, controlling the automatic jitter buffer's rate of decrease in size following a decrease in network jitter. When the network's jitter changes, the Containerized Decomposed Media Server automatic jitter buffer adapts by expanding or shrinking. A large buffer increases delay; a small buffer risks dropped packets. For large values: • The buffer size shrinks slowly, reducing the risk of dropping packets if network jitter decreases temporarily. • Delay reduction lags decreases in network jitter by a longer period of time. For small values: • Delay is more responsive to network jitter decreases. • Higher risk of dropping packets on temporary decreases in network jitter. The supported value range is from 150 to 60000. The default value is 5000. Changes to this field take effect immediately.

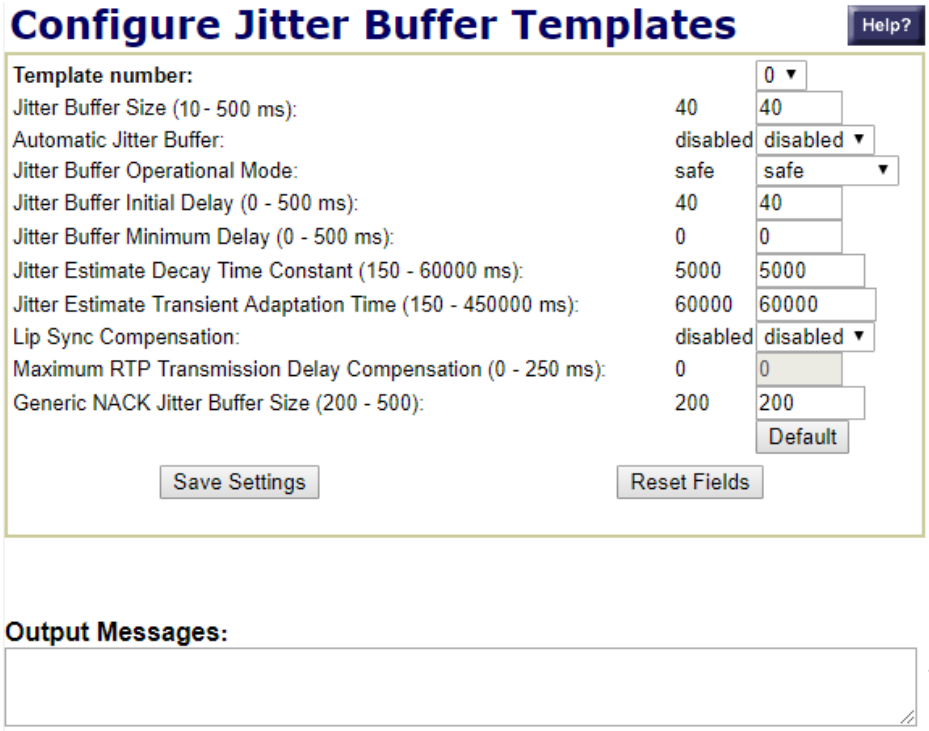
Table 28. Jitter Buffer Templates Information Required

Value	Description
Jitter Estimate Transient Adaptation Time (150 - 450000 ms)	Sets a time constant, in milliseconds, controlling the automatic jitter buffer's rate of increase in size following a high jitter measurement. When the network's jitter changes, the MRFP automatic jitter buffer adapts by expanding or shrinking. A large buffer increases delay; a small buffer risks dropped packets. For large values: • The buffer size expands slowly, keeping delay low despite spikes in network jitter. • Higher risk of dropping packets if network jitter increases rapidly. For small values: • Lower risk of dropping packets when network jitter increases rapidly. • Spikes in network jitter can increase delay. The supported value range is from 150 to 450000. The default value is 60000. Changes to this field take effect immediately.
Lip Sync Compensation	Enables lip sync compensation. Default value is false.Changes to this field take effect immediately.
Maximum RTP Transmission Delay Compensation (0 - 250 ms)	Sets the maximum amount of RTCP transmission delay equalization, in milliseconds. The supported value range is from 0 to 250. The default value is 0 (off). Changes to this field take effect immediately.
Generic NACK Jitter Buffer Size (200 - 500)	Sets the jitter buffer size for Generic-NACK, in milliseconds. This is required to maintain common audio and video jitter buffers (ingress and egress), which are used to support the missing RTP packet retransmissions by sending and receiving the Generic-NACK feedback messages. The supported value range is from 200 to 500. The default value is 200. ***NOTE:*** This setting overrides the **Jitter Buffer Size** configuration setting. Changes to this field take effect immediately.

To configure jitter buffer templates:

1. Click **Configuration** > **Node Configuration** > **Configure Jitter Buffer Templates**.

   The Configure Jitter Buffer Templates page displays.



2. Select the template you want to configure.
3. Enter the jitter buffer information as described in the above table.
4. Click **Default**. Populates the fields of the selected template with default values for all parameters.
5. Click **Save Settings** to commit the information.

   Changes take effect immediately.

   Confirmation message displays in the **Output Messages:** box.
6. Optionally, click **Reset Fields** to reset the changes made to previously saved values.

Configure Media ICMP

The Configure Media ICMP page enables you to specify the behavior of the MRFP media ports when they receive ICMP Destination Unreachable messages. The configured backoff behavior also applies when an IPv6 ICMP (ICMPv6) Packet Too Big message is received.

When a message is received the MRFP begins the following cycle of responses, on a port-by-port basis:

1. After a Destination Unreachable or a Packet Too Big message has been received on an RTP port, the MRFP stops sending on that port. The MRFP waits (“backs off”) for a specified retry period, and then begins transmitting again.
2. If another Destination Unreachable or a Packet Too Big message is received, the MRFP waits for an interval of 2* the original retry period, and then begins transmitting again.

3. This cycle of resuming transmission and backing off continues for a configured “retry number”, which is the total number of times the MRFP transmits (including the original transmission). The backoff period doubles for each successive iteration (T, 2T, 4T, and so on). If a Destination Unreachable message is received after the maximum configured allowable retries, the MRFP stops transmitting RTP permanently to that port.

   ICMP messages may be received during backoff periods. For example, this might happen when round-trip delays are larger than the packetization interval or when video sent in bursts causes a burst of returned ICMP messages. These additional messages are not counted toward the maximum retry number.
4. After RTP transmission has been permanently stopped, the configured parameter “automatic connection delete” is used to specify whether or not the connection must be deleted.
5. At any time during the transmission/backoff cycle, if the MRFP is able to transmit for a configured interval (the “reset time”) without receiving a Destination Unreachable or a Packet Too Big message, the algorithm resets to the initial retry period. The MRFP continues to transmit normally unless a new Destination Unreachable or a Packet Too Big message is received.

You can view the information set on this page on the *Show Node Configuration*.

The following table shows the media ICMP information you can configure.

Table 29. Media ICMP Information

Value	Description
Retry time (ms)	The initial “backoff” period in msec, after which the MRFP will attempt to transmit again. Retry time doubles with each successive iteration from the configured initial interval. For example, if retry time is configured to be 150 (T), the MRFP will initially wait 150 msec (T), will wait 300 msec (2T) in the second backoff period, 600 msec (4T) in the third backoff period, and so on. Retry time has a granularity of 10 msec. If you specify a value that is not a multiple of 10 (for example, 12), the value is rounded up to the next multiple of 10 (for example, to 20). Setting all three of retry time, number of retries, and reset timeout to 0 disables MRFP responses to an ICMP/ICMPv6 Destination Unreachable message or an ICMPv6 Packet Too Big message. The retry time and the number of retries must be set so that: *(2 * num-retries) * retry-time* < 2^32 The default is 150 msec. Changes to this field take effect immediately.

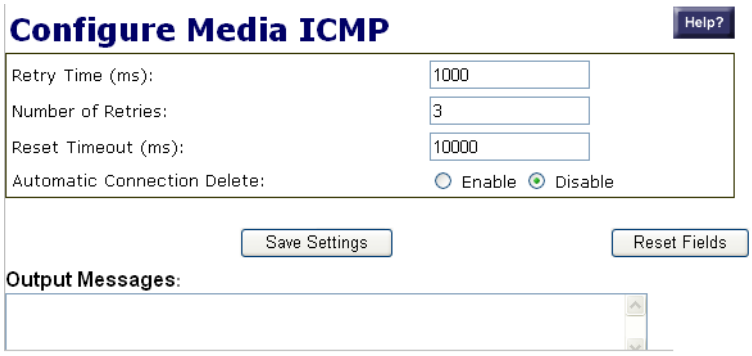
Table 29. Media ICMP Information

Value	Description
Number of retries	The maximum number of times in total that the MRFP will attempt to transmit. (This includes the initial transmission attempt.) After attempting to transmit the maximum number of times, the MRFP permanently stops transmitting RTP. Setting all three of retry time, number of retries, and reset timeout to 0 disables MRFP responses to an ICMP/ICMPv6 Destination Unreachable message or an ICMPv6 Packet Too Big message. The retry time and the number of retries must be set so that: *(2 * num-retries) * retry-time* < 2^32 The default is 3. Changes to this field take effect immediately.
Reset timeout (ms)	The amount of time in msec after which, if the MRFP successfully retransmits without receiving a Destination Unreachable or Packet Too Big message, the ICMP response algorithm resets to the initial configured retry time. Reset timeout has a granularity of 10 msec. If you specify a value that is not a multiple of 10 (for example, 251), the value is rounded up to the next multiple of 10 (for example, to 260). Setting all three of retry time, number of retries, and reset timeout to 0 disables MRFP responses to an ICMP/ICMPv6 Destination Unreachable message or an ICMPv6 Packet Too Big message. The retry time must be less than 2^32 milliseconds. The default is 10000 msec (10 seconds). Changes to this field take effect immediately.
Automatic connection delete	Allows you to specify whether a connection where RTP transmission has been permanently stopped should be automatically deleted. • **Enable.** Automatically delete connections where RTP has been stopped. • **Disable.** Do not delete connections where RTP has been stopped. The default is disable. Changes to this field take effect immediately.

To configure media ICMP:

1. Click **Configuration** > **Node Configuration** > **Configure Media ICMP**.

   The Configure Media ICMP page displays.



2. Enter the media ICMP information described in the table above.
3. To disable ICMP response, set all three of retry time, maximum allowable number of retries, and reset timeout to 0.
4. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message displays in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to previously saved values.

Configure Audio Codec List

The Configure Audio Codec List page enables you to customize the audio codec list and set the order in which codecs are offered in SIP for 3PCC calls.

NOTE: This audio codec list is for 3PCC codec negotiation.

An audio codec list allows the Containerized Decomposed Media Server to list supported codecs in order of preference for codec negotiation for a control protocol. Each control protocol has its own audio codec list.

When the Containerized Decomposed Media Server generates an offer, it offers all supported codecs listed on its preferred codec list, provided the Containerized Decomposed Media Server has sufficient resources to support the codec.

Negotiations for 3PCC and for inline call control use separate audio codec lists.

The following table shows the default payload values of audio formats in the audio codec list.

Table 30. Default Payload of the Audio Codec List

Name	Default Payload	Description
pcmu	0	G.711 μ-law
pcma	8	G.711 a-law
g729	18	G.729/G.729A
amr-nb-oa	102	AMR speech codec, octet-aligned
amr-nb-oa-r	116	AMR speech codec, octet-aligned with restricted mode
amr-nb-be	103	AMR speech codec, bandwidth efficient
amr-nb-be-r	117	AMR speech codec, bandwidth efficient with restricted mode
g722	9	G.722 7-kHz audio-coding within 64 kbps
amr-wb-oa	108	AMR-WB speech codec, octet-aligned
amr-wb-oa-r	118	AMR-WB speech codec, octet-aligned with restricted mode
amr-wb-be	109	AMR-WB speech codec, bandwidth efficient
amr-wb-be-r	119	AMR-WB speech codec, bandwidth efficient with restricted mode

Table 30. Default Payload of the Audio Codec List

Name	Default Payload	Description
telephone-events	96 (Telephone Event/8000: 96, Telephone Event/16000:112, Telephone Event/48000: 115)	RFC 2833 telephone events
opus	114	RFC 6716 Opus speech and audio
evs	120	EVS audio codec
evs-r	121	EVS audio codec with restricted mode
cn	13	RFC 3389 comfort noise
evrc	123	EVRC audio codec
evrc0	105	EVRC0 audio codec
evrcb	124	EVRCB audio codec
evrcb0	106	EVRCB0 audio codec
evrcnw	126	EVRCNW audio codec
evrcnw0	125	EVRCNW0 audio codec

NOTE: The Containerized Decomposed Media Server now supports configurable payload type for all the above listed codec. Configurable in SIP (audio and video codec) value between 0-63 and 96-127.

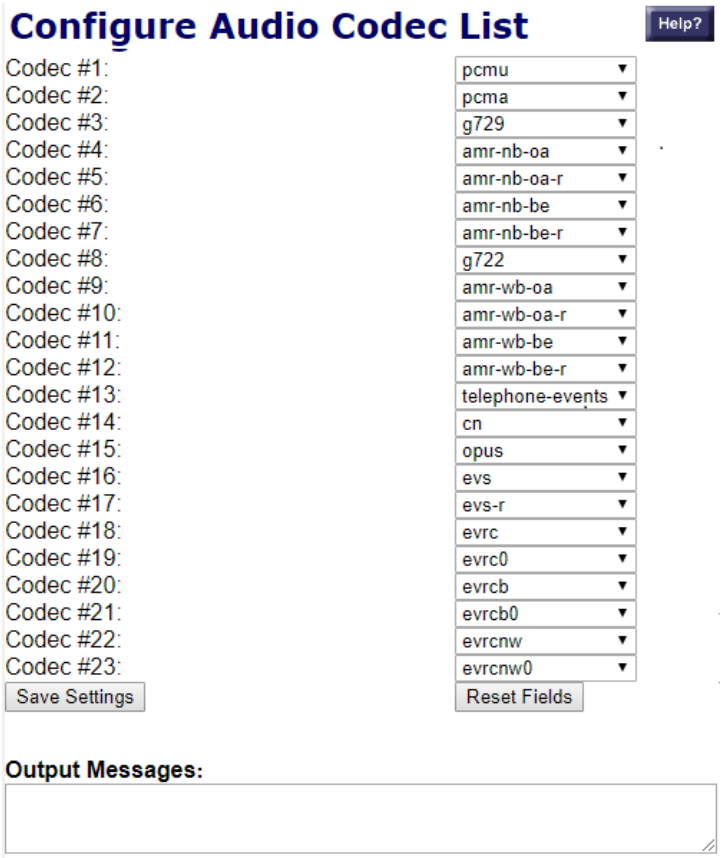
When creating a list of preferred audio codecs:

- At least one codec must be assigned (selecting only telephone-events and cn are not supported. You must select the relevant codec for telephone-events and cn. For example, select either pcma or pcmu for cn).
- No codec can be assigned twice.

To configure the audio codec list:

1. Click **Configuration** > **Node Configuration** > **Configure Audio Codec List**.

   The Configure Audio Codec List page displays.



2. Assign audio codecs in order of preference, starting with **Codec #1** field. Select **none** for any remaining codec fields beneath the list of preferred codecs.
3. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message displays in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Audio

The Configure Audio page enables you to specify parameters for audio media, such as the default format used for audio recording and the VAD's sensitivity, the default packetization interval for audio codecs, whether or not to enable ITU G.711 Appendix 1 packet loss concealment, ITU G.722 Appendix IV packet loss concealment, and voice quality enhancing (VQE).

You can view the information set on this page on the *Show Node Configuration*.

Recording Formats

The Containerized Decomposed Media Server supports recording audio in the following formats: PCM, G.711 µ-law, G.711 a-law, G.729 Annex A, G.722, AMR, and AMR-WB. You can configure the Containerized Decomposed Media Server audio-recording format through the control protocol, subject to the control protocol's restrictions on recording formats, or use the default audio-recording format.

NOTE: When recording EVS audio streams into one of the above file formats, audio transcoding is required.

The default recording format options are PCMU or G729.

Packetization

The following table shows the packetization intervals supported by the Containerized Decomposed Media Server.

The default interval used by the Containerized Decomposed Media Server is shown in parentheses for each encoding.

NOTE: Five-millisecond packetization is supported only with five-millisecond DSP processing cycle.

You can configure the default interval value of the audio codec (not including fax codec) using the Containerized Decomposed Media Server management interface. The single management setting is applied to all types of audio codec. As the following table shows, the supported interval value varies with the codec type. If the configured setting is not supported for the selected codec, the Containerized Decomposed Media Server continues to use the default value shown in the table for that codec. For example, if the configured setting is 30 milliseconds, the default interval for AMR will still be 20 milliseconds; however other codec types will have the default interval changed to 30 milliseconds. For control protocols other than SIP, this setting is ignored. Codecs for which management configuration is not supported continue to use the original default packetization interval.

Table 31. Packetization Periods

Encoding Name	Supported Packetization Periods (Audio)	Supported Packetization Periods (Fax)
AMR	If AMR without RED: (20), 40, 60, 80 If AMR with RED: (20)	—
AMR-WB	If AMR-WB without RED: (20), 40, 60, 80 If AMR-WB with RED: (20)	—
G729	10, (20), 30, 40	—
PCMU	5, 10, (20), 30, 40	With **Custom 2** profile: 5, (10), 20, 30, 40 Without **Custom 2** profile: 5, 10, (20), 30, 40
PCMA	5, 10, (20), 30, 40	With **Custom 2** profile: 5, (10), 20, 30, 40 Without **Custom 2** profile: 5, 10, (20), 30, 40
CN	5, 10, (20), 30, 40	With **Custom 2** profile: 5, (10), 20, 30, 40 Without **Custom 2** profile: 5, 10, (20), 30, 40

Table 31. Packetization Periods

Encoding Name	Supported Packetization Periods (Audio)	Supported Packetization Periods (Fax)
G722	5, 10, (20), 30, 40	—
Opus	20	—
EVS	(20), 40, 60, 80	—
EVRC	If EVRC0 negotiating header free format: (20) If EVRC negotiating in interleaved or bundled format: (20), 40, 60, 80	—
EVRCB	If EVRCB0 negotiating header free format: (20) If EVRCB negotiating in interleaved or bundled format: (20), 40, 60, 80	—
EVRCNW	If EVRCNW0 negotiating header free format: (20) If EVRCNW negotiating in interleaved or bundled format: (20), 40, 60, 80	—

Packet Loss Concealment

Packet Loss Concealment (PLC) allows the user to enable or disable PLC on the audio port when codec type is G.711 and G.722. If PLC is enabled in profile, the audio port uses the G.711 and G.722 PLC settings as supported in Web GUI for all G.711 and G.722 audio port. If PLC is disabled in profile, G.711 and G.722 PLC are disabled on audio port, regardless of the Web GUI setting. This profile setting is ignored on audio port with other codec type. For G.729, AMR, AMR-WB, EVRC, EVRCB, EVRCNB, and Opus codec, PLC is one of the codec's built-in and is always enabled.

NOTE:

- ITU G.711 Appendix 1 packet loss concealment for G.711 codec is supported for all service contexts and transcode bypass.
- ITU G.722 Appendix IV packet loss concealment for G.722 codec is supported for all service contexts and transcode bypass.

Noise Gating

Noise gating is a technique, similar to squelching on two-way FM radio, that reduces perceived noise by attenuating an incoming signal when speech is not detected. This technique is especially effective in reducing the background noise in conferences during intervals when no one is speaking, which is when the accumulated background noise of all active speakers’ ports is most noticeable.

Audio Parameters

The following table shows the audio information you can configure.

Table 32. Audio Information Required

Value	Description
Record Audio Format	The encoding algorithm to be used when no format is specified in protocol messages. The supported values are: • **forcedG.711.** Uses the G.711μ-law codec. • **forcedG.729.** Uses the G.729 Annex A codec. The default value is forcedG.711. Changes to this field take effect immediately, applying to all new recordings.
Default Packetization Interval	The packetization interval for codecs, in milliseconds. This value is used when the packetization period is not negotiated in SDP. The supported values are 5, 10, 20, 30, 40, 50, 60, and 80. The default value is 20 milliseconds. If the configured value is not supported by a codec and a supported value is not negotiated in SDP, the default value defined for SDP negotiation is used. Changes to this field take effect immediately, applying to all new ports.
Packet Loss Concealment for G.711	Enables packet loss concealment (PLC), as defined in ITU G.711 Appendix 1, for the G.711 codec. The supported values are: • **Enabled.** Enables PLC. • **Disabled.** Disables PLC. The default value is Disabled. Changes to this field take effect immediately, applying to all new ports. ***NOTE:*** Supported for all service contexts and transcode bypass.
Packet Loss Concealment for G.722	Enables packet loss concealment (PLC), as defined in ITU G.722 Appendix IV, for the G.722 codec. The supported values are: • **Enabled.** Enables PLC. • **Disabled.** Disables PLC. The default value is Disabled. Changes to this field take effect immediately, applying to all new ports. ***NOTE:*** Supported for all service contexts and transcode bypass.
Noise Gating Attenuation	The attenuation, in dB, to be applied to a port when the speaker is silent. The value range is from 0 to 96, where 0 disables noise gating. (For typical applications, values between 10 to 20 are recommended for balancing noise attenuation and a more natural-sounding silence for pauses in speech.) Changes to this field take effect immediately, applying to all new ports. For MSML 1.1, this field is overridden by the **attenuation** attribute of the `<ng>` element, when specified for a port.
Noise Gating Attenuation Attack Time	The period, in milliseconds, over which the specified noise gating attenuation is ramped up. The value range is from 0 to 1000. The default value is 120 milliseconds. Changes to this field take effect immediately, applying to all new ports.
Noise Gating Attenuation Release Time	The period, in milliseconds, over which currently applied noise gating attenuation is ramped down. The value range is from 0 to 100. The default value is 40 milliseconds. Changes to this field take effect immediately, applying to all new ports.

Table 32. Audio Information Required

Value	Description
VAD Sensitivity for Recording	The sensitivity, as an integer attenuation value in dB, of the Voice Activity Detector used for starting and ending recordings. The value range is from 0 to 96. Higher attenuation results in lower sensitivity to voice. The default value is 0, which results in the factory-configured default sensitivity. If this value is set to 96 dB, the VAD becomes insensitive to voice. Changes to this field take effect immediately, applying to all new recordings.
AEC (Acoustic Echo Cancellation)	Enables acoustic echo cancellation. The supported values are: • **Enabled.** Enables AEC. • **Disabled.** Disables AEC. The default value is Disabled. AEC can only be enabled, with this field or through MSML 1.1, when AEC monitor resources have been reserved. Changes to this field take effect immediately, applying to all new ports. AEC and NR are applicable for both narrowband and wideband ports. For MSML 1.1, this field is overridden by the **enabled** attribute of the <aec> element, when specified for a port.
AEC Maximum Supported Bulk Delay	The maximum bulk delay, in milliseconds, that the AEC should support detecting. The value range is from 100 to 512. The default value is 512 ms. Changes to this field take effect immediately, applying to all new ports.
AEC echo canceller resources to be reserved	The number of echo canceler resources that the AEC should reserve. The value range is from 0 to 1000, where 0 disables echo canceling. Canceler resources are distributed equally among DSPs allocated for audio traffic. (DSPs allocated for processing video traffic are not used for AEC.) Each DSP's resources are available for servicing audio ports on that DSP only, not shared across DSPs. The Containerized Decomposed Media Server rounds up[a] the configured number of canceler resources to an integer multiple of the DSPs allocated for audio. The default value is 0 (no resources are reserved for cancelling). Changes to this field require a MRFP restart to take effect.
AEC echo monitor resources to be reserved	The number of echo monitor resources that the AEC should reserve. The value range is from 0 to 1000, where 0 disables AEC. Monitor resources are distributed equally among DSPs allocated for audio traffic. (DSPs allocated for processing video traffic are not used for AEC.) Each DSP's resources are available for servicing audio ports on that DSP only, not shared across DSPs. The Containerized Decomposed Media Server rounds up[b] the configured number of monitor resources to an integer multiple of the DSPs allocated for audio. The default value is 0 (AEC is disabled). Changes to this field require a MRFP restart to take effect.
AEC reserved resources	This parameter specifies whether to reserve AEC resources for NB or NB-WB. For backward compatibility, AEC resources are reserved for NB. The supported values are: • **0.** NB • **1.** NB and WB both The default value is 0 (NB). Changes to this field require a MRFP restart to take effect.

Table 32. Audio Information Required

Value	Description
AI-based Noise Reduction	Enables or disables the AI-based noise reduction. The supported values are. • **Enabled.** Supports the NR algorithm based on Artificial Intelligence. When enabled, the Media Server supports the AI-based NR in NB and WB modes and mid-call change between NB and WB codecs. • **Disabled.** Supports the NR algorithm based on spectral subtraction. The default value is Disabled. Changes to this field require a reboot to take effect.
Noise Reduction	Enables noise reduction. The supported values are: • **off.** Disables noise reduction. • **always on.** Enables noise reduction. • **automatic.** Automatically turned on or off by the Containerized Decomposed Media Server. Noise reduction is turned on for a connection using this mode when the: • number of connections using automatic noise reduction is not over the configured maximum • noise on the connection is above the configured threshold. Noise reduction is turned off for a connection using automatic noise reduction when the noise on the connection drops below the configured threshold. In turning automatic noise reduction on or off, the Containerized Decomposed Media Server uses a (non-configurable) hysteresis to prevent rapid vacillations. The default value is off. The changes to this field take effect immediately and applies to all new ports. For MSML 1.1, this field is overridden by the enabled and active-mode attributes of the `<nr>` element, when specified for a port.
Automatic Noise Reduction Threshold	Specifies the threshold, in dBm0, for turning on or off automatic noise reduction. In turning automatic noise reduction on or off, the Containerized Decomposed Media Server uses a (non-configurable) hysteresis to prevent rapid vacillations. The value range is from –96 to –20. The default value is –37 dBm0. Changes to this field take effect immediately, applying to all new ports. For MSML 1.1, this field is overridden by the **threshold** attribute of the <nr> element, when specified for a port.
Maximum Automatic Noise Reduction Ports	The maximum number of connections configured to use automatic noise reduction that can simultaneously be turned on. The value range is from 0 to 65535. The default value is 0 (no set limit; the actual maximum is limited by the Containerized Decomposed Media Server's capacity for the application). Changes to this field take effect immediately for increases. For decreases, the new value takes effect only once the number of ports in automatic mode that are currently active does not exceed the configured value (this field does not deactivate noise reduction on currently active ports).

Table 32. Audio Information Required

Value	Description
Pre-Announcement Silence Duration	Specifies the duration of silence in ms, to be played before streaming the audio, video, or multi-media announcement. The value range is from 0 to 100. The configured value is in multiples of 100. The default value is 0 (silence streaming is disabled). This parameter does not require a restart and takes effect on new announcement requests.
Post-Announcement Silence Duration	Specifies the duration of silence in ms, to be played after streaming the audio, video, or multi-media announcement. The value range is from 0 to 100. The configured value is in multiples of 100. The default value is 0 (silence streaming is disabled). This parameter does not require a restart and takes effect on new announcement requests.
TTY Clamping	The Containerized Decomposed Media Server clamps the TTY tones in the RTT/TTY session. The supported values are: • **noClamping.** The Containerized Decomposed Media Server does not clamp the TTY tone for a RTT/TTY session. • **clampingWithoutLeakageSupp.** The Containerized Decomposed Media Server clamps the TTY tone for a RTT/TTY session but minor leak is observed in the audio port. • **clampingWithLeakageSupp.** The Containerized Decomposed Media Server clamps 100% TTY tone for a RTT/TTY session and does not add a delay of more than 60 ms. The default value is noClamping. This parameter does not require a restart and takes effect on the next RTT/TTY session.
Max Announcement Speed	Allows to configure maximum speed for audio announcements on the MSML port. The supported values are 1.0, 1.2, 1.4, 1.6, 1.8, and 2.0. The default value is 2.0. This parameter does not require a restart and takes effect on the next MSML announcement.
Min Announcement Speed	Allows to configure minimum speed for audio announcements on the MSML port. The supported values are 0.4, 0.6, 0.8, and 1.0. The default value is 0.4. This parameter does not require a restart and takes effect on the next MSML announcement.
Optimal Clip Recording	Enables or disables optimal clip recording to record an audio port through a forceful transcode bypass, where the recorded file follows the optimal clip naming convention. The default value is disabled. ***NOTE:*** When this field is enabled, the Containerized Decomposed Media Server overwrites the **Record Audio Format** settings. This parameter does not require a restart and takes effect on the next recording request.

Table 32. Audio Information Required

Value	Description
VAD Controlled ASR	Enables or disables the Voice Activity Detector (VAD) feature for announcement barge-in and post-speech silence detection under noisy background in the ASR session. The supported values are: • **Enabled.** The Containerized Decomposed Media Server barges the ongoing announcement when speech is detected (if **barge=true**). Later, the Containerized Decomposed Media Server detects post-speech silence for the configured **ASR End Of Speech Detection Timeout** and start streaming zero output towards the ASR stream. • **Disabled.** The Containerized Decomposed Media Server disables the VAD feature for announcement barge-in and post-speech silence detection in the ASR session. The default value is Disabled. Changes to this field take effect immediately.
ASR End Of Speech Detection Timeout	Specifies the timeout interval, in milliseconds, for end of speech detection in the ASR session. The supported value is an integer from 500 to 10000. The value is in multiples of 100. The default value is 2000. ***NOTE:*** This feature is enabled only if **VAD Controlled ASR** is enabled. Changes to this field take effect immediately.
VAD Noise Threshold	Specifies the threshold value, in dBFS, for expected background noise levels. This parameter is applicable for the VAD controlled ASR and voice barge announcement features. The Containerized Decomposed Media Server ignores the background noise until the configured threshold value to determine whether an announcement must be barged. The supported value is an integer from -45 to -20. The default value is -35. Changes to this field take effect immediately.
Force Multi Clip Audio Annc. with Bandwidth Change	Enables or disables force transcoding of the multi-clip audio announcement when clips of different bandwidths are encountered. The supported values are: • **Enabled.** While playing the multi-clip announcements, when clips are partially parsed, the Containerized Decomposed Media Server forces announcement to be transcoded and continues to play the announcement when multiple bandwidth clips are encountered outside the parsed clips. • **Disabled.** While playing the multi-clip announcements, when clips are partially parsed and the announcements are played in the bypass mode, the Containerized Decomposed Media Server may fail the announcements if multiple bandwidth clips are encountered outside the parsed clips. The default value is Disabled. This parameter does not require a reboot and takes effect on the next announcements request.

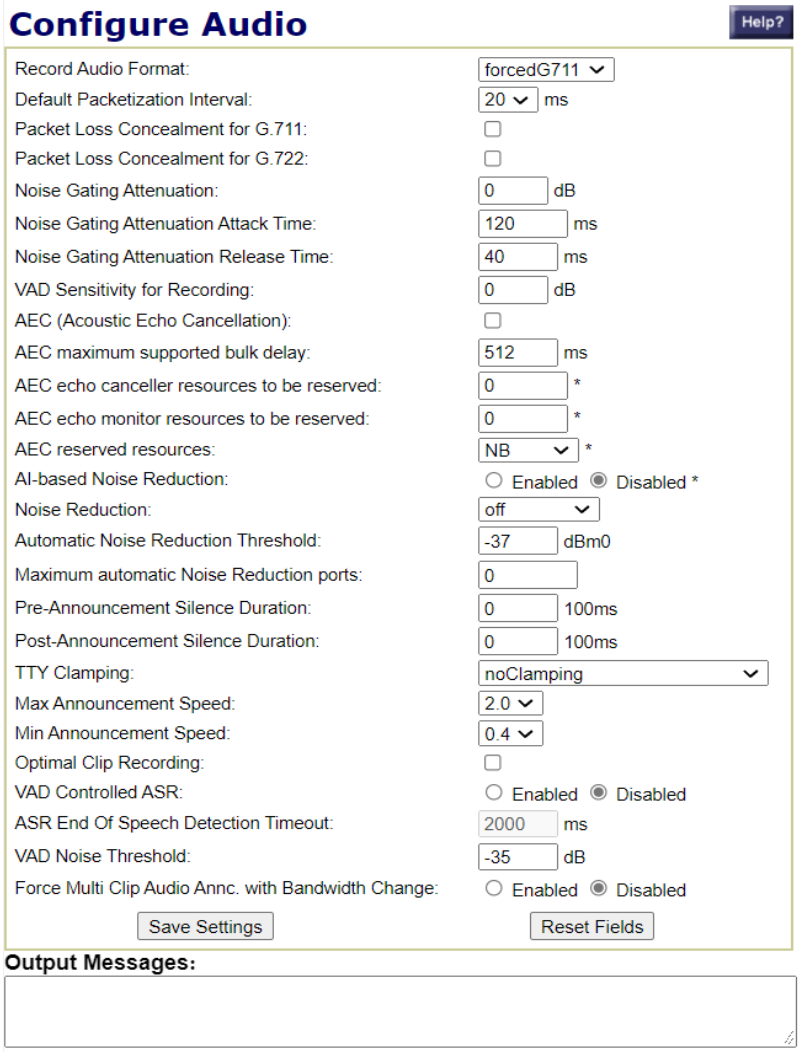
[a] For example, if 3 DSPs are allocated for audio processing and AEC Canceller Resources to be Reserved is configured to 5, the Containerized Decomposed Media Server reserves 6 canceler resources.

[b] For example, if 3 DSPs are allocated for audio processing and AEC Monitor Resources to be Reserved is configured to 1, the Containerized Decomposed Media Server reserves 3 monitor resources.

To configure audio:

1. Click **Configuration** > **Node Configuration** > **Configure Audio**.

   The Configure Audio page displays.



2. Configure the audio setting information as described in the above table.
3. Click **Save Settings**.

   Changes other than AEC resource reservation take effect immediately. AEC resources reservation require a MRFP restart to take effect.

   Confirmation message displays in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Opus

On the Configure Opus page, you can configure opus settings for the Containerized Decomposed Media Server controlled by Opus.

The Opus codec is supported in all the service contexts.

The following table describes the information you can configure for the Opus.

Table 33. Opus Information Required

Value	Description
Opus Codec Operation Bit Rate	Optional. Specifies the Opus Codec Operation Bit Rate. The supported values are: • **VBR.** Variable bit rate • **CBR.** Constant bit rate The default is VBR.
Opus Maximum Sampling Rate	Optional. Specifies the Opus Codec Maximum Sampling Rate in Hz. The supported sampling rates are 8000, 12000, 16000, 24000, and 48000 Hz. The default is 48000 Hz.
Opus Maximum Channel Number	Optional. Specifies the Opus Codec Maximum channel number. The supported values are mono and stereo. The default is mono.
Opus Maximum Average Bit Rate	Optional. Specifies the Opus Codec Maximum Average Bit Rate, in bps. The range is 6000 to 510000. The default is 128000 bps.

To configure Opus:

1. Click **Configuration > Node Configuration > Configure Opus**.

2. Enter the Opus configuration settings as described in above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure EVRC

On the Configure EVRC page, you can specify EVRC characteristics. The information set on this page can be viewed on the Show Node Configuration page.

The following table shows the defined modes for EVRC and the additional non variable modes.

Table 34. EVRC Operating Modes

Mode	Fraction of Rate 1	Packets Set to	Mode Description
	Rate 1	Rate 1/2	
Rate Reduction Mode 0	1	0	Rate is set solely by the encoder to 1 frame.
Rate Reduction Mode 1	3/4	1/4	Changes 25% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 2	1/2	1/2	Changes 50% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 3	1/4	3/4	Changes 75% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 4	0	1	Changes all of the rate 1 frames to rate 1/2.
Non-Variable Modes:			
Fixed Full Rate	—	—	Radisys proprietary non-variable full rate.
Fixed Half Rate	—	—	Radisys proprietary non-variable half rate.

The following table shows the defined modes for EVRC-B and the additional non variable modes.

Table 35. EVRC-B Operating Modes

Mode	Average Source Encoding Bit-rate [kbps]	Mode Description
Rate Reduction Mode 0	8.3	No quarter rate frames.
Rate Reduction Mode 1	7.57	
Rate Reduction Mode 2	6.64	
Rate Reduction Mode 3	6.18	
Rate Reduction Mode 4	5.82	
Rate Reduction Mode 5	5.45	
Rate Reduction Mode 6	5.08	
Rate Reduction Mode 7	4.0	Half rate max, no quarter rate frames
Non-Variable Modes:		
Fixed Full Rate 8	8.8	Non-variable full rate
Fixed Half Rate 9	4.0	Non-variable half rate

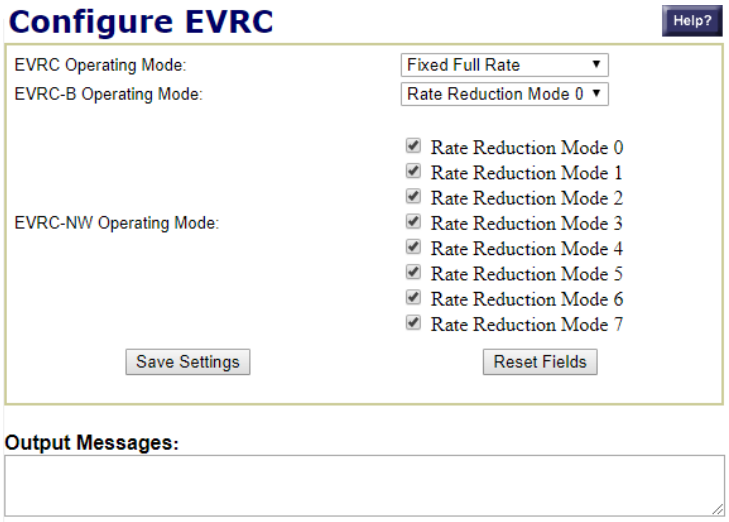
The following table shows the defined modes for EVRC-NW and the additional non variable modes.

Table 36. EVRC-NW Operating Modes

Mode	Average Source Encoding Bit-rate [kbps]	Compatible Mode	Mode Description
Rate Reduction Mode 0	7.5		Mode 0 is wideband mode only.
Rate Reduction Mode 1	8.3	0	
Rate Reduction Mode 2	6.64	2	
Rate Reduction Mode 3	6.18	3	
Rate Reduction Mode 4	5.82	4	
Rate Reduction Mode 5	5.45	5	
Rate Reduction Mode 6	5.08	6	
Rate Reduction Mode 7	4.0	7	Half rate max

To configure the EVRC:

1. Click **Configuration** > **Node Configuration** > **Configure EVRC**.



2. Select the **EVRC Operating Mode**, **EVRC-B Operating Mode**, and **EVRC-NW Operating Mode**.
3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Silence Suppression

The Configure Silence Suppression page enables or disables silence suppression performed by the Containerized Decomposed Media Server Voice Activity Detector in SIP-based 3PCC applications. It also enables you to configure the Silence Insertion Descriptor (SID) interval for sending the SID frames periodically. Particular ports can override this setting through the SDP **silenceSupp** attribute or payload specific parameter.

Enabling or disabling silence suppression on this page does not affect silence suppression for codecs where silence suppression is built into the codec.

NOTE:

- The information displayed on this Web GUI page before **Execute** action is not the actual status of the silence suppression feature.
- Radisys recommends not to use silence suppression with music on hold or DTMF detection in voice band.

For more information, see *Silence Suppression on page 40*.

The following table describes the information you can configure for the silence suppression.

Table 37. Silence Suppression Information Parameters

Value	Description
Enable Silence Suppression	Allows to enable the silence suppression. Changes to this field take effect immediately.
Disable Silence Suppression	Allows to disable the silence suppression. Changes to this field take effect immediately.
Configure SID Interval	Allows to configure the SID interval, in milliseconds, for sending the SID frames periodically when silence suppression is enabled. This SID/CN duration is the **MAXIMUM SID** interval between the successive SIDs/CNs that are sent from the Containerized Decomposed Media Server when there is no change in the background noise. When there is a change in the background noise conditions, the Containerized Decomposed Media Server sends the SIDs/CNs immediately. The supported value range is 0 to 65000. The default value is 0. Where 0 disables the configuration of the SID interval. ***NOTE:*** • The SID interval must be specified in multiples of 20. • It is recommended to configure the SID interval value to 160. Changes to this field take effect immediately.

To configure silence suppression for SIP applications:

1. Click **Configuration** > **Node Configuration** > **Configure Silence Suppression**.

   The Configure Silence Suppression page displays.

2. Enter the silence suppression information described in the table above.
3. Click **Execute**.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

Configure NFS

The Configure NFS page enables you to configure the Containerized Decomposed Media Server to use an NFS server for external play and record. You can only specify NFS configuration when the Containerized Decomposed Media Server is already configured with its network information.

Using NFS

The Containerized Decomposed Media Server can record to and play back recordings from external NFS servers. The Containerized Decomposed Media Server can record to and play back from up to 5 separate NFS exported directories, known as **mount points**. The Containerized Decomposed Media Server uses the root user (group and user ID of zero) to mount the external file system, and does not limit its size.

Each mount point must be mounted onto the Containerized Decomposed Media Server. Once the directory is mounted, you can refer to files in the directory using the **file://mnt** scheme, plus the path relative to the mount point and the filename, as follows:

```
file://mnt/nfs_server_ip/path/file_name
```

where nfs_server_ip is the IP address or hostname of the external NFS server, and *path/file_name* are the path to the file relative to the exported directory and the name of the file, respectively.

If MSML 1.1 is the control protocol, the **nfs://** header can be used, as follows:

```
nfs://nfs_server_ip/path/file_name
```

For example, suppose the IP address of the NFS server is 10.10.4.102, the server is known by the DNS name server as **gecko**, and the exported directory is **/annc/prompts**. To play a clip **welcome.wav** located in **/annc/prompts/english/**, you can specify either of the following URIs:

```
file://mnt/10.10.4.102/english/welcome.wav
file://mnt/gecko/english/welcome.wav
```

In MSML you can also specify the following:

```
nfs://10.10.4.102/english/welcome.wav
nfs://gecko/english/welcome.wav
```

NFS Mount Points

Mount points are identified by the NFS server identifier—either a domain name or an IP address—and the server identifier must be unique for each mount point. If your mount points are all located on separate NFS servers, no special configuration is required.

However, if you want to configure multiple mount points on a single NFS server, you must be able to reference the server by more than one unique identifier, and the IP address cannot be used as the identifier. That is, you must use domain names, and you must also use a different domain name for each reference to the server (that is, each mount point located on that server), so that the NFS server must have multiple entries in the DNS server. If you are not using DNS, each mount point must be located on a different NFS server.

For example, suppose you are mounting three directories from NFS server **lizard**, and the domain name lizard is mapped to 192.168.20.5 on the DNS server. To begin with, you must use the domain name lizard, and not the IP address. Next, you must create two additional entries in the DNS server—for instance, domain names gecko and iguana—which also map onto 192.168.20.5. When configuring the three mount points, you must specify each of these names exactly once.

External NFS Caching

The Containerized Decomposed Media Server can cache clips played from external NFS servers to enhance performance of applications such as announcement servers. The effect of caching on performance depends on the application: number of clips used, clip sizes, usage pattern, and so on. Principle use cases for NFS caching are:

- Playing multiple short clips in sequence, where each clip represents a word or a phrase from a sentence
- Playing long clips when the file server is close to capacity
- Call-parking and music on hold, which can require five or six (2 to 5 MB) files to be cached

While sufficient cache memory is available, the Containerized Decomposed Media Server caches announcement files streamed from external NFS servers (version 2 or version 3). If the cache memory is temporarily insufficient (when caching a clip can exceed available memory space, shared with internal clips) or for files that are particularly large, the Containerized Decomposed Media Server continues playing announcements directly off the NFS server without caching. NFS caching is enabled through the management interface.

NFS Health Check

The Containerized Decomposed Media Server has features that increase resiliency of the connection between itself and the NFS servers. These features improve the Containerized Decomposed Media Server's ability to detect, recover from, and report NFS connectivity failures.

- **Periodic Health Check.** The Containerized Decomposed Media Server sends a periodic health check to all provisioned NFS servers at a default rate of once every 10 seconds. If the server returns an invalid response to the health check, or if it fails to respond, the Containerized Decomposed Media Server retries the connection three times by default. If it is unable to re-connect, the Containerized Decomposed Media Server reports the error in syslog and generates an alarm (NFS server unavailable).
- **Auto-Remount Attempts.** The Containerized Decomposed Media Server attempts to remount an NFS mount point up to three times after an initial mount failure. A failure to remount the configured maximum number of times causes the Containerized Decomposed Media Server to generate a Mount failure alarm.

The health check interval and maximum number of retries are both configurable through the management interface.

The Containerized Decomposed Media Server does not switch health checking protocols after starting up. After the health check protocol is established, any change in protocol on the NFS server side causes health checks to fail and the NFS server to be declared unavailable. To change the NFS health checking protocol, you must disable the mount point and then re-enable it. The Containerized Decomposed Media Server then re-discovers the health check protocol.

NOTE: The Containerized Decomposed Media Server immediately rejects NFS recording, announcement, and fax send and receive requests if the,

- NFS server is unavailable
- mount operational mode of the NFS mount point is disabled
- mount is unsuccessful

However, if the NFS request is received prior to detecting the NFS server unavailability, the request fails after NFS file operations (file opening, reading, and writing) time-out.

Slow NFS

The slow NFS server sometimes causes announcement failures and delayed session clean up, when the user terminates the session. In some cases, this may cause hung ports and denial of the port creation or announcement service.

When the slow NFS throttling interval feature is configured through the management interface, the Media Server detects the slow NFS server and throttles the subsequent NFS requests (announcement) to the particular NFS server for the configured time and raises the alarm. Throttling can be disabled by configuring the slow NFS throttling interval to 0.

The following table shows NFS information you can configure.

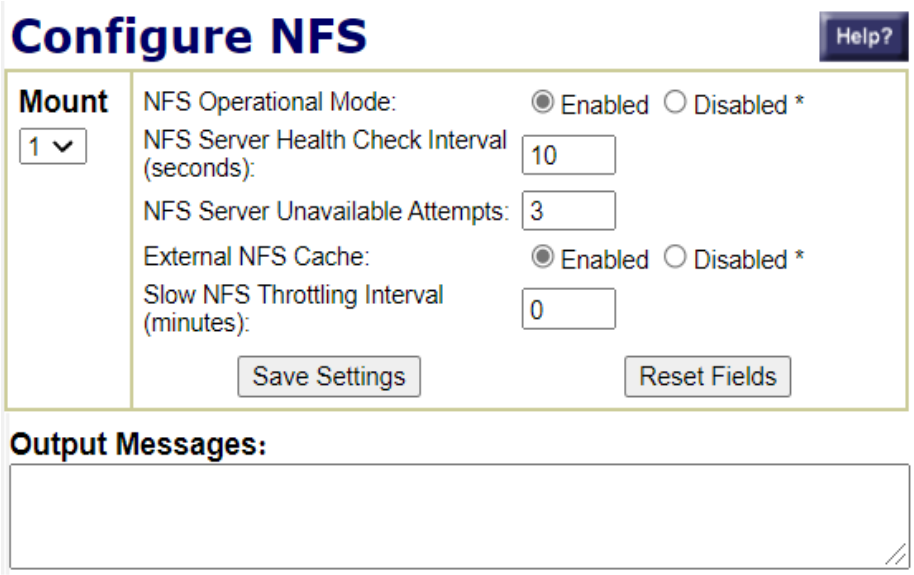
Table 38. NFS Information Required

Value	Description
Mount	The unique number by which this directory (mount point) can be identified. You can specify up to 5 NFS directories. Changes to this field take effect immediately.
NFS Operational Mode	The operational mode set for NFS. The supported values are: • **Enabled.** Enables NFS. • **Disabled.** Disables NFS without discarding configuration. The default value is Disable. Changes to this field require a MRFP restart to take effect.
NFS Server Health Check Interval (seconds)	The interval in seconds at which a health check packet is sent to the NFS server. The health check is considered successful only if a valid response is received before the next health check is issued. The supported value range is 5 to 60. The default value is 10. Changes to this field take effect immediately.
NFS Server Unavailable Attempts	The number of health check failures after which the server is declared unavailable. In this case, an alarm is generated. The supported value range is 3 to 10. The default value is 3. Changes to this field take effect immediately.
External NFS Cache	The mode set for external NFS cache. The supported values are: • **Enabled.** Enables caching of external NFS files. • **Disabled.** Disables caching of external NFS files. The default value is Enabled. Changes to this field require a MRFP restart to take effect.
Slow NFS Throttling Interval (minutes)	Indicates the slow NFS throttling interval in minutes. The supported value range is 0 to 15. The default value is 0. ***NOTE:*** • The **NFS Operational Mode** must be enabled to configure the slow NFS throttling interval. • When the value is 0, the Containerized Decomposed Media Server does not support the slow NFS throttling mechanism and it does not raise an alarm. When any non-zero value is configured, the Containerized Decomposed Media Server applies the throttling for the value that is configured in minutes and also raises an alarm. Changes to this field take effect immediately.

To configure NFS information:

1. Click **Configuration** > **Node Configuration** > **Configure NFS**.

   The Configure NFS page displays.



2. Enter the NFS information described in the table above.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

NOTE: Successfully changing configuration information does not mean that a mount point can be successfully mounted. If the mount point information is invalid or the exported directory cannot be mounted for some other reason, the system provides you with a notification at the time the mount attempt fails. The notification may take some time after configuration.

Configure RTP

The Configure RTP page enables you to enable RTP characteristics. This can be:

- Enabling symmetric RTP
- Enabling source port screening
- Enabling secure RTP (sRTP)
- Enabling encrypt RTCP packets for SDES
- Setting RTP redundancy level
- Setting RTP payload
- Setting RTP Redundancy Level for T.140
- Setting secure RTP key negotiation method

- Setting RTP media multiplexing
- Setting media ID

Information set on this page can be viewed on the *Show Node Configuration*.

Symmetric RTP

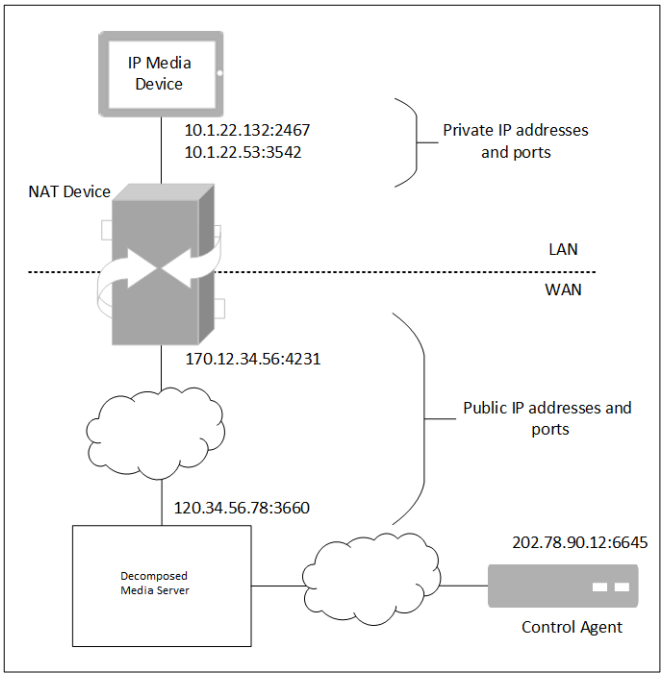
The Containerized Decomposed Media Server uses symmetric RTP to communicate with a client behind a NAT device. NAT (Network Address Translation) allows a local-area network (LAN) to use one set of IP addresses for internal traffic (private IP addresses) and a second set of addresses for external traffic (public IP addresses). A NAT device located at the boundary between the LAN and the wide-area network (WAN) performs the IP address translations.

IP addresses can be either IPv4 or IPv6 (but the Containerized Decomposed Media Server does not translate between the two IP versions). NAT provides:

- Some network security, as it hides the internal configuration of the corporate network.
- An additional pool of IP addresses for corporate use. Private IP addresses are not reachable from the Internet, so they can be re-used from company to company without fear of conflict.

In a NAT scenario, the client resides across the WAN from the Containerized Decomposed Media Server, behind a NAT device. The control agent resides across the WAN. The client and the LAN-side interface of the NAT device have private IP addresses, while the Containerized Decomposed Media Server, the control agent, and the WAN-side interface of the NAT device have public IP addresses, as shown in the figure below.

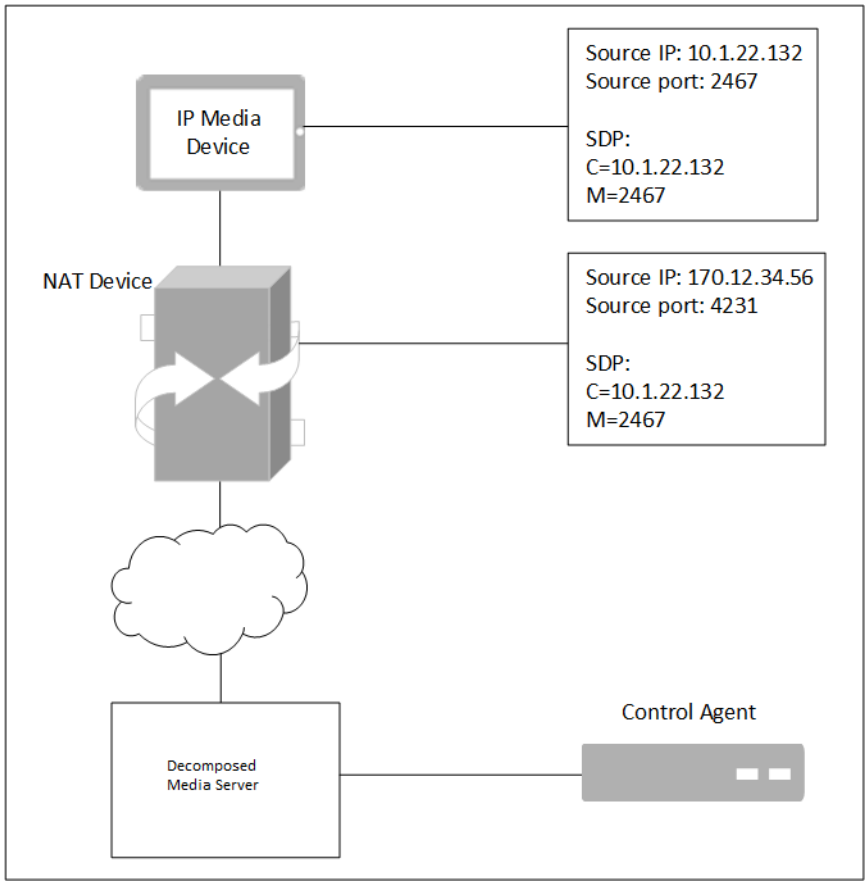
Figure 23. Client behind NAT Device



When it transmits, the client reports its private IP address and port number (in the figure, **10.1.22.132:2467**) in the SDP of the control message. This IP address and port number are also recorded as the source IP address and port in the RTP packet header.

When the NAT device receives the outgoing packet, it replaces the private IP address and port in the packet header with its own public IP address and port (in the figure, **170.12.34.56:4231**). However, it does not replace the IP address and port recorded in the SDP, which now differs from the source IP and port in the packet header. This is shown in the figure below.

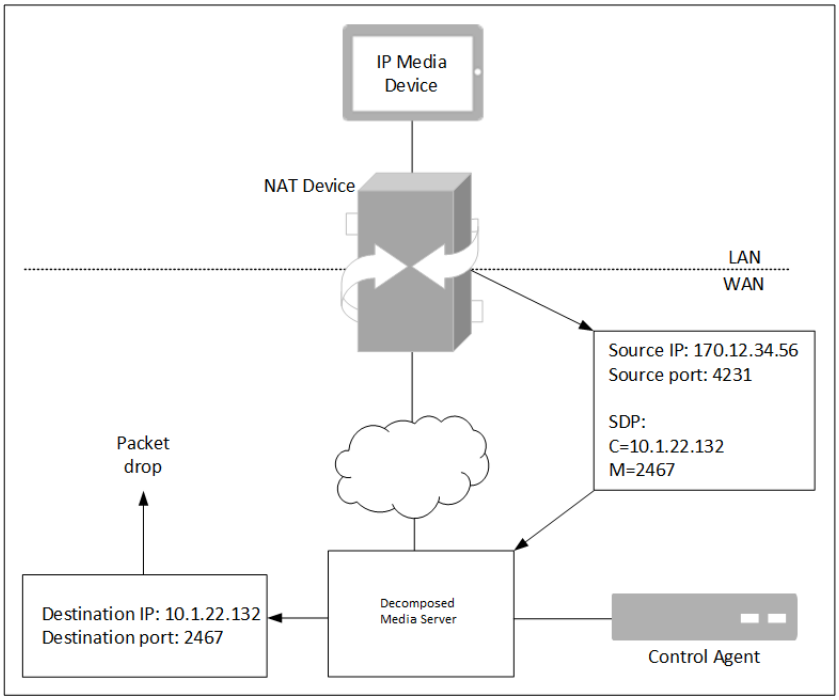
Figure 24. NAT Replacement of Packet Header IP Address and Port



During ordinary communication, the Containerized Decomposed Media Server uses the address provided in SDP, not the packet header, for transmitting RTP. When the client is behind a NAT device, the address in SDP is still the private IP address of the client, even though the NAT device's public IP is in the packet header.

Because the Containerized Decomposed Media Server uses SDP instead of the packet header, it will try to send the RTP to the private IP address of the client. Since private IP addresses are not reachable from the public network, these messages will be discarded by the network and the RTP will not reach the client, as shown in the figure below.

Figure 25. Network Discards Packet to Private IP Address



The same problem will also occur if the control agent sets up a call for a client that is behind a NAT device, as shown in the below figure.

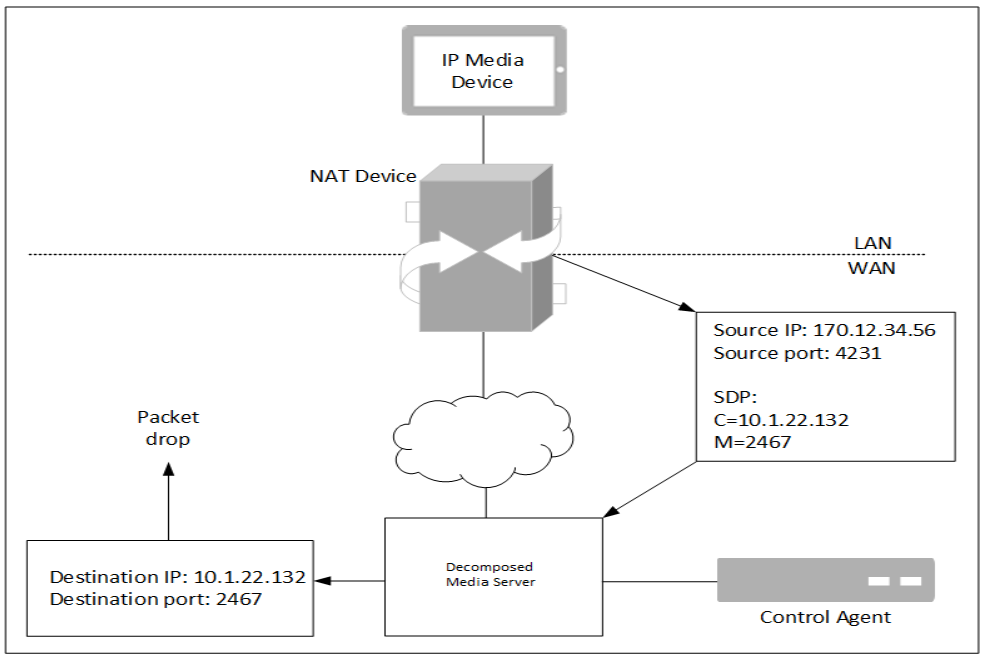
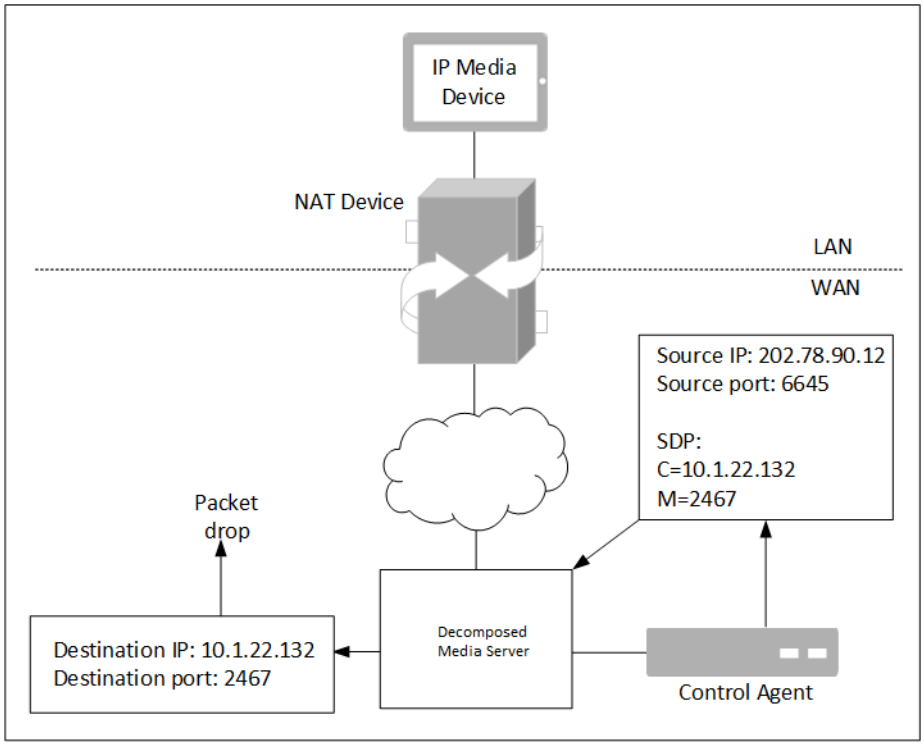


Figure 26. Network Discards Packet to Private IP Address - 2



To reach the client, the Containerized Decomposed Media Server must send the RTP packets to the external IP address and port of the NAT device.

When symmetric RTP is enabled, the Containerized Decomposed Media Server examines the source IP address and port in the packet header of the first RTP packet received, and compares it with that in the SDP. If they are different, the Containerized Decomposed Media Server uses the IP address and port in the header as its transmit address.

Once the Containerized Decomposed Media Server has changed addresses in this way once, it will not change the transmit address again unless three packets in a row are received from a new address. This ensures that the Containerized Decomposed Media Server locks on to the address in a timely manner, but does not “flip” addresses for stray or erroneous packets.

The network should be configured to return an ICMP “Destination Unreachable” message in this case, instead of silently discarding the packets. The Containerized Decomposed Media Server can be configured to respond to a Destination Unreachable message by backing off, and stopping transmission if repeated messages are received. If the Containerized Decomposed Media Server is not notified that the destination is unreachable, it will continue to stream RTP packets to the network.

The Containerized Decomposed Media Servers response to ICMP Destination Unreachable messages should be configured to give the Containerized Decomposed Media Server enough time to receive media from users requiring symmetric RTP, but not so much time that it sends significant unwanted traffic to the network. When the Containerized Decomposed Media Server receives RTP that updates its destination, it will immediately reset the ICMP algorithm and begin sending to the correct destination.

Source Port Screening

Normally a Containerized Decomposed Media Server port receives RTP addressed to it from any sending source. When port source screening is enabled, the Containerized Decomposed Media Server discards packets from all sources except the one that is specified in SDP.

For source port screening to be used:

- The source port screening option must be enabled in the Containerized Decomposed Media Server management interface.
- The far-end IP address (IPv4 or IPv6) must be set to something other than 0.0.0.0.
- Until the new port receives SDP containing the far-end IP address and UDP port number, it receives RTP packets addressed to it from any sending source.
- After it receives SDP containing the far-end IP address and UDP port number, the port accepts only RTP packets from the specified source.

Changes to this configuration do not affect existing ports.

NOTE: Source port screening cannot be used in conjunction with symmetric RTP; if source port screening is to be enabled, symmetric RTP must be disabled.

Secure RTP

The Secure Real Time Transport Protocol (SRTP) is a profile of the Real Time Protocol (RTP) defined in RFC 3711. SRTP is designed to provide secure transmission of RTP data between endpoints. Secure transmission includes:

- Encryption
- Authentication
- Integrity checking
- Replay protection

The Containerized Decomposed Media Server SIP interface supports SRTP for all media types excluding T.38 fax. However, SRTP cannot be used for the following RTP streams:

- Audio from external speech servers
- Audio for media replication (for example, as used in lawful intercept)
- RFC 4117 transcoding audio

The Containerized Decomposed Media Server supports an SRTP replay protection with a window size of at least 64. Master Key Identifier (MKI) in SRTP is not supported and should not be sent to the Containerized Decomposed Media Server.

The Containerized Decomposed Media Server supports 128-bit and 256-bit AES encryption and decryption for both SRTP and SRTCP.

Encrypt RTCP Packets for SDES

The Media Server supports negotiating the **UNENCRYPTED_SRTCP** SDP session parameter on the SRTP port. The Media Server does not encrypt the RTCP packets when the **UNENCRYPTED_SRTCP** session parameter is negotiated on the port. The Media Server encrypts the RTCP packets when the **UNENCRYPTED_SRTCP** session parameter is not negotiated on the port.

RFC 2198 Redundant RTP

RFC 2198 defines a redundant RTP packet that multiplexes the current encoding with one or more redundant encodings. This allows for reconstruction of a media stream in conditions of packet losses. The level of redundancy, that is, the number of redundant encodings added to the current encoding, determines the maximum recoverable loss.

The Containerized Decomposed Media Server supports redundant RTP packets with all encodings using a single payload type. The Containerized Decomposed Media Server supports RTP redundancy for the AMR and AMR-WB audio codecs (bandwidth efficient or octet aligned, all supported modes) and T.140 text codec only. Silence suppression is supported.

The jitter buffer size must at least match or exceed the level of redundancy (for example, for level 5 RTP redundancy, set the jitter buffer size to at least 5 times the packetization interval) plus the expected network jitter. When using the Audio Automatic Jitter Buffer, set the Audio Jitter Buffer Minimum Delay to the level of redundancy.

RTP redundancy is negotiated through SDP.

NOTE:

- The AMR and AMR-WB RTP Redundancy parameters are separate and may be configured differently.
- The Containerized Decomposed Media Server does not support sending packets with RFC 2198 Redundancy when SRTP is enabled.

Secure RTP Key Negotiation Method

Datagram Transport Layer Security (DTLS) protocol is also known as TLS over datagram transport. DTLS provides authentication, data integrity, and confidentiality for communication between the two end-points over UDP. DTLS has additional capabilities such as sequence number and retransmission.

The Containerized Decomposed Media Server supports DTLS for SRTP/SRTCP streams only over a media network. The Containerized Decomposed Media Server also supports SRTP using Session Description Protocol Security Descriptions (SDES) as a key management protocol.

SDES is a signaling plane key exchange scheme that enables the media sender to specify the unique session keys and related security parameters such as key lifetime, key index, and cryptographic algorithms. These session keys and security parameters protect the media stream through an SDP attribute `a=crypto`. The end-point sends an **INVITE** request with fingerprint SDP attribute to establish DTLS based media sessions. The fingerprint SDP attribute has an encrypted digital certificate for the calling endpoint (Containerized Decomposed Media Server). The Containerized Decomposed Media Server validates the certificates received in the DTLS handshake against the finger print received in the SDP offer. The Containerized Decomposed Media Server performs a DTLS handshake between the local and far-end RTP and RTCP ports independently. The DTLS handshake can be initiated from either end-point based on the `setup` SDP attribute.

Configure RTP Payload

The RTP payload type specifies the format of an RTP stream. The Containerized Decomposed Media Server maps the payload type to a media format (G.711, G729a, AMR, AMR-WB, and so on) that the Containerized Decomposed Media Server uses to process the incoming media stream.

The Containerized Decomposed Media Server supports the configurable RTP payload value for each supported codec. For a new installation it keeps the current (hard-coded) payload value for a codec as a default value. The Containerized Decomposed Media Server continues to use the previous negotiated payload value for the well-established connections even after the configuration of new payload value. You cannot configure a duplicate payload value for any supported codec through the management interface.

The newly configured payload value is used with an immediate effect; when the Containerized Decomposed Media Server is offering the codec for next new request. The management interface configured payload type is only used when the Containerized Decomposed Media Server makes the offer.

The Containerized Decomposed Media Server uses the last successful configured payload value for a codec after restart. RTP payload type is supported in the SIP protocols.

The following table shows the payload value for both audio and video codec.

Table 39. Default Ordering of the Video and Audio Codec List

Name	Payload Type	Description
PCMU	0	G.711 µ-law
PCMA	8	G.711 a-law
G729	18	G.729/G.729A
AMR-NB-OA	102	AMR speech codec, octet-aligned
AMR-NB-OA-R	116	AMR speech codec, octet-aligned with restricted mode
AMR-NB-BE	103	AMR speech codec, bandwidth efficient
AMR-NB-BE-R	117	AMR speech codec, bandwidth efficient with restricted mode

Table 39. Default Ordering of the Video and Audio Codec List

Name	Payload Type	Description
AMR-WB-OA	108	AMR-WB speech codec, octet-aligned
AMR-WB-OA-R	118	AMR-WB speech codec, octet-aligned with restricted mode
AMR-WB-BE	109	AMR-WB speech codec, bandwidth efficient
AMR-WB-BE-R	119	AMR-WB speech codec, bandwidth efficient with restricted mode
G722	9	G.722 7-kHz audio-coding within 64 kbps
Telephone Event/8000	96	RFC 2833 telephone events
Telephone Event/16000	112	RFC 2833 telephone events
Telephone Event/48000	115	RFC 2833 telephone events
RED	97	RFC 2198 redundancy
CN	13	RFC 3389 comfort noise
H.264	104	H.264 payload format as per RFC 6184, previously RFC 3984
H.264 Mode 1	113	H.264 payload format as per RFC 6184, previously RFC 3984
OPUS	114	RFC 6716 Opus speech and audio
VP8	111	The format of VP8 RTP payload is **draft-ietf-payload-vp8**. The VP8 RTP payload format is supported in all service context.
EVS	120	audio codec
EVS-R	121	audio codec with restricted mode
H265	122	H.265 payload format as per RFC 7798
EVRC	123	EVRC audio codec with interleaved or bundled format as per the 3GPP2 C.S0014-A service option 3
EVRC0	105	EVRC audio codec with header free format as per the RFC 3588
EVRCB	124	EVRCB audio codec with interleaved or bundled format as per the 3GPP2 C.S0014-B service option 68
EVRCB0	106	EVRC audio codec with header free format as per the RFC 5188 and RFC 3588
EVRCNW	126	EVRC audio codec with interleaved or bundled format as per the 3GPP2 C.S0014-D service option 73
EVRCNW0	125	EVRC audio codec with header free format as per the RFC 6884 and RFC 3588

RTP Parameters

The following table shows RTP information.

Table 40. RTP Information Required

Value	Description
Symmetric RTP	Optional. Enables or disables use of symmetric RTP on the Containerized Decomposed Media Server. Note that symmetric RTP and source port screening may not be enabled at the same time. The default value is disabled. Changes to this field take effect immediately.
Source Port Screening	Optional. Enables or disables use of source port screening on the Containerized Decomposed Media Server. Note that symmetric RTP and source port screening may not be enabled at the same time. The default value is disabled. Changes to this field take effect immediately.
Secure RTP	Optional. Enables or disables use of secure RTP on the Containerized Decomposed Media Server. The default value is disabled. Changes to this field require a MRFP restart to take effect.
Encrypt RTCP Packets for SDES	Enables or disables the encryption of RTCP packets in SDES-SRTP ports. The default value is Enabled. Changes to this field take effect immediately on the next call.
RTP Redundancy Level for AMR-NB	Optional. Sets the level of RFC 2198 redundancy for AMR narrowband. Supported range of values is 0 to 5, where 0 disables RTP redundancy. The default value is 0 (no RTP redundancy). Changes to this field take effect immediately, applying to all new ports.
RTP Redundancy Level for AMR-WB	Optional. Sets the level of RFC 2198 redundancy for AMR wideband. Supported range of values is 0 to 5, where 0 disables RTP redundancy. The default value is 0 (no RTP redundancy). Changes to this field take effect immediately, applying to all new ports.
RTP Redundancy Level for T.140	The supported range of values is 0 to 5, where, 0 disables RTP redundancy. The default value is 2. The changes to this field take effect immediately.
Secure RTP Key Negotiation Method	Allows to configure the secure RTP key negotiation method. The supported values are: • **SDES.** The Session Description Protocol Security Descriptions (SDES) is a signaling plane key exchange scheme that enables the media sender to specify the unique session keys and related security parameters such as key lifetime, key index, and cryptographic algorithms. • **DTLS.** The Datagram Transport Layer Security (DTLS) protocol is also known as TLS over datagram transport. DTLS provides authentication, data integrity, and confidentiality for communications between the two end-points over UDP. • **SDES-DTLS.** The Containerized Decomposed Media Server offers both SDES and DTLS. The default value is SDES. ***NOTE:*** • This SDES and DTLS works only when the **Secure RTP** is enabled. • This field is applicable only for the Containerized Decomposed Media Server generated offer. The Containerized Decomposed Media Server accepts the DTLS offer by far-end irrespective of this configuration. Changes to this field take effect on the new port creation.

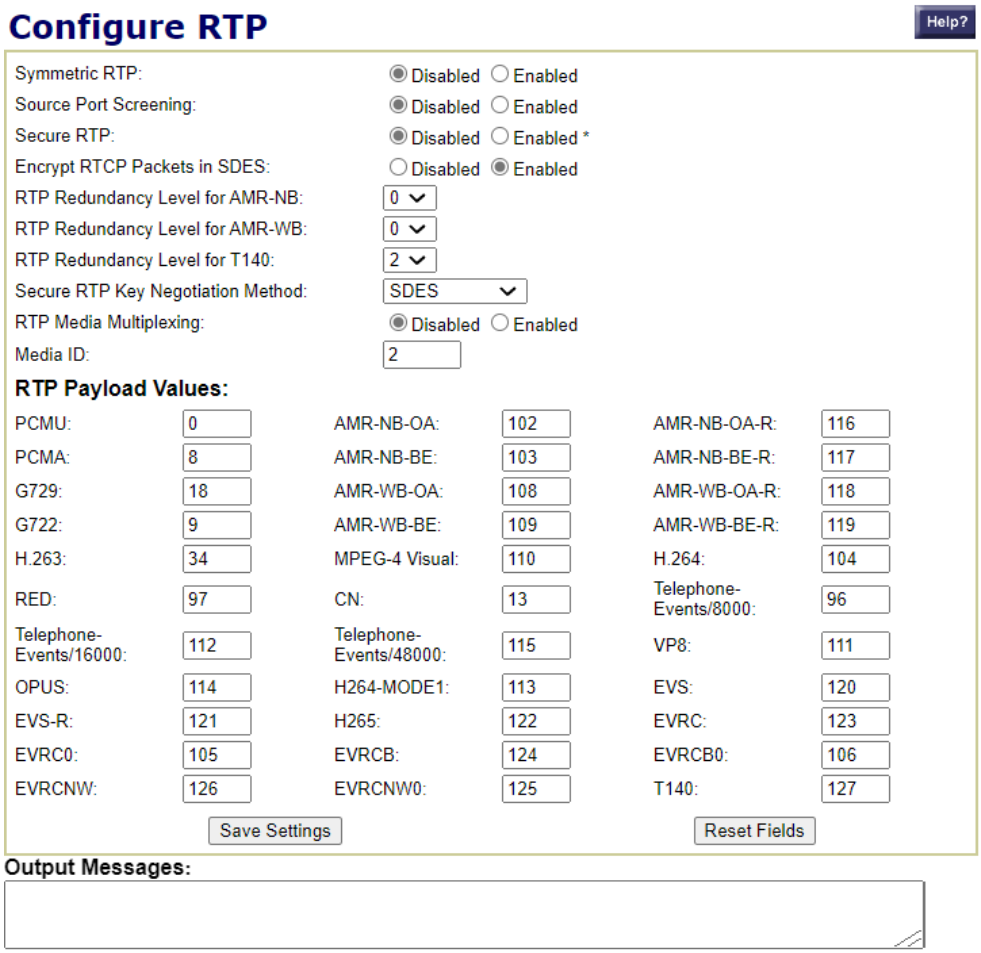
Table 40. RTP Information Required

Value	Description
RTP Media Multiplexing	Enables or disables the multiplexing of audio and video media streams in the Containerized Decomposed Media Server. The default value is Disabled. ***NOTE:*** The **RTCP** and **RTP-RTCP Multiplexing** parameters are mandatory to enable this feature. Changes to this field take effect immediately on the next call.
Media ID	Allows the user to configure the media ID. The Containerized Decomposed Media Server uses this ID for SDP negotiation in the BUNDLE feature. The Media ID value is negotiated through the SDP offer/answer. In Containerized Decomposed Media Server offer call flow, the value is set in the RTP extension header for BUNDLE. The format is as follows: `a=extmap:<Media ID> urn:ietf:params:rtp-hdrext:sdes:mid` For example, `a=extmap:3 urn:ietf:params:rtp-hdrext:sdes:mid` ***NOTE:*** In a slow start scenario, the Containerized Decomposed Media Server uses the Web GUI configured value. The supported value range is 1 to 14. The default value is 2. Changes to this field take effect immediately on the next call.
RTP Payload Values	Optional. Enables the user to configure the payload value for each codec. The Containerized Decomposed Media Server does not accept the duplicate payload value. If a same payload type is used for more than one codec, the whole request is rejected. The supported value range is 0 to 63 and 96 to 127. Changes to this field take effect immediately.

To configure RTP:

1. Click **Configuration** > **Node Configuration** > **Configure RTP**.

   The Configure RTP page displays.



2. Configure the RTP setting information as described in the above table.

   NOTE: You cannot enable both symmetric RTP and source port screening at the same time.

3. Click **Save Settings**.

   Changes take effect immediately, applying to all new ports. The exception is secure RTP, which requires the MRFP restart.

   Confirmation message is displayed in the **Output Messages:** box.

4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure RTCP

The Configure RTCP page enables you to set RTCP behavior. .

The Containerized Decomposed Media Server does not support the following RTCP Timeout for any of the following:

- T.38 Fax - does not use RTP
- RTP media streams to ASR/TTS servers
- RTP media streams to RTSP servers

You can view the information set on this page on the *Show Node Configuration*.

The following table shows RTCP information you can configure.

Table 41. RTCP Information Required

Value	Description
RTCP	Enables or disables RTP Control Protocol (RTCP). The default is disabled. Changes to this field take effect immediately for new calls.

RTCP BYE Packet Processing	Enables or disables the Containerized Decomposed Media Server's processing of received RTCP BYE packets. The supported values are:
	• **Enabled.** When enabled, the Containerized Decomposed Media Server takes the following actions upon receiving an RTCP BYE.
	  • On a SIP call leg, the Containerized Decomposed Media Server sends a SIP BYE
	  • On an ASR or TTS port, the Containerized Decomposed Media Server deletes the port while continuing the associated MSML dialog or VoiceXML script
	  • On an RTSP port, the Containerized Decomposed Media Server deletes the port while continuing the associated MSML dialog or VoiceXML script
	• **Disabled.** When disabled, the Containerized Decomposed Media Server does not process the received RTCP BYE packets.
	The default is Disabled.
	NOTE: This field is enabled only when **RTCP** is Enabled.
	Changes to this field take effect immediately for new calls.

Exclude rtcp-xr in SDP Negotiation	Includes or excludes the `rtcp-xr` attribute in the SDP offer or answer that is generated by the Containerized Decomposed Media Server. The supported values are: • **Enabled.** The `rtcp-xr` attribute is excluded in the SDP offer generated by the Containerized Decomposed Media Server. The `rtcp-xr` attribute is excluded in the SDP answer, when the received SDP offer does not have the `rtcp-xr` attribute. • **Disabled.** The `rtcp-xr` attribute is included in the SDP offer and answer generated by the Containerized Decomposed Media Server. The default value is Disabled. ***NOTE:*** This field is enabled only when **RTCP** is Enabled. Changes to this field take effect immediately for new calls.

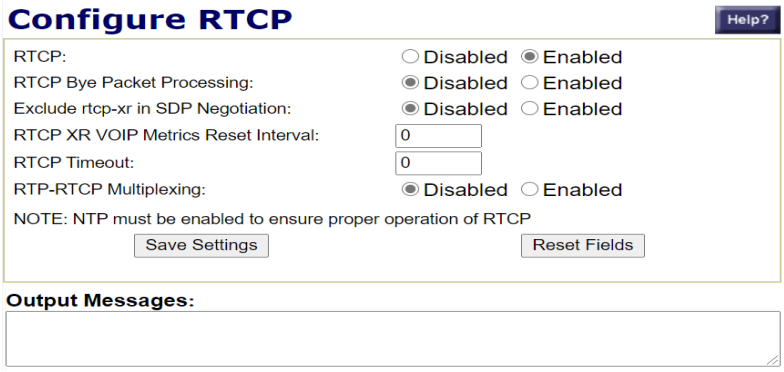
Table 41. RTCP Information Required

Value	Description
RTCP-XR VOIP Metrics Reset Interval	The interval, in seconds, at which the Containerized Decomposed Media Server resets RTCP-XR Voice Over IP metrics. The supported values are 0 and range from 1 to 1000, where zero means the metrics are not periodically reset. The default is 0 (disabled). ***NOTE:*** This field is enabled only when **RTCP** is Enabled. Changes to this field take effect immediately for new calls.
RTCP Timeout	Allows to update the RTCP timeout value, in seconds. The supported value range is from 0 to 7200 with a granularity of 1 second. The default is 0. RTCP timeout is disabled if this value is set to 0. ***NOTE:*** • This field is enabled only when **RTCP** is Enabled. When the **RTCP Timeout** is configured to a non-zero value and no RTCP messages are received within the configured time interval, the Containerized Decomposed Media Server deletes the SIP connection with associated RTP and RTCP media streams. For more information, see *RTCP Timeout on page 118*.
RTP-RTCP Multiplexing	Enables or disables RTP-RTCP multiplexing. The supported values are: • **Enabled.** The Containerized Decomposed Media Server includes the `a=rtcp-mux` attribute in the outgoing SDP offer. RTP-RTCP multiplexing can be enabled only when negotiated through the SDP `a=rtcp-mux` attribute on the port. • **Disabled.** The Containerized Decomposed Media Server excludes the `a=rtcp-mux` attribute in the outgoing SDP offer. The Containerized Decomposed Media Server can negotiate the RTP-RTCP multiplexing message when answering to offers. The default value is Disabled. ***NOTE:*** This field is enabled only when **RTCP** is Enabled. Changes to this field take effect immediately on the next port creation.

To configure RTCP:

1. Click **Configuration** > **Node Configuration** > **Configure RTCP**.

   The Configure RTCP page displays.



2. Enable or disable RTCP.
3. Configure the RTCP settings as described in the table.

   These settings are used for both RTCP (when enabled on this page) and RTCP-XR per-port statistics (when enabled through SIP or MSML).
4. Click **Save Settings**.

   Changes take effect immediately. Confirmation message is displayed in the **Output Messages:** box.

   NOTE: For proper functioning of RTCP, use Network Time Protocol (NTP) to synchronize the Containerized Decomposed Media Servers system clock to the network.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure RTCP Feedback

The Configure RTCP Feedback page assists you to enable the RTCP-based feedback message mechanism.

RTCP-FB is a mechanism to solve media quality (audio and video) issues in on time. RTCP- FB is a part of Real-time Transport Protocol/Audio Video Profile Feedback.

(RTP/AVPF) is an extension to RTP/AVP profile as defined in RFC 4585.

The RTCP-FB messages are defined under RFC 4585. For example, RTCP-PLI message is used to indicate picture loss, which triggers a new I-frame to be generated. The SDP attribute **a=rtcp-fb** is also defined in this RFC to indicate the RTCP FB message can be transmitted over the media session. The Containerized Decomposed Media Server supports negotiating the SDP attribute **a=rtcp-fb** in the media session when RTP/AVPF profile is enabled on that media session.

RTP/AVPF is supported in SIP control protocol in all service contexts.

You can view the information set on the *Show Node Configuration* page.

The following table shows RTCP feedback information you can configure.

Table 42. RTCP Feedback Information Required

Value	Description

RTCP Feedback	Optional. Enables or disables RTCP based feedback profiles. The supported values are:
	• **Enabled.** The Containerized Decomposed Media Server sends RTCP based feedback profiles RTP/AVPF and UDP/TLS/RTP/SAVPF, apart from non-RTCP based feedback profiles in the same media port in a separate **m= lines**. The IP address, port number, and codec list are identical between theses **m= lines**. The Containerized Decomposed Media Server supports negotiating the SDP attribute `a=rtcp-fb` in the media session when RTCP based feedback profile is enabled on that media session.
	• **Disabled.** The Containerized Decomposed Media Server sends only RTCP based feedback profiles and no feedback message is received. This is applicable for audio and non-RTCP based feedback.
	NOTE:
	• The **RTCP Feedback** and **RTCP Feedback Message** are co-related. The following configurations are applicable:
	  • If **RTCP Feedback** is enabled and **RTCP Feedback Message** is disabled, the feedback message is not received.
	  • If **RTCP Feedback** and **RTCP Feedback Message** are enabled, the feedback (RTCP-PLI) message is received for the packet loss.
	  • If **RTCP Feedback** is disabled, the **RTCP Feedback Message** is automatically disabled and the feedback is not received. This is the default state.
	• RTCP feedback is supported only for RTP/AVPF and DTLS calls. RTCP feedback is not supported for SDES SRTP.
	Changes to this field take effect immediately on the next port creation.

Table 42. RTCP Feedback Information Required

Value	Description

RTCP Feedback Message	Optional. Specifies that the Containerized Decomposed Media Server sends the RTCP-FB messages. Supported RTCP-FB messages are:
	• RTCP-PLI
	• RTCP-FIR
	• RTCP-TMMBR
	• GENERIC-NACK
	• transport-cc
	The **RTCP Feedback** and **RTCP Feedback Message** are co-related. The following configurations are applicable:
	• If **RTCP Feedback** is enabled and **RTCP Feedback Message** is disabled, the feedback message is not received.
	• If **RTCP Feedback** is disabled, the **RTCP Feedback Message** is automatically disabled but the Containerized Decomposed Media Server can negotiate the feedback message when answering to offers.
	• If **RTCP Feedback** is enabled, and:
	  • When the RTCP-FB message (RTCP-PLI) is enabled, the Containerized Decomposed Media Server offers RTCP-PLI capability for video sessions through the SDP attribute `a=rtcp-fb`.
	  • When the RTCP-FB message (RTCP-FIR) is enabled, the Containerized Decomposed Media Server offers RTCP-FIR capability for video sessions through the SDP attribute `a=rtcp-fb`.
	  • When the RTCP-FB message (RTCP-TMMBR) is enabled, the Containerized Decomposed Media Server offers TMMBR capability for video sessions through the SDP attribute `a=rtcp-fb`.
	  • When the RTCP-FB message (GENERIC-NACK) is enabled, the Containerized Decomposed Media Server offers Generic-NACK capability for video sessions through the SDP attribute `a=rtcp-fb`.
	  • When the RTCP-FB message (transport-cc) is enabled, the Containerized Decomposed Media Server offers transport-cc, which includes Transport-Wide Congestion Control (TWCC) capability for video sessions through the SDP attribute `a=rtcp-fb:<PT> transport-cc`.
	NOTE: If RTCP-PLI, RTCP-FIR, RTCP-TMMBR, GENERIC-NACK, or transport-cc is offered, the Containerized Decomposed Media Server includes the same in the answer. If the control agent offer does not include RTCP-PLI, RTCP-FIR, RTCP-TMMBR, or transport-cc, the Containerized Decomposed Media Server does not include RTCP-PLI, RTCP-FIR, RTCP-TMMBR, GENERIC-NACK, or transport-cc in the answer, even if configured in the management interface.
	The default state is disabled. Changes to this field take effect immediately on the next port.

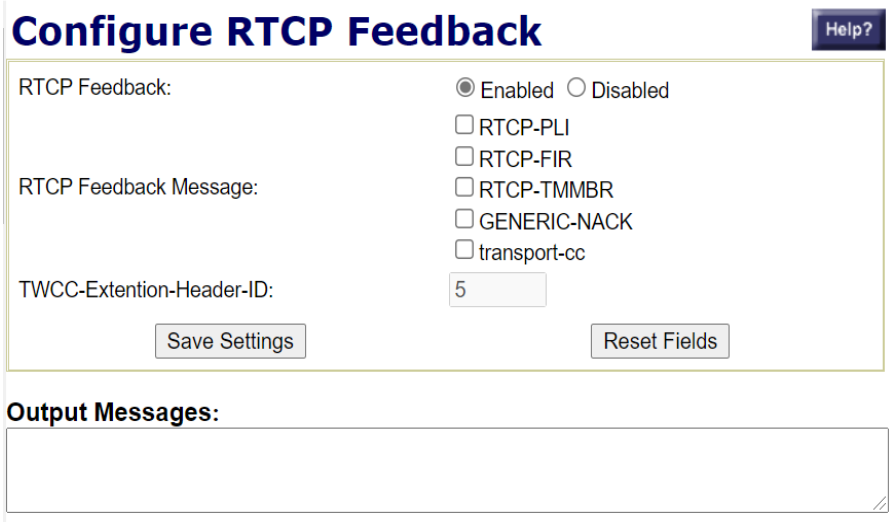
Table 42. RTCP Feedback Information Required

Value	Description
TWCC-Extension-Header-ID	Specifies the Containerized Decomposed Media Server Transport-Wide Congestion Control (TWCC) extension header ID. This is applicable only when the **transport-cc** field is enabled. The format is as follows: `a=extmap: <value>["/"<direction>] <URI> <extensionattributes>` For example, `a=extmap:5 http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01` The supported value range is from 1 to 15. The default value is 5. This parameter does not require a reboot and takes effect on newly created ports.

To configure RTCP Feedback:

1. Click **Configuration** > **Node Configuration** > **Configure RTCP Feedback**.

   The Configure RTCP Feedback page displays.



2. Enter the RTCP Feedback information described in the above table.
3. Click **Save Settings**.

   Changes takes effect on the next port.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure RTSP

The Configure RTSP page enables you to configure settings related to the Real Time Streaming Protocol.

You can view the information set on this page on the *Show Node Configuration*.

The following table shows RTSP information you can configure.

Table 43. RTSP Information Required

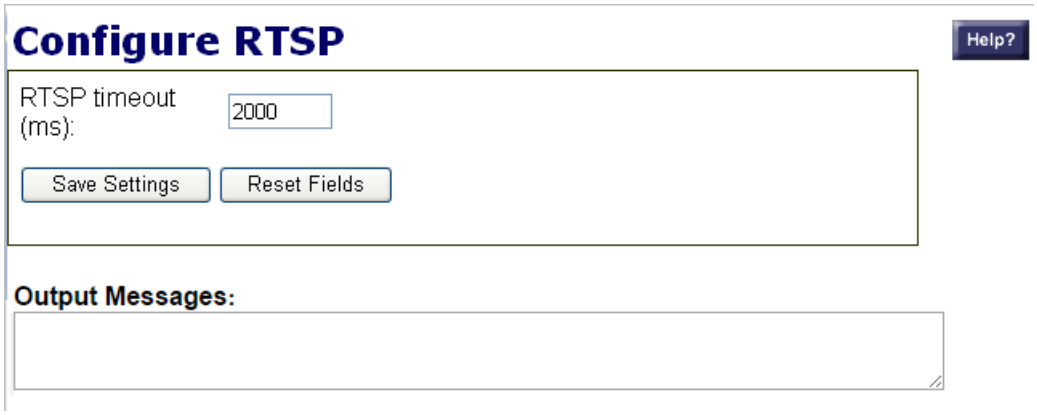
Value	Description
RTSP timeout (ms)	Optional. The period, in milliseconds, for which the Containerized Decomposed Media Server waits before terminating an RTSP announcement when RTP packets stop streaming from an RTSP server. Range is 1000 to 20,000. The default is 2000. Changes to this field take effect immediately.

NOTE: Like the Containerized Decomposed Media Servers RTSP Timeout, the RTSP server may have its own timeout period. For example, the Darwin Streaming Server version 5.5.5 has a configurable rtp_timeout, set by default to 120 seconds, that terminates announcements if RTCP is not received from its client—if the Containerized Decomposed Media Server is not configured to send RTCP at short enough intervals, this timeout period must be set to an appropriately large value when playing long announcements.

To configure RTSP:

1. Click **Configuration** > **Node Configuration** > **Configure RTSP**.

   The Configure RTSP page displays.



2. Specify the desired RTSP timeout period.
3. Click **Save Settings**.

   Changes take place immediately.

   Confirmation message is displayed in the **Output Messages:** box.

Configure Video

The Configure Video page enables you to specify video parameters.

The values specified here including the picture size and MPI specified on the video codec list are used as limits for codec negotiation. When the Containerized Decomposed Media Server negotiates media and session characteristics with SDP, the specified characteristics are negotiated to fall within the values defined here.

The following table shows the video configuration information you can configure.

Table 44. Video Configuration Information

Value	Description
Video MTU	Optional. Applies to all video codecs. The maximum transmission unit, in bytes, for video RTP packets. The range is 750 to 1492. The default is 1492. • The value of this field must always be less than or equal to the media interface **MTU** value configured in the heat template. • If the **Video MTU** value is greater than the media interface MTU size, the Web GUI displays an error message. Therefore, modify the **Video MTU** value to be equal to the media interface MTU size. Changes to this field take effect immediately, applying to the new ports that are created after the configuration is changed.
Allowable Encoder Frame Rate Drop%	The percentage of frame to drop for 720p and 4CIF encoding in order to increase capacity. This applies to HC H.264 and VP8. The range is 0 to 80.
Video Scaling Method	To configure the scaling of the picture when the aspect ratio of source and destination of the picture are different. And also used when scaling for Continuous Presence Video (CPV) conferencing, text and icon overlay. The supported values are: • letter-box • crop The default is crop. ***NOTE:*** The Video Scaling Method is applicable in text and icon overlay only if the image attribute is negotiated. Changes to this field take effect immediately.
Video I-Frame Request Method(s)	Optional. The method the Containerized Decomposed Media Server must use to send IDR requests (H.264). Supported values is. **SIP-INFO**: The Containerized Decomposed Media Server generates I-frame requests in a SIP INFO message. Use this option, if the I-frame request is sent to the SIP application server. The SIP application server forwards the request to the video terminal. By default, the check box is cleared. Changes to this field take effect immediately.

Table 44. Video Configuration Information

Value	Description
Duplicate Initial Video I-Frames	Optional. Determines the I-frame behavior for video announcements in VAS conferences. The supported values are: • **Enabled**. The Containerized Decomposed Media Server sends duplicate I-frames at the beginning of the video announcements when a new user is added to a VAS conference. • **Disabled**. The Containerized Decomposed Media Server sends a single I-frame at the beginning of the video announcements when a new user is added to a VAS conference. The default is **Disabled**. Changes to this field takes effect at the next video session. Note that this setting does not affect continuous presence conferences.
I-Frame Timeout	Optional. Determines the I-frame behavior for video calls. The value is 500 through 60000 milliseconds (ms). The default is 5000 ms. ***NOTE:*** The I-frame time out must increment with multiples of 10 ms. Change to this field takes effect on the next video port.
I-Frame Request Maximum Retries	Optional. Sets the maximum number of retries before the Containerized Decomposed Media Server stops sending I-Frame requests. If the I-frame request is received or the maximum number of retries is requested, the Containerized Decomposed Media Server stops requesting I-frame. The retry feature is disabled, if you enter 0 in this field. The supported values are 0 through 10. The default value is 3. Changes to this field take effect on the next video port.
Default H.264 Profile Level ID (hex)	Optional. Sets the default H.264 Mode 0 and Mode 1 profile level ID. This setting is used only when H.264 profile-level-id parameter is not specified by far-end in the SDP. The default value is 42800A and must be in hexadecimal format. Changes to this field take effect immediately.
Enable Asymmetric H.264 Codec[a]	Optional. The Containerized Decomposed Media Server supports this feature for the H.264 codec based on the configuration in the management interface. By default, this feature is disabled, you can use the Containerized Decomposed Media Server SNMP or Web GUI to enable this feature. Enabling this feature allows you to use different levels and bandwidth settings for encoding and decoding. The Containerized Decomposed Media Server uses the negotiated level in the SDP for the H.264 encoding. However, for decoding, the Asymmetric H.264 codec uses the Containerized Decomposed Media Server SNMP or Web GUI configured H.264 level, regardless of what is offered by far-end in the SDP. This feature helps to ensure that the Containerized Decomposed Media Server can process video when an endpoint negotiates specific video parameters, but sends video using a different set of parameters. Enables or disables Asymmetric H.264 codec. The default is disabled. Changes to this field take effect immediately.

Table 44. Video Configuration Information

Value	Description
TMMBR Transcode Bypass	Optional. This parameter controls whether transcode bypass is permitted for the output video stream of the TMMBR capable ports when the Containerized Decomposed Media Server cannot change its video bitrate as transcode bypass is active. • **Enabled.** The transcode bypass is permitted on the TMMBR enabled ports, even if the Containerized Decomposed Media Server cannot change the bit rate. • **Disabled.** The Containerized Decomposed Media Server transcodes the TMMBR capable ports when the bit rate cannot be changed. The default is **Enabled**. This parameter does not require a restart to take effect and is synchronized for redundancy.
Video Orientation for CPV Conference	Optional. This parameter specifies the video orientation of a CPV root picture size. The supported values are: • landscape • portrait The default is portrait. Changes to this field take effect immediately.
CVO ID	This parameter allows to configure the Coordinated Orientation of Video (CVO) ID. The Containerized Decomposed Media Server does not require that all the ports negotiating CVO in a relay group use the same CVO ID. The supported value is an integer from 0 to 14. • **0.** Disable CVO. • **1 to 14.** Enable CVO with the value being the CVO ID. The default value is 1. Changes to this field take effect immediately.
Conference encoder sharing method	This parameter allows to configure the encoder sharing method when video port or recording service joins the conference. The supported values are: • **on.** The video port or recording service joining the conference can share the existing encoder (if any) with same codec and codec parameters in the conference or recording. The bitrate of the shared encoder can be changed by the other participants. The changed bitrate impacts all the video port or recording service sharing the same encoder. • **off.** The video port or recording service does not share the existing encoder. In this scenario, the Containerized Decomposed Media Server creates a separate encoder for the video port or recording service. The bitrate change does not impact the video port or recording service. • **auto.** The video port or recording service shares the encoder with same codec and codec parameters. The encoder bitrate must not be changed by the other participants sharing the encoder. The default value is on. ***NOTE:*** Currently, the Containerized Decomposed Media Server does not support VAS recording with transcoding. Changes to this field take effect immediately.

Table 44. Video Configuration Information

Value	Description
H.264 Video Encoder Quality	This parameter allows to configure H.264 video encoder quality. The supported values are: • **Highest-Quality.** Enables the high quality H.264 video encoding. • **Best-Performance.** Disables the high quality H.264 video encoding. The default value is Best-Performance. ***NOTE:*** The H.264 video encoder quality is supported for all the profile levels of H.264. Changes to this field take effect for the newly created H.264 ports or during the mid-call when a new H.264 port is created.
CPV Multimixer	This parameter enables or disables the multi-mixer feature on the CPV conference. The supported values are: • **Enabled.** Enables the multi-mixer feature on the CPV conference. • **Disabled.** Disables the multi-mixer feature on the CPV conference. The default value is Disabled. This parameter does not require a restart and takes effect from the next conference creation.
CPV HC User Orientation	This parameter allows to configure the default orientation for HC users in CPV conference. This is applicable when multi-mixer feature is enabled. The supported values are: • landscape • portrait The default value is landscape. This parameter does not require a restart and takes effect from the next conference creation.
CPV Non HC User Orientation	This parameter allows to configure the default orientation for non-HC users in CPV conference. This is applicable when multi-mixer feature is enabled. The supported values are: • landscape • portrait The default value is portrait. This parameter does not require a restart and takes effect from the next conference creation.

Table 44. Video Configuration Information

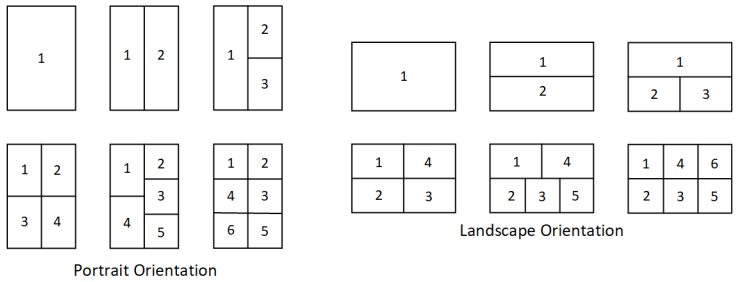
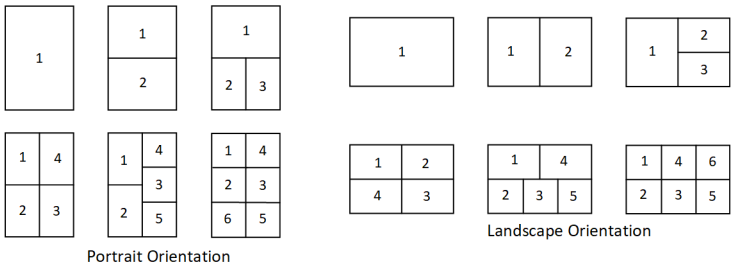
Value	Description
Split Method In Auto Split CPV	Allows to set the method used for splitting the video layout in the auto-split CPV conference. The supported values are: • **Method1.** The Containerized Decomposed Media Server splits the screen vertically in the portrait orientation and horizontally in landscape orientation.  • **Method2.** The Containerized Decomposed Media Server splits the screen horizontally in the portrait orientation and vertically in landscape orientation.  The default value is Method2. Changes to this field take effect immediately.
VAS Transcode	This parameter enables or disables the transcode feature on the VAS conference. The supported values are: • **Enabled.** Enables the transcoding feature on the VAS conference. • **Disabled.** Disables the transcoding feature on the VAS conference. The default value is Disabled. This parameter does not require a restart and takes effect on new VAS conferences creation.
Far End Sprop Parameter Set Based Picture Size	This parameter enables or disables the outgoing picture size generation as per far-end **sprop-parameter-sets** of H.264 (Mode0 and Mode1) port in the CPV (MSML or MSCML) and transcoded VAS (MSML, MSCML, or SIP NETANN) service. The supported values are: • **Enabled.** Enables the outgoing picture size generation as per far-end **sprop-parameter-sets**. • **Disabled.** If this field is disabled, generates the default picture size of the codec or profile. The default value is Disabled. ***NOTE:*** This field has no impact if `a=imageattr` attribute is negotiated on the port. This parameter does not require a restart and takes effect on newly created ports.

Table 44. Video Configuration Information

Value	Description
Port Image Size SDP Negotiation	This parameter enables or disables the port image size `(a=imageattr)` SDP negotiation. The supported values are: • **Enabled.** Enables the port image size SDP negotiation. When enabled, the Containerized Decomposed Media Server negotiates the `a=imageattr` attribute in SDP. • **Disabled.** Disables the port image size SDP negotiation. When disabled, the Containerized Decomposed Media Server discards the `a=imageattr` attribute in SDP and does not include in the outgoing SDP offer/answer. The default value is Disabled. This parameter does not require a restart and takes effect on newly created ports.
Transcoding Based on Image Attribute	This parameter decides whether the port image size negotiated through the `a=imageattr` attribute must be considered while making the transcode bypass decision. The supported values are: • **Enabled.** The Containerized Decomposed Media Server considers the port image size negotiated through the `a=imageattr` attribute in SDP while making the transcode bypass decision except CPV. • **Disabled.** The Containerized Decomposed Media Server does not consider the port image size negotiated through the `a=imageattr` attribute in SDP while making the transcode bypass decision. The default value is Disabled. This parameter does not require a restart and takes effect only on the next port or service creation.
Add SPROP parameter in SDP	This parameter includes or excludes the SPROP parameters set for the H.264 video codec in the outgoing SDP from the Containerized Decomposed Media Server. The supported values are: • **Enabled.** The SPROP parameters set is included in the outgoing SDP from the Containerized Decomposed Media Server. • **Disabled.** The SPROP parameters set is excluded in the outgoing SDP from the Containerized Decomposed Media Server. The default value is Enabled. ***NOTE:*** This parameter is applicable only for MSML service context. This parameter does not require a restart and takes effect from the next H.264 port creation.

Table 44. Video Configuration Information

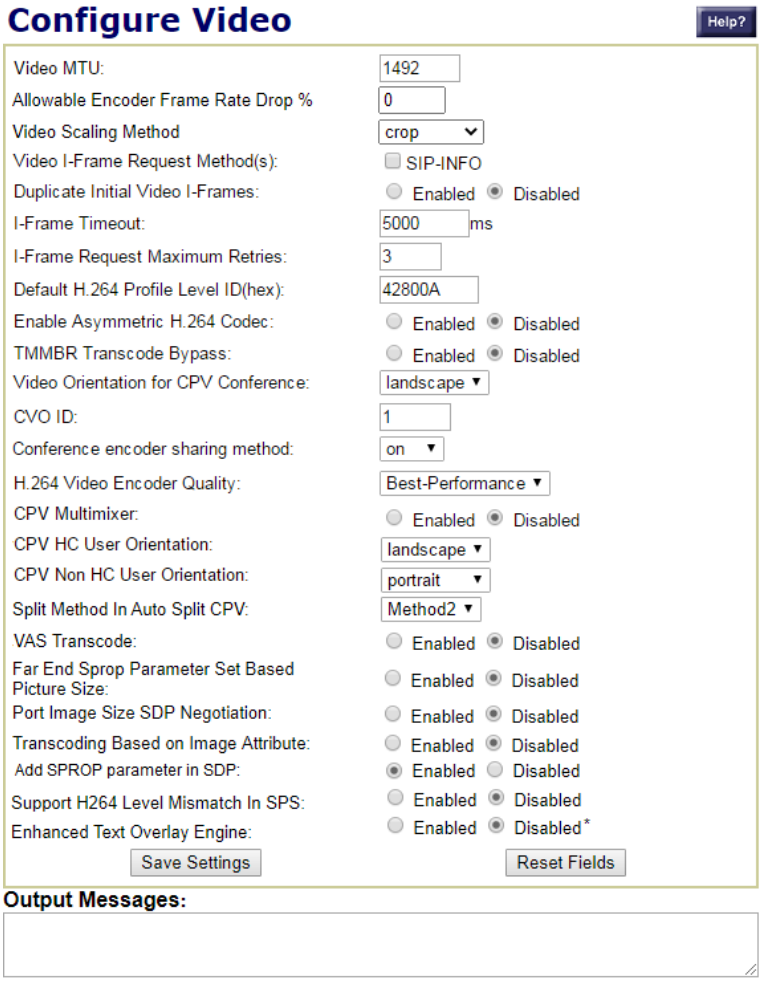
Value	Description
Support H264 Level Mismatch In SPS	Enables or disables decoding of the H.264 packets that contain H.264 level mismatch in SPS, which are received from a specific far-end terminal. In the Sequence Parameter Set (SPS) Network Abstraction Layer (NAL), a mismatch between the profile/level and the number of macroblocks is observed in the H.264 media packets received from specific non-conformant far-end terminals. Supported values are. • **Enabled.** The Containerized Decomposed Media Server decodes the H.264 packets that contain H.264 level mismatch in SPS, which are received from a specific far-end terminal. • **Disabled.** The Containerized Decomposed Media Server does not decode the H.264 packets that contain H.264 level mismatch in SPS, which are received from a specific far-end terminal. The default value is Disabled. ***NOTE:*** • When this field is enabled, the **Enable Asymmetric H.264 Codec** parameter must be disabled. • This feature is supported only in CPV and P2P (sip:tc and msml join) and not supported in recording, VAS, and announcements. This parameter does not require a restart and takes effect from the next H.264 port creation.
Enhanced Text Overlay Engine	Enables or disables the enhanced text overlay engine support. • **Enabled.** The Containerized Decomposed Media Server enables the enhanced text overlay engine support. That is the Containerized Decomposed Media Server automatically breaks the text string, which exceeds the screen width, into multiple lines, and overlays the text string. • **Disabled.** The Containerized Decomposed Media Server disables the enhanced text overlay engine support. By default, this field is Disabled. Changes to this field require a MRFP restart to take effect.

[a] When Asymmetric H.264 codec feature is enabled, the H.264 decoder setting is using the Web GUI setting. The setting can be changed during run-time, but the new setting takes effect on the next H.264 port and does not affect the existing H.264 port.

To configure support for video:

1. Click **Configuration** > **Node Configuration** > **Configure Video**.

   The Configure Video page displays.



2. Enter the video information described in the table above.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Video Codec List

The Configure Video Codec List page enables you to customize the video codec support communicated to other devices.

In order for the media to support video recording, playback, or conferencing, a video codec must be configured on this list.

The values for the codecs specified here—as well as the video bandwidth specified on the Configure Video page—are used as limits for codec negotiation. When the Containerized Decomposed Media Server negotiates media and session characteristics with SDP, these characteristics are negotiated to fall within the values defined here.

The video codec list allows Containerized Decomposed Media Servers to list supported video codecs for codec negotiation. The most-preferred video codecs are entered at the top of the list, and the least-preferred at the bottom.

When the Containerized Decomposed Media Server generates an offer, it offers all codecs listed on its preferred codec list, provided the Containerized Decomposed Media Server has sufficient resources to support the codec.

By default, no video codecs are offered. For the Containerized Decomposed Media Server to use video, you must specify at least one video codec.

The following table shows the default ordering of video formats in the video codec list.

Table 45. Default Ordering of the Video Codec List

Name	RTP Payload	Description
None	—	Default value
H.264	104	H.264 payload format as per RFC 3984
VP8	111	The format of VP8 RTP payload is **draft-ietf-payload-vp8**.
H.264-Mode1	113	H.264 payload format as per RFC 6184, previously RFC 3984
H.265	122	H.265 payload format as per RFC 7798

The following table shows the video codec information you can configure for each item in the video codec list.

Table 46. Video Codec Information

Value	Description
Video Codec	Optional. The codec to be used to compress video packets. The supported values are: • **None.** Video is not supported. The Containerized Decomposed Media Server will not offer video during codec negotiation. • H.264 • VP8 • H.264-Mode1 • H.265 The default is **None**. Changes to this field take effect immediately.
Profile	Available for H.264 and H.264-Mode1. • The value supported for H.264 and H.264-Mode1 is **Constrained Baseline**.The value supported for H.265 is **Main**.
Level	Available for H.264 and H.264-Mode1. • The values supported for H.264 and H.264-Mode1 are: **Level 1, Level 1b, Level 1.1, Level 1.2, Level 1.3, Level 2, Level 2.1, Level 2.2, Level 3,** and **Level 3.1**. • The values supported for H.265 are: **Level 1, Level 2, Level 2.1, Level 3,** and **Level 3.1**. For H.264, from Level 2.1 onwards supports HC type.

Table 46. Video Codec Information

Value	Description
Maximum Bandwidth	Available bandwidth for the listed video codecs. The supported values, in kbps, are. • **H.264.** Range is 20-4000. The default is 1000. • **H.264-Mode1.** Range is 20-4000. The default is 1000. • **VP8.** Range is 20-2000. The default is 768. • **H.265.** Range is 20-4000. The default is 1000.
Frame Size (MB)	Available for VP8 only. Following are the available frame size. • 99 [QCIF (176x144)] • 225 [180p (320x 180)] • 396 [CIF (352x 288)] • 900 [360p 0x 360)] • 1200 [480p (640x 480)] • 1350 [480p (720 x 480)] • 3600 [720p (1280x720)] The default is 396 [CIF (352x 288)]. Changes to this field take effect on the next video port.
Maximum Frame Rate (fps)	Available for VP8 only. The maximum frame rate is hard-coded and not user configurable. The maximum frame rate for VP8 is 30 fps.
Max I-Frame Period	Available for all video codecs. The values are 2 to 1000 sec. The default value is 15.

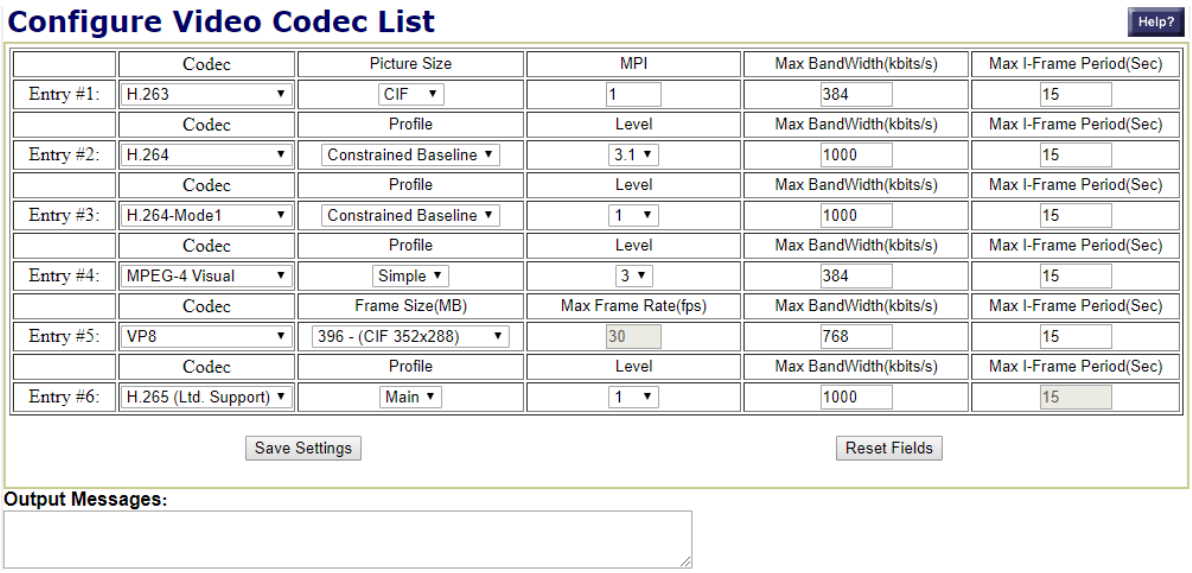
NOTE:

- If the source of the video is a VP8 port, and if the picture resolution is not in multiples of 16, then the H.264 encoder needs to modify the size to the next higher multiples of 16 before it is encoded.
- Large I-frame periods are not recommended.

To configure the video codec list:

1. Click **Configuration** > **Node Configuration** > **Configure Video Codec List**.

   The Configure Video Codec List page displays.



Configure Video Codec List

Help?

	Codec	Picture Size	MPI	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #1:	H.263	CIF	1	384	15
	Codec	Profile	Level	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #2:	H.264	Constrained Baseline	3.1	1000	15
	Codec	Profile	Level	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #3:	H.264-Mode1	Constrained Baseline	1	1000	15
	Codec	Profile	Level	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #4:	MPEG-4 Visual	Simple	3	384	15
	Codec	Frame Size(MB)	Max Frame Rate(fps)	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #5:	VP8	396 - (CIF 352x288)	30	768	15
	Codec	Profile	Level	Max BandWidth(kbits/s)	Max I-Frame Period(Sec)
Entry #6:	H.265 (Ltd. Support)	Main	1	1000	15

Save Settings Reset Fields

Output Messages:

2. For each codec you want to offer, select and configure an item in the video codec list. Note that you must specify video codec support if you want to be able to use video.
   - For H.264, you can leave the profile as they are, select level settings, and enter the bandwidth.
   - For H.264-Mode1, you can leave the profile as it is, select the level settings, and enter the bandwidth.
   - For VP8, select the frame size and enter the bandwidth. Frame rate is hard-coded.
   - For H.265, you can leave the profile as it is, select the level settings, and enter the bandwidth.

   NOTE: Selecting **None** in the Codec Type disallows the selection of other codec. Only one codec can be assigned to each video card.
3. Click **Save Settings**.

   The Containerized Decomposed Media Server begins using the updated codec list immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Video Recording

The Configure Video Recording page enables you to specify the Containerized Decomposed Media Servers video recording parameters.

The following table shows the video recording information you can configure.

Table 47. Video Recording Information

Value	Description
CIF Default Bitrate	Used only for continuous presence recording. The default bit rate, in kilobits per second, to be used for CIF recordings when no bit rate is explicitly specified. The range is 20 to 768. The default is 384. Changes to this field take effect immediately.
CIF Default MPI	Used only for continuous presence recording. The default MPI to be used for CIF recordings when no MPI is explicitly specified. The range is 1 to 32. The default is 1. Changes to this field take effect immediately.
QCIF Default Bitrate	Used only for continuous presence recording. The default bit rate, in kilobits per second, to be used for QCIF recordings when no bit rate is explicitly specified. The range is 20 to 768. The default is 384. Changes to this field take effect immediately.
QCIF Default MPI	Used only for continuous presence recording. The default MPI to be used for QCIF recordings when no MPI is explicitly specified. The range is 1 to 32. The default is 1. Changes to this field take effect immediately.

To configure video recording:

1. Click **Configuration** > **Node Configuration** > **Configure Video Recording**.

   The Configure Video Recording page displays.

2. Enter the video recording information:
   - Set the CIF default bitrate.
   - Set the CIF default MPI.
   - Set the QCIF default bitrate.
   - Set the QCIF default MPI.
3. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure SNMP Agent

The Configure SNMP page enables you to set the SNMPv2c community string, SNMPv3 parameters, and SNMP agent listening port for the Containerized Decomposed Media Server.

The SNMPv2c community string acts as a simple password-like mechanism, by which SNMP managers can authenticate themselves to the Containerized Decomposed Media Server. The one community string is used to authenticate all SNMPv2c managers attempting to communicate with the Containerized Decomposed Media Server.

For SNMPv3, the Containerized Decomposed Media Servers administration username and password can be used for authentication and privacy.

You can view the information set on this page on the *Show Node Configuration*.

The following table shows the SNMP agent information you can configure.

Table 48. SNMP Agent Information

Option	Description
When SNMPv2c is enabled	
SNMPv2c community string	Community string, up to 20 characters, which includes alphanumeric and special ASCII characters (33-126), used by the destination host to authenticate the Containerized Decomposed Media Server. ***NOTE:*** Backslash (\), single quote ('), and blank space are not accepted, but any leading or trailing blank spaces are ignored. The default is CONV. The changes to this field require OAMP pod restart to take effect.
When SNMPv3 is enabled	
Current Administration Username	The administration username currently configured for the Containerized Decomposed Media Server. This is used for encrypting when privacy is configured. Valid values are strings of 6 to 32 characters from ASCII range 0x20 to 0x7E with the exception of double quote (“, 0x22), single quote (‘, 0x27), colon (:, 0x3A), and hash (#, 0x23). The string cannot begin with a hyphen (-, 0x2D). Default is blank.

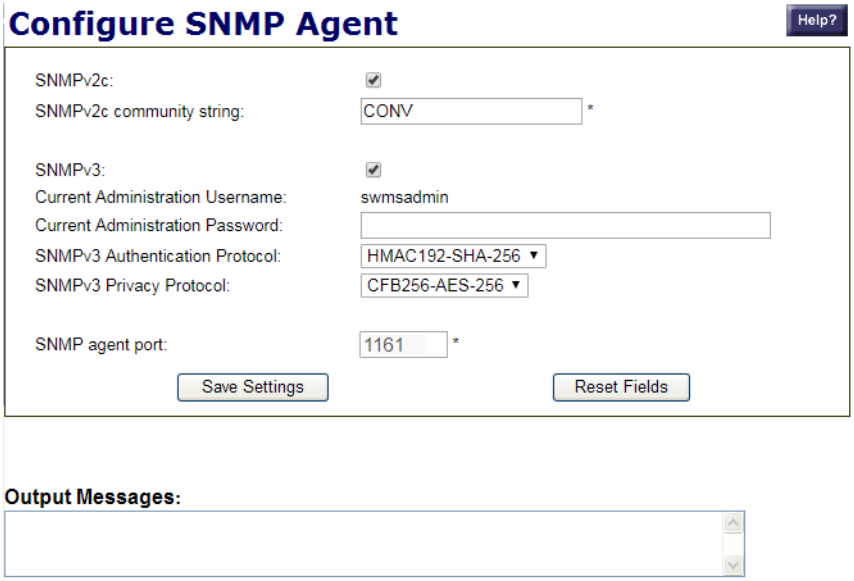
Table 48. SNMP Agent Information

Option	Description
Current Administration Password	The administration password currently configured for the Containerized Decomposed Media Server. This is used for encrypting when privacy is configured. Valid values are strings of up to 64 characters from ASCII range 0x20 to 0x7E with the exception of double quote (“, 0x22) and single quote (‘, 0x27). Default is blank.
SNMPv3 Authentication Protocol	The authentication protocol used for SNMPv3 communications. • **None.** No authentication is used. • **HMAC-MD5-96.** Uses MD5 hash-function in HMAC mode and truncates the output to 96 bits. • **HMAC-SHA-96.** Uses the SHA hash-function in HMAC mode and truncates the output to 96 bits. • **HMAC128-SHA-224.** Uses the SHA hash-function in HMAC mode and truncates the output to 224 bits. • **HMAC192-SHA-256.** Uses the SHA hash-function in HMAC mode and truncates the output to 256 bits. • **HMAC256-SHA-384.** Uses the SHA hash-function in HMAC mode and truncates the output to 384 bits. • **HMAC384-SHA-512.** Uses the SHA hash-function in HMAC mode and truncates the output to 512 bits. The default value is HMAC192-SHA-256. The changes to this field take effect immediately.
SNMPv3 Privacy Protocol	The privacy protocol use for SNMPv3 communications. The supported values are: • **None.** No authentication is used. • **CBC-DES.** Uses the Data Encryption Standard in Cipher Block Chaining mode. • **CFB128-AES-128.** Uses the Advanced Encryption Standard with key size of 128 in Cipher Feedback mode. • **CFB192-AES-192.** Uses the Advanced Encryption Standard with key size of 192 in Cipher Feedback mode. • **CFB256-AES-256.** Uses the Advanced Encryption Standard with key size of 256 in Cipher Feedback mode. The privacy cannot be used if authentication is not used. The default value is CFB256-AES-256. The changes to this field take effect immediately.
SNMP agent port	The SNMP agent listening port for the Containerized Decomposed Media Server. This field is non-editable.

To configure the SNMP agent information:

1. Click **Configuration** > **Node Configuration** > **Configure SNMP Agent**.

   The Configure SNMP Agent page is displayed.



2. Select or deselect **SNMPv2c** and/or **SNMPv3** check box.
3. If **SNMPv2c** is selected, in the **SNMPv2c community string** field, enter the value.
4. If **SNMPv3** is selected, in the **Current Administration Password** field, enter the password.
5. Optionally specify the SNMP agent listening port.
6. Click **Save Settings** to apply the new setting.

   The GUI prompts you to restart the OAMP for changes to SNMPv2c community string and SNMP agent port. The changes to SNMPv3 settings take effect immediately. OAMP cannot be restarted from Web GUI. For the commands on restating the OAMP, refer to the *Installation Guide*.

   Confirmation message is displayed in the **Output Messages:** box.
7. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Add SNMP Trap Destination

The Add SNMP Trap Destination page enables you to configure a new destination for SNMP traps.

NOTE: You cannot modify the settings of an SNMP trap destination. To modify settings, delete the destination and add it again with the new information.

The following table shows the information you must provide to configure an SNMP trap destination.

Table 49. SNMP Trap Destination Settings

Option	Description
Destination IP address or hostname	IP address of the destination host, in dotted quad format for IPv4 or the supported notations for IPv6. If DNS is being used, you can enter a hostname of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". The changes to this field take effect immediately.
Enter trap UDP port number	UDP port on which the SNMP destination host is listening for traps. The range is 1 to 65535. The changes to this field take effect immediately.
Enter trap community name	Community string used by the destination host to authenticate the Containerized Decomposed Media Server. Valid values are strings of up to 20 characters. Default is “CONV”. The changes to this field take effect immediately.

To add a destination for SNMP traps:

1. Click **Configuration** > **Node Configuration** > **Add SNMP Trap Destination**.

2. Enter the destination host information.
   - Enter the destination IP address or hostname.
   - Enter the trap UDP port for SNMP traps on the destination.
   - Enter the trap community name.
3. Click **Execute**.

   The Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

Delete SNMP Trap Destination

On the Delete SNMP Trap Destination page, you can remove a configured destination for SNMP traps.

NOTE: You cannot delete the localhost (127.0.0.1) as a trap destination.

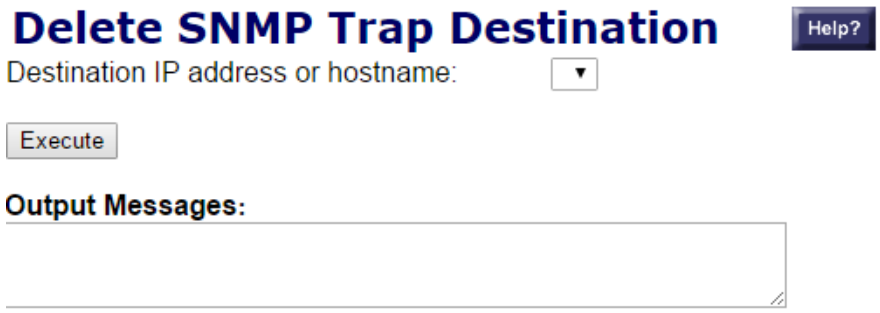
The following table shows the information to configure SNMP trap destination.

Table 50. Delete SNMP Trap Destination Settings

Option	Description
Destination IP address or hostname	IP address of the destination host, in dotted quad format for IPv4 or the supported notations for IPv6. If DNS is being used, you can enter a hostname of up to 80 characters. The changes to this field take effect immediately.

To remove a destination for SNMP traps:

1. Click **Configuration** > **Node Configuration** > **Delete SNMP Trap Destination**.



2. Select the target destination (IP address: port) that you want to remove.
3. Click **Execute** to remove the destination.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

NOTE: This operation also removes the mapping of trap destination with its corresponding SNMPv3 users.

Configure SNMPv3 User and Trap Destination

The Configure SNMPv3 User and Trap Destination page allows you to configure the SNMPv3 user and its mapping to the corresponding trap destination.

The following table shows the information you can configure for SNMPv3 user trap.

Table 51. SNMPv3 User and Trap Configuration Information

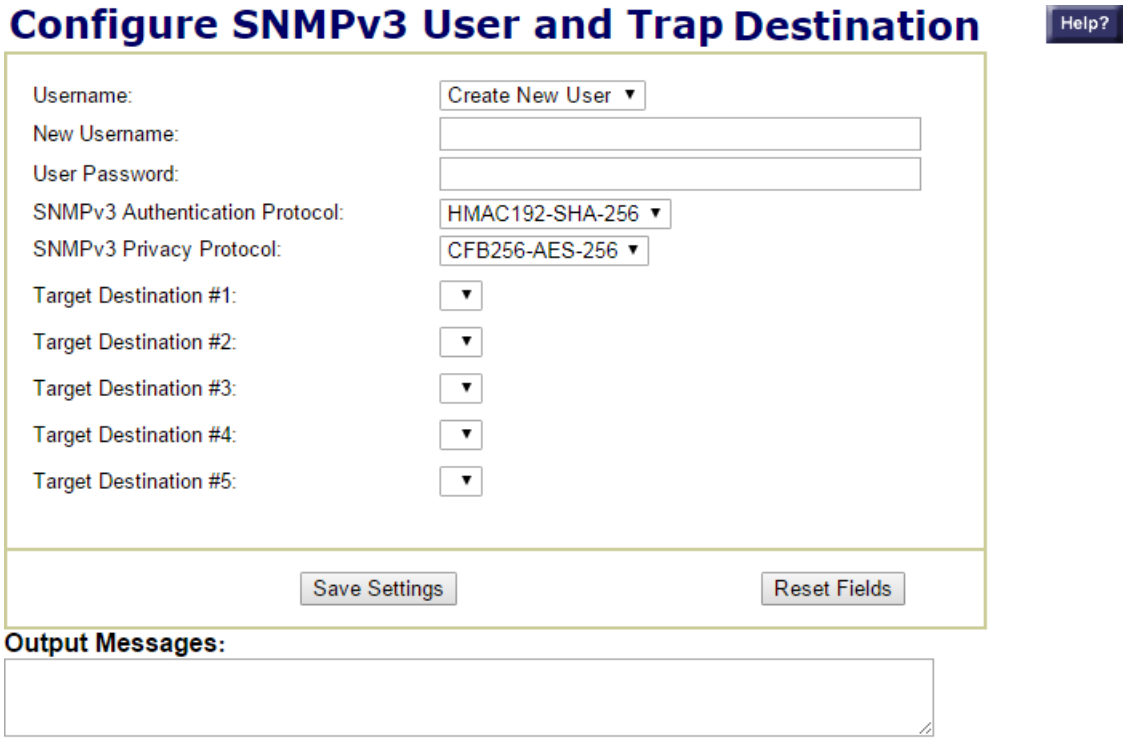
Value	Description
Username	The SNMPv3 user name currently configured for the Containerized Decomposed Media Server. Valid values are **Create New User** and the existing user. The default value is Create New User, which allows the new SNMPv3 user configuration.
New Username	New Username allows to configure new SNMPv3 user name. This field is displayed only when Create New Username is selected in the Username. Valid values are strings of 6 to 64 characters. ***NOTE:*** Duplicate entry for identical users cannot be created.
User Password	The password currently configured for the SNMPv3 user. Valid values are text strings of 8 to 64 characters. ***NOTE:*** • User password is entered only when an SNMPv3 user is created or modified. • The password for the admin cannot be changed through this page.
SNMPv3 Authentication Protocol	The authentication protocol use for SNMPv3 communications. • **None.** No authentication is used. • **HMAC-MD5-96.** Uses MD5 hash-function in HMAC mode and truncates the output to 96 bits. • **HMAC-SHA-96.** Uses the SHA hash-function in HMAC mode and truncates the output to 96 bits. • **HMAC128-SHA-224.** Uses the SHA hash-function in HMAC mode and truncates the output to 224 bits. • **HMAC192-SHA-256.** Uses the SHA hash-function in HMAC mode and truncates the output to 256 bits. • **HMAC256-SHA-384.** Uses the SHA hash-function in HMAC mode and truncates the output to 384 bits. • **HMAC384-SHA-512.** Uses the SHA hash-function in HMAC mode and truncates the output to 512 bits. The default value is HMAC192-SHA-256. The changes to this field take effect immediately.

Table 51. SNMPv3 User and Trap Configuration Information

Value	Description
SNMPv3 Privacy Protocol	The privacy protocol use for SNMPv3 communications. The supported values are: • **None.** No authentication is used. • **CBC-DES.** Uses the Data Encryption Standard in Cipher Block Chaining mode. • **CFB128-AES-128.** Uses the Advanced Encryption Standard with key size of 128 in Cipher Feedback mode. • **CFB192-AES-192.** Uses the Advanced Encryption Standard with key size of 192 in Cipher Feedback mode. • **CFB256-AES-256.** Uses the Advanced Encryption Standard with key size of 256 in Cipher Feedback mode. The privacy cannot be used if authentication is not used. The default value is CFB256-AES-256. The changes to this field take effect immediately.
Target Destination #1 to #5	The IP address of the UDP port configured in Add SNMP Trap Destination webpage.

To configure SNMPv3 User and Trap Destination from the Web GUI:

1. Click **Configuration** > **Node Configuration** > **Configure SNMPv3 User and Trap Destination**.



2. Enter the user and Trap Destination information:
   - Select Create New User or existing username in the Username.

     NOTE: Enter the New Username, if Create New Username is selected. When creating new SNMPV3 user, ensure that SNMPV3 is enabled from the Configure SNMP Agent page, for the SNMPV3 traps to be sent successfully.
   - Enter the **User Password**.
   - Select the **SNMPv3 authentication Protocol.**
   - Select the **SNMPv3 Privacy Protocol**.
   - Select the **Target Destinations**.

     NOTE: Target Destination is entered only when the user wants to configure SNMPv3 Trap Destination.
3. Click **Save Settings** to store the configuration data. Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Click **Reset Fields** to reset the changes made to previous values.

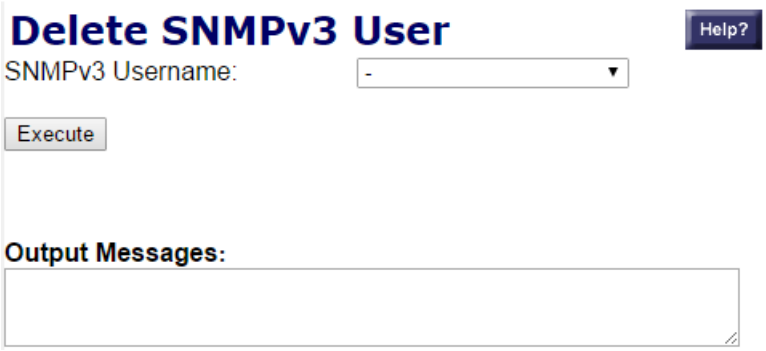
To configure the SNMPv3 users and trap destination using SNMP commands, refer *SNMP Interface Reference*.

Delete SNMPv3 User

The Delete SNMPv3 User page allows you to delete a configured SNMPv3 user and the mapping of trap destinations for the selected user.

To remove a SNMPv3 User

1. Click **Configuration** > **Node Configuration** > **Delete SNMPv3 User**.



2. Select the SNMPv3 Username that you want to remove.
3. Click **Execute** to remove the SNMPv3 user. Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

   NOTE: The admin user cannot be deleted from this page.

Configure Transcode Bypass

The Configure Transcode Bypass page enables you to enable and disable transcode bypass for a codec (G.711, G.729, G.722, EVS, EVRC, EVRC-B, AMR-NB, and AMR-WB).

When transcode bypass is enabled, the Containerized Decomposed Media Server bypasses codecs when the played announcements or recording files use the same compression method as the port. When transcode bypass is disabled, the Containerized Decomposed Media Server transcodes regardless of port codec and file compression method.

You can view the information set on this page on the *Show Node Configuration*.

The following table describes the information you must configure for the transcode bypass.

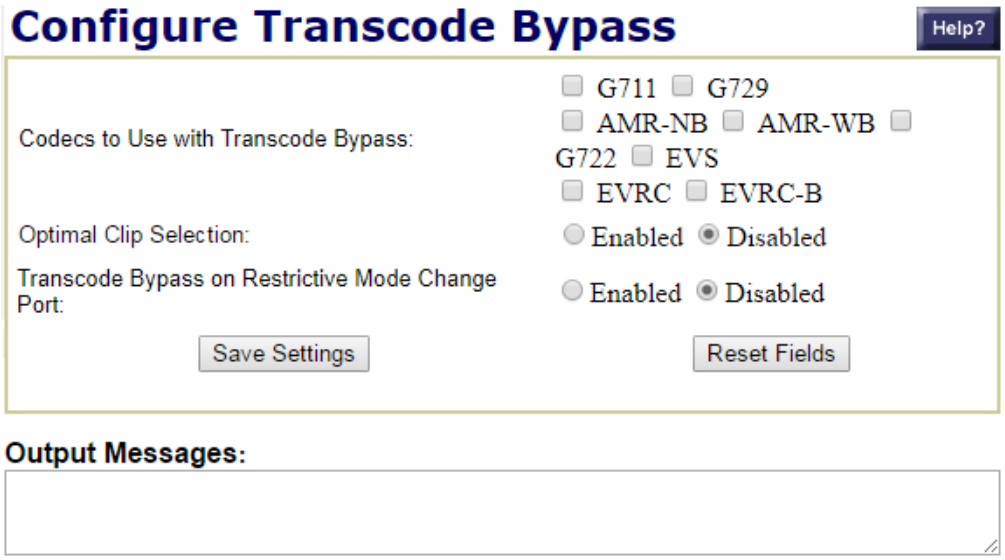
Table 52. Transcode Bypass Information

Value	Description
Codec to Use with Transcode Bypass	Indicates which audio codecs must use the transcode bypass feature, whenever possible. The supported codecs are G.711, G.729, AMR-WB, AMR-NB, G.722, EVS, EVRC, and EVRC-B.
Optimal Clip Selection	Enables or disables the optimal clip selection feature. Supported values are: • **Enabled.** The Containerized Decomposed Media Server translates the original clip name specified in the play request to the optimal clip, based on the port codec. The Containerized Decomposed Media Server tries to play the optimal clip first. If the optimal clip is not found, the Containerized Decomposed Media Server plays the base clip. • **Disabled.** The Containerized Decomposed Media Server retains the original clip name specified in the play request. The default value is Disabled. The changes to this field take effect on the new announcement requests.
Transcode Bypass on Restrictive Mode Change Port	Enables or disables the transcode bypass feature on restrictive EVS (AMR-WB-IO mode only), AMR-NB, and AMR-WB ports. The EVS (AMR-WB-IO mode only), AMR-NB, and AMR-WB ports are considered restrictive when mode change parameters **mode-change-period=2** and/or **mode-change-neighbor=1** are negotiated in the SDP. The supported values are: • **Enabled.** The Containerized Decomposed Media Server enables transcode bypass feature on restrictive EVS (AMR-WB-IO mode only), AMR-NB, and AMR-WB ports. • **Disabled.** The Containerized Decomposed Media Server disables transcode bypass feature on restrictive EVS (AMR-WB-IO mode only), AMR-NB, and AMR-WB ports. The default value is Disabled. The changes to this field take effect on the new announcement requests.

To configure transcode bypass:

1. Click **Configuration** > **Node Configuration** > **Configure Transcode Bypass**.

   The Configure Transcode Bypass page displays.



2. Check the codecs that must use transcode bypass.
3. Select the **Optimal Clip Selection**.
4. Select the **Transcode Bypass on Restrictive Mode Change Port**.
5. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
6. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure HTTP Media and Cache

The Configure HTTP Media and Cache page enables you to configure the mode of operation for HTTP media, as well as the cache used in the cached mode of operation. You can also configure a path to a post processing CGI script.

HTTP Operating Modes

The Containerized Decomposed Media Server supports two modes of operation for HTTP media.

- Streamed mode
- Cached mode

In streamed mode, the Containerized Decomposed Media Server streams clips directly from external HTTP servers at clip play speed. There is at least one HTTP connection per announcement. For example, if the Containerized Decomposed Media Server is concurrently playing a five-minute clip to 100 connections, all 100 HTTP connections will be kept open for the full five minutes. The Containerized Decomposed Media Server supports WAV, MP3, and MP4 container file formats in streamed mode.

In cached mode, the Containerized Decomposed Media Server cache media clips and stream clips to connections from the internal cache. The Containerized Decomposed Media Server retrieves a clip from the external HTTP server only if the clip is not cached, or if it needs to be re-validated. This allows the Containerized Decomposed Media Server to retrieve the clips at near–line speed. HTTP connections remain open only during clip retrieval. When the cache is full, the Containerized Decomposed Media Server applies a Least Recently Used algorithm to replace stale clips. The Containerized Decomposed Media Server supports WAV, MP3, MP4, 3GP, 3G2, AMR, and AWB container file formats in cached mode.

HTTP media caching reduces the burden on the external HTTP server. In addition, cached clips are retrieved very much faster than streamed clips. Using HTTP media caching can significantly increase capacity for applications where media streaming is a critical operation.

The Containerized Decomposed Media Server supports playing chunked streams in the HTTP and HTTPS announcements for mp3 and wav files. The Containerized Decomposed Media Server reads the chunk-size field from the chunk data and decodes the chunk packets. The Containerized Decomposed Media Server considers the end of chunked encoding only after receiving the chunk size as zero.

The principle use cases for HTTP caching are:

- Playing multiple short clips in sequence, where each clip represents a word or a phrase from a sentence
- Playing long clips when the media or file server is close to capacity
- Using HTTP for audio prompting for Voicemail applications written in VoiceXML
- Call-parking and music on hold, which can require five or six (2 to 5 MB) files to be cached

HTTP caching is enabled through the management interface.

Cache Behavior

Based on the content of HTTP headers and other heuristics, clips that are placed in the cache may continue to be stored in the cache once they have been played. This further reduces the load on servers and decreases play start latency for those clips that can be cached. Some latency may still be incurred if the Containerized Decomposed Media Server needs to revalidate the cache entry.

For revalidation, an HTTP client queries a server to determine whether the cached copy is still valid for use. If the cached entry remains valid, the server sends a response code that allows the client to use the cached resource. If the cached entry is no longer valid, the server returns a new copy of the resource.

Not all clips that are retrieved can be stored in the cache. Whether or not a clip can be cached depends on the values of some HTTP headers (for example, the **Cache-Control** header).

Clips that are returned as a result of an HTTP GET with a URI that has a query string may be cached. However if the query string contains values that are session specific, it is unlikely that other subsequent requests will have the same query values. In that case, although clips may actually have the same audio content, they are identified by different URIs, and hence the new requests always result in a cache miss and subsequent HTTP retrieval.

There may be some streaming capacity reduction in the Containerized Decomposed Media Server when caching is used if there is a high percentage of cache misses. That is, if the Containerized Decomposed Media Server is never or seldom able to play a clip from the cache without first retrieving it from the HTTP server.

The cache size is configurable through the management interface. Memory used for the HTTP cache is not available for other uses such as storing clips locally.

Note that caching large files could delay the Containerized Decomposed Media Server's response to a SIP INVITE. In cases when the preroll buffer has been set to a value longer than allowed response time for the SIP INVITE, then the Containerized Decomposed Media Server may not respond to the INVITE in a sufficiently timely manner when a large file is cached. In this case, the caller could time out on the INVITE, possibly resulting in a canceled call.

Cache Control

HTTP defines both public and private caches. Public caches are intermediate network caches that are accessed by multiple disparate clients. The Containerized Decomposed Media Server implements a private cache. As such, it ignores any cache control directives intended for public caches.

The following provides additional detail on how the Containerized Decomposed Media Servers maintains the cache:

- The Containerized Decomposed Media Server supports and uses the **HTTP Expires** and **Cache-Control** headers (if present) to determine the validity of cached files.
- The Containerized Decomposed Media Server will cache a file that is labeled **no-cache** but will validate it before using the file.
- The Containerized Decomposed Media Server does not cache a file that is labeled **no-store**.
- If the HTTP request retrieving the file did not include either a **Cache-Control** or **Expires** header, the Containerized Decomposed Media Server assumes that the file is valid for the time period configured in the management interface.
- The Containerized Decomposed Media Server maintains **ETag** headers and **Last-Modified** headers (if present) and returns them to the server when doing cache validation.

  ETags serve as a version number that can be used by a server to determine whether to return a new copy of the file when a client requests validation.
- The Containerized Decomposed Media Server uses a least-recently-used cache replacement strategy.

Post-processing CGI Scripts

For HTTP external record to operate with full functionality, the Containerized Decomposed Media Server expects a CGI script to reside on the server to post-process the file. Creating and installing such a script is optional. However, for full functionality of the real-time streaming feature, the required CGI script must:

- Update the WAV header to reflect the real length of the audio file.

  In real-time streaming of audio files, the Containerized Decomposed Media Server cannot predict the length of the file. To accommodate this, the Containerized Decomposed Media Server either specifies a large file to the HTTP server (the maximum available, “0xFFFF”) or uses chunked transfer encoding.
- Trim silence and trailing DTMF tone from the resulting audio file.
- Return an appropriate HTTP response code to the Containerized Decomposed Media Server.

If an appropriate script is not found on the server, problems may result when attempting to play back recordings using some audio players. This is because, without the CGI script:

- The trailing silence and the start of the DTMF tone will still be present at the end of the recording.
- The WAV header of the saved recording always shows, when chunked transfer encoding is not used, that the file size is the maximum available (“0xFFFF”), regardless of the actual file size. When chunked transfer encoding is used, the file size does not reflect the real length. This may cause some applications to consider the file as corrupt, even if the file is sound.
- After the file operation is complete, no information is returned by the operation, including HTTP response codes. Thus, the Containerized Decomposed Media Server has no way of knowing if the clip has been successfully recorded and, in the future, an audio player could attempt to play back a clip that does not exist.

HTTP Parameters

The following table shows the information you can configure for HTTP mode and caching.

Table 53. HTTP Mode and Caching Information

Value	Description
HTTP Play	
HTTP Media Mode	The mode of operation with respect to HTTP media. The supported values are: • **Streamed.** Use streamed HTTP media mode. • **Cached.** Allow HTTP caching. The default is Cached. HTTP caching can be used in conjunction with NFS server caching. Changes to this field require a MRFP restart to take effect.

Table 53. HTTP Mode and Caching Information

Value	Description
Cache Size (MB)	The size of the cache in MB used for cached HTTP media. The value range is 5 to 1024. The default value is 100. This setting is ignored if **Streamed Mode** is selected. Changes to this field require a MRFP restart to take effect.
Default Cache Max Age (minutes)	The default time in minutes after which a file in the cache must be revalidated. This value is used when the HTTP response to a request for an audio clip contains neither an `Expires` nor `Cache-Control` header. The value range is 0 to 1440, where 0 means files are always re-validated. The default value is 5. This setting is ignored if **Streamed Mode** is selected. Changes to this field take effect immediately.
Preroll Buffer (s)	The duration in seconds of clip play time that must be buffered before the clip starts to play. The value range is 1 to 1800. The default is 30. This setting is ignored if **Streamed Mode** is selected. ***NOTE:*** When the preroll buffer has been set to a value longer than the allowed response time for SIP INVITE, then the Containerized Decomposed Media Server may not respond to the INVITE in a sufficiently timely manner when large files are being cached. In this case, the caller could time out on the INVITE, possibly resulting in a canceled call. Changes to this field take effect immediately.
Preroll Timeout (s)	The maximum time in seconds to allow for the preroll buffer to be filled. The value range is 1 to 60. The default value is 5. This setting is only valid in **Cached Mode** of operation and is ignored if **Streamed Mode** is selected. Changes to this field take effect immediately.
Underrun Timeout (s)	The maximum time in seconds to allow where no media is available to stream, once streaming has begun. The value range is 0 to 60. The default value is 1. This setting is ignored if **Streamed Mode** is selected. Changes to this field take effect immediately.
Http Media Timeout (ms)	Allows to configure the HTTP response timeout from the HTTP server for announcement and recording service, in milliseconds. The supported value range is 900 to 5000. The default value is 900. ***NOTE:*** While connecting to the HTTP server, the Containerized Decomposed Media Server tries the HTTP connection twice. For example, if this field is configured to 5000 ms, the timeout is 10000 ms (2 x 5000 ms). This setting is only valid in the **Streamed Mode**. Changes to this field take effect immediately.

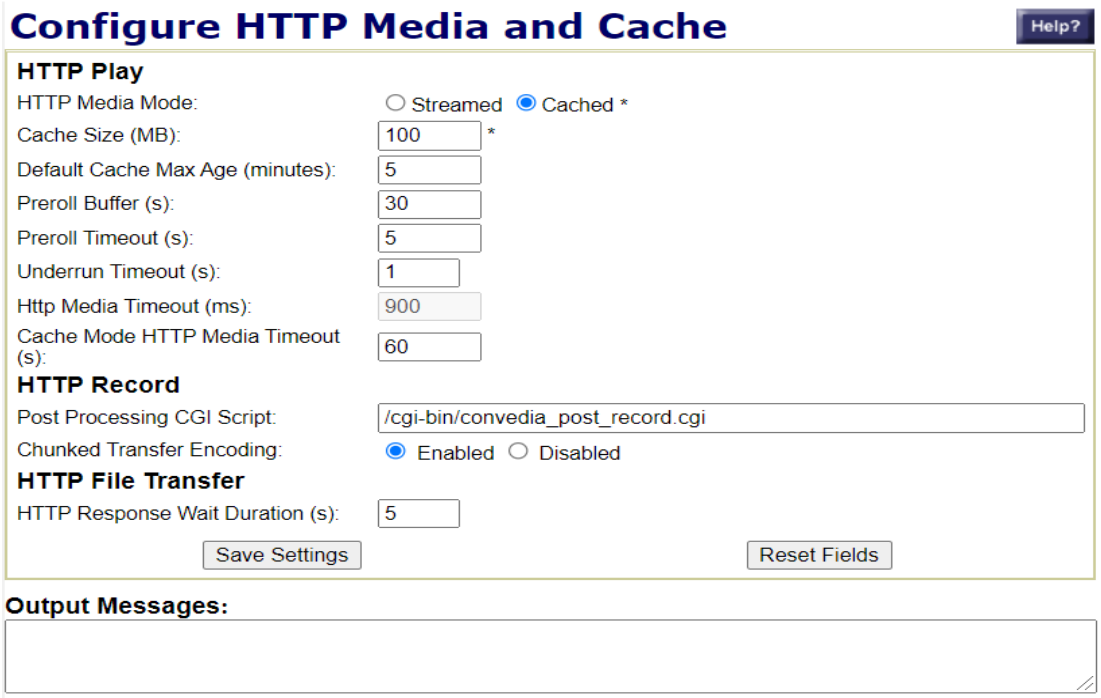
Table 53. HTTP Mode and Caching Information

Value	Description
Cache Mode HTTP Media Timeout (s)	Allows to configure the HTTP media timeout for the cached mode announcement, in seconds. The supported value range is 5 to 60. The default value is 60. This setting is only valid in **Cached Mode** of operation and is ignored if **Streamed Mode** is selected. Changes to this field take effect on the next HTTP/HTTPS announcement request.
HTTP Record	
Post Processing CGI Script	The path to a post processing CGI script. Format is a 255-character string of the <path>/<query> components of a generic URI as defined in RFC 2396. The default is **/cgi-bin/convedia_post_record.cgi**. If no path is specified, the Containerized Decomposed Media Server does not invoke a CGI script. Changes to this field take effect immediately.
Chunked Transfer Encoding	Enables or disables chunked transfer encoding for HTTP recordings. • **Enabled.** The Containerized Decomposed Media Server creates HTTP recordings using chunked transfer encoding. • **Disabled.** The Containerized Decomposed Media Server creates HTTP recordings by specifying the maximum available file size in the PUT. The default setting is Enabled. Changes to this field take effect immediately.
HTTP File Transfer	
HTTP Response Wait Duration (s)	Specifies the duration for final response (in seconds) from the HTTP server, after sending out the file data. The value range is 1 to 60. The default value is 5. Changes to this field take effect from the next HTTP file transfer request.

To configure HTTP Media and Cache information:

1. Click **Configuration** > **Node Configuration** > **Configure HTTP Media and Cache**.

   The Configure HTTP Media and Cache page displays.



2. Enter the HTTP media and cache information described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Resource Management

The Configure Resource Management page enables you to configure the settings for the Containerized Decomposed Media Server overload protection features.

The Containerized Decomposed Media Server protects itself against overload conditions due to its running out of memory. The Containerized Decomposed Media Server can prevent service degradation, memory exhaustion, processing resources, and instance resets without exceeding overload thresholds. To protect from the overload conditions, the Containerized Decomposed Media Server monitors its CPU and memory usage, and compares these with threshold levels.

When **Overload Detection Method** is set to **Basic**, the Containerized Decomposed Media Server supports the following threshold levels.

- **Service overload level**. The Containerized Decomposed Media Server has a hard (that is, non-configurable) threshold on CPU and memory usage. When the system is functioning at this level, the Containerized Decomposed Media Server rejects all requests for new calls and all new service requests for existing calls. However, the Containerized Decomposed Media Server accept call delete requests.

- **Call overload level**. This level is configurable. When this threshold is exceeded, the Containerized Decomposed Media Server begins rejecting a new calls. However, SIP timers continues to process normally and control agent retry continues to be accepted.

You can also set a threshold for high disk partition usage, and set the duration of time you will allow the Containerized Decomposed Media Server to persist in a service overload condition before restarting.

When **Overload Detection Method** is set to **Enhanced**, the Containerized Decomposed Media Server supports the following threshold levels for call shedding.

- **Service overload level**. The Containerized Decomposed Media Server has a hard (that is, non-configurable) threshold on CPU and memory usage. When the system is functioning at this level, the Containerized Decomposed Media Server rejects all requests for new calls and all new service requests for existing calls. However, the Containerized Decomposed Media Server accept call delete requests.
- **Minor.** Indicates the minor threshold level for the monitored system resources. A minor *alarm 189 Exceeded minor threshold level for X* is raised when any of the monitored system resources exceed the configured minor threshold level. The minor alarm 189 is cleared when all the monitored system resources are below the configured minor threshold level.

  The Containerized Decomposed Media Server declines a configured percentage of the regular calls. These calls are independent of the features (for example, IVR, transcoding, legal intercept, conferencing) or resources (for example, audio only, audio and video, MSRP, text) requested. However, the new priority calls are still accepted.
- **Major.** Indicates the major threshold level for the monitored system resources. A major alarm *188 Exceeded major threshold level for X* is raised when any of the monitored system resources exceed the configured major threshold level. The major alarm 188 is cleared when all the monitored system resources are below the configured major threshold level.

  The Containerized Decomposed Media Server declines all the regular calls and accepts only the audio priority calls. In `sip:tc` service context, calls with audio and text ports are accepted. Fax calls are rejected.
- **Critical.** Indicates the critical threshold level for the monitored system resources. A critical *alarm 187 Exceeded minor threshold level for X* is raised when any of the monitored system resources exceed the configured critical threshold level. The critical alarm 187 is cleared when all the monitored system resources are below the configured critical threshold level.

  The MRFP is de-registered and tagged as out of service until the critical threshold level alarm is cleared. The MRFP does not accept any further calls.

You can view the resource management configurations on the *Show Resource Management Configuration*.

The following table shows the information you can configure for resource management.

Table 54. Resource Management Configuration Information

Value	Description
Overload Detection Method	Allows to configure the overload detection method. The supported values are: • **Basic.** Configures the **Basic** overload detection method and allows you to configure the threshold. • **Enhanced.** Configures the **Enhanced** overload detection method and allows you configure the threshold for each of the resource counters. The default value is Basic. Changes to this field require a MRFP restart to take effect.
When the Overload Detection Method is set as Basic	
Call overload CPU threshold (%)	The call overload threshold for processing resources, in percentage. If CPU usage exceeds this threshold, the instance is in a call overload state. The value range is from 80 to 100. The default value is 90. This value must be set lower than the service overload threshold (100%). The changes to this field take effect immediately.
Call overload memory threshold (%)	The call overload threshold for memory, in percentage. If memory usage exceeds this threshold, the Containerized Decomposed Media Server will be in a call overload state. The value range is from 90 to 95. The default value is 94. This value must be set lower than the service overload threshold (by default 95%). Changes to this field take place immediately.
Overload reboot duration (Min)	The length of time you will permit the Containerized Decomposed Media Server to remain in an overload state before automatically rebooting, in minutes. The value range is 0 or from 20 to 60, where 0 means the Containerized Decomposed Media Server never restarts because of overload. The default value is 20. Changes to this field take effect immediately.
Maximum Audio Load Configuration (%)	The user can configure the maximum audio load, in percentage, which can run on the Containerized Decomposed Media Server. The value range is from 10 to 90. The default value is 90. Changes to this field take effect immediately. In a virtualized hyperthreaded setup, ensure that this value is set in the range from 80 to 90 for optimum performance of the virtual machines.
Maximum Video Load Configuration (%)	The user can configure the maximum video load, in percentage, which can run on the Containerized Decomposed Media Server. The value range is from 10 to 90. The default value is 90. Changes to this field take effect immediately. In a virtualized hyperthreaded setup, ensure that this value is set in the range from 50 to 55 for optimum performance of the virtual machines. This does not impact the Enhanced Multi-media Priority Service (EMPS) feature.
When the Overload Detection Method is set as Enhanced	

Table 54. Resource Management Configuration Information

Value	Description
Call overload CPU threshold (%)	The threshold for call overload CPU usage, in percentage. If the control processor CPU usage exceeds or equal to the following threshold values, the Containerized Decomposed Media Server is in a call overload state and raises an alarm accordingly. • **Critical.** The value range is from 0 to 100 and the default value is 90. • **Major.** The value range is from 0 to 100 and the default value is 80. • **Minor.** The value range is from 0 to 100 and the default value is 70. The changes to this field take effect immediately.
Call overload memory threshold (%)	The threshold for call overload system memory usage, in percentage. If the system memory usage exceeds the following threshold values, the Containerized Decomposed Media Server is in a call overload state and raises an alarm accordingly. • **Critical.** The value range is from 0 to 95 and the default value is 94. • **Major.** The value range is from 0 to 95 and the default value is 80. • **Minor.** The value range is from 0 to 95 and the default value is 70. • Changes to this field take place immediately.
Modeled Audio DSP Usage threshold (%)	The threshold for modeled audio DSP usage, in percentage. If the modeled audio DSP usage exceeds the following threshold values, the Containerized Decomposed Media Server raises an alarm accordingly. • **Critical.** The value range is from 0 to 100 and the default value is 100. • **Major.** The value range is from 0 to 100 and the default value is 90. • **Minor.** The value range is from 0 to 100 and the default value is 80. Changes to this field take effect immediately.
Actual Audio DSP Usage threshold (%)	The threshold for actual audio DSP usage, in percentage. If the actual audio DSP usage exceeds the following threshold values, the Containerized Decomposed Media Server raises an alarm accordingly. • **Critical.** The value range is from 0 to 100 and the default value is 100. • **Major.** The value range is from 0 to 100 and the default value is 90. • **Minor.** The value range is from 0 to 100 and the default value is 80. Changes to this field take effect immediately.
Bandwidth Usage threshold (%)	The threshold for bandwidth usage on the media interface, in percentage. If the bandwidth usage exceeds the following threshold values, the Containerized Decomposed Media Server raises an alarm accordingly. • **Critical.** The value range is from 0 to 100 and the default value is 95. • **Major.** The value range is from 0 to 100 and the default value is 80. • **Minor.** The value range is from 0 to 100 and the default value is 70. Changes to this field take effect immediately.

Table 54. Resource Management Configuration Information

Value	Description
Packet loss rate threshold (%)	The threshold for packet loss rate on the media interface, in percentage. If the packet loss rate exceeds the following threshold values, the Containerized Decomposed Media Server raises an alarm accordingly. • **Critical.** The value range is from 0 to 15 and the default value is 15. • **Major.** The value range is from 0 to 15 and the default value is 10. • **Minor.** The value range is from 0 to 15 and the default value is 5. Changes to this field take effect immediately.
Overload reboot duration (Min)	The length of time is permitted for the Containerized Decomposed Media Server to remain in service overload state before automatic reboot, in minutes. The value range is 0 or 20-60, where 0 means the Containerized Decomposed Media Server will never restart because of overload. The default value is 20. Changes to this field take effect immediately.
Minor Overload Call Rejection (%)	The percentage of regular calls that the Containerized Decomposed Media Server will reject when it is operating in minor overload state. The value range is from 1 to 100. The default value is 25. Changes to this field require a MRFP restart to take effect.
Maximum Audio Load Configuration (%)	The user can configure the maximum audio load, in percentage, which can run on the Containerized Decomposed Media Server. The value range is from 10 to 90. The default value is 90. Changes to this field take effect immediately. In virtualized hyperthreaded setup, ensure that this value is set in the range from 80 to 90 for optimum performance of the virtual machines.
Maximum Video Load Configuration (%)	The user can configure the maximum video load, in percentage, which can run on the Containerized Decomposed Media Server. The value range is from 10 to 90. The default value is 90. Changes to this field take effect immediately. In virtualized hyperthreaded setup, ensure that this value is set in the range from 50 to 55 for optimum performance of the virtual machines. This does not impact the Enhanced Multi-media Priority Service (EMPS) feature.

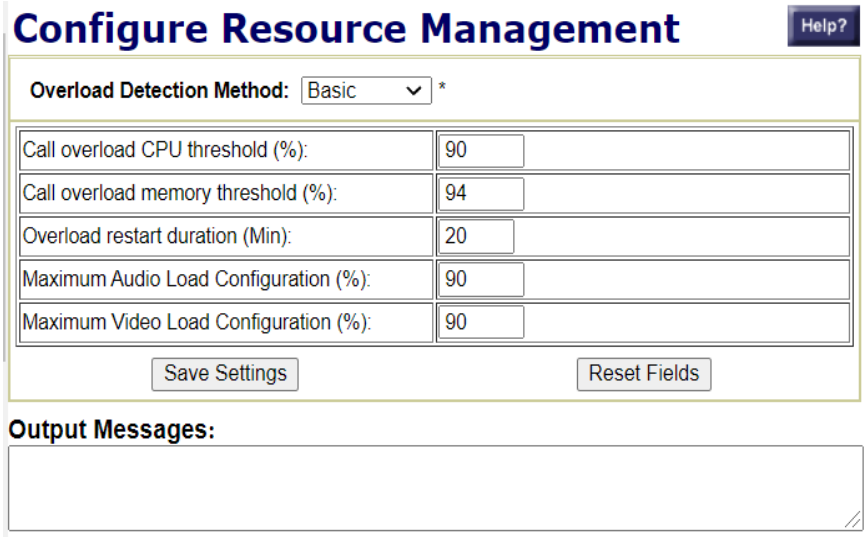
NOTE:

- The Containerized Decomposed Media Server does not monitor the resource usage if all the critical, major, and minor threshold values for that resource is set to 0.
- Ensure that the critical value is greater than or equal to the major value.
- Ensure that the major value is greater than or equal to the minor value.

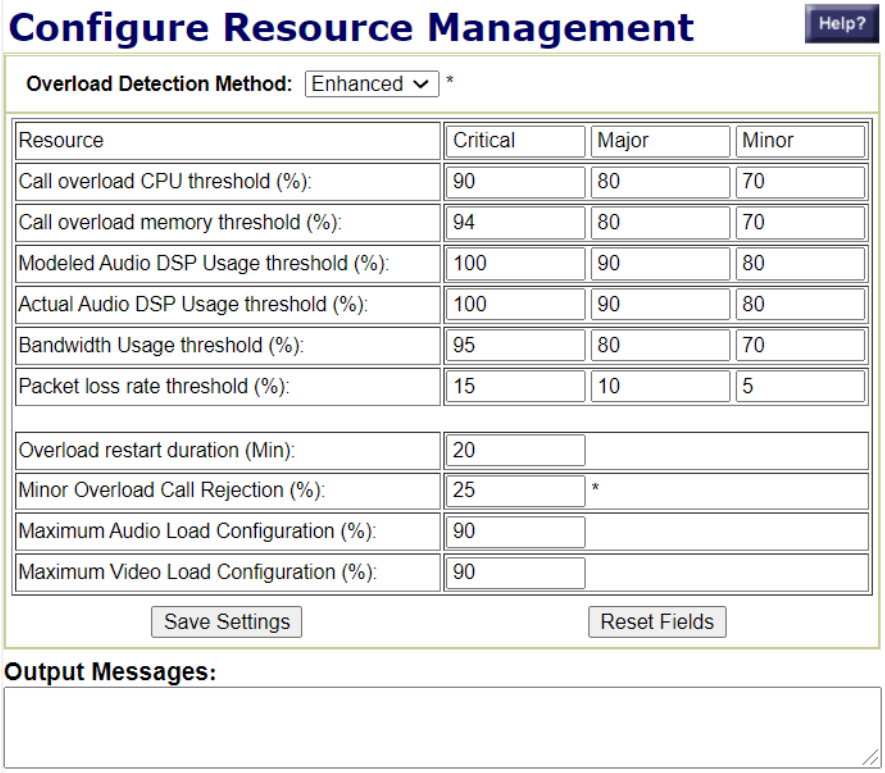
To configure resource management information:

1. Click **Configuration** > **Node Configuration** > **Configure Resource Management**.

   When the **Overload Detection Method** is set as **Basic**, the *Configure Resource Management* page displays as follows.



   When the **Overload Detection Method** is set as **Enhanced**, the *Configure Resource Management* page displays as follows.



2. Enter the resource management information based on above table:
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to previously saved values.

Configure VoiceXML Parameters

The Configure VoiceXML Parameters page enables you to specify the characteristics for SIP/VoiceXML dialogs.

The following table shows the information you can configure for the VoiceXML protocol.

Table 55. VoiceXML Parameters

Value	Description
HTTP cookies	Optional. Enables or disables the use of VoiceXML cookies. The supported values are: • **Enabled.** VoiceXML cookies is used. • **Disabled.** VoiceXML cookies is not used. The default value is Enabled. Changes to this field take effect immediately.
DOM Cache	Optional. Enables or disables caching for the Document Object Model (DOM). The supported values are: • **Enabled.** The DOM cache is enabled. • **Disabled.** The DOM cache is not enabled. The default value is Disabled. For more information, refer to the *VXML Interface Reference*. Changes to this field take effect immediately.
Maximum Document Fetches	Optional. Specifies the maximum number of VoiceXML documents that can be fetched in a single VoiceXML session. The supported value range is from 50 to 2000. The default value is 100. The VXML document fetches for submit, subdialog, goto, link, and the initial application document. Root documents and external SRGS grammars are not counted for this counter. For more information, refer to the *VXML Interface Reference*. Changes to this field take effect immediately.
Beep Clip	Optional. Specifies which provisioned audio clip is to be played when a beep tone is required. The default is empty string and in this case no beep is played. The changes to this field take effect immediately.
Error Clip	Optional. Specifies which provisioned audio clip is to be played when an error tone is required. The default is empty string and in this case no error is played. The changes to this field take effect immediately.

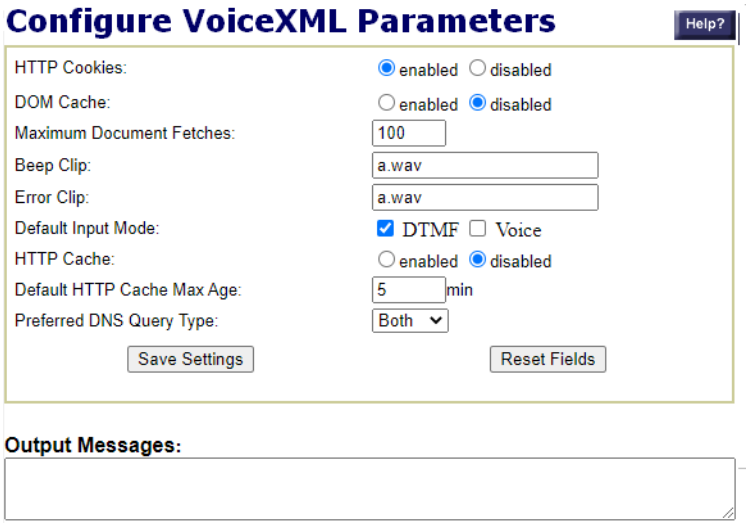
Table 55. VoiceXML Parameters

Value	Description
Default Input Mode	Mandatory. The default input mode for a connection if the input mode is not explicitly specified. The supported values are: • **DTMF.** The default input mode is DTMF. • **Voice.** The default input mode is voice. The default is DTMF. Changes to this field take effect immediately.
HTTP Cache	Enables or disables caching of the VXML documents fetch from the HTTP server. The supported values are: • **enabled.** Enables caching of the VXML documents fetch from the HTTP server. • **disabled.** Disables caching of the VXML documents fetch from the HTTP server. The default value is disabled. Changes to this field take effect immediately.
Default HTTP Cache Max Age	Allows to configure the default HTTP cache maximum age, in minutes, for the VXML documents. The supported values are 0 and from 5 to 1440. The default value is 5. The value 0 means default caching is disabled. The default caching is used when the expiry cannot be determined based on cache entry validators or cache-control directives. Changes to this field take effect from the next cache write.
Preferred DNS Query Type	Allows to configure the preferred query type for Containerized Decomposed Media Server to perform the Fully Qualified Domain Name (FQDN) resolution for VXML fetches. The supported values are: • **Both.** The Containerized Decomposed Media Server performs both **A** and **AAAA** queries while resolving the HTTP URL for the VXML fetches. • **A.** The Containerized Decomposed Media Server performs only **A** query while resolving the HTTP URL for the VXML fetches. **A** query is used to obtain the IPv4 address. • **AAAA.** The Containerized Decomposed Media Server performs only **AAAA** query while resolving the HTTP URL for the VXML fetches. **AAAA** query is used to obtain the IPv6 address. The default value is Both. Changes to this field take effect from the next HTTP FQDN resolution in VXML.

To configure VoiceXML parameters:

1. Click **Configuration** > **Node Configuration** > **Configure VoiceXML Parameters**.

   The Configure VoiceXML Parameters page displays.



2. Enter the VoiceXML parameter information as described in the above table.
3. Click **Save Settings**.

   Changes take effect immediately. Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Conference

The Configure Conference page enables you to specify the sample rates for conferences, either narrowband (8 kHz), wideband (16 kHz), super wideband (32 kHz), or auto, and enable the large-conferencing feature.

You can view the information set on this page on the *Show Conference Configuration*.

Large Conferences

In a standard conference, the number of send-receive participants is limited to 125. When the large conference feature is enabled, the Containerized Decomposed Media Server automatically internally cascades conferences when the number of send-receive listeners exceeds 125, so that the maximum number of send-receive and listen-only participants is limited only by the overall Containerized Decomposed Media Server capacity. No intervention on the part of the control agent is required.

The large conference feature is disabled by default, and can be enabled using the Containerized Decomposed Media Servers management interface. When enabled, no explicit control is required to use it.

Internal cascading can introduce delays and latency. In general, though, enabling large conferencing should not affect conference announcements and recordings, wide-band conferences, personalized-mix conferences, or the audio mix in VAS conferences.

NOTE: Large conferences cannot be cascaded using the Containerized Decomposed Media Servers cascaded conferencing feature.

N-Loudest behavior is slightly different for large conferences. As a result of internal cascading, participants may hear up to N * x participants, where N is the configured number of N-loudest speakers, and x is the number of internally cascaded conferences. It may also be that the N * x heard speakers are not the absolute loudest speakers in the conference.

NOTE: The large conference feature cannot be used with DTMF pass-through. When enabling large conferencing for SIP Netann and MSML conferences, ensure that DTMF pass-through is disabled.

ASN behavior also changes slightly for large conferences. The Containerized Decomposed Media Server combines the active speaker list from each cascaded conference and sends an aggregate ordered ASN report to the control agent. The active speakers in the report are ordered by input position for the aggregate large conference. This means that for a given configured value of N, the number of active speakers reported will be greater than N.

Full-mix notification is not supported on large conferences.

The following table shows conferencing information that you can configure.

Table 56. Conferencing Configuration Information

Value	Description
Default Sample Rate	The conference rate, in Hz, to be used for conferences by default. The supported values are: • **8000 Hz.** Narrowband conferencing. • **16000 Hz.** Wideband conferencing. • **32000 Hz.** Super Wideband conferencing. • **Auto.** Automatically sets the audio mixer sample rate. The default is 8000 Hz. Changes made to this parameter take effect immediately.
Large Conference	Enables or disables large conferencing, which uses internal cascading by the Containerized Decomposed Media Server. The application can cascade conferences to allow more than 125 users by external cascading. The supported values are: • **Enabled**. Enables large conferencing. • **Disabled.** Disables large conferencing. The default value is Disabled. Changes to this parameter take effect immediately, applying to all new conferences.

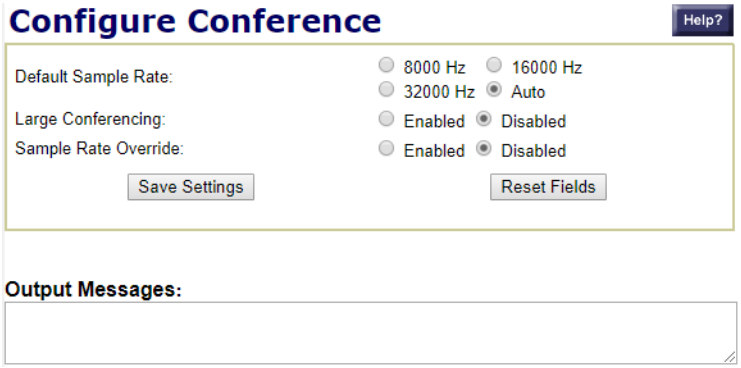
Table 56. Conferencing Configuration Information

Value	Description
Sample Rate Override	Enables or disables the override of the sample rate. The supported values are: • **Enabled.** Enables the sample rate override feature. The Containerized Decomposed Media Server overrides the sample rate specified in the SIP request URI of netann (including MSCML) and MSML audio conferences with the configured **Default Sample Rate** value. • **Disabled.** Disables the sample rate override feature. The default value is Disabled. This parameter does not require a restart, takes effect on a new conference mixer creation, and does not impact on-going conferences.

To configure conference parameters:

1. Click **Configuration** > **Node Configuration** > **Configure Conference**.

   The Configure Conference page displays.



2. Specify the conference sample rate.
3. Enable or disable the large conferencing.
4. Enable or disable the sample rate override.
5. Click **Save Settings** to commit the information.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
6. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Fax

The Configure Fax page enables you to specify parameters for the Containerized Decomposed Media Servers fax service.

Information set on this page can be viewed on the Show Node Configuration page.

The following table shows the fax parameters you can configure.

Table 57. Fax Parameters

Parameter	Description
Number of T.38 Error Recovery Frames—Signal Packets	The number of Forward Error Correction packets the Containerized Decomposed Media Server sends with control packets. Supported values are integers in the range of 0 to 3. The default is 3. Changes made to this parameter take effect immediately.
Number of T.38 Error Recovery Frames—Data Packets	The number of Forward Error Correction packets the Containerized Decomposed Media Server sends with data packets. Supported values are integers in the range of 0 to 3. The default is 1. Changes made to this parameter take effect immediately.
Fax Auto Switch	Enables or disables the fax auto switch capability. The supported values are: • **Enabled.** Enables the fax auto switch capability. When enabled, the Containerized Decomposed Media Server supports switching audio or audio-video to fax after receiving a fax operation request, and converts fax to audio or audio-video after receiving re-INVITE without an SDP offer. • **Disabled.** Disables the fax auto switch capability. The default value is Disabled. ***NOTE:*** The **Full Capabilities in Mid Call offer** must be enabled for the Containerized Decomposed Media Server to convert fax to audio or audio-video after receiving re-INVITE without an SDP offer. The changes to this field take effect on the next MSML call, without reboot.
Fax Capabilities in Mid Call Offer	Enables or disables the fax mid-call offer capability. The supported values are: • **Enabled.** Enables the fax mid-call offer capability. When enabled, the Containerized Decomposed Media Server includes fax codec list (G.711 a/u-law and T.38) in addition to audio, video, or audio-video capabilities. • **Disabled.** The Containerized Decomposed Media Server does not include fax codec in a mid-call offer. The default value is Disabled. ***NOTE:*** This feature is enabled only if both **Full Capabilities in Mid Call offer** and **FAX Auto Switch** are enabled. The changes to this field take effect on the next MSML call, without reboot.

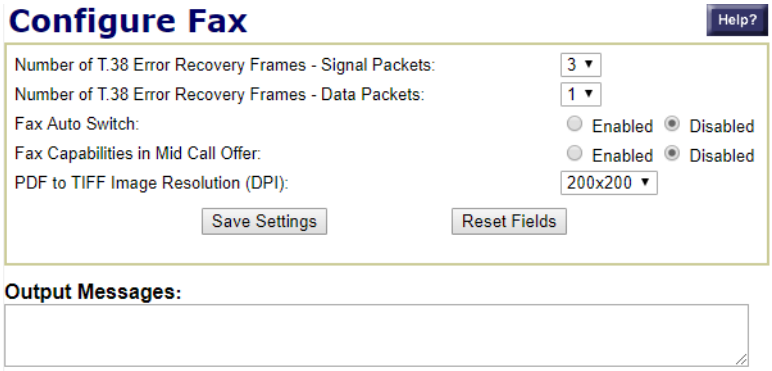
Table 57. Fax Parameters

Parameter	Description
PDF to TIFF Image Resolution (DPI)	Sets the default resolution of TIFF images generated from the PDF files, in DPI (dots per inch). The supported values are: • 204x98 • 204x196 • 204x391 • 200x200 • 300x300 • 400x400 • 408x391 The default value is 200x200. The changes to this field take effect on the next PDF to TIFF conversion, without reboot.

To configure the fax settings:

1. Click **Configuration** > **Node Configuration** > **Configure Fax**.

   The Configure Fax page displays.



2. Set the fax information described in the table above.
3. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Fax Codec List

The Configure Fax Codec List page enables you to assign fax codecs the Containerized Decomposed Media Server uses in negotiating fax service.

The fax codec list allows the Containerized Decomposed Media Server to list supported fax codecs in order of preference for codec negotiation. The most-preferred codecs are entered at the top of the list, and the least-preferred at the bottom.

When the Containerized Decomposed Media Server generates an offer, it offers all codecs listed on its preferred codec list, provided the Containerized Decomposed Media Server has sufficient resources to support the codec. This list signals the Containerized Decomposed Media Servers order of preference for a given set of fax codecs.

This list contains all the fax formats supported by the Containerized Decomposed Media Server.

You can view the information set on this page on the *Show Fax Codec List*.

The following table shows the default ordering of fax formats in the fax codec list.

Table 58. Default Ordering of the Fax Codec List

Name	Description	Order
T.38	T.38 fax	1
PCMU	G.711 μ-law	2
PCMA	G.711 a-law	3

To configure the fax codec list:

1. Click **Configuration** > **Node Configuration** > **Configure Fax Codec List**.

   The Configure Fax Codecs List page displays.

2. Assign fax codecs in order of preference. The first selection of none ends the list, and codecs specified after **none** are ignored.
3. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Call Progress Analysis

The Configure Call Progress Analysis (CPA) page enables you to edit user-defined templates of thresholds and parameters for how and when the Containerized Decomposed Media Server generates call progress events. The events are then forwarded to the control agent in SIP INFO messages.

The Containerized Decomposed Media Server maintains a static set or “template” of CPA attributes. You can view this template using the Containerized Decomposed Media Server’s management interface.

You can create and save up to two user-defined templates of CPA attributes. Creating templates allows the control agent to configure and select a set of CPA attribute values to use when enabling CPA on a per-call basis.

When you configure CPA attributes through the management interface, you are configuring attributes of the user-defined CPA templates. The template of default values is template “0”; the two user-defined templates are template 1 and template 2. Changes to template configuration take effect without a reboot.

You can view the information set on this page on the *Show Call Progress Analysis Configuration on page 187*.

The following table shows call progress analysis values that can be configured for each user-defined template (***NOTE:*** The default template, template 0 is non-configurable).

Table 59. Configurable Call Progress Analysis Information

Value	Description
Silence Level (dBm0)	Optional. The average energy value, in dBm0, below which the signal is considered to be silence (that is, noise). The supported value range is from –43 to –31. The default value is –39. Changes to this field take effect immediately.
Silence Time (ms)	Optional. The minimum time, in milliseconds, since voice has been detected to qualify for voice is OFF, or loss of energy. The supported value range is from 10 to 65535. The default value is 25. Silence Time must be less than Silence Short. Changes to this field take effect immediately.

Table 59. Configurable Call Progress Analysis Information

Value	Description
Silence Short (ms)	Optional. The minimum time, in milliseconds, that voice must be OFF before the Containerized Decomposed Media Server sends a CP_VOICE_END_SHORT event. The supported value range is from 10 to 2097151. The default value is 1000. Silence Short must be greater than Silence Time, and must be less than Silence Long. Changes to this field take effect immediately.
Silence Long (ms)	Optional. The minimum time, in milliseconds, that voice must be OFF before the Containerized Decomposed Media Server sends a CP_VOICE_END event. The supported value range is from 10 to 2097151. The default value is 1500. Silence Long must be greater than Silence Short. Changes to this field take effect immediately.
Voice On Time (ms)	Optional. The minimum time, in milliseconds, that voice must be detected before call progress reports the voice begin event CP_VOICE. The supported value range is from 10 to 65535. The default value is 50. Changes to this field take effect immediately.
Max Ringback Duration (ms)	Optional. The maximum duration, in milliseconds, of a ringback tone required to distinguish it from dial tone. Most ringback tones are between 1 to 2 seconds in duration. The larger the value, the longer it takes to qualify a tone as a dial tone. The supported value range is from 10 to 2097151. The default value is 3000. Max Ringback Duration must be greater than Slow Busy Max Period. Changes to this field take effect immediately.
No Answer Ringback Tone Count	Optional. The number of ringback tones required to trigger a CP_NOANSWER event. The supported value range is from 1 to 2147483647. The default value is 5. Changes to this field take effect immediately.
Ringback Stop Period (ms)	Optional. The time, in milliseconds, since the last ringback tone required to consider the ringback has stopped, meaning that the called terminal is off the hook without voice, CED tone, or Special Information Tone. The supported value range is from 0 to 2097151. The default value is 5000. Changes to this field take effect immediately.
Slow Busy Max Period (ms)	Optional. The maximum period (on time plus off time), in milliseconds, required to distinguish between a slow busy tone and a ringback tone. Busy signals typically have a period of one second and a 50% duty cycle. The supported value range is from 0 to 2097151. The default value is 1500. Slow Busy Max Period must be less than Max Ringback Duration, and must be greater than Fast Busy Max Period. Changes to this field take effect immediately.
Fast Busy Max Period (ms)	Optional. The maximum period (on time plus off time), in milliseconds, required to distinguish between a slow busy tone and a ringback tone. The supported value range is from 0 to 2097151. The default value is 700. Fast Busy Max Period must be less than Slow Busy Max Period. Changes to this field take effect immediately.
Busy Tone Count	Optional. The number of busy tones or reorder (fast busy) pattern to trigger a CP_BUSY or CP_RO event respectively. The supported value range is from 1 to 2147483647. The default value is 4. Changes to this field take effect immediately.

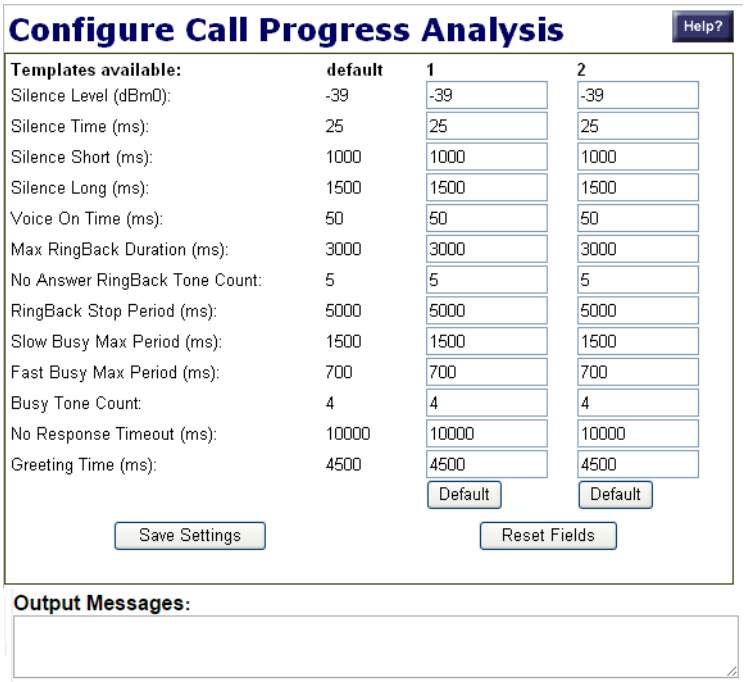
Table 59. Configurable Call Progress Analysis Information

Value	Description
No Response Timeout (ms)	Optional. The maximum time, in milliseconds, that can elapse with no response from the network before reporting a CPA_TIMEOUT event. The supported value range is from 0 to 2097151. The default value is 10000. No Response Timeout must be greater than all of Silence Time, Silence Short, Silence Long, Voice On Time, and Greeting Time. Changes to this field take effect immediately.
Greeting Time (ms)	Optional. The minimum time, in milliseconds, of voice that must occur to generate a CP_GREETING event. The supported value range is 0 to 2097151. The default value is 4500. Changes to this field take effect immediately.

To configure a CPA template:

1. Click **Configuration** > **Node Configuration** > **Configure Call Progress Analysis**.

   The Configure Call Progress Analysis page displays.



2. Configure the settings for one or both of the user-defined templates as described in the above table.
3. Optionally click one of the **Default** buttons to copy the settings of the default template into the user-defined template above that Default button.
4. Click **Save Settings**.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
5. Optionally click **Reset Fields** to reset the changes made to previous values.

Configure Clip Path Translation

The Configure Clip Path Translation page enables you to translate control agent clip paths into a format supported by the Containerized Decomposed Media Server.

Clip path translation allows you to reconcile differences between the file path formats supported by a control agent and the file path formats supported by the Containerized Decomposed Media Server. In a clip translation, the Containerized Decomposed Media Server maps the path format preferred for the control agent (the **original** path) onto the path format supported by the Containerized Decomposed Media Server (the **translated** path).

SIP supports clip path translation for MSML announcements.

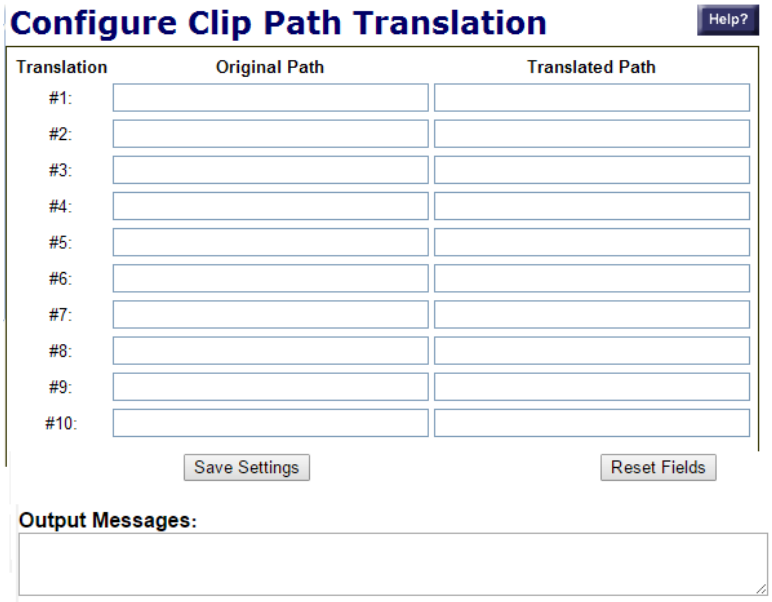
Up to 10 clip translations are supported.

You can view the information set on this page on the *Show Clip Path Translation*.

To configure clip path translation settings:

1. Click **Configuration** > **Node Configuration** > **Configure Clip Path Translation**.

   The Configure Clip Path Translation page displays.



2. For each clip path translation, specify the string representing the original path and the string representing the translated path.
3. Click **Save Settings** to apply the settings.

   Changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

Configure Text

On the Configure Text page, you can configure the embedded text parameters.

The following table shows text attribute that can be configured.

Table 60. Configure Text Information

Value	Description
T.140 Buffer Interval(ms)	Indicates T.140 Packet Transmission Interval in milliseconds. The supported value range is 100 to 500. The default is 300. Changes to this field takes effect immediately.
T.140 Conference Aware Support	Enables or disables the Conference Aware Support. The supported values are: • **Enabled.** Enables the Conference Aware Support. • **Disabled.** Disables the Conference Aware Support. The default value is Disabled. Changes to this field takes effect immediately.

To configure Text settings:

1. Click **Configuration** > **Node Configuration** > **Configure Text**.

2. Specify the **T.140 Buffer Interval** period.
3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to previously saved values.

Configure Text Codec List

The Configure Text Codec List page allows you to specify the list of supported text codecs in order of preference for codec negotiation with most preferred at the top.

To configure Text Codec List:

1. Click **Configuration** > **Node Configuration** > **Configure Text Codec List**.

1. Select the attribute for **codec #1** as **t140**.
2. Click **Save Settings**.

   The text codec list information is displayed in the **Output Messages:** box.

   The changes take effect immediately.
3. Click **Reset Fields** to reset the changes made to previously saved values.

Configure Resource Server Redundancy

The Configure Resource Server (RS) Redundancy page enables you to configure the following settings related to the RS Redundancy:

- Common RS health parameters and RS Load Balancing (Instance specific)
- RS specific parameters

The input frame of the page has the following sections:

- The first section allows the general parameters to be configured for the RS.
- The second section allows the Resource Server to be added, modified or removed. This section has input elements for RS specific parameters.

NOTE: The input elements are preloaded with current values for the specified instance. If you select another RS, all the element values are preloaded with the current values for the selected **RS**. The Containerized Decomposed Media Server supports up to five resource servers.

The following table shows the RS redundancy information that you can configure.

Table 61. Configurable Resource Server Redundancy information

Option	Description
RS Health Check Interval T1	The health check interval, in milliseconds, to poll an alive instance. The supported value range is 100 to 10000. The default value is 300. Changes to this field take effect immediately.
RS Health Check Interval T2	The health check interval, in milliseconds, to poll a failed instance.The supported value range is 100 to 10000. The default value is 1000. Changes to this field take effect immediately.
RS Health Check Retries	The number of health check retries. The supported value range is 1 to 10. The default value is 2. An RS instance becomes dead to alive or alive to dead based on the health check result (success or failure) consecutively for the configured number of retries. ***NOTE:*** The switching from T1 to T2 or T2 to T1 happens when the RS instance is changed from alive to dead or dead to alive. Changes to this field take effect immediately.
RS Load Balancing	Enables or disables resource server redundancy feature in load balancing mode. The supported values are: • **Enabled.** The Containerized Decomposed Media Server distributes the HTTP fetch requests using a round-robin method for clips (announcement and file transfer) and VXML document among the active servers. • **Disabled.** The Containerized Decomposed Media Server performs the RS Redundancy feature to play the HTTP clips (announcement and file transfer) and fetches the VXML document. The default value is Disabled. Changes to this field take effect from the next HTTP FQDN resolution.
Resource Server	The ID of the resource server. The supported value range is 1 to 5. The default value is 1.
RS FQDN	The Fully Qualified Domain Name (FQDN) (domain name and host) of the resource server. The maximum length is 256 characters. The default value is an empty string. The RS is removed if **RS FQDN** is blank. Changes to this field take effect immediately.
RS Primary Address	The IP address of the primary instance of the resource server. The supported values are strings of 64 characters. The default value is an empty string. The supported address notation can be IPv4 or IPv6. The RS Primary instance is removed if **RS Primary Address** is blank. Changes to this field take effect immediately.
RS Secondary Address	The IP address of the secondary instance of the resource server. The supported values are strings of 64 characters. The default value is an empty string. The supported address notation can be IPv4 or IPv6. The RS Secondary instance is removed if **RS Secondary Address** is blank. Changes to this field take effect immediately.

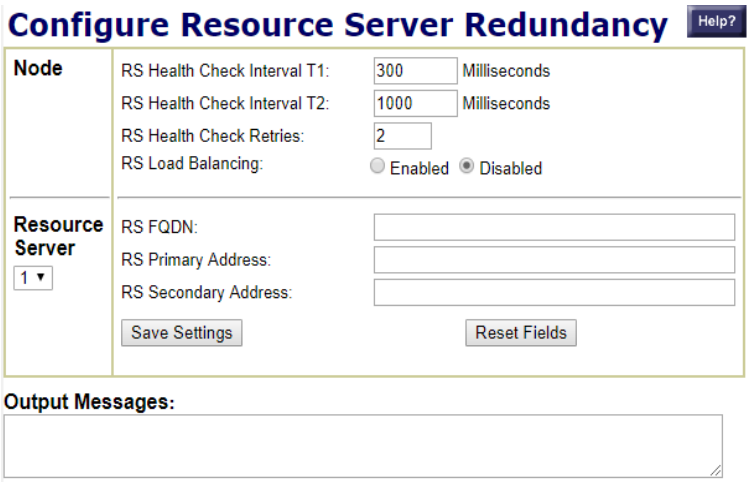
Table 61. Configurable Resource Server Redundancy information

Option	Description
RS Third Address	The IP address of the third instance of the resource server. The supported values are strings of 64 characters. The default value is an empty string. The supported address notation can be IPv4 or IPv6. The RS third instance is removed if **RS Third Address** is blank. ***NOTE:*** This field is available when the **RS Load Balancing** is enabled. Changes to this field take effect immediately.
RS Fourth Address	The IP address of the fourth instance of the resource server. The supported values are strings of 64 characters. The default value is an empty string. The supported address notation can be IPv4 or IPv6. The RS fourth instance is removed if **RS Fourth Address** is blank. ***NOTE:*** This field is available when the **RS Load Balancing** is enabled. Changes to this field take effect immediately.

To configure the RS Redundancy:

1. Click **Configuration** > **Node Configuration** > **Configure Resource Server Redundancy**.

   The Configure Resource Server Redundancy page displays.



2. Modify the RS health parameters for the selected **Resource Server** (Optional).
3. Enter the input elements for the resource server specific parameters.
4. Click **Save Settings**.

   The changes in the configuration data take effect immediately. Confirmation message is displayed in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Per Port Statistics

The Configure Per Port Statistics page enables you to configure the per-port statistics parameters for 3PCC services.

The following table shows the per-port statistics information that you can configure.

Table 62. Configurable Per-port Statistics Information

Option	Description
Audio PPS	
Packet Statistics	Enables or disables audio PPS packet statistics. The supported values are: • **Enabled.** Enables the audio PPS packet statistics. • **Disabled.** Disables the audio PPS packet statistics. The default value is disabled. If Packet Statistics is enabled, the following audio packet statistics can be configured. • Octet Sent • Octet Received • Packet Sent • Packet Received • Packet Loss • Duration • Average Jitter • Jitter Buffer Frame Dropped • Jitter Buffer Adjustments
Audio Statistics	Enables or disables the audio statistics. The supported values are: • **Enabled.** Enables the audio statistics. • **Disabled.** Disables the audio statistics. The default value is disabled. If Audio Statistics is enabled, the following audio statistics can be configured. • Peak Amplitude • RMS SpeechPower Avg • RMS SpeechPower Min • RMS SpeechPower Max • RMS NoisePower Avg • RMS NoisePower Min • RMS NoisePower Max • Avg DC Offset • SNR Avg • SNR Min • SNR Max

Table 62. Configurable Per-port Statistics Information

Option	Description
AEC Statistics	Enables or disables the AEC statistics. The supported values are: • **Enabled.** Enables the AEC statistics. • **Disabled.** Disables the AEC statistics. The default value is disabled. If AEC Statistics is enabled, the following AEC statistics can be configured. • Enable Time • Active Time • Out of Resource • Bulk Delay • Bulk Delay Min • Bulk Delay Max • ERL • ERL Min • ERL Max • ERLE • ERLE Min • ERLE Max
RTCP XR Statistics	Enables or disables audio PPS RTCP-XR group statistics. The supported values are: • **Enabled.** Enables the RTCP-XR Statistics. • **Disabled.** Disables the RTCP-XR Statistics. The default value is disabled. If RTCP XR Statistics is enabled, the following RTCP XR group statistics are configured. • RTCP XR Summary Statistics • RTCP XR Voip Metrics Statistics

Table 62. Configurable Per-port Statistics Information

Option	Description
RTCP XR Summary Statistics	Enables or disables the RTCP-XR summary statistics. The supported values are: • **Enabled.** Enables the RTCP-XR summary statistics. • **Disabled.** Disables the RTCP-XR summary statistics. The default value is disabled. If RTCP XR Summary Statistics is enabled, the following RTCP-XR summary statistics can be configured. • Beg Seq • End Req • Lost Packets • Dup Packets • Min Jitter • Max Jitter • Mean Jitter • Dev Jitter • min_ttl_or_hl • max_ttl_or_hl • mean_ttl_or_hl • dev_ttl_or_hl

Table 62. Configurable Per-port Statistics Information

Option	Description
RTCP XR Voip Metrics Statistics	Enables or disables the RTCP-XR Voip metrics statistics. The supported values are: • **Enabled.** Enables the RTCP-XR Voip statistics. • **Disabled.** Disables the RTCP-XR Voip statistics. The default value is disabled. If RTCP XR Voip Metrics Statistics is enabled, the following RTCP-XR Voip statistics can be configured. • loss rate • discard rate • burst density • gap density • burst duration • gap duration • round trip delay • end system delay • signal level • noise level • rerl • gmin • r-factor • ext-r-factor • mos-listen • mos-conver • rx-config • jb-nominal • jb-maximum • Jb-abs-max
RTCP R-Factor Statistics	Enables or disables the R-Factor statistics. The supported values are: • **Enabled.** enables the RTCP R-Factor statistics. • **Disabled.** disables the RTCP R-Factor statistics. The default value is disabled. If RTCP R-Factor Statistics is enabled, the following RTCP R-factor statistics can be configured. • cq-before • mos-cq-before • cq-after • mos-cq-after
Video PPS	

Table 62. Configurable Per-port Statistics Information

Option	Description
Packet Statistics	Enables or disables the video packet statistics. The supported values are: • **Enabled.** Enables the video packet statistics. • **Disabled.** Disables the video packet statistics. The default value is disabled. If Packet Statistics is enabled, the following video packet statistics can be configured. • Octet Sent • Octet Received • Packet Sent • Packet Received • Packet Loss • Packet Duration
Fax PPS	
Packet Statistics	Enables or disables the fax packet statistics. The supported values are: • **Enabled.** Enables the fax packet statistics. • **Disabled.** Disables the fax packet statistics. The default value is disabled. If Packet Statistics is enabled, the following fax packet statistics can be configured. • Octet Sent • Octet Received • Packet Sent • Packet Received • Packet Loss • Packet Duration
Text PPS	
Packet Statistics	Enables or disables the text packet statistics. The supported values are: • **Enabled.** Enables the text packet statistics. • **Disabled.** Disables the text packet statistics. The default value is disabled. If Packet Statistics is enabled, the following text packet statistics can be configured. • Octet Sent • Octet Received • Packet Sent • Packet Received • Packet Loss • Packet Duration

To configure the per-port statistics:

1. Click **Configuration** > **Node Configuration** > **Configure Per Port Statistics**.

   The Configure Per Port Statistics page displays.

2. Enable per-port statistics.
3. Click **Save Settings**.

   The changes in the configuration data take effect immediately.
4. Optionally, click **Reset Fields** to reset the changes made to the previous values.

Configure EVS

On the Configure EVS page, you can specify the EVS codec characteristics. The information set on this page can be viewed on the *Show Node Configuration*.

EVS bit rate range is displayed based on the selected EVS bandwidth.

EVS Information you can configure:

The following table describes the information you can configure for the EVS.

Table 63. EVS Information Required

Value	Description
EVS Mode Switch	Optional. Specifies the supported modes of EVS codec that Containerized Decomposed Media Server uses to send the media. The supported values are: • EVS Primary Mode • AMR-WB-IO Mode However, the Containerized Decomposed Media Server can receive EVS media in any of the above modes. The default is EVS Primary Mode. The changes to this field take immediate effect.
EVS Bandwidth	Optional. Specifies the supported bandwidths for the EVS codec that Containerized Decomposed Media Server uses to send media. The supported bandwidths are. • NB • WB • NB-WB • SWB • NB-SWB ***NOTE***: • EVS bandwidth SWB is compatible with EVS bitrate 9.6 to 128 kbps only. • However, the Containerized Decomposed Media Server can receive EVS media in any of the above bandwidths. The default bandwidth is NB-WB. The changes to this field take immediate effect.

Table 63. EVS Information Required

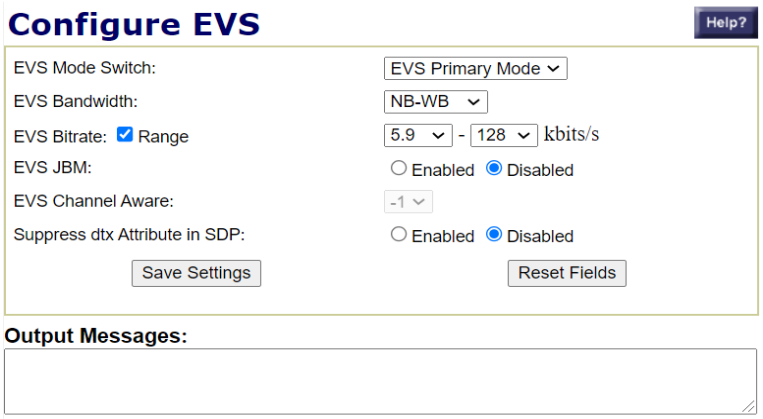
EVS Bitrate	Optional. Specifies the supported bitrate range for EVS codec in kbps, which Containerized Decomposed Media Server uses to send media. However, the Containerized Decomposed Media Server receives all valid bitrates from the far end. • If Range is disabled, the supported bit rate can be selected from the drop-down list. The default bitrate is 5.9 kbps. • If Range is enabled, the supported bitrate range can be selected from the drop-down list. The default minimum bitrate is 5.9 and maximum bitrate is 128 kbps. ***NOTE:*** EVS NB bandwidth is compatible with EVS bitrates from 5.9 up to 24.4 kbps only. The bitrate **Range** check box is enabled, by default. The changes to this field take immediate effect.
EVS JBM	Enables or disables the EVS Jitter Buffer Management (JBM) feature. The supported values are: • Enabled • Disabled Default value is Disabled. The changes to this field take immediate effect.

Table 63. EVS Information Required

EVS Channel Aware	Indicates the EVS channel aware mode. The EVS channel aware mode adds partial redundancy to the EVS frames and reduces the impact of packet loss at the receiver end. The Containerized Decomposed Media Server supports EVS channel aware mode in both the ingress and egress directions. The supported values are: • **-1.** Disabled. • **0.** EVS channel aware with Forward Error Correction (FEC) offset as 0. Initially no FEC data is sent, however the encoder is ready to send channel aware FEC data based on a valid CMR request. • **2.** The encoder is configured to send channel aware data with FEC offset as 2. • **3.** The encoder is configured to send channel aware data with FEC offset as 3. • **5.** The encoder is configured to send channel aware data with FEC offset as 5. • **7.** The encoder is configured to send channel aware data with FEC offset as 7. Default value is -1. ***NOTE:*** This field is available only when the EVS JBM feature is enabled. The Containerized Decomposed Media Server continues to encode channel aware FEC data in the egress direction irrespective of whether EVS JBM is enabled or disabled, based on the user channel aware FEC offset preference. The changes to this field take immediate effect.
Suppress dtx Attribute in SDP	Enables or disables the suppression of the Discontinuous Transmission (DTX) attribute in the SDP offer/answer for EVS port. The supported values are. • **Enabled.** The Containerized Decomposed Media Server excludes the `dtx` attribute in the outgoing SDP. • **Disabled.** The Containerized Decomposed Media Server includes the `dtx` attribute in the outgoing SDP. Default value is Disabled. When the `dtx` attribute is received in the incoming SDP, the Containerized Decomposed Media Server acknowledges the `dtx` attribute irrespective of the **Suppress dtx Attribute in SDP** configuration. ***NOTE:*** This field is applicable only when the silence suppression is enabled in the *Configure Silence Suppression* Web GUI page. The changes to this field take effect on the next SDP offer/answer exchange without rebooting the Containerized Decomposed Media Server.

To configure the EVS:

1. Click **Configuration** > **Node Configuration** > **Configure EVS**.



2. Enter the EVS information described in the above table.
3. Click **Save Settings**.

   The changes take effect immediately. Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure SIP Load Balancing

The Configure SIP Load Balancing page enables you to configure the load balancing method for MRFP. The information set on this page can be viewed on the *Show Node Configuration*.

For the Containerized Decomposed Media Server load balancing feature to function, load balancing method must be set to same value in both MRFP and MRFC. For information on configuring the load balancing method for MRFC, see *MRFC Configuration on page 509*.

Information that you can configure:

The following table describes the load balancing method for MRFP that you can configure.

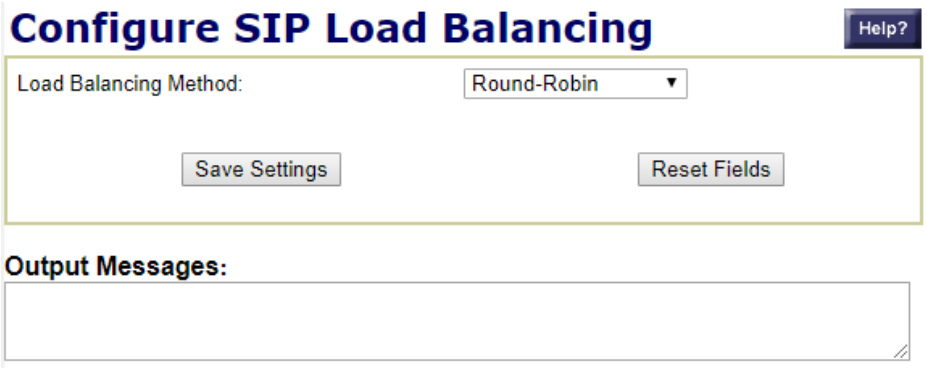
Table 64. MRFP Parameter Settings

Parameter	Description
Load Balancing Method	Specifies the load balancing methods for forwarding the initial SIP INVITE requests to the respective MRFPs. The supported values are: • **Round-Robin.** When Round-Robin method is enabled, MRFCtrl distributes the incoming calls on MRFPs in a round-robin method, without considering a load on the individual MRFP. • **Dynamic-Feedback.** When Dynamic-Feedback method is enabled, MRFPs report their current resource utilization to MRFCtrl at regular intervals through the `SIP REGISTER` request. MRFCtrl uses this information to evaluate the resource utilization for each MRFP, bucketizes the MRFPs, and routes the new incoming call on MRFPs. Default value is Round-Robin. Changes to this field take effect on the next call presented to MRFP.

To configure the SIP load balance method:

1. Click **Configuration** > **Node Configuration** > **Configure SIP Load Balancing**.

   The Configure SIP Load Balancing page displays.



2. Select the **Load Balancing Method**.
3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previous saved values.

Configure MSCML

The Configure MSCML page enables you to configure the characteristics for MSCML parameters.

The following table shows the MSCML parameters that you can configure.

Table 65. MSCML Parameter Settings

Option	Description
Escape Key Timer	Allows you to configure the escape key time interval in milliseconds. The supported value range is 1000 to 24000. The default value is 1000. The changes to this field take effect on the next `<playrecord>` request.
Beep Clip	Allows you to configure the audio clip path followed by clip file. The audio clip is used in an audio message to play a beep. The maximum length is 128 characters. ***NOTE:*** • The clip name must be in **.wav** format. • When the beep clip value is blank, no clip is played. The changes to this field take effect on the next `<playrecord>` request.
Implicit Stop	Enables or disables MSCML implicit stop feature in `sip:ivr` and `sip:mscmlvideo` service contexts. The supported values are: • **Enabled.** Enables MSCML implicit stop in `sip:ivr` and `sip:mscmlvideo` service contexts. When enabled, the Containerized Decomposed Media Server treats a SIP re-INVITE that modifies the established SDP parameters as an implicit `<stop>` request. As a result, the Containerized Decomposed Media Server immediately terminates the active `<play>`, `<playcollect>`, or `<playrecord>` request and sends a `<response>` indicating `reason=stopped`. • **Disabled.** Disables MSCML implicit stop in `sip:ivr` and `sip:mscmlvideo` service contexts. The default value is Disabled. Changes to this field take effect on the next SDP change.
File Extension and the Codec Type	
Wav File type	Indicates the encoding format in which the Containerized Decomposed Media Server stores the recording when the recoded file extension is WAV (.wav) file format. The supported values are: • pcmu • pcma • g729 • g722 The default value is pcmu. Changes to this field take effect immediately.

Table 65. MSCML Parameter Settings

Option	Description
3gp File type	Indicates the encoding format in which the Containerized Decomposed Media Server stores the recording when the recoded file extension is 3GP (.3gp) file format. The supported values are: • amr • amrwb The default value is amr. Changes to this field take effect immediately.
3gpp File type	Indicates the encoding format in which the Containerized Decomposed Media Server stores the recording when the recoded file extension is 3GPP (.3gpp) file format. The supported values are: • amr • amrwb The default value is amr. Changes to this field take effect immediately.
Qt File type	Indicates the encoding format in which the Containerized Decomposed Media Server stores the recording when the recoded file extension is QT (.mov) file format. The supported values are: • pcmu • pcma The default value is pcmu. Changes to this field take effect immediately.
Mixer Information	
Mixer Type	Allows you to configure the video conference type for the MSCML conference context. The supported values are: • VAS • CPV The default value is VAS. Changes to this field require a MRFP restart to take effect.
Mixer Root Height	Allows you to configure the mixer root window height in pixels. The supported value is in multiples of 16, from 144 to 1280. The default value is 288. Changes to this field require a MRFP restart to take effect.
Mixer Root Width	Allows you to configure the mixer root window width in pixels. The supported value is in multiples of 16, from 144 to 1280. The default value is 352. Changes to this field require a MRFP restart to take effect.
Active Border Width	Allows you to configure the active border width in pixels. The supported values are 0 and in multiple of 2. The default value is 0, which means voice activated border (VAB) feature is disabled. Changes to this field require a MRFP restart to take effect.

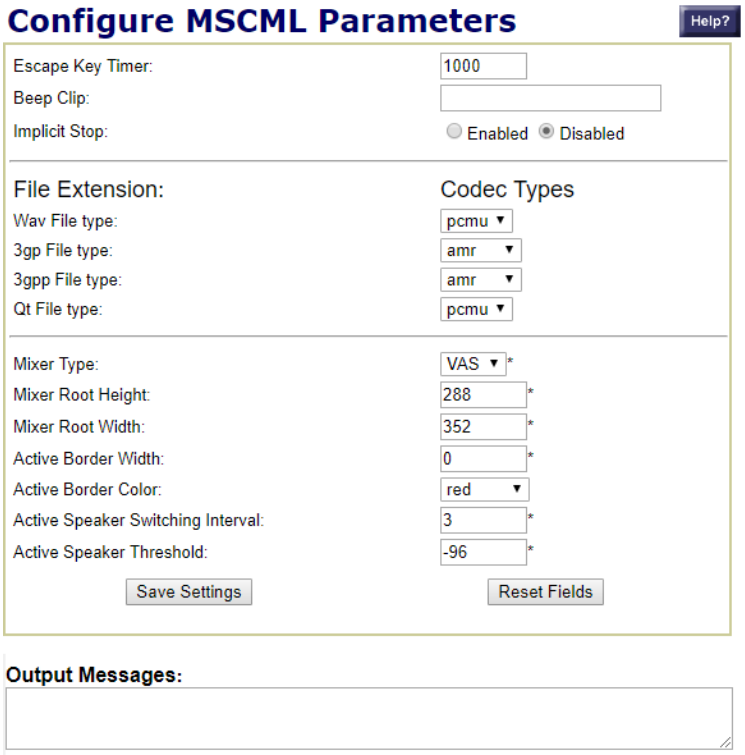
Table 65. MSCML Parameter Settings

Option	Description
Active Border Color	Allows you to configure the active border color. The supported values are: • aqua • black • blue • fuchsia • gray • green • lime • maroon • navy • olive • purple • red • silver • teal • white • yellow The default value is red. Changes to this field take effect immediately.
Active Speaker Switching Interval	Allows you to configure the switching interval in seconds that the Containerized Decomposed Media Server must wait before switching the active border for the regions of non-loudest layouts. The supported value is from 3 to 600. The default value is 3. Changes to this field require a MRFP restart to take effect.
Active Speaker Threshold	Allows you to configure the active speaker threshold level in dB. This field is applicable for both Active Speaker in Largest Video Tile (ASL) and VAB. The supported values is from 0 to -96. The default value is -96. Changes to this field require a MRFP restart to take effect.

To configure the MSCML:

1. Click **Configuration** > **Node Configuration** > **Configure MSCML**.

   The Configure MSCML page displays.



2. Enter the MSCML information described in the above table.
3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Netconf Agent

The Configure Netconf agent page allows you to view the NETCONF agent port number for the NETCONF session.

To view the NETCONF agent information:

1. Click **Configuration** > **Node Configuration** > **Configure Netconf Agent**.

   The Configure Netconf Agent page displays.

2. The **Agent Port Number** is non-editable.

   The **Output Messages:** box displays the NETCONF agent port number is not configurable.

Configure System Security

The Configure System Security page enables you to configure the system security information.

The following table shows the system security parameters that you can configure.

Table 66. System Security Parameter Settings

Option	Description
Client Alive Time	The time, in minutes, for which the client is active to serve the NETCONF sessions. The range is from 1 to 120. The default value is 15. ***NOTE:*** On RHEL 8.x, this parameter does not support a session timeout value more than 15 minutes. The changes to this field take effect immediately.
MaxRetries	The maximum number of times the Containerized Decomposed Media Server attempts to connect to a NETCONF session. The range is from 1 to 4. The default is 4. ***NOTE:*** • The value set on **MaxRetries** includes a public key and password authentication. Public key authentication accounts for one time try and the remaining is used for password authentication. Therefore in case of failures, the SSH prompts for a password for (MaxRetries - 1) times. • If you are configuring the **MaxRetries** with a lower value, ensure that there is no failure condition for the SSH login and the **MaxRetries** must be more than 3. Otherwise, the Containerized Decomposed Media Server will reject the ssh login. The changes to this field take effect immediately.

Table 66. System Security Parameter Settings

Option	Description
Authentication Method	The authentication method for the NETCONF session. The supported values are: • Password • PublicKey By default, both the authentication methods are enabled. The changes to this field take effect immediately.

Encrypt Subscriber Data	Enables or disables the user to encrypt or decrypt subscriber data. The supported values are.
	• **Enable.** When this feature is enabled,
	  • The Containerized Decomposed Media Server encrypts all the subscriber generated media files using AES-256-CBC cipher.
	  • The Containerized Decomposed Media Server encrypts internal (transient and persistent) and external recordings (NFS and HTTP).
	• **Disable.** When this feature is disabled,
	  • The Containerized Decomposed Media Server fails to play the announcement, if the media file is encrypted. The Containerized Decomposed Media Server plays the announcement, if the media file is decrypted.
	  • The recording file is stored in non-encrypted format.
	The default value is Disable.
	Changes to this field require a MRFP restart to take effect.

Mask DTMF Digits	Enables or disables masking of detected DTMF digits in the syslog and protocol logs. The supported values are: • **Enable.** Masks the DTMF digits that are logged in the syslog and protocol logs. • **Disable.** Unmasks the DTMF digits that are logged in the syslog and protocol logs. The default value is Disable. ***NOTE:*** The Containerized Decomposed Media Server displays the masked DTMF digits as **xxxxx**, where **xxxxx** is a string and does not represent the actual number of digits that are reported by the Containerized Decomposed Media Server. The changes to this field take effect immediately.

NOTE: The file transfer fails if the permissions or ownership of the key directories are modified manually.

Decryption Tool Usage

The Containerized Decomposed Media Server provides an offline decryption tool for Linux. The operator can execute this tool from the command line to decrypt the media files, which were previously encrypted by the Containerized Decomposed Media Server. This tool allows the operator to provide the decrypted media file to the subscriber, when requested.

Execute the tool on the command line as per the following syntax.

```
msdecryptfile.sh <input-file>  <output-file>  <format>
```

where,

`<input-file>` is the encrypted file name with the extension

`<output-file>` is the decrypted file name with the extension

`<format>` can be wav, 3gp, qt, amr, or fax

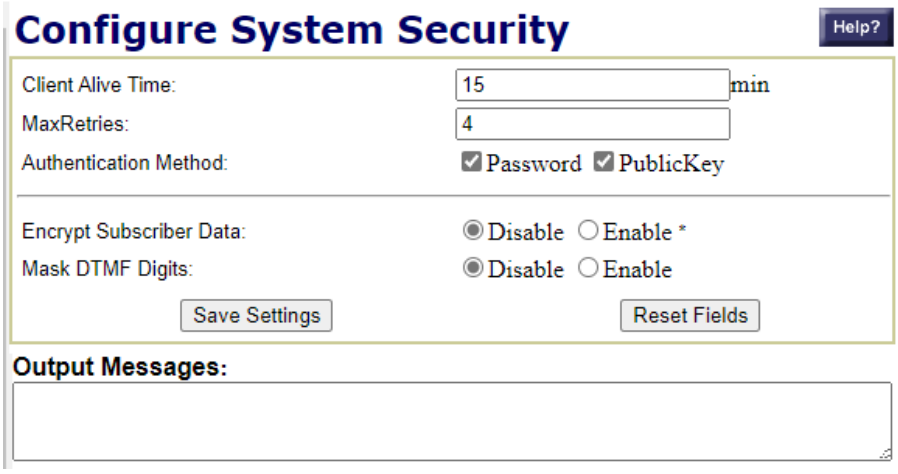
NOTE:

- For both awb and amr extensions the format argument value is amr.
- The decryption tool is released only as a 32 bit binary; however, tool can be executed on both 32 and 64 bit OS versions. We recommend you to use RHEL 6.x OS version.

To configure the system security information:

1. Click **Configuration** > **Node Configuration** > **Configure System Security**.

   The Configure System Security page displays.



2. Enter the system security information described in the above table.
3. Click **Save Settings**.

   The changes require a MRFC restart to take effect and a confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure CPV Layout Template

The CPV Layout Template page allows you to configure the Continuous Presence Video (CPV) layout template types.

The following table shows the CPV Layout Template parameters that you can configure.

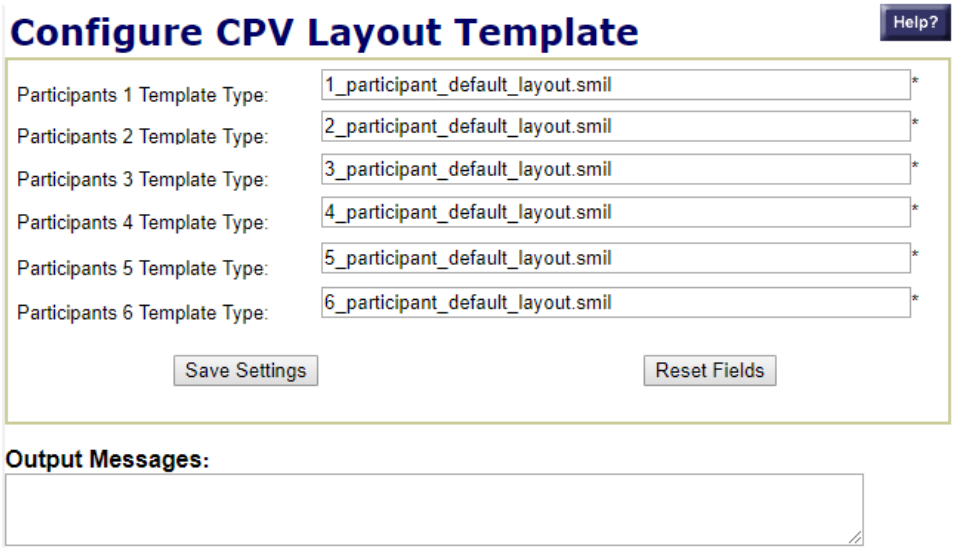
Table 67. CPV Layout Template Parameter Settings

Option	Description
Participants 1 Template Type	Configures the template type for the CPV conference, when the number of participants is 1. Changes to this field require a MRFP restart to take effect.
Participants 2 Template Type	Configures the template type for the CPV conference, when the number of participants are 2. Changes to this field require a MRFP restart to take effect.
Participants 3 Template Type	Configures the template type for the CPV conference, when the number of participants are 3. Changes to this field require a MRFP restart to take effect.
Participants 4 Template Type	Configures the template type for the CPV conference, when the number of participants are 4. Changes to this field require a MRFP restart to take effect.
Participants 5 Template Type	Configures the template type for the CPV conference, when the number of participants are 5. Changes to this field require a MRFP restart to take effect.
Participants 6 Template Type	Configures the template type for the CPV conference, when the number of participants are 6. Changes to this field require a MRFP restart to take effect.

To configure the CPV layout template type information:

1. Click **Configuration** > **Node Configuration** > **Configure CPV Layout Template**.

   The Configure CPV Layout Template page displays.



2. Enter the CPV layout template parameters information described in the above table.
3. Click **Save Settings**.

   The changes require a restart to take effect and a confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Lawful Intercept

The Configure Lawful Intercept page allows you to configure the information of the intercepted call content over the X3 interface.

The following table shows the lawful intercept parameters that you can configure.

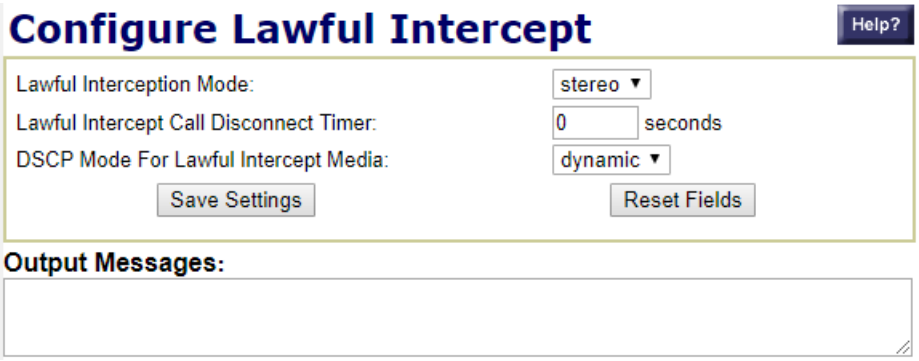
Table 68. Lawful Intercept Parameter Settings

Option	Description
Lawful Interception Mode	Configures the lawful interception mode for audio media type only. The supported interception modes are. • **stereo.** The Containerized Decomposed Media Server delivers the received and transmitted streams from the intercepted port, in two separate RTP streams to the Lawful Intercept Gateway (LIG). • **mono.** The Containerized Decomposed Media Server mixes the received and transmitted streams from the intercepted port and delivers a single RTP stream to the LIG. The default mode is stereo. Changes to this field take effect immediately.
Lawful Intercept Call Disconnect Timer	Indicates the lawful intercept call disconnect timer, in seconds. The range is from 0 to 60. The default value is 0, which means the timer is disabled. Changes to this field take effect immediately.
DSCP Mode For Lawful Intercept Media	Configures the Differentiated Services Code Point (DSCP) mode for the Lawful Intercept (LI) service media packets. The supported values are. • **static.** The Containerized Decomposed Media Server updates the DSCP value in the outgoing media packet with the configured DSCP value through the management interface. • **dynamic.** The Containerized Decomposed Media Server sends the DSCP value in the outgoing media packet whatever is received in the incoming media packets. The default mode is dynamic. Changes to this field take effect on the next LI group.

To configure the lawful intercept information:

1. Click **Configuration** > **Node Configuration** > **Configure Lawful Intercept**.

   The Configure Lawful Intercept page displays.



2. Enter the lawful intercept information described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Manage Certificates

The Manage Certificates page allows you to manage the local and remote certificates. These certificates are used by the Containerized Decomposed Media Server to establish SSL connection, perform SIP over TLS, obtain the announcement clips or recordings using HTTPS, and perform the SANE certification.

For information on managing HTTP and HTTPS for the Web-based management interface, see *Configure HTTP Server* Web GUI page.

Provisioning procedure for Containerized Decomposed Media Server (acting as HTTPS client)

Following are the provisioning procedures for the Containerized Decomposed Media Server, when the Containerized Decomposed Media Server acts as an HTTPS client.

- Certificate validation of server required or no validation of the client certificate
  1. Set the **Certificate Type** to CA Certificate.
  2. Upload the web server certificate.

     Repeat Step 1 and Step 2 for each web server.
- Certificate validation of server and client certificate required
  1. Set the **Certificate Type** to CA Certificate.
  2. Upload the web server certificate.

     Repeat Step 1 and Step 2 for each web server.
  3. Set **Certificate Type** to Machine Certificate.

4. Upload the certificate that the Containerized Decomposed Media Server provides in response to the web server *CertificateRequest* message.
5. Set the **Certificate Type** to Machine Key.
6. Upload the Private Key.
7. After executing Step 4 and Step 6, reboot the Containerized Decomposed Media Server.

NOTE: There are the default machine key and certificate available after installation. If you want to use user-defined machine key and CA certificate instead of the default certificates, the Step 4 and Step 6 are required.

Provisioning procedure for Containerized Decomposed Media Server (using SIP over TLS)

- Containerized Decomposed Media Server acting as TLS server
  1. On the *Configure SIP* Web GUI page, enable **SIP over TLS**.
  2. On the *Configure SIP* Web GUI page, configure **SIP-TLS Port**.

     The default value is 5061.
  3. On the *Configure SIP* Web GUI page, enable **SIP-TLS Mutual Authentication**.

     When the Containerized Decomposed Media Server acts as a TLS server during a TLS handshake, the Containerized Decomposed Media Server sends a certificate request and authenticates the client certificate with the client public key.
  4. On the *Configure SIP* Web GUI page, disable **SIP-TLS Mutual Authentication**.

     When the Containerized Decomposed Media Server acts as a TLS server during a TLS handshake, the Containerized Decomposed Media Server does not send a certificate request to the client.
- Containerized Decomposed Media Server acting as TLS client
  1. On the *Configure SIP* Web GUI page, enable **SIP over TLS**.
  2. On the *Configure SIP* Web GUI page, configure **SIP-TLS Port**.

     The default value is 5061. When the Containerized Decomposed Media Server acts as a TLS client during TLS handshake, the Containerized Decomposed Media Server always accepts a certificate request from the TLS server, irrespective of the **SIP-TLS Mutual Authentication** settings.
  3. Set **Certificate Type** to Machine Certificate.
  4. Upload the certificate that the Containerized Decomposed Media Server provides in response to the web server *CertificateRequest* message.
  5. Set **Certificate Type** to Machine Key.
  6. Upload the Containerized Decomposed Media Server private key.
  7. After executing Step 4 and Step 6, reboot the Containerized Decomposed Media Server.

The following table shows the manage certificates parameters that you can configure.

Table 69. Manage Certificates Settings

Option	Description
Certificate type	The certificate type. The supported values are: • **CA Certificate.** List of the CA certificates that are stored in the Containerized Decomposed Media Server to validate the received certificates from the TLS server for the ClientHello message. The file format is *.cert*. The Containerized Decomposed Media Server copies the certificates to */var/opt/swms/cert/ca/CA.crt*. • **Machine Key.** This is the Containerized Decomposed Media Server private key. In SIP over TLS, where the Containerized Decomposed Media Server acts as the server, the Containerized Decomposed Media Server uses its machine (private) key to decrypt the messages received from the far-end. The file format is *.pem*. The Containerized Decomposed Media Server copies the certificates to */var/opt/swms/cert/local/machine-key.pem*. • **Machine Certificate.** The certificate provided by the Containerized Decomposed Media Server in response to a CertificateRequest sent by the TLS client. In SIP over TLS, where the Containerized Decomposed Media Server acts as the server, the Containerized Decomposed Media Server sends the machine certificate in response to the ClientHello message. The file format is *.pem*. The Containerized Decomposed Media Server copies the certificates to */var/opt/swms/cert/local/machine-cert.pem*. The default value is CA Certificate. For CA Certificate, changes to this field take effect immediately. For Machine Key and Machine Certificate, changes require a restart to take effect. ***NOTE:*** • While deploying the Containerized Decomposed Media Server, if the **extCert** (Certificate Manager) parameter in the *values.yaml* file is enabled, the **Machine Key** and **Machine Certificate** parameters are not applicable. For more information on **extCert** parameter, refer *Containerized Decomposed Media Server Installation Guide*. • This field is enabled when the Provision Certificate check-box is checked.

Table 69. Manage Certificates Settings

Option	Description
Certificate transfer Subsystem	Allows to provision the machine certificates and keys for the subsystem interfaces that use TLS. The supported values are: • All • SipOverTls • AnnouncementRecording • VXML • DTLS • LDAP • SAML • Annlab • HTTPS • Prometheus The default value is All. ***NOTE:*** • This field is enabled when the **Certificate type** field is set to **Machine Key** or **Machine Certificate**. • The Annlab, SAML, Prometheus, HTTPS, and LDAP interfaces require an OAMP pod service restart. • The AnnouncementRecording, DTLS, and VXML interfaces require MRFP restart. • The SipOverTls interface requires MRFP restart and MRFC switchover. • For Prometheus, HTTP and HTTPS are supported. The Prometheus certificates are uploaded for the HTTPS communication between Containerized Decomposed Media Server and Prometheus.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** • Do not begin the name with "#" or "~". • This field is editable if the Provision Certificate check box is checked. Changes to this field take effect immediately.

Table 69. Manage Certificates Settings

Option	Description

Path and name of certificate file on remote server	The absolute path and name of certificate file on the remote file server. The supported values are strings of up to 256 characters.
	Allowed set of characters is.
	• uppercase alphabetic characters (A-Z)
	• lowercase alphabetic characters (a-z)
	• numeric characters (0-9)
	• special characters (/#.-_@=+%:~)
	NOTE:
	• Do not begin the name with "#" or "~".
	• This field is editable if the Provision Certificate check box is checked.
	• In HTTPS provisioned certificate,
	  • while downgrading the Media Server, if the HTTPS provisioned certificate length is greater than 4096, the default certificate is selected after downgrade.
	  • while downgrading the Media Server, if the HTTPS provisioned certificate length is less than or equal to 4096, the provisioned certificate is selected after downgrade.
	• This field cannot be blank.

Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

To configure the Manage Certificates information:

1. Click **Configuration** > **Node Configuration** > **Configure Manage Certificates**.

   The Configure Manage Certificates page displays.

2. Enter the manage certificate information as described in the above table.

   NOTE: If the certificate is **CA Certificate**, reboot is not required. If the certificate is **Machine Key** and **Machine Certificate**, changes require a reboot to take effect.

3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.

Configure Keyword Detection

The Configure Keyword Detection page allows you to configure the keyword detection related parameters.

Keyword Description Package File

The keyword description package file contains the keyword model file and a text file containing the corresponding list of keywords, and a text file containing the mode type.

The naming convention of the keyword description package file is *<KWM>-Version-<X.Y.Z>.tar.gz*. The keyword model file inside this package is named as *<KWM>-Model-Version.<X.Y.Z>* and the keyword list file containing the list of supported keywords in the model file is named as *<KWM>-Descriptor-Version.<X.Y.Z>.txt*. The mode type file is named as <KWM>-ModeType.txt.

where,

- X represents the major version for the keyword package
- Y represents the minor version for the keyword package
- Z represents the patch version for the keyword package

Format of the model text File

NOTE: This section explains the keyword format in the model text file, which is provided in the release package. However, Radisys recommends not to modify the model text file.

The keywords that are used for detection are provided inside the model file in the text format.

The valid pattern is a comma separated list of <keyword>. Each word in <keyword> must be separated by an underscore (_). Allowed set of characters is.

- uppercase alphabetic characters (A-Z)
- lowercase alphabetic characters (a-z)
- special characters (_)

The Containerized Decomposed Media Server supports a maximum of 16 distinct keywords for detection in US-English accent. In the ASR mode, the Containerized Decomposed Media Server supports detection of a maximum of 10 digits in a sequence using the DigitSet model. In the ASR mode, the Containerized Decomposed Media Server does not support detection and interpretation of words like double and triple; each digit required to be distinctly pronounced.

For example Wakewords or commands in HotWord mode: PLAY_MUSIC, PAUSE_MUSIC, NEXT_SONG, PREVIOUS_SONG, STOP_MUSIC

For example DigitSet sequence in ASR mode: ZERO, ONE, TWO, THREE, FOUR, FIVE, SIX, SEVEN, EIGHT, NINE, OH, NOUGHT, STAR, HASH, CANCEL, and STOP. The CANCEL or STAR and STOP or HASH digits are expected to terminate the DigitSet sequence. However, other digits can also be configured to terminate the DigitSet sequence.

Valid values are strings of 1024 characters.

NOTE: The keyword list is preserved in full backup and restore operations.

Format of the Mode Type File

The mode type file is named as <KWM>-ModeType.txt. The mode type text file contains the following mode types.

- **HotWord mode.** The HotWord mode is defined as 0. This mode supports Keyword and command set detection.
- **ASR mode.** The ASR mode is defined as 1. This mode supports ASR grammar model.

The following table shows the keyword detection parameters that you can configure.

Table 70. Keyword Detection Settings

Option	Description
Keyword List	Displays the list of keywords on uploading the <KWM>-Model-Version.<X.Y.Z> file. The displayed list of keywords in this field corresponds to a list of keywords inside the *<KWM>-Descriptor-Version.<X.Y.Z>.txt* file. ***NOTE:*** The Containerized Decomposed Media Server is initialized with a default keyword set on fresh restart. The default value is YES,NO.
Current Uploaded Model File	Indicates the recently uploaded keyword model file. The default keyword model file name is YesNo-enUS-Model-Version.1.0.0.
Mode Type	Displays the mode type from the model file package. The HotWord mode is defined as 0, and ASR mode is defined as 1. The displayed mode type in this field corresponds to the value inside the *<KWM>-ModeType.txt* file. The default mode type is 0(HotWord mode).
Upload Model File	Allows to upload a single keyword description package file. This package file contains the keyword model file and a text file containing the corresponding list of keywords. After uploading the keyword description package file, the Containerized Decomposed Media Server displays the list of keywords in the **Keyword List** parameter. The changes to this field require a MRFP restart to take effect.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).

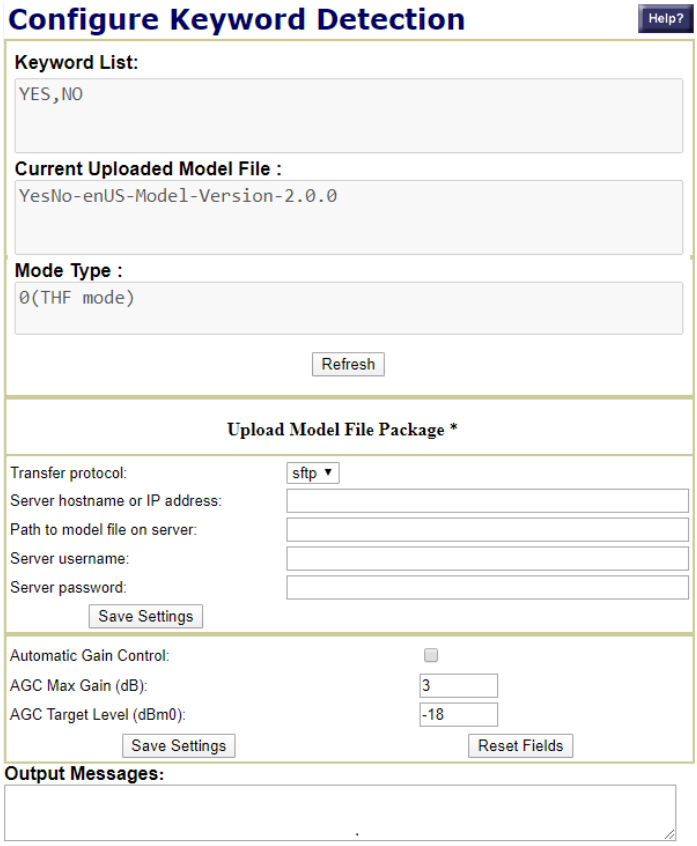
Table 70. Keyword Detection Settings

Option	Description
Server hostname or IP address	The IP address in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to model file on server	The path of the keyword model file on the file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	User name configured on the file server. The supported values are strings of up to 128 characters.
Server password	Password configured on the file server. The supported values are strings of up to 128 characters.
Automatic Gain Control	Enables or disables the Automatic Gain Control (AGC) on the MSML and VXML keyword detection ports. When this field is checked, the Containerized Decomposed Media Server automatically adjusts the level of audio to a configured target level, limited by a configured maximum amount of gain. By default this field is unchecked. This parameter does not require a restart and takes effect only on the new keyword detection sessions.
AGC Max Gain (dB)	Specifies a limit on the maximum gain, in decibels that can be applied when AGC is enabled. The value range is from 0 to 40. The default value is 3. This parameter does not require a restart and takes effect only on the new keyword detection sessions.
AGC Target Level (dBm0)	Specifies the desired target level for AGC, in dBm0. The value range is from -40 to 0. The default value is -18. This parameter does not require a restart and takes effect only on the new keyword detection sessions.

To configure the keyword detection information:

1. Click **Configuration** > **Node Configuration** > **Configure Keyword Detection**.

   The Configure Keyword Detection page displays.



2. Enter the keyword detection information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Add SMIL File

The Add SMIL File page allows you to provision the Synchronized Multimedia Integration Language (SMIL) file.

The following table shows the SMIL file parameters that you can configure.

Table 71. Add SMIL File Settings

Option	Description
Transfer protocol	The SMIL file transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address in dotted quad format for IPv4, or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is: • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". Changes to this field take effect immediately.
Path and name of smil file on remote server	The absolute path and name of the SMIL file on the remote file server. The supported values are strings of up to 256 characters. Allowed set of characters is: • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

NOTE: When the **Password Less Transfer to/from Remote Server** parameter on the *Configure System Security* Web GUI page is enabled, the **Server password** is non-editable.

To configure the SMIL file information:

1. Click **Configuration** > **Node Configuration** > **Add SMIL File**.

   The Add SMIL File page displays.

2. Enter the SMIL file configuration information as described in the above table.
3. Click **Save Settings**.

   Changes require a reboot to take effect and a confirmation message is displayed in the **Output Messages:** box.

Configure TLS

The Configure TLS page enables you to configure the TLS setting applicable on the following interfaces.

- SIP over TLS
- HyperText Transfer Protocol Secure (HTTPS) for Web GUI
- Security Assertion Markup Language (SAML)
- Datagram Transport Layer Security (DTLS)
- Lightweight Directory Access Protocol (LDAP)
- VoiceXML
- HTTPS announcement and recoding

The information set on this page can be viewed on the *Show TLS* page.

The following table shows the TLS parameters that you can configure.

Table 72. TLS Configuration Information

Parameter	Description
Tls Config Version	Allows to set the supported TLS version on the Containerized Decomposed Media Server. The supported values are: • 1.0 • 1.1 • 1.2 By default,1.2 is selected for the TLS version. ***NOTE:*** • On RHEL 8.x, the TLS versions 1.0 and 1.1 are not supported. • The TLS version 1.2 is recommended to enhance the Containerized Decomposed Media Server security. Changes to this field require MRFP and OAMP pod restart to take effect.
Preferred Cipher List	Allows to configure a list of cipher suites that are preferred for the TLS connection. The preferred cipher list is a colon separated list. Valid values are text strings of 0 to 2048 characters. The default value is ' '. For example, ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA: ***NOTE:*** The SAML supports a subset of all the ciphers supported in the Containerized Decomposed Media Server. For the list of supported ciphers on the SAML interface, *see* Table 73. Changes to this field require MRFP and OAMP pod restart to take effect.
Ecdhe Curve	Allows to set the Elliptic-curve Diffie–Hellman (ECDHE) curve. The ECDHE curve can be a single curve or a colon separated list. Valid values are text strings of 0 to 1024 characters. The default value is ' '. For example, secp256k1:secp384r1:secp521r1:prime256v1 ***NOTE:*** Ecdhe curve is not supported in HTTPS for Web GUI, LDAP, and SAML interfaces. Changes to this field require MRFP and OAMP pod restart to take effect.

Table 73 provides the preferred cipher behavior changes with different interfaces. The ciphers are supported based on the configured TLS version in the Web GUI.

Table 73. Preferred Cipher List Behavior

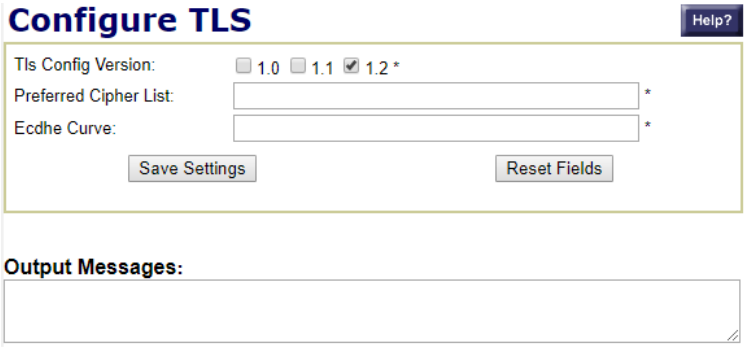
Interface	Acting as	Remarks
SIP over TLS	Server and Client	Ciphers preference are as follows: • When acting as a server, the preferences are based on server ciphers. If preference is not configured on the server, the client preferences are considered. • When acting as a client, the preferences are based on server configuration value.
HTTPS for Web GUI	Server	The preferences are based on server ciphers if configured.
SAML[a]	Client	The preferences are based on server configuration. If preference is not configured on the server, the client preferences are considered.
LDAP	Client	If preferred ciphers are configured through the Web GUI, the Containerized Decomposed Media Server supports TLS handshake with these ciphers. If preferred cipher is empty or not configured through the Web GUI, the Containerized Decomposed Media Server supports the list of cipher as per supported TLS version for the TLS handshake. The preferences are based on server configuration.
VXML	Client	If preferred ciphers are configured through the Web GUI. The server preferences are based on server configuration.
HTTPS announcement and recording	Client	The preferences are based on server configuration.

[a] The Containerized Decomposed Media Server supports the following OpenSSL ciphers for the SAML interface.
RC4-MD5, RC4-SHA, DES-CBC3-SHA, DES-CBC-SHA, EXP-RC4-MD5, EXP-RC2-CBC-MD, NULL-MD5, NULL-SHA, EXP1024-DES-CBC-SHA, EXP1024-RC4-SHA, AES128-SHA, AES256-SHA, ECDH-ECDSA-NULL-SHA, ECDH-ECDSA-RC4-SHA, ECDH-ECDSA-DES-CBC3-SHA, ECDH-ECDSA-AES128-SHA, ECDH-ECDSA-AES256-SHA, ECDHE-ECDSA-NULL-SHA, ECDHE-ECDSA-NULL-SHA, ECDHE-ECDSA-DES-CBC3-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES256-SHA, ECDH-RSA-NULL-SHA, ECDH-RSA-RC4-SHA, ECDH-RSA-DES-CBC3-SHA, ECDH-RSA-AES128-SHA, ECDH-RSA-AES256-SHA, ECDHE-RSA-NULL-SHA, ECDHE-RSA-NULL-SHA, ECDHE-RSA-DES-CBC3-SHA, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, AECDH-NULL-SHA, AECDH-RC4-SHA, AECDH-DES-CBC3-SHA, AECDH-AES128-SHA, and AECDH-AES256-SHA.

To configure TLS information:

1. Click **Configuration** > **Node Configuration** > **Configure TLS**.

   The Configure TLS page displays.



2. Enter the TLS information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure ICE

The Configure ICE enables you to configure the Interactive Connectivity Establishment (ICE) functionality for external communication.

NOTE:

- Currently, the ICE feature is supported in **MSML** and **sip:conf** service context.
- The ICE Support parameter is removed from the *Configure SIP* Web GUI page and the ICE related configurations can be configured in *Configure ICE* Web GUI page.

The following table provides the configuration parameters for ICE page.

Table 74. ICE Configuration Information

Parameter	Description
ICE Implementation	Allows to configure the ICE implementation. The supported values are: • **None.** • **ICE-Lite.** The ICE-Lite is a minimal version of the ICE specification, intended for servers running on a public IP address. • **Full-ICE.** Full ICE is a full implementation of ICE specification. • **Trickle-ICE.** Trickle ICE is an extension of ICE specification. Trickle ICE accelerates the process of establishing a communication session. The default value is None. Changes to this field takes effect immediately, applying to all new calls.
STUN Configurations	

Table 74. ICE Configuration Information

Parameter	Description
STUN Server Address	The server address used for ICE candidates gathering to get the server reflexive addresses. It supports IPv4, IPv6, and FQDN. The supported length is 0 to 255. The default value is empty. Changes to this field takes effect immediately, applying to all new calls.
STUN Server Port	The STUN server control port, on which the server is listening for STUN messages. The port range is 1 to 65535. The default value is 3478. Changes to this field takes effect immediately, applying to all new calls.
TURN Configurations	
TURN Server Address	The server address used for ICE candidates gathering and allocating the relay addresses. It supports IPv4 and FQDN. The supported length is 0 to 255. The default value is empty. Changes to this field takes effect immediately, applying to all new calls.
TURN Server Port	The TURN server control port, on which the server is listening for TURN messages. The port range is 1 to 65535. The default value is 3478. Changes to this field takes effect immediately, applying to all new calls.
TURN Server username	The username to authenticate the Media Server while allocating the relay addresses on the TURN server. The supported length is 0 to 128. The default value is empty string. Changes to this field takes effect immediately, applying to all new calls.
TURN Server password	The password to authenticate the Media Server while allocating the relay addresses on the TURN server. The supported length is 0 to 128. The default value is empty string. Changes to this field takes effect immediately, applying to all new calls.

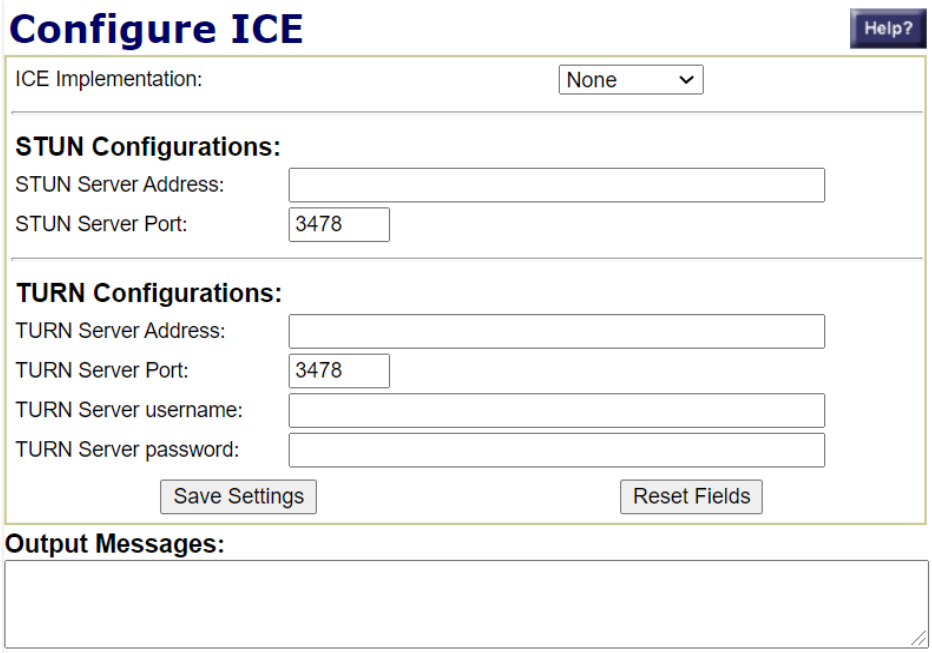
NOTE:

- If the **TURN server username** is empty, the value resets in the DB.
- If the **TURN server password** is empty, the value resets in the DB.
- The user must configure the **TURN server username** and **TURN server password** when they are configuring any parameters in the *Configure ICE* page, even if an active TURN server connection is already established.

To configure ICE information:

1. Click **Configuration** > **Node Configuration** > **Configure ICE**.

   The Configure ICE page displays.



2. Enter the ICE information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Media Storage Management

The Media Storage Management option of the Configuration screen allows you to work with settings for playing, recording, and storing audio clips.

When the Media Storage Management option is clicked, it shows the following options.

Show Audio Segment Configuration

You can view the name of the sets and variables definition file used for audio segment configuration.

For information about audio segment configuration and the sets and variables file, refer *Radisys Sets and Variables Interface Reference*.

To view the audio segment configuration:

1. Click **Configuration** > **Media Storage Management** > **Show Audio Segment Configuration**.
2. Click **Execute**.

   The name of the installed audio segment configuration file displays in the **Output Messages:** box.

Show Audio Segment Storage

On the Show Audio Segment Storage page, you can view the amount of space available for audio segment configuration.

To view the audio segment storage information:

1. Click **Configuration** > **Media Storage Management** > **Show Audio Segment Storage**.
2. Click **Execute**.

   The amount of space available for the XML audio configuration file displays with the amount of space used by the file.

Show DRI Parameters

The Show DRI Parameters page displays the configured Diction Rule Implementation (DRI) information.

The information displayed on this page is set on the *Configure DRI Parameters* page.

To view DRI Configuration:

1. Click **Configuration** > **Media Storage Management** > **Show DRI Parameters**.

   The Show DRI Parameters page displays.
2. Select the **DRI Language ID**. If you want to view information for all DRI language ID, select all.

3. Click **Execute**.

   The Output Messages: box displays the configured DRI information.

Delete Recorded Clips

On the Delete Recorded Clips page, you can remove all recorded media clips from the Containerized Decomposed Media Server.

To remove all recorded clips from the Containerized Decomposed Media Server:

1. Click **Configuration** > **Media Storage Management** > **Delete Recorded Clips**.
2. Click **Execute**.

   All transient recorded clips are removed from the Containerized Decomposed Media Server.

Configure Audio Segments

The audio segment configuration file is also referred to as the sets and variables file. This file maps sets and logical clip names onto actual audio clips, as described in the R*adisys Media Server Sets and Variables Interface Reference*.

On the Configure Audio Segments page, you can install the sets and variables file also referred to as an audio segment configuration file, or restore the file from a backup. The file is placed on a file server and then downloaded to the Containerized Decomposed Media Server through SFTP. When you install a new audio segment configuration file, the previous file is overwritten.

For more information about the file map sets and logical clip names onto actual audio clips, see *Sets and Variables Interface Reference*.

NOTE: Installing or restoring the audio segment configuration file can take up to 10 minutes, depending on the file size.

For more information about backing up the sets and variables file, see *Backup Audio Segment Configuration*.

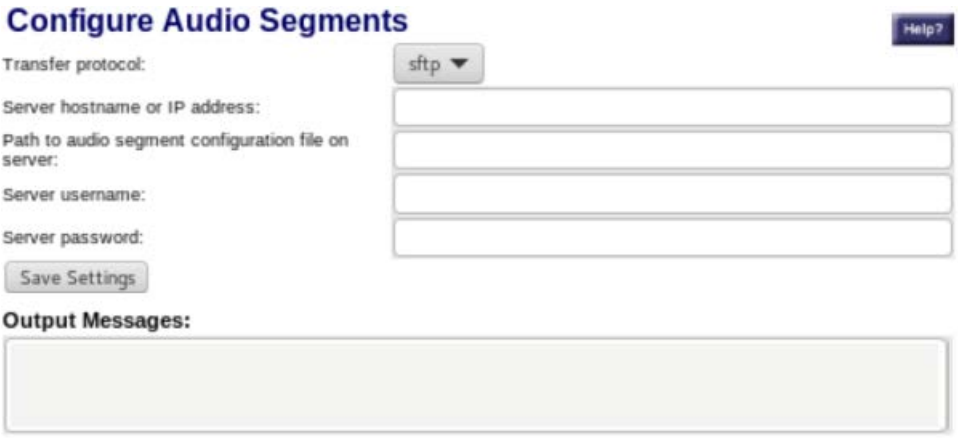
The following table shows the information you must provide to use SFTP to download the audio segment file from a file server.

Table 75. File Transfer Information—Installing the Audio Segments File Settings

Option	Description
Transfer protocol	The transfer protocol to be used in communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. If you are using DNS, you can use the hostname. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to audio segment configuration file on server	The absolute path to audio segment configuration file on the file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	User name configured on the file server, up to 128 characters.
Server password	Password configured on the file server, up to 128 characters.

To install or restore the audio segment configuration file:

1. Ensure that SFTP is running on the file server, and that its root directory is set. The file server must be on the same subnet as the Containerized Decomposed Media Server.
2. Click **Configuration** > **Media Storage Management** > **Configure Audio Segments**.



3. Enter the information described in the above table.:
4. Click **Save Settings**.

   The Containerized Decomposed Media Server starts using the new sets and variables file when the download is complete.

   Confirmation message is displayed in the **Output Messages:** box.

Backup Audio Segment Configuration

On the Backup Audio Segment Configuration page, you can back up the audio segment configuration to a file on an external server through SFTP or HTTP (Web download). If needed, you can then restore the audio segment configuration from the file.

When you back up the audio segment configuration, the previous backup of the configuration file is overwritten. To maintain more than one backup, copy the file to another location or rename it.

To restore audio segment configuration from a backup file, use the procedure given in *Configure Audio Segments on page 340*.

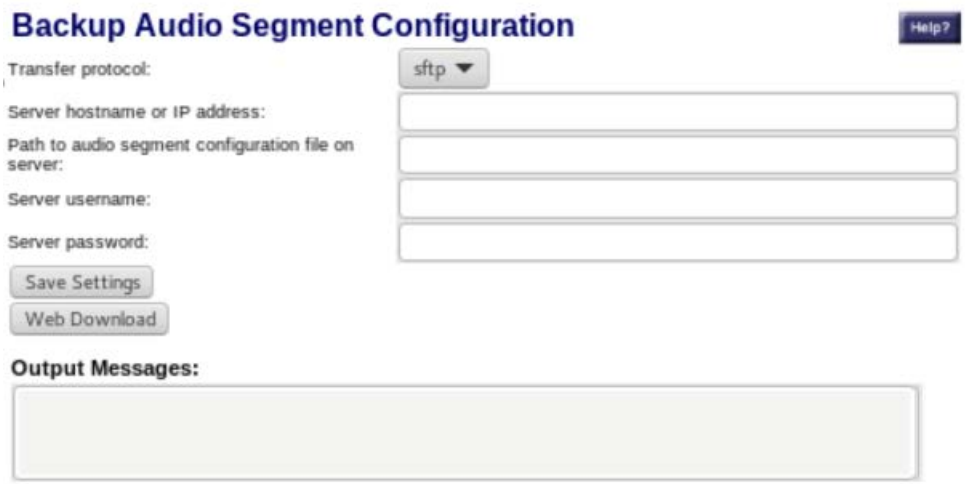
The following table shows the information you must provide to use SFTP to back up the audio segment file to a file server. This information is not needed for a Web download.

Table 76. File Transfer Information—Backing Up the Audio Segments File Settings

Option	Description
Transfer protocol	The transfer protocol to be used in communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	IP address of the file server. If you are using DNS, you can use the hostname. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to audio segment configuration file on server	The absolute path to the audio segment configuration file on server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	User name configured on the file server, up to 128 characters.
Server password	Password configured on the file server, up to 128 characters.

To back up an audio segment configuration file:

1. Click **Configuration** > **Media Storage Management** > **Backup Audio Segment Configuration**.



2. Enter the required backup audio segment configuration settings described in the above table.
3. Click **Save Settings** to backup the file onto the file server.

   Confirmation message is displayed in the **Output Messages:** box.
4. Click **Web Download** to download the backup file using HTTP through your Web browser.

   For a Web download, use the pop-up window to save the backup file.

Retrieve Audio Segment Errors

The Containerized Decomposed Media Server generates an audio segment parse file that records errors that occurred when the system attempted to parse the XML sets and variables file. You can retrieve this file and store it through SFTP or HTTP (Web download) on an external server and then view it with a text editor.

The following table shows the information you must provide to use SFTP to post the audio segment file to a file server. This information is not needed for a Web download.

Table 77. File Transfer Information—Retrieving Audio Segments Errors Files

Option	Description
Transfer protocol	The transfer protocol to be used in communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. If you are using DNS, you can use the hostname. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to audio segment error file on server	The absolute path to audio segment error file on the file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	User name configured on the file server. Supported values are strings of up to 128 characters.
Server password	Password configured on the file server. Supported values are strings of up to 128 characters.

To save the error file on a file server:

1. Click **Configuration** > **Media Storage Management** > **Retrieve Audio Segment Errors**.

2. Enter the file transfer information to retrieve audio segment errors settings described in the above table.
3. Click **Save Settings** to post the errors file to the file server.

   Confirmation message is displayed in the **Output Messages:** box.
4. Click **Web Download** to download the backup file using HTTP through your Web browser.

   For a Web download, use the pop-up window to save the errors file.

Configure Local Persistent Recording Path

The Configure Local Persistent Recording Path page enables you to configure the local directory path for persistent clip recording in the Containerized Decomposed Media Server.

The following table shows the local persistent recording path information that can be configured.

Table 78. Local Persistent Recording Path Information

Value	Description
Persistent Clip Path	Indicates the local directory path for persistent clip recording. Valid values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** • Do not begin the name with "#" or "~". • Pathname must start and end with /.

NOTE:

- If the configured path is other than */var/opt/swms/clips* or any of its sub-directory you must manually modify the directory owner to **admin** user.
- Ensure that permission of the provisioned directory and sub-directories (*/var/opt/swms/clips/persistent/provisioned*) must be 755 and the permission of the clip files must be 644.

To configure local persistent recording path settings:

1. Click **Configuration** > **Media Storage Management** > **Configure Local Persistent Recording Path.**

   The Configure Local Persistent Recording Path page displays.

2. Set the **Persistent Clip Path**.

   IMPORTANT! If the configured path in the **Persistent Clip Path** field is same or superset of transient or provisioned clips, the recorded clip behavior is same as provisioned or transient clips.

3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.

4. Optionally, click **Reset Fields** to reset the changes made to the previous values.

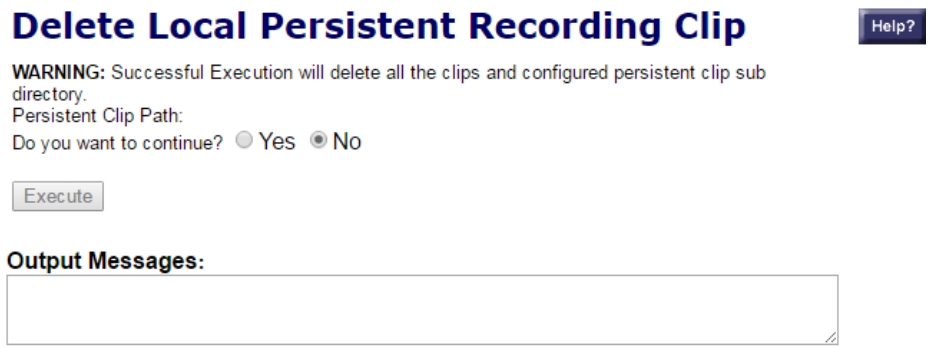
Delete Local Persistent Recording Clip

The Delete Local Persistent Recording Clip page enables you to delete all the persistent clips from the configured persistent clip directory.

To delete local persistent recording clip:

1. Click **Configuration** > **Media Storage Management** > **Delete Local Persistent Recording Clip.**

   The Delete Local Persistent Recording Clip page displays.



2. Select **Yes** for the warning message to enable **Execute**, else select **No**. By default it is set to **No**.
3. Click **Execute**.

   Deletes all the clips and the configured persistent clip sub directory from the Containerized Decomposed Media Server.

   Confirmation message is displayed in the **Output Messages:** box.

Announcement Lab

The AnnLab page (AnnLab manager) is a web interface to provision, process, and manage the media clip requests. From AnnLab page, you can manage the repository clients, announcements (media files), and directories using the AnnLab manager. You can perform a number of operations based on the access rights.

NOTE:

- When an AnnLab operation such as bulk clip provisioning is in-progress, the Containerized Decomposed Media Server Web GUI session may timeout due to idle timeout interval (default is 15 minutes). To prevent this, you must increase the Containerized Decomposed Media Server Web GUI session timeout interval by configuring the **Inactivity time** in the *Configure Web Interface* Web GUI page.
- To access AnnLab GUI, the Containerized Decomposed Media Server Web GUI must be opened with the nodePortIp mentioned in the *values.yaml* file.

Containerized Decomposed Media Server AnnLab

The Containerized Decomposed Media Server supports AnnLab for provisioning and transcoding the media clips. The AnnLab consists of the AnnLab server and AnnLab client. The AnnLab server responds to the incoming requests from the AnnLab clients through the AnnLab manager (a web interface).

- **AnnLab server.** This module runs as a container within the OAMP pod. The user is connected to the AnnLab server using the management interface floating IP. It provides the Web GUI and REST API access for the user to load the clips onto the OAMP PVC storage. When the user provisions the clip, the AnnLab server uploads the clip to the PVC storage. The AnnLab server creates and manages the clusters, Virtual File System (VFS), folders, and clips, and manages bulk upload, clip play, and audit functionalities.

  The AnnLab server manages the media file repository and database that store the metadata about the media files. The media files are replicated to the AnnLab clients using the **rsync** application. **rsync** is a utility for transferring and synchronizing the files across computer systems, by checking the timestamp and size of files.
- **AnnLab client.** This module runs on the AnnLab client container within the OAMP pod. During the start-up, it syncs the provisioned clips from the AnnLab server to the AnnLab client PVC. This AnnLab PVC is mounted on all MRFP pods. Any change in the provisioned clips is updated in the AnnLab client container.

Mass Provisioning

Mass provisioning is the process of uploading bulk media files into the repository server through a single command. The bulk media files are sent in .zip format on the repository server. The ZIP file contains the following files.

- **Excel description file.** This file contains the description of media files present in the .zip file. This file is mandatory and the name of the file is **mfgm.xls**. Excel file templates consist the following fields.
  - **Source file name.** Optional field. Provides the source file name. For example, *AudibleRing.wav*.
  - **Destination file name.** Mandatory field. Provides the absolute path from the cluster name. This field contains the directories and sub-directories that are created automatically under the target directory selected in the Web GUI during the import operation. For example, *AudibleRing.wav.*
  - **Media type.** Mandatory field. Provides the Multipurpose Internet Mail Extensions (MIME) types. For example, audio/g.711.
  - **Description field.** Optional field. Provides the target directory automatically created during the import operation. The directory is created in the VFS source directory from where the import operation is launched. For example, Test1.
  - **File version.** Mandatory field. Provides the version number of the file. For example, 0.
  - **File creation date.** Optional field. Provides the file creation date and time in *DD/MM/YY* and hh-mm in 24 hour format.
  - **Availability date.** Optional field. Provides the file availability date and time in *DD MM YYYY* and hh mm in 24 hour format followed by file permission.
- **Media files.** The media files are the announcement files present in the .zip.

To import bulk clips into the repository server, perform the following procedure.

1. Select the target directory from the **File List**.
2. Click **Import Archive** to archive the media files.

   The Import Zip Archive dialog displays.
3. Click **Attach** to browse and select the .zip on the Containerized Decomposed Media Server.

   NOTE: The .zip file must include the **Excel description file** (*mfgm.xls*) and **media files**.
4. Click **OK**.

The media files are uploaded.

Virtual File System Management

A Virtual File System (VFS) is a set of files structured using directories. Each file and directory of the VFS has a corresponding physical file or directory in the AnnLab server file system (host operating system). AnnLab server also stores additional information about the files in the VFS database.

Announcements (media files) are stored in a structured way using directories. A media file has an associated Multipurpose Internet Mail Extensions (MIME) type, which represents the coding algorithm used to generate the media files. Using VFS, you can create, rename, or delete the directories or announcements (media files).

Audit

The audit feature finds inconsistencies between the AnnLab server and AnnLab client such as inconsistencies between the VFS and database.

Inconsistencies are found in the audit if,

- any version of the file is missing or corrupted from the disk
- any version and its replications are missing from the database
- a folder is missing from the database or file system
- the dimension of the file is different in the client and server

To resolve inconsistencies, perform the following procedure.

1. Select **Virtual File System** from the **File List**.
2. Click **Audit**.

   The INCONSISTENCIES STATUS dialog displays.
3. Click **Resolve inconsistencies**.

   Inconsistencies issues are resolved and the AUDIT FINISHED dialog displays.

NOTE: If any data is missing from the database, it is considered as database corruption and is not resolved by the audit feature.

AnnLab Prerequisites

Following are the prerequisites to access the AnnLab page.

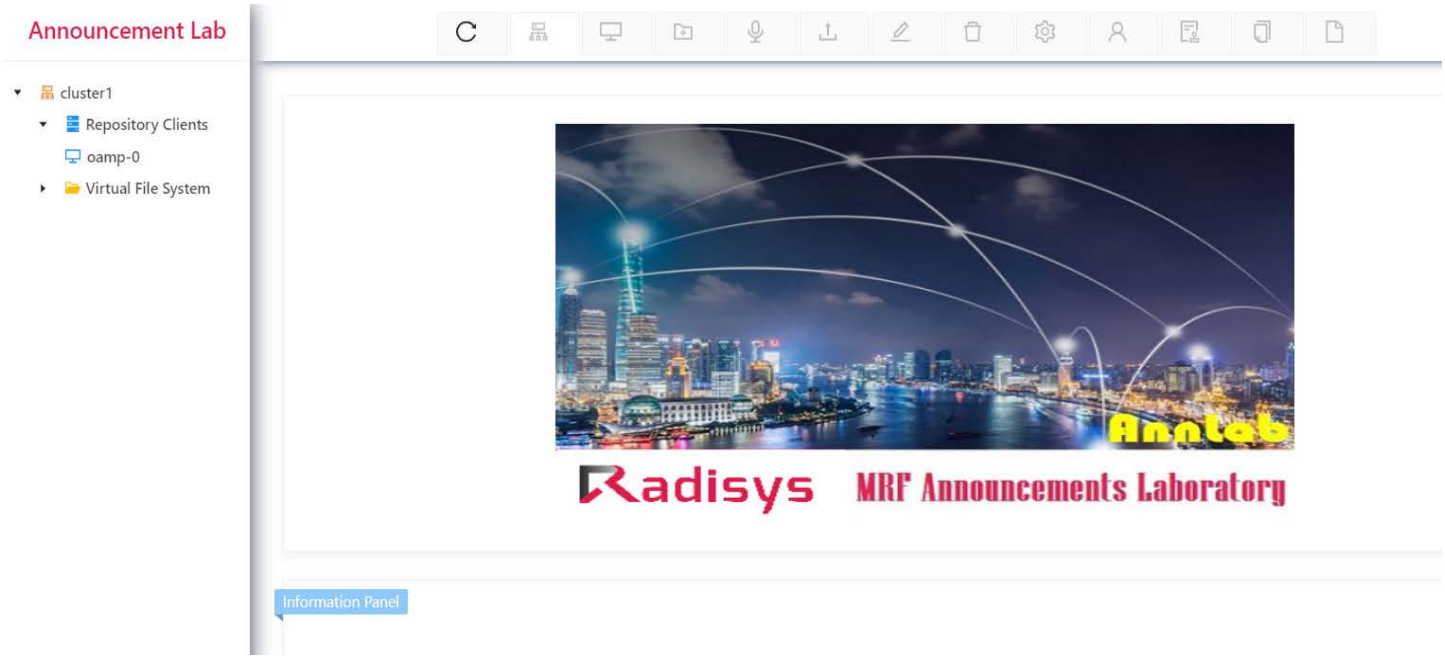
- Browsers supported
  - Internet Explorer version 11.0.49 or higher
  - Firefox version 43.0.1 to 52.0

To access Announcement Lab:

1. Click **Configuration** > **Media Storage Management** > **Announcement Lab**.

   The Announcement Lab page displays.

Figure 27. Announcement Lab GUI



The AnnLab page has the following components.

- **File List.** File list displays the list of media files and folders in the selected directory.
- **Information Panel.** Information panel displays useful information about the executed commands such as success messages, errors, and warnings.
- **Repository Client Status.** Repository client status icon indicates the repository client's content synchronization status.

NOTE: The Java Applet in the AnnLab GUI is deprecated and the AnnLab GUI has been enhanced for better usability.

2. Perform the Announcement Lab operations as per the following table.

Table 79. AnnLab Toolbar and Operations

Toolbar	Description
	Creates a new cluster. ***NOTE:*** Not supported in this release.
	Creates a new repository client in the current cluster. Click **New Repository Client**. Enter the new repository client in *New Repository Client* dialog, enter the name and hostname, and click **Save**. The new repository client is created and displayed in the tree view under the cluster's repository client node.
	Creates a new directory in the current cluster or path. Click **New Directory**. Enter the new directory name in *Add directory* dialog and click **Create**. The new cluster is created and displayed in the tree view.
	Adds a new media file in the current cluster or path. Click **New Media file**. Enter the new media file name, file type and select date in *Add new file* dialog and click **Add**. ***NOTE:*** Only one file is added at a time. The Decomposed Media Server supports audio/g711, audio/g722, audio/g729, audio/amr, audio/pcm, video/3gp, video/mov, audio/awb, video/3g2, and video/qt media files. The new file is created and displayed in the tree view.
	Refreshes the content of AnnLab entities. Click **Refresh** to refresh the content of AnnLab entities.
	Imports the content of a zip archive, which contains the media files. Click **Import Archive** to archive the media files.
	Renames the selected repository client or directory from the tree view. Select the relevant option, click **Rename**, the relevant rename dialog opens, make the necessary changes, and click **Rename**. The selected repository client or directory is renamed in the tree view.
	Deletes the selected repository client or directory from the tree view. Select the relevant option, click **Delete**, the relevant delete dialog opens. Click the **Delete** option to delete the relevant directory or file. The selected repository client or directory is deleted from the tree view.
	Displays the properties of the current entity. You can view the file properties such as file description and file permission using **File Properties** dialog. Click **Properties**, the **File Properties** dialog opens, modify the file description, and click **Save**.
	Displays the user or group management dialog. ***NOTE:*** Not supported in this release.
	Launches the audit dialog for a selected cluster or Virtual File System (VFS). Click **Audit,** the *Audit* dialog opens, click **Perform audit**, click **OK**. The audit result is displayed in the Information Panel.

Toolbar	Description
	Copies the files and folders from one location to another location. Click **Copy,** the *Copy* dialog opens, click **Copy**.
	Pastes the files and folders from one location to another location. Click **Paste,** the *Paste* dialog opens, click **Paste**.

NOTE: Toolbar (except **Refresh** and **Import archive**) is enabled or disabled based on the current context.

The AnnLab is always accessed through HTTPS. If the management interface is enabled with HTTP, the AnnLab server also listens on HTTP. The AnnLab client periodically sends messages on HTTPS to the AnnLab server and synchronizes the repository client. The AnnLab manager displays the selected repository client's status. The following table shows the repository client's status.

Table 80. Repository Client's Status Icon

Repository Client's Status	Description
	Displays the connected status.
	Displays the disconnected status.

NOTE:

If you are switching from HTTP to HTTPS or vice-versa to access the AnnLab GUI, you need to restart the OAMP.

In the OAMP container, restart the OAMP services using the following command.

```
/opt/swms/bin/swms_service_restart.sh
```

Configure Local Root Directory Path

The Configure Local Root Directory Path page enables you to configure the root or base directory path for media files on the Containerized Decomposed Media Server.

The following table shows the local root directory path information that you can configure.

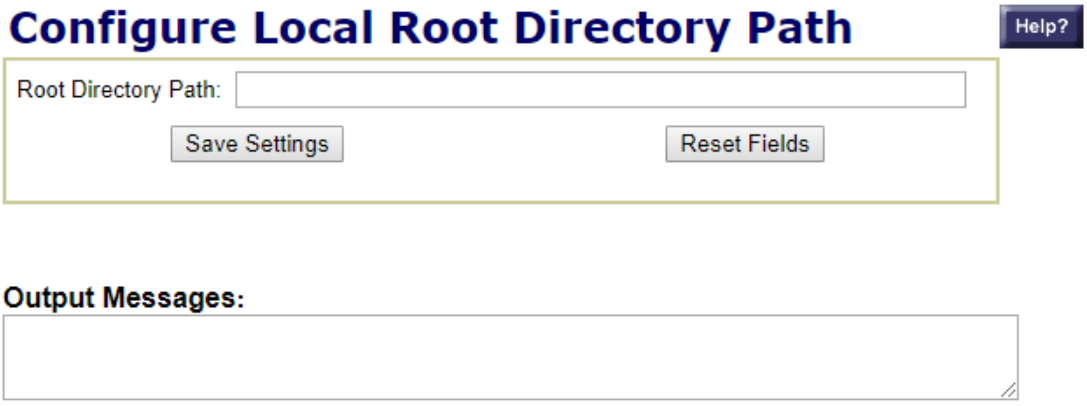
Table 81. Local Root Directory Path Information

Value	Description
Root Directory Path	Indicates the root or base directory path for media files on the Containerized Decomposed Media Server. Valid values are strings of a maximum of 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** • Do not begin the name with "#" or "~". • Pathname must start and end with /. • The Containerized Decomposed Media Server derives the absolute path for the clip translation based on this configuration. For more information on the clip file URI scheme translation, refer to the *SIP Interface Reference* and *MSCML Interface Reference*. • The `swmsadmin` must have the appropriate permissions to ensure announcement or recording requests do not fail

To configure local root directory path settings:

1. Click **Configuration** > **Media Storage Management** > **Configure Local Root Directory Path.**

   The Configure Local Root Directory Path page displays.



2. Set the **Root Directory Path**.
3. Click **Save Settings**.

   The changes take effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previous values.

Configure DRI Parameters

The Configure DRI Parameters page enables you to configure the language specific parameters to configure the DRI libraries.

The information configured on this page is viewed on the *Show DRI Parameters* page.

The Containerized Decomposed Media Server supports Diction Rule Implementation (DRI) to play variable announcements in MSML and MSCML service contexts in addition to sets and vars. However, for a given language, only one method (sets and vars or DRI) is applicable. The DRI takes the precedence over the sets and vars.

In DRI, the variable announcement grammar is specified in the DRI library for a given language and linked to the Containerized Decomposed Media Server. Each language configured in the Containerized Decomposed Media Server is associated with one DRI library. The Containerized Decomposed Media Server allows you to upload a maximum of 32 DRI libraries through the management interface, and only 16 languages are activated at any time for handling variable announcements through the DRI mechanism.

For information on language specific configuration and variable type, refer *Sets & Vars Interface Reference*.

The following table shows the DRI parameters that you can configure.

Table 82. DRI Parameters Settings

Parameter	Description
Node	
Annlab Global Path	Indicates the <*GlobalPath*> used by all interpreters that use a relative path to access theirs announces. The default value is /var/opt/swms/clips/persistent/provisioned/. ***NOTE:*** The folder configured in this parameter must be sub-folder of the */var/opt/swms/clips/persistent/provisioned/* path. If another path is configured, the clips are not played. If the path is null, the Containerized Decomposed Media Server takes the default path. The length of the clip-path must not exceed 256 characters string. Changes to this field require MRFP restart to take effect.
Default Locale	The default locale is used when the locale is not received in the INFO message. The supported values are strings of 0 to 100 characters. ***NOTE:*** The audio segment flow does not impact when default locale value and library are configured to English. Changes to this field require MRFP restart to take effect.
Language ID	Indicates the language ID, where the Containerized Decomposed Media Server provisions the language specific parameters. The supported values are 1 to 16.
Service	Indicates the <*service*> usage, relative to language. The supported values are strings of 0 to 100 characters. The default value is mediaserver. Changes to this field require MRFP restart to take effect.

Table 82. DRI Parameters Settings

Parameter	Description
Customer Ref	Indicates the <*customer*> usage, relative to language. The supported values are strings of 0 to 100 characters. The default value is fixed. Changes to this field require MRFP restart to take effect.
Language	Indicates the <*language*> usage, relative to the DRI library. The supported values are strings of 0 to 100 characters. Example: fr_fr, en_gB, and fr_can ***NOTE:*** This value must be same as the locale received in the INFO message and must be unique. Changes to this field require MRFP restart to take effect.
DRI Library Name	Indicates the DRI library name specific to a language. The library name is case-sensitive. DRI defines the rules of pronunciation that are specific to the language. Notice variables announce are created by the DRI libraries and for the given grammar depending on the language characteristic. The supported values are strings of 0 to 100 characters. ***NOTE:*** The value is one of the library names uploaded using the *Add DRI Library* Web GUI page. Changes to this field require MRFP restart to take effect.
Format Date	Indicates the default subtype format for date. The supported value is an integer from 0 to 65535. The default value is 0. Changes to this field require MRFP restart to take effect.
Format Integer	Indicates the default subtype format for integer. The supported value is an integer from 0 to 65535. The default value is 0. Changes to this field require MRFP restart to take effect.
Format Digits	Indicates the default subtype format for digits. The supported value is an integer from 0 to 65535. The default value is 0. Changes to this field require MRFP restart to take effect.
Format Price	Indicates the default subtype format for price. The supported value is an integer from 0 to 65535. The default value is 0. Changes to this field require MRFP restart to take effect.
Format Time	Indicates the default time format applied to DRI. Applicable when variable subtype is not available. The supported value is an integer from 0 to 65535. The default value is 9. Changes to this field require MRFP restart to take effect.
Format Time 12	Indicates the default time format applied to DRI. Applicable when variable subtype is t12. The supported value is an integer from 0 to 65535. The default value is 2591. Changes to this field require MRFP restart to take effect.
Format Time 24	Indicates the default time format applied to DRI. Applicable when variable subtype is t24. The supported value is an integer from 0 to 65535. The default value is 2059. Changes to this field require MRFP restart to take effect.

Table 82. DRI Parameters Settings

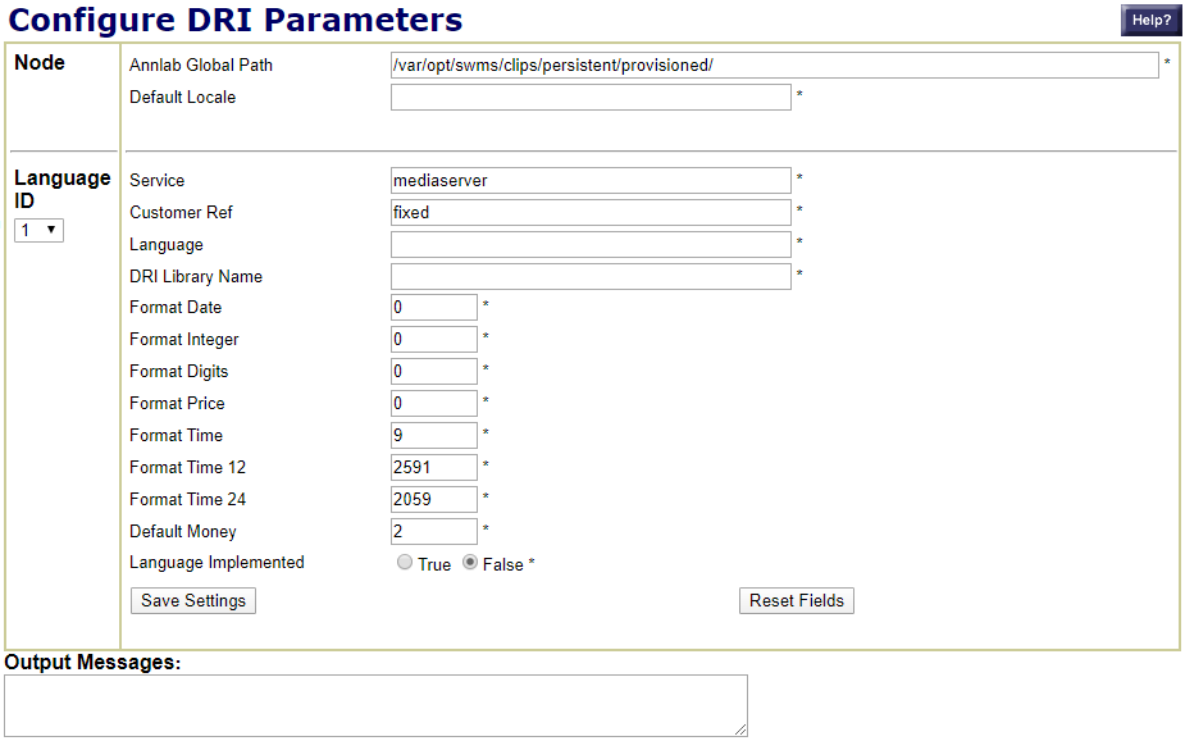
Parameter	Description
Default Money	Indicates the default money format specific to each language. The supported value is an integer from 0 to 65535. The default value is 2. The default value for money mapping is as follows: • EURO - 0 • POUND - 3 • RIAL - 50 • USD - 2 Changes to this field require MRFP restart to take effect.
Language Implemented	Indicates whether the corresponding DRI library is initialized or not. The supported value are: • **True.** The Containerized Decomposed Media Server initializes the DRI. • **False.** The Containerized Decomposed Media Server does not initialize the DRI. The default value is False. Changes to this field require MRFP restart to take effect.

NOTE: Except **Annlab Global Path** and **Default Locale** parameters, all other parameters are specific to language.

To configure DRI information:

1. Click **Configuration** > **Media Storage Management** > **Configure DRI Parameters**.

   The Configure DRI Parameters page displays.



2. Enter the DRI information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Add DRI Library

The Add DRI Library page allows you to upload the Diction Rule Implementation (DRI) libraries.

The following table shows the add DRI library parameters that you can configure.

Table 83. Add DRI Library Settings

Option	Description
DRI file identifier	Alphanumeric name or numeric index of the DRI file. The maximum length of the DRI file identifier is 240 characters.
Transfer protocol	The transfer protocol to be used in communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address in dotted quad format for IPv4, or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of a maximum of 80 characters. Allowed set of characters is: • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to file on remote server	The path of the DRI file on the remote file server. The supported values are strings of a maximum of 128 characters. Allowed set of characters is: • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of a maximum of 128 characters.
Server password	The password configured on the file server. The supported values are strings of a maximum of 128 characters.

To add the DRI Library:

1. Click **Configuration** > **Media Storage Management** > **Add DRI Library**.

   The Add DRI Library page displays.

2. Enter the information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.

Delete DRI Library

The Delete DRI Library page allows you to delete a configured Diction Rule Implementation (DRI) library from the Containerized Decomposed Media Server.

To remove a DRI Library:

1. Click **Configuration** > **Media Storage Management** > **Delete DRI Library**.

2. Enter the DRI file identifier that you want to remove.

   The supported values for **DRI file Identifier** are strings of a maximum of 240 characters.
3. Click **Execute**.

   The specified DRI library is deleted from the Containerized Decomposed Media Server.

   Confirmation message is displayed in the **Output Messages:** box.

List DRI Library

The List DRI Library page allows you to list the configured Diction Rule Implementation (DRI) libraries.

To list a DRI Library:

1. Click **Configuration** > **Media Storage Management** > **List DRI Library**.

2. Enter the **DRI file Identifier** that you want to list.

   The supported values for **DRI file Identifier** are strings of a maximum of 240 characters.

   NOTE: If the **DRI file Identifier** is null, the Containerized Decomposed Media Server lists all the DRI library or individual DRI library. That is when you provide a string or sub-string in the **DRI file Identifier**, the Containerized Decomposed Media Server list all the libraries matching with that string or sub-string.

3. Click **Execute**. Changes take effect immediately.

   Information for the specified DRI library is displayed in the **Output Messages:** box.

Network Management

The Network Management option of the Configuration screen allows you to configure the Containerized Decomposed Media Servers network settings.

Show ToS/Traffic Class

You can view the Quality of Service (QoS) values that are set for various kinds of outgoing packets, in the IPv4 header Type of Service (ToS) byte and IPv6 header Traffic Class.

The following table shows the semantics for RFC 2474 6-bit DSCP values, you are required to configure equivalent ToS to decimal values from 0 to 255.

Table 84. RFC 2474 DSCP Values for the DiffServe Field

DSCP [Binary]	DSCP [Decimal]	Drop Rate	Meaning	Configure ToS to[a]:
101 110xx	46	N/A	Expedited forwarding (EF)	184
000 000 xx	0	N/A	Default: Best-effort traffic	0
001 010 xx	10	Low	Assured forwarding (AF) 11	40
001 100 xx	12	Medium	Assured forwarding (AF) 12	48
001 110 xx	14	High	Assured forwarding (AF) 13	56
010 010 xx	18	Low	Assured forwarding (AF) 21	72
010 100 xx	20	Medium	Assured forwarding (AF) 22	80
010 110 xx	22	High	Assured forwarding (AF) 23	88
011 010 xx	26	Low	Assured forwarding (AF) 31	104
011 100 xx	28	Medium	Assured forwarding (AF) 32	112
011 110 xx	30	High	Assured forwarding (AF) 33	120
100 000 xx	32	N/A	Class Selector (CS) 4	128
100 010 xx	34	Low	Assured forwarding (AF) 41	136
100 100 xx	36	Medium	Assured forwarding (AF) 42	144
100 110 xx	38	High	Assured forwarding (AF) 43	152

[a] This value sets the two least significant bits to zero. Different settings of the two least significant bits are equivalent for non-media traffic. For example, in the first row, configuring the ToS/Traffic Class byte to a decimal value between 184 to 187 sets the DSCP for non-media traffic to “101110” (46). Other settings of these bits might affect particular networks’ prioritizing of media traffic.

To show ToS byte/Traffic Class configuration:

1. Click **Configuration**> **Network Management** > **Show ToS/Traffic Class**.
   The Show ToS/Traffic Class page displays.
2. Click **Execute**.

   Quality of Service information displays in the **Output Messages:** box.

Configure ToS/Traffic Class

On the Configure ToS/Traffic Class page, you can set Quality of Service (QoS) values for outgoing traffic in the IPv4 header Type of Service (ToS) byte and IPv6 header Traffic Class.

You can specify QoS settings when the Containerized Decomposed Media Server has already been configured with its network information.

Quality of service (QoS) can be used for specifying forwarding behavior of a network for packets to allow classification of traffic into service classes, and traffic conditioning such as metering, policing, and shaping.

The Containerized Decomposed Media Server does not itself make any QoS forwarding decisions when transmitting packets. However, the Containerized Decomposed Media Server can write QoS information, for many types of egressing traffic, into the IPv4 header Type of Service (ToS) byte and the IPv6 header Traffic Class:

- Management
- Control
- Audio
- Video
- HTTP media
- Fax
- SIP ETS prioritized calls
- SIP WPS prioritized calls
- Text media
- MSRP media

For media traffic, the Containerized Decomposed Media Server supports rewriting the entire ToS/Traffic Class byte. This is consistent with setting RFC 791 3-bit IP precedence, RFC 1349 4-bit ToS values, or setting 6-bit RFC 2474 DiffServe Code Point (DSCP) values. For non-media traffic, the Containerized Decomposed Media Server supports setting 6-bit RFC 2474 DiffServe Code Point (DSCP) values of the ToS/Traffic Class byte. To provide maximum flexibility in QoS deployments, the Containerized Decomposed Media Server is lenient with respect to QoS semantics: values are not validated against any particular semantic. The Containerized Decomposed Media Server sets the default ToS value (0x00) for egress NFS traffic associated with port or conference announcement.

The Containerized Decomposed Media Server uses the **Default UDP Control** value for DSCP while resolving DNS query over UDP, on both IPv4 and IPv6 address types. Similarly, the Containerized Decomposed Media Server uses the **Default TCP Control** value for DSCP while resolving DNS query over TCP on both IPv4 and IPv6 address types.

For SIP messages in priority calls over UDP, the Containerized Decomposed Media Server uses the values in DSCP as per namespace (ets or wps) in the `Resource-Priority` header and in the non-priority calls over UDP, the Containerized Decomposed Media Server uses the **Default UDP Control** value for DSCP. However, the Containerized Decomposed Media Server uses **Default TCP Control** value for DSCP in SIP messages regardless of priority or non-priority calls.

The Containerized Decomposed Media Server sets the ToS value for egress HTTP traffic associated with conference announcement or recording service based on configured **Default HTTP Media** value.

The following table shows the semantics for RFC 2474 6-bit DSCP values, however you can configure DSCP decimal values from 0 to 255.

Table 85. RFC 2474 DSCP Values for the DiffServe Field

DSCP [Binary]	DSCP [Decimal]	Drop Rate	Meaning	Configure ToS to[a]:
101 110xx	46	N/A	Expedited forwarding (EF)	184
000 000 xx	0	N/A	Default: Best-effort traffic	0
001 010 xx	10	Low	Assured forwarding (AF) 11	40
001 100 xx	12	Medium	Assured forwarding (AF) 12	48
001 110 xx	14	High	Assured forwarding (AF) 13	56
010 010 xx	18	Low	Assured forwarding (AF) 21	72
010 100 xx	20	Medium	Assured forwarding (AF) 22	80
010 110 xx	22	High	Assured forwarding (AF) 23	88

Table 85. RFC 2474 DSCP Values for the DiffServe Field

DSCP [Binary]	DSCP [Decimal]	Drop Rate	Meaning	Configure ToS to[a]:
011 010 xx	26	Low	Assured forwarding (AF) 31	104
011 100 xx	28	Medium	Assured forwarding (AF) 32	112
011 110 xx	30	High	Assured forwarding (AF) 33	120
100 000 xx	32	N/A	Class Selector (CS) 4	128
100 010 xx	34	Low	Assured forwarding (AF) 41	136
100 100 xx	36	Medium	Assured forwarding (AF) 42	144
100 110 xx	38	High	Assured forwarding (AF) 43	152

[a] This value sets the two least significant bits to zero. Different settings of the two least significant bits are equivalent for non-media traffic. For example, in the first row, configuring the ToS/Traffic Class byte to a decimal value between 184 to 187 sets the DSCP for non-media traffic to “101110” (46). Other settings of these bits might affect particular networks’ prioritizing of media traffic.

The following table shows the semantics for RFC 1349 4-bit ToS field values.

Table 86. RFC 1349 Values for the ToS Field

TOS [Binary]	TOS [Decimal]	Meaning	Configure ToS to[a]:
xxx1000x	8	Minimize delay	16
xxx0100x	4	Maximize throughput	8
xxx0010x	2	Maximize reliability	4
xxx0001x	1	Minimize monetary cost	2
xxx0000x	0	Normal service	0

[a] This value sets the least significant bit and three most significant bits to zero. Other settings of these bits might affect particular networks’ prioritizing of traffic. RFC 1349 is supported only for media traffic.

The following table shows the semantics for RFC 791 3-bit IP precedence field values.

Table 87. RFC 791 Values for the IP Precedence Field

Precedence [Binary]	Precedence [Decimal]	Meaning	Configure ToS to[a]:
000xxxxx	0	Routine	0
001xxxxx	1	Priority	32

Table 87. RFC 791 Values for the IP Precedence Field

Precedence [Binary]	Precedence [Decimal]	Meaning	Configure ToS to[a]:
011xxxxx	3	Flash	96
100xxxxx	4	Flash Override	128
101xxxxx	5	Critical	160

[a] This value sets the five lower bits to zero. Different settings of the two least significant bits are equivalent for non-media traffic. For example, in the first row, configuring the ToS/Traffic Class byte to a decimal value between 0 to 3 sets the DSCP for non-media traffic to “000” (0). Other settings of these bits might affect particular networks’ prioritizing of media traffic.

The following table shows QoS information you can configure.

Table 88. QoS Information Required

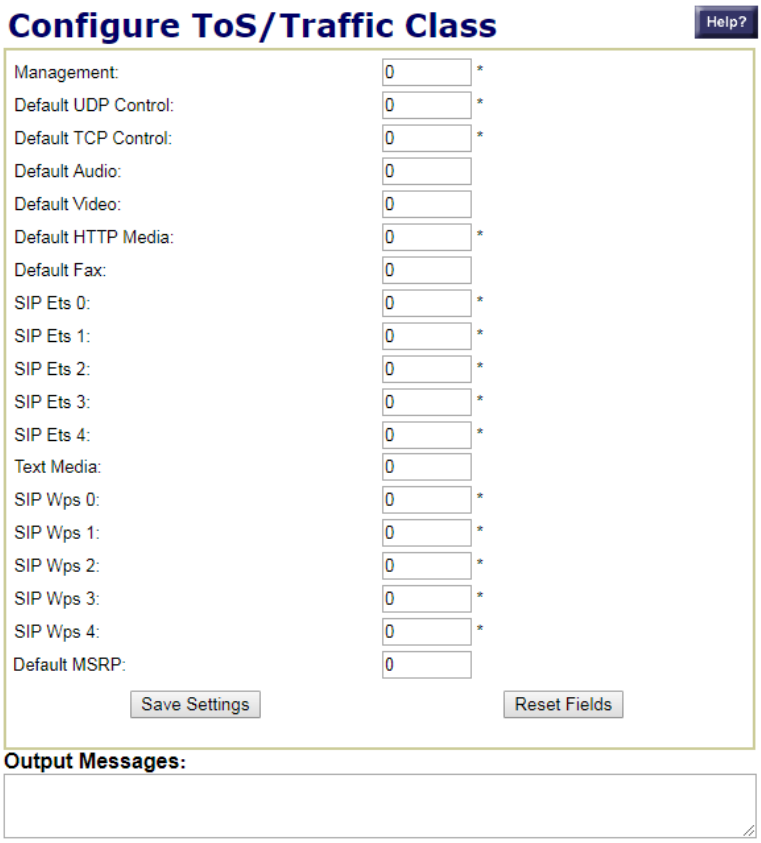
Option	Description
Management	Sets the QoS information for outgoing management packets. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field require an OAMP pod restart to take effect.
Default UDP Control	Sets the configured control DSCP value for SIP over UDP messages and DNS query over UDP to resolve the SIP FQDN. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
Default TCP Control	Sets the configured control DSCP value for SIP over TCP messages and DNS query over TCP to resolve the SIP FQDN. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
Default Audio	Sets the QoS information for outgoing audio packets in non-prioritized calls. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field take immediate effect.
Default Video	Sets the QoS information for outgoing video packets in non-prioritized calls. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field take immediate effect.
Default HTTP Media	Sets the QoS information for outgoing HTTP media packets in non-prioritized calls. Value ranges from 0 to 255, where 0, specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
Default Fax	Sets the QoS information for outgoing fax packets in non-prioritized calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field take immediate effect.
SIP Ets 0	Sets the QoS information for outgoing control and media packets in ETS priority 0 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Ets 1	Sets the QoS information for outgoing control and media packets in ETS priority 1 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.

Table 88. QoS Information Required

Option	Description
SIP Ets 2	Sets the QoS information for outgoing control and media packets in ETS priority 2 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Ets 3	Sets the QoS information for outgoing control and media packets in ETS priority 3 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Ets 4	Sets the QoS information for outgoing control and media packets in ETS priority 4 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
Text Media	Sets the QoS information for outgoing text media packets in non-prioritized calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field take immediate effect.
SIP Wps 0	Sets the QoS information for outgoing control and media packets in WPS priority 0 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Wps 1	Sets the QoS information for outgoing control and media packets in WPS priority 1 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Wps 2	Sets the QoS information for outgoing control and media packets in WPS priority 2 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Wps 3	Sets the QoS information for outgoing control and media packets in WPS priority 3 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
SIP Wps 4	Sets the QoS information for outgoing control and media packets in WPS priority 4 calls. Value ranges from 0 to 255, where, 0 specifies normal service. The default value is 0. Changes to this field require MRFP restart to take effect.
Default MSRP	Sets the QoS information for outgoing Message Session Relay Protocol (MSRP) media packets in non-prioritized calls. Value ranges from 0 to 255. The default value is 0. Changes to this field take effect on the next LI group.

To configure Quality of Service information:

1. Click **Configuration** > **Network Management** > **Configure ToS/Traffic Class**.



2. Enter the ToS or traffic class information described in the table above.
3. Click **Save Settings**.

   The changes require a restart to take effect. Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

MRFP Redundancy

You can manage the redundancy on groups of MRFPs.

NOTE: The internal interface must not go down. However, when the internal interface goes down, the switchover happens automatically due to heartbeat loss, and the standby MRFP remains in the fault state. The *Alarm 88: Automatic switchover: <switchover detail>* and *Alarm 83: MRFP redundancy is unavailable for group* are raised. Whenever this issue happens, a reboot of the fault standby MRFP instance is required.

When the MRFP Redundancy option is clicked, it shows the following Web GUI pages.

Show MRFP Redundancy Groups

You can view the configured MRFP redundancy groups. For each redundancy group, the Show MRFP Redundancy Groups page displays the redundancy role, redundancy status, and service mode of each instance in the group.

To view MRFP redundancy group information:

1. Click **Configuration** > **MRFP Redundancy** > **Show MRFP Redundancy Groups**.

   The MRFP redundancy group information displays on the page. This information is automatically refreshed every five seconds.

Manage MRFP Redundancy Groups

You can perform actions associated with MRFP redundancy. You can:

- Create a redundancy group starting with a standalone MRFP
- Add a standalone MRFP to a redundancy group
- Remove an MRFP from a redundancy group
- Force an MRFP in a redundancy group into standby status by rebooting it

  NOTE: You cannot delete an MRFP redundancy group from this page. To delete an MRFP redundancy group, use the Delete MRFP Redundancy Group page.

The information about MRFP redundancy groups can be viewed from the Show MRFP Redundancy Groups page.

To create an MRFP redundancy group:

1. Click **Configuration** > **MRFP Redundancy** > **Manage MRFP Redundancy Groups**.
   If the MRFP is not in the redundancy group, the below Manage MRFP Redundancy Groups page displays, where, you can create a new redundancy group starting with the instance or add an instance to the existing redundancy group.

Instance:	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Group:	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Role:	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Status:	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Service:	In	In	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out

Manage MRFP Redundancy Groups Help?

Instance-RG#	
3	Create new group starting with this Instance: Go Add Instance to group and restart Instance: Go

Output Messages:

If the MRFP is in the Redundancy Group, the below Manage MRFP Redundancy Groups page displays, where, you can remove the MRFP instance from the existing redundancy group or force the instance in the redundancy group to be in the standby state.

Instance:	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Group:	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Role:	Stby	Active	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Status:	Online	Online	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Service:	Out	In	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out

Manage MRFP Redundancy Groups Help?

Instance-RG#	
3-RG1	Remove Instance from group: Go Make Instance the standby and restart Instance: * There will be a temporary loss of redundancy. * Service may be interrupted if standby is offline. Go

Output Messages:

2. Select the MRFP instance to be the first member of the redundancy group from the **Instance-RG#** drop-down list.

   NOTE: The instance must be an out-of-service, standalone MRFP. Use the S*et MRFP Service Mode* Web GUI page to place the instance in-service or out-of-service.

3. Next to **Create new group starting with this Instance**, click **Go**. The instance reboots as the standby.

   The redundancy group is created with the MRFP instance as the first member.

4. The instance is required to be placed back in-service, which is completed by using the *Set MRFP Service Mode* Web GUI page. See *Set MRFP Service Mode on page 217*.

To add instance to an existing redundancy group:

1. Select the MRFP instance number to be the next member of the redundancy group from the **Instance-RG#** drop-down list.
2. In the **Add Instance to group** drop-down list, select the redundancy group to add the instance, and click **Go**.

   NOTE: The instance must be an out-of-service, standalone MRFP. Use the S*et MRFP Service Mode* Web GUI page to place the instance in-service or out-of-service.

   The instance restarts as a member of the selected redundancy group.

3. The instance is required to be placed back in-service, which is completed by using the *Set MRFP Service Mode* Web GUI page. See *Set MRFP Service Mode on page 217*.

Delete MRFP Redundancy Group

The Delete MRFP Redundancy Group page allows you to remove a group that is providing redundancy for MRFPs.

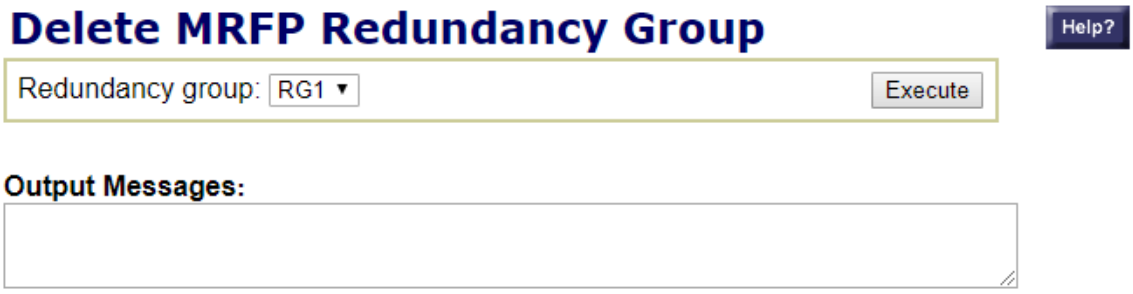
If a redundancy group is deleted, all instances in that group lose redundancy.

The information about MRFP redundancy groups can be viewed from the Show MRFP Redundancy Groups page.

To delete an MRFP redundancy group:

1. Click **Configuration** > **MRFP Redundancy** > **Delete MRFP Redundancy Group**.
   The Delete MRFP Redundancy Group page displays.

Instance:	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Group:	1	1	1	1	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Role:	Active	Active	Active	Active	Active	Stby	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Status:	Online	Online	Online	Online	Online	Online	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Service:	In	In	In	In	In	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out	Out



2. Select the redundancy group you want to delete from the **Redundancy group** drop-down.
3. Click **Execute**.
   The changes take effect immediately.

Web GUI Maintenance

Web GUI Maintenance Options

The Maintenance screen provides options for configuring software version, license information, backup and restore operations, and shutting down or rebooting the Containerized Decomposed Media Server.

Show Software Versions

The Show Software Versions page displays the software version of the MRFC that is installed and running on the Containerized Decomposed Media Server.

To show software version information for Containerized Decomposed Media Server software:

1. Click **Maintenance** > **Show Software Versions**. The Show Software Versions page is displayed.
2. Click **Execute**.

   The **Output Messages:** box displays the version numbers for the current installed and running software applications.

Show License PortLimits

The Show license portlimits page displays the information about the port limits for all the features in the installed license and the count of the bundle licenses provisioned separately for each audio codec.

To show license portlimits information:

1. Click **Maintenance** > **Show License PortLimits**.

   The Show License PortLimits page displays.
2. Click **Execute**.

   The **Output Messages:** box displays the supported features and the corresponding port limits. If license is not installed, an error message `Information not available` is displayed.

   NOTE:

   - If Port limit is Unlimited for a specific feature it displays as unlimited and zero if the feature is not provisioned in the license file.
   - PLC port limit is applicable for codecs G.711 and G.722.

Show License Thresholds

The Show license thresholds page displays the information about the license expiry warning threshold and port limit usage warning threshold configuration.

To show license threshold information:

1. Click **Maintenance** > **Show License Thresholds**.

   The Show License threshold page displays.
2. Click **Execute**.

   The **Output Messages:** box displays the license expiry and port limit warning threshold.

Show Licensing

The Show Licensing page displays the Node ID, the current node license state, license expiry date, and number of licensed MRFP.

To show licensing information for Containerized Decomposed Media Server:

1. Click **Maintenance** > **Show Licensing**.

   The Show Licensing page displays.

   Node ID, the current node license state, license expiry date, and number of licensed MRFP are displayed on the page.

Show Scheduled Backup

The Show Scheduled Backup page displays the existing scheduled backup configurations.

To show scheduled backup configuration:

1. Click **Maintenance** > **Show Scheduled Backup**.

   The Show Scheduled Backup page displays.
2. Select the **Policy** from the drop-down list.

   The supported values are all and from 1 to 5. The default value is **all**.
3. Click **Execute**.

   The **Output Messages:** box displays the existing scheduled backup configurations for the selected policy.

   The information shown on this page is set on the *Configure Scheduled Backup on page 388*.

Configure License Thresholds

The Configure license threshold page enables you to configure license threshold.

The following table shows the information you must provide to configure license threshold.

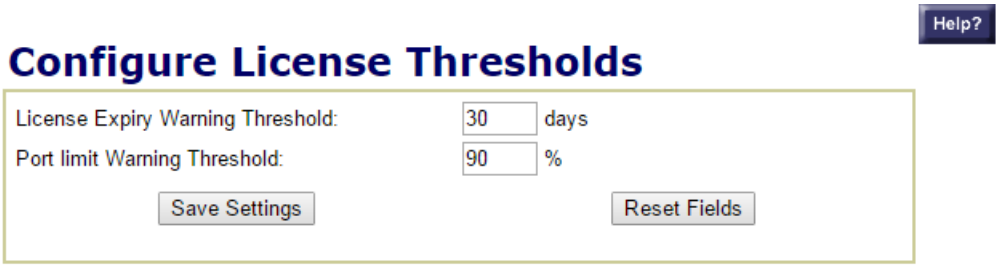
Table 89. License Threshold Information

Value	Description
License Expiry Warning Threshold	The number of days before the expiry date of license, which triggers the License Expiry Warning Alarm (Alarm 154). The supported values are 0 to 30 days. Default value is 30. Setting this value to zero disables the alarm.
Port limit Warning Threshold	The percentage of the block limit of ports, which triggers the Port Limit Warning Alarm (Alarm 156). The supported values are 0 to 90 percentage. This is configured only in multiples of 10. Default value is 90. Setting the value to zero disables the alarm.

To configure license threshold information:

1. Click **Maintenance** > **Configure License Thresholds**.

   The Configure License Threshold page displays.



2. Enter the **License Expiry Warning Threshold** and **Port limit Warning Threshold** values.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure NodeID

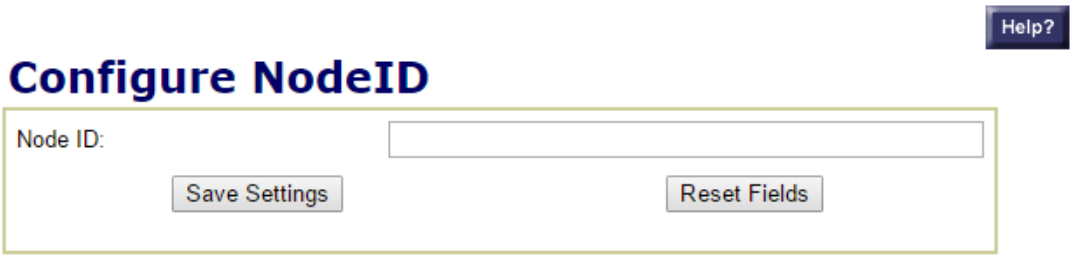
The Configure NodeID page enables you to configure NodeID. When the user provisions the node ID, it overrides the Containerized Decomposed Media Server generated node ID for validation of license file.

NOTE: This feature is applicable when the Containerized Decomposed Media Server operates only in the specific cloud platform.

To configure NodeID information:

1. Click **Maintenance** > **Configure NodeID**.

   The Configure NodeID page displays.



2. Enter the **Node ID** value**.**
3. Click **Save Settings**.

   The changes takes effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Manage Licensing

The Manage Licensing page provides the user the ability to provision a license file.

The following table shows the information you must provide to use SFTP to provision a license from file server.

Table 90. File Transfer Information–Manage Licensing

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters.
Path and name of license file on remote server	The absolute path and name on the remote file server, where the license file is present. The supported values are strings of up to 128 characters. This field cannot be blank.
Server username	The user name configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

To view or change licensing information:

1. Click **Maintenance** > **Manage Licensing**.

   The Manage Licensing page displays.

2. Enter the required manage licensing information described in the above table.
3. Click **Save Settings**.

   The Containerized Decomposed Media Server transfers and validates the license file. If the license is valid, the Containerized Decomposed Media Server provisions the license file. The changes take effect immediately.

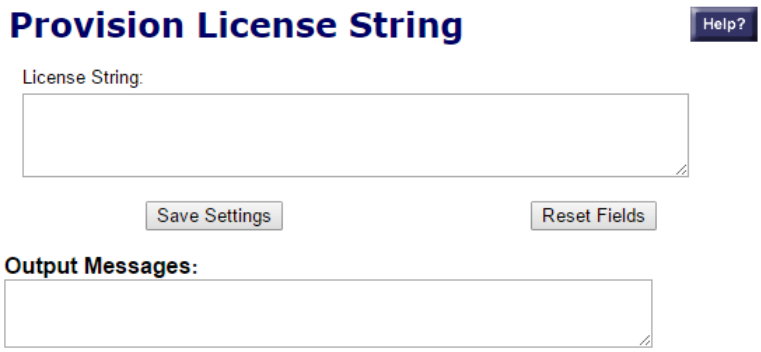
   Confirmation message is displayed in the **Output Messages:** box.

Provision License

The provision license page provides information on the user ability to provision a license string.

To provision the license string:

1. Click **Maintenance** > **Provision License**. The Provision License page displays.



2. Enter the **License String**. The supported values are text strings up to 4096 characters.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Backup Configuration

The Backup Configuration page allows you to back up the configuration of the entire Containerized Decomposed Media Server to a file on a remote file server using SFTP or HTTP (Web download). The configuration is backed up to a file called `backup_config.ms`. You can use this file to restore the Containerized Decomposed Media Server configuration.

For security, this backup does not include the database of locally provisioned users. Backing up and restoring user configuration is managed separately.

For more information about restoring configuration, see *Restore Configuration on page 378*.

NOTE: Audio segment configuration is backed up separately from node configuration. For more information, see *Backup Audio Segment Configuration on page 342*.

The following table shows the information you must provide to use SFTP to post the configuration backup file to a file server. This information is not needed for a Web download.

Table 91. File Transfer Settings–Backup Configuration

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".

Table 91. File Transfer Settings–Backup Configuration

Value	Description
Path to configuration backup file on server	The absolute path on the file server, where the configuration backup file (`backup_config.ms`) is to be saved. Do not include the file name. The supported values are strings of maximum of 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.
Include Hostname	Saves the *backup_config.ms* file in the subfolder that is created with the name of the Containerized Decomposed Media Server hostname. • If this field is checked, the Containerized Decomposed Media Server creates a sub-folder **cfg_backup_<Containerized Decomposed Media Server hostname>** in the path mentioned in the **Path to configuration backup file on server** field and the *back-up_config.ms* file is placed in this subfolder. • If this field is unchecked, the Containerized Decomposed Media Server places the *backup_config.ms* file in the path mentioned in the **Path to configuration backup file on server** field. By default, this field is unchecked. ***NOTE:*** • This feature is not available for the **Web Download** option. • The complete path until the subfolder must be provided for the restore operation. Changes to this field take effect immediately.

To back up the Containerized Decomposed Media Server configuration:

1. Ensure that the file server is running and that its SFTP root directory is set. The file server must be on the same subnet as the Containerized Decomposed Media Server.

2. Click **Maintenance** > **Backup Configuration**.
   The Backup Configuration page displays.

3. For HTTP, click the **Web Download**. For SFTP, enter the file transfer information described in the above table.
4. Click **Save Settings**.

   For a Web download, use the pop-up window to save the configuration file. The backup can take several minutes to complete. Confirmation message is displayed in the **Output Messages:** box.

Restore Configuration

The Restore Configuration page allows you to restore the entire or a part of the configuration of the Containerized Decomposed Media Server from a backup stored on a file server.

When MRFP reboots in the In-Service Configuration Restore operation, this page displays the restore status as follows:

```
Reboot Status: MRFP is rebooting.....
```

To view this message, first verify on the Restore Configuration Web GUI page, thereafter this message is also displayed on all the other Web GUI pages until MRFP reboots.

For more information about creating the backup file, see *Backup Configuration on page 376*.

NOTE: Restoring configuration from a backup server interrupts service.

After decrypting the *backup_Config.ms* file, the network configuration parameters are included as part of the full backup operation. When the **Preserve Data** field is checked in the *Restore Configuration* Web GUI page, the Containerized Decomposed Media Server does not restore the following network configuration from the downloaded database and retains the existing network configuration on the system.

Table 92. backup_Config.ms—Network Configuration

Containerized Decomposed Media Server Web GUI	Network Configuration Parameters
Configure Hostname	Hostname
Configure Network Interfaces	• IPv4 Netmask Interface • IPv6 Prefix Len Interface • Device Name Interface • Vlan ID Interface • Bond #<n>:Dev #1 • Bond #<n>:Dev #2 • Bond MAC Failover Policy Bond • Bond G-ARP/UnsolicitedNACount • Bond Updelay • Management Interface • Control Interface • Media Interface
Configure Ethernet Mode	Connection Mode Interface

The following table shows the information you must provide to use SFTP to restore the Containerized Decomposed Media Server configuration from a backup on a file server. This information is not needed for a Web download.

Table 93. File Transfer Settings–Restore Configuration

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".

Table 93. File Transfer Settings–Restore Configuration

Value	Description
Path to configuration backup file on server	The absolute path on the file server, where the configuration backup file (`backup_config.ms`) is to be saved. Do not include the file name. The supported values are strings of up to 256 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.
Preserve Data	Includes or excludes the network configuration to be preserved during the restore operation. • If this field is checked, the Containerized Decomposed Media Server does not restore the network configuration from the downloaded database and retains the existing network configuration on the system. • If this field is unchecked, the Containerized Decomposed Media Server restores the network configuration from the downloaded database and overrides the network configuration file on the system. By default this field is unchecked. This parameter does not require a reboot to take effect.
Preserve Node ID	Includes or excludes the Node ID to be preserved during the restore operation. • If this field is checked, the Containerized Decomposed Media Server does not restore the Node ID from the downloaded database and retains the existing Node ID on the system. • If this field is unchecked, the Containerized Decomposed Media Server restores the Node ID from the downloaded database and overrides the existing Node ID on the system. By default this field is unchecked. This parameter does not require a reboot to take effect.

NOTE: When the **Password Less Transfer to/from Remote Server** parameter on the *Configure System Security* Web GUI page is enabled, the **Server password** is non-editable.

To restore configuration from a backup:

1. Ensure that the file server is running, and that its SFTP root directory is set. The file server must be on the same subnet as the Containerized Decomposed Media Server.
2. Click **Maintenance** > **Restore Configuration**.

3. Enter the restore configuration information described in the above table.
4. Click **Save Settings**.

   The restore operation takes several minutes to complete. The Containerized Decomposed Media Server automatically reboots after the restore. During that period, the Containerized Decomposed Media Server is unavailable for service. When the restore operation is complete, the message is displayed in the **Output Messages:** box.

Dump Configuration

The Dump Configuration page allows you to download the configuration file of the Containerized Decomposed Media Server in *.csv* format on a remote server.

The following table shows the information you must provide to use SFTP to download the dump configuration file from a backup on a file server. This information is not needed for a Web download.

Table 94. File Transfer Settings - Dump Configuration

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".

Value	Description
Path to config dump file on server	The absolute path on the remote file server, where the configuration dump file is to be saved. Do not include the file name. The supported values are strings of up to 256 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.
Instance number	The instance number of the Containerized Decomposed Media Server. The supported values are 1 and 3 to 22.

To download the dump configuration file:

1. Click **Maintenance > Dump Configuration.**

2. For HTTP, click **Web Download**. For SFTP, enter the file transfer information:
   - Enter the IP address or hostname of the file server.
   - Enter the path to the config dump file.
   - Select the instance number from the drop-down list.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.

Full Backup

The Full Backup page allows you to use SFTP to back up all configurable elements of the Containerized Decomposed Media Server to a file server. The full backup operation includes the output of the backup configuration. This includes:

- All configurations performed through the management interface except web user database.
- The audio segment configuration file (sets and variables file)
- The provisioned license file
- The AnnLab configurations
- The Diction Rule Implementation (DRI) configurations
- The HTTPS keys and certificates

For security, this backup does not include the database of locally provisioned users. Backing up and restoring user configuration are managed separately.

Configuration information and the audio segment configuration file are compressed into a set of backup files before they are transferred.

NOTE: The backup license file is not created if it is not present in the Containerized Decomposed Media Server.

The Containerized Decomposed Media Server creates the following files and directories in the SFTP directory:

Table 95. Backup Files Created during Full Backup

Filename	Description
backupComplete	File indicating that the file backup has completed successfully.
ftp_result.txt	Results of the full backup or restore.
as_config	Directory containing the audio segment configuration file. The name of this file is user-specified when the file is installed.
oamp_config	Directory containing the **backup_config.ms** configuration file.
backup_config.ms	Configuration specified through the Containerized Decomposed Media Server management interface.
license	Directory containing the **SWMS_backup.mslic** license file.
SWMS_backup.mslic	Provisioned license file in the Containerized Decomposed Media Server.
annlab-db	Directory containing the AnnLab database.
annlab-json-file	Directory containing the AnnLab JSON file.
mrfc-config	Directory containing the MRFC configuration file.
annlab-clips	Clips loaded to annlab.
clips	SMIL files are backed up under clips folder.
cert	Directory containing the certificate uploaded through the Containerized Decomposed Media Server management interface. CA certificates and keys are available under this directory.
kwd	Directory containing the keyword detection information.
dri_library	Directory containing the DRI library information.

You can use this feature to back up all configuration data in a single operation, and subsequently audio segment configuration, Containerized Decomposed Media Server configuration, or license file using other backup methods.

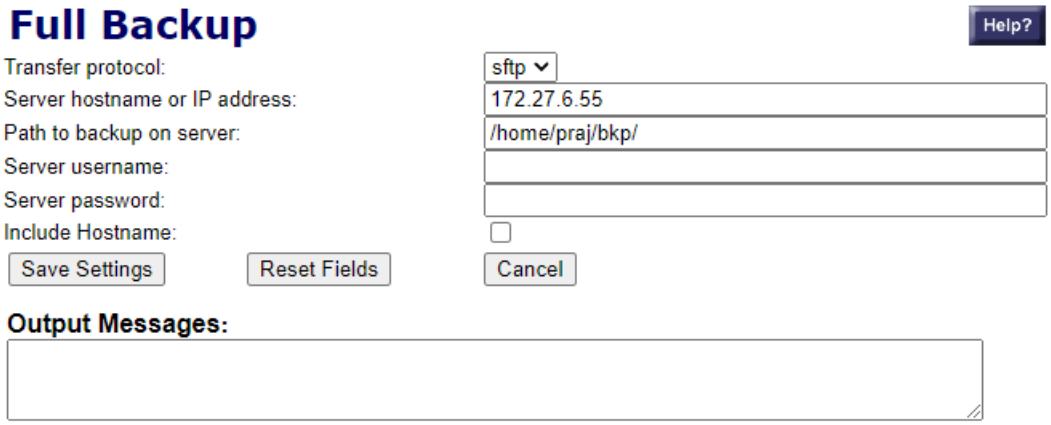
The following table shows the information you must provide to use SFTP to post the full configuration backup file to a file server.

Table 96. File Transfer Information–Full Backup

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to backup on server	The absolute path on the file server, where the full configuration backup file are to be saved. The supported values are strings of maximum of 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank. Multiple periods (".") are supported to delimit the file name from the file extension.
Server username	The user name configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.
Include Hostname	Saves the full backup files in the subfolder that is created with the name of the Containerized Decomposed Media Server hostname. • If this field is checked, the Containerized Decomposed Media Server creates a sub-folder **fbr_backup_<Containerized Decomposed Media Server hostname>** in the path mentioned in the **Path to backup on server** field and the full backup files are placed in this subfolder. • If this field is unchecked, the Containerized Decomposed Media Server places the full backup files in the path mentioned in the **Path to backup on server** field. By default, this field is unchecked. ***NOTE:*** The complete path until the subfolder must be provided for the restore operation. Changes to this field take effect immediately.

To perform a full backup of the Containerized Decomposed Media Server:

1. Click **Maintenance** > **Full Backup**.
   The Full Backup page displays.



2. Enter the required full backup information as described in the above table.
3. Click **Save Settings**.

   Backup takes a few minutes. When the backup is complete, a message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.
5. Click **Cancel** to cancel the backup.

Full Restore

The Full Restore page allows you to use SFTP to restore the Containerized Decomposed Media Server full configuration from a backup previously stored on a file server. This includes:

- Configurations performed through the management interface except web user database.
- The audio segment configuration file (sets and variables file)
- The license file
- The Annlab clips and AnnLab database
- MRFCtrl and AnnLab configuration files
- OAMP configuration files
- The Diction Rule Implementation (DRI) configurations
- The HTTPS keys and certificates

To perform restore, you must have previously performed a complete backup using the Full Backup page. The set of files in this backup must include a valid BackupComplete file.

NOTE: If there is no license file or an invalid license file is present in the backup, the current license configured before the restore operation will not be affected.

After the restore is complete:

- The **result.txt** file on the file server is overwritten with the results of the restore operation.
- The Containerized Decomposed Media Server automatically restarts to guarantee that the restored configuration values take effect.
- The administration and root user configurations are not affected. These accounts are not overwritten and retain the values configured before the restore operation.

The following table shows the information you must provide to use SFTP to restore a full configuration from a backup file on a file server.

Table 97. File Transfer Information–Full Restore

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to backup on server	The absolute path on the file server, where the full configuration backup file are saved. The supported values are strings of a maximum of 240 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank. Multiple periods (“.”) are supported to delimit the file name from the file extension.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

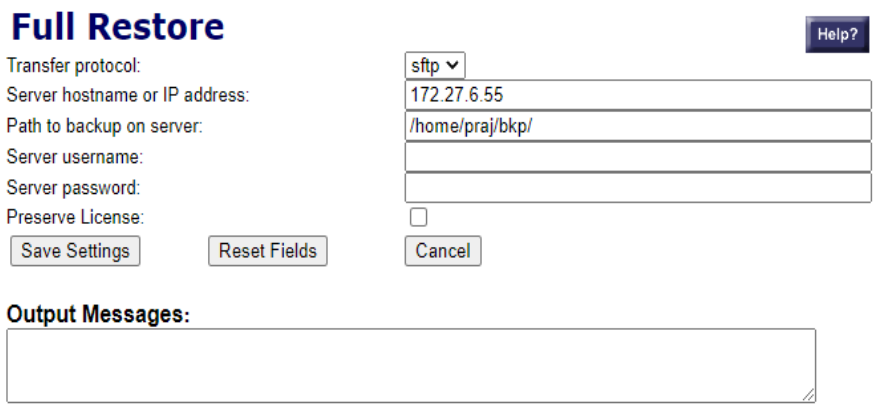
Table 97. File Transfer Information–Full Restore

Value	Description
Preserve Data	Includes or excludes the network configuration to be preserved during the restore operation. • If this field is checked, the Containerized Decomposed Media Server does not restore the network configuration from the downloaded database and retains the existing network configuration on the system. • If this field is unchecked, the Containerized Decomposed Media Server restores the network configuration from the downloaded database and overrides the network configuration file on the system. By default this field is unchecked. This parameter does not require a reboot to take effect.
Preserve License	Includes or excludes the license file to be preserved during the restore operation. • If this field is checked, the Containerized Decomposed Media Server does not restore the license file from the downloaded database and retains the existing license file on the system. • If this field is unchecked, the Containerized Decomposed Media Server restores the license file from the downloaded database and overrides the existing license file on the system. By default this field is unchecked. This parameter does not require a reboot to take effect.

NOTE: When the **Password Less Transfer to/from Remote Server** parameter on the *Configure System Security* Web GUI page is enabled, the **Server password** is non-editable.

To perform a full restore of the Containerized Decomposed Media Server:

1. Ensure that you have a set of backup files from a complete instance backup, including a valid BackupComplete file.
2. Click **Maintenance** > **Full Restore**.
   The Full Restore page displays.



3. Enter the full restore information described in the above table.

4. Click **Save Settings**.

   The restore can take a few minutes. When the restore is complete, a message is displayed in the **Output Messages:** box, and the Containerized Decomposed Media Server reboots so that the restored configuration values can take effect.
5. Click **Cancel** to cancel the full restore.
6. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

NOTE: After full restore, perform audit from the AnnLab GUI, to sync AnnLab clips on all MRFP's.

Configure Scheduled Backup

The Configure Scheduled Backup page allows you to configure the Containerized Decomposed Media Server to perform scheduled backup operations.

The following table shows the information that you can configure.

Table 98. File Transfer Settings–Scheduled Backup Configuration

Value	Description
Policy	The scheduled backup policy. ***NOTE:*** Displays all the policy related parameter fields with previously configured values for the selected policy. The range is from 1 to 5. Default value is 1. Changes to this field take effect immediately.
Transfer Protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server host or IP Address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of a maximum of 80 characters. Changes to this field take effect immediately.
Path to scheduled backup on remote server	The absolute path on the remote file server, where the scheduled configuration backup file is to be saved. Do not include the file name. The supported values are strings of a maximum of 128 characters. This field cannot be blank. Changes to this field take effect immediately.
User name	The username configured on the file server. The supported values are strings of a maximum of 128 characters. Changes to this field take effect immediately.
Password	The password configured on the file server. The supported values are strings of a maximum of 128 characters. Changes to this field take effect immediately.
Schedule Backup	Enables or disables the scheduled backup operation. The supported values are: • **Enabled.** Enables the policy for scheduled backup. • **Disabled.** Disables the policy for scheduled backup. Default value is Disabled. Changes to this field take effect immediately.

Table 98. File Transfer Settings–Scheduled Backup Configuration

Value	Description
Backup Type	The type for backup operation. The supported values are: • **Configuration.** Allows you to back up the configuration of the entire Containerized Decomposed Media Server to a file on a file server. ***NOTE:*** The Containerized Decomposed Media Server creates a subfolder **cfg_backup_<Containerized Decomposed Media Server hostname>** in the path mentioned in the **Path to scheduled backup on remote server** field and the *backup_config.ms* file is placed in this subfolder, when the **Include Hostname** field is enabled in the *Backup Configuration* Web GUI. • **Full.** Allows you to back up all configurable elements of the Containerized Decomposed Media Server through the management interface except web user database, audio segment configuration file, and provisioned license file to a file server. ***NOTE:*** The Containerized Decomposed Media Server creates a subfolder **fbr_backup_<Containerized Decomposed Media Server hostname>** in the path mentioned in the **Path to scheduled backup on remote server** field and the full backup files are is placed in this subfolder, when the **Include Hostname** field is enabled in the *Full Backup* Web GUI. • **User Database.** Allows you to back up the Containerized Decomposed Media Server locally provisioned users and their configuration by saving the user database to a file server. • **Audio Segment File.** Allows you to back up the audio segment configuration to a file on a file server. Default value is Configuration. Changes to this field take effect immediately.
Frequency Type	The re-occurrence pattern of the scheduled backup operation. The supported values are: • **One Time.** There is no re-occurrence of backup operation. • **Daily.** Daily re-occurrence pattern. • **Weekly.** Weekly re-occurrence pattern. • **Monthly.** Monthly re-occurrence pattern. Default value is One Time. Changes to this field take effect immediately.
Start Time(hh-mm)	The start time to trigger the backup operation, represented in 24 hour format. The start time format is *hh-mm*, where, hh is hour from 00 to 23 and mm is minute from 00 to 59. Changes to this field take effect immediately.

Table 98. File Transfer Settings–Scheduled Backup Configuration

Value	Description
Interval	The Containerized Decomposed Media Server allows to configure the interval in terms of days, months, or days of the week to trigger the backup operation. The interval depends on the configured Frequency Type field. • When the selected Frequency Type is Daily, the Containerized Decomposed Media Server allows to configure the interval in terms of days to trigger the backup operation. The range is from 1 to 1000. Default value is 1. For example, if the value is set to 5, the Containerized Decomposed Media Server initiates backup operation on every 5th day, starting from the configured Start Date and Start Time. • When the selected Frequency Type is Monthly, the Containerized Decomposed Media Server allows to configure day of the month to trigger the backup operation. The range is from 1 to 31. Default value is 1. If this value is more than the total number of days in the given month, the Containerized Decomposed Media Server triggers the backup operation on the last day of the month. For example, if Monthly Interval is set to 31 and month in the Start Date is set June, the Containerized Decomposed Media Server triggers backup operation on the 30th day for the June month. • When the selected Frequency Type is Weekly, the Containerized Decomposed Media Server select the days of the week to trigger the backup operation. The supported values are: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday Changes to this field take effect immediately.
Start Date(YYYY-MMM-DD)	Configures the date on which the backup operation is scheduled when the frequency type is One Time. For re-occurring backups, this field specifies the start date. The start date format is *YYYY-MMM-DD*, where, YYYY is the year, MMM is the month, and DD is the day. For example: 2017-Aug-15 Changes to this field take effect immediately.
End Date(YYYY-MMM-DD)	Configures the end date for re-occurring backups. The end date format is *YYYY-MMM-DD*, where, YYYY is the year, MMM is the month, and DD is the day. For example: 2017-Aug-15 ***NOTE:*** This field is not available when the selected Frequency Type is One Time. Changes to this field take effect immediately.

Table 98. File Transfer Settings–Scheduled Backup Configuration

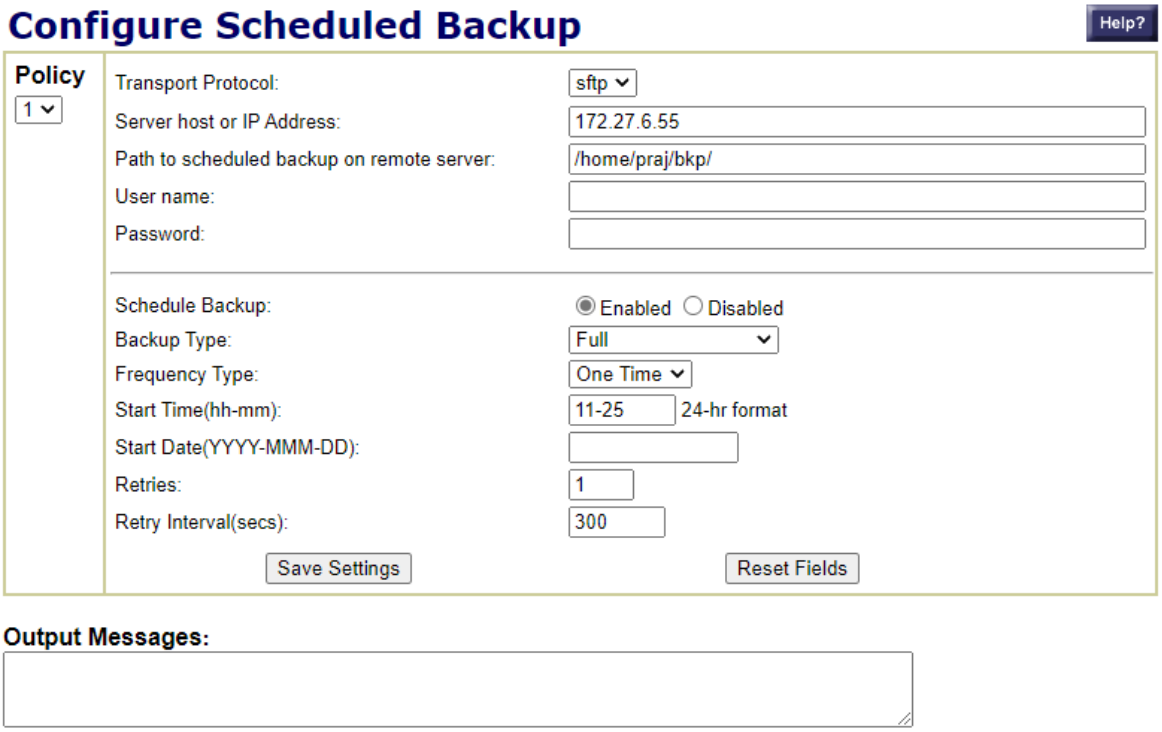
Value	Description
Retries	Configures the number of retries if the backup operation fails. The range is from 0 to 5. Default value is 1. Whenever a scheduled backup operation fails, the Containerized Decomposed Media Server retries the operation as per the configured value. The Containerized Decomposed Media Server stops the retry when the backup operation attempt is successful or when the backup operation fails after the maximum number of attempts configured in this field is reached.
Retry Interval(secs)	The retry interval period, in seconds. The Containerized Decomposed Media Server waits as per the this value before the next retry. The range is from 60 to 3600. Default value is 300. Changes to this field take effect immediately.

NOTE:

- Only one remote destination is supported for remote backups.
- Updating the SFTP/FTP settings in one policy for scheduled backup applies to all other policies.
- If the user configures more than two scheduled backup policies, it is recommended to have ten minutes difference between the policies.

To configure scheduled back up the Containerized Decomposed Media Server:

1. Click **Maintenance** > **Configure Scheduled Backup**.
   The Configure Scheduled Backup page displays.



2. Update the scheduled backup information described in the above table.
3. Click **Save Settings**.

   The scheduled backup can take several minutes to complete and a confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previous saved values.

Chapter 10

Fault Management

This chapter describes the alarm and log facilities of the Containerized Decomposed Media Server.

Alarms

This section describes the alarm feature of the Containerized Decomposed Media Server.

For more information about the list of alarms the Containerized Decomposed Media Server can generate and the description of each alarm, see *Appendix A, List of Alarms, on page 525*.

About Alarms

Alarms alert you to faults in the system. These can be either ongoing states, such as a hardware fault, or events, such as a reboot.

Alarm Severity

Alarms are categorized according to severity—critical, major, and minor. The following table describes the general meaning of alarm severities.

Table 99. Meaning of Alarm Severities

Severity	Meaning
Critical	Generated by conditions that cause the Containerized Decomposed Media Server to fail or stop operating, such as link failures or Ethernet configuration errors.
Major	Generated by conditions where the equipment is still operating, but service is or might be affected such as routing configuration errors or audio clip download failure.
Minor	Generated by conditions that you should be aware of but do not affect service, such as DNS failure or a user-initiated reboot. Minor alarms are often temporary conditions that self-correct.

Alarm States

Alarms can be either active or deactivated. Active or deactivated alarms can be either acknowledged or unacknowledged.

Alarms become **active** when the alarm condition starts. The Containerized Decomposed Media Server generates the alarm and activates it.

Alarms can become **deactivated** in a number of ways. For some alarms, the Containerized Decomposed Media Server automatically deactivates the alarm when the condition clears. For other alarms (for example, reboots and most software upgrade errors), the Containerized Decomposed Media Server automatically deactivates the alarm after a short interval. Other alarms require a reset or reboot to deactivate them.

When alarms are generated, they are unacknowledged. Both active and deactivated alarms can be **acknowledged** by a user, from either the Web GUI or the SNMP interface. An alarm can be acknowledged only once.

For information about how a specific alarm is deactivated, see *Appendix A, List of Alarms, on page 525*.

3GPP Alarm Formats

The Containerized Decomposed Media Server supports the 3rd Generation Partnership Project (3GPP) alarm format to send and clear the alarm traps as per ETSI X.733 and 3GPP TS 32.111. This format is supported in both SNMPv2c and SNMPv3 community strings. The Containerized Decomposed Media Server generates the traps in the 3GPP alarm format or the existing alarm format based on the management interface configuration.

NOTE: The Containerized Decomposed Media Server is partially complaint to the 3GPP alarm format.

For detailed information on the 3GPP alarm syntax to send and clear, refer to the *SNMP Interface Reference*.

Kafka Alarm Formats

The Containerized Decomposed Media Server supports the Kafka alarm format by sending the alarms to Kafka broker in JSON format. The alarm trigger, raise, and clear events are sent to Kafka broker, excluding the alarm acknowledgment. If the Kafka broker cannot process the alarms for some reason, for example, if the Kafka broker is down and the network is unreachable, the Containerized Decomposed Media Server does not re-transmit the alarms. The Containerized Decomposed Media Server supports only a single Kafka cluster, and does not support SSL.

The following Kafka broker configurations must be filled in the *values.yaml* file of the Containerized Decomposed Media Server.

- **enableKafkaFM**. To enable or disable the Kafka broker. The default value is false.
- **kafkaBrokerAddr**. To configure the IP or FQDN and port of the Kafka broker with comma separated values. For example, `ip:port`, `fqdn:port`, `ip:port`.
- **kafkaTopic**. To configure the topic name.

To enable the Kafka broker, the **enableKafkaFM** value must be set to true. The **kafkaBrokerAddr** and **kafkaTopic** must have valid values, and must not be empty. There is no validation for **kafkaBrokerAddr** and **kafkaTopic**.

NOTE: The port 8092 is reserved for internal kafka communication. This port number must not be used for other purposes.

For detailed information on the Kafka alarm formats, see *Appendix B, Kafka Alarm Formats, on page 553*.

Generic Alarm Template Formats

The Containerized Decomposed Media Server sends the customized alarm format to **stdout** in the user described JSON format. The input template is configured in the *values.yaml* file, and if the **generic alarm template format** is enabled, the alarm content is dumped into */var/log/fm_alarmtemplate* log and moved into the **stdout** through the sidecar **fm-logs**.

The following are the three fields in the alarmTemplate of the configmap section.

- **isEnabled.** To enable or disable the generic alarm format. The supported values are true or false.
- **alarmRaiseTemplate.** The JSON format in which the raised alarm is framed.
- **alarmClearTemplate.** The JSON format in which the clear alarm is framed.

If any of these fields is empty, the generic alarm template is disabled.

There are few variables in the **alarmRaiseTemplate** and **alarmClearTemplate**, which are indicated within <>. The user can replace these variable values based on the requirement.

For detailed information on the generic alarm template formats, see *Appendix C, Generic Alarm Template Formats, on page 557*.

Fault Management (Alarm) Data Integration

The Containerized Decomposed Media Server supports the FM integration with Fluentd. The Containerized Decomposed Media Server provides a Helm parameters `enableFM` to enable or disable the redirection of the alarms to the standard output. When the attribute `enableFM: true` is set, the Containerized Decomposed Media Server redirects the alarms to the stdout and Fluentd can be used to filter those alarms.

The Containerized Decomposed Media Server logs the alarms in below JSON format.

Table 100. Alarm JSON Format

Field Name	Data Type	Description
CNFHostName	String	Defines the hostname of the OAMP Pod. For example, oamp-0.
PodUuId	String	Defines the OAMP Pod Identifier. For example, 42db696d-f553-42e6-8054-4016293002cc.
ProductName	String	The name of the product. For example, cDMRF.
Namespace	String	Defines the Namespace. For example, Default.
Type	String	Defines the type of the log. For example, Fault.
EventType	String	Indicates whether an alarm to be triggered or cleared. For example, Activate/Deactivate.
AlarmCorrelationId	Integer	Defines the Alarm identifier of an alarm in the Alarm table. This uniquely identifies an entry in the Alarm table. For example, 724.
AlarmNotificationId	Integer	Defines the Notification Identifier. This is the unique value used for a notification. For example, 6819.
AlarmEventTime	String	Defines the event time, time of occurrence of the event in the Network Element (NE). The event time is set as per the time zone configured on the Containerized Decomposed Media Server. For example, X.
AlarmId	Integer	Defines the alarm Id for each type of the alarm. For example, 170.

Field Name	Data Type	Description
AlarmDescription	String	Defines the alarm text and contains basic information about the Fault. The alarm description includes trigger and clear conditions based on the event type.
AlarmTriggerReason	String	Defines the reason for triggering the alarm.
AlarmClearingMechanism	String	Defines the recommended actions to clear the alarm.
AlarmPerceivedSeverity	String	Represents the severity of the Fault. For example, Critical, Major, and Minor. This field is cleared after the alarm got cleared.
AlarmAdditionalText	String	Defines the additional text and provides further qualification on the Fault.
AlarmProbableCause	Integer	Defines the probable cause of the alarm. For example, 1. The alarm format is as per 3GPP alarm format.
AlarmEventType	Integer	Defines the event type. For example, 10. The alarm format is as per 3GPP alarm format.
AlarmSpecificProblem	Integer	Defines the specific problem assigned to the Fault situation. For example, 136116. The alarm format is as per 3GPP alarm format.
AlarmInstance	Integer	Defines the slot ID of MRFC/MRFP on which this alarm is triggered. For example, 3.

Following is the sample JSON format.

```
header
{
CNFHostName: "oamp-0",
PodUuId: "e4edab27-ad8c-4cc2-a4be-a2b169e69771",
Namespace: "ns2",
ProductName: "cDMRF",
"Type": "fault",
"EventType": "Activate",
}
body
{
"AlarmCorrelationId": "0",
"AlarmNotificationId": "1",
"AlarmEventTime": "2021-06-30 12:39:09 IST",
"AlarmId":"16",
"AlarmDescription": "Cause of the last reboot is unknown on Instance 1",
"AlarmTriggerReason": "Detection of an unexpected card reset.",
"AlarmClearingMechanism" : "Check the alarms leading up to the reboot. Check the
system logs for the period prior to this alarm, to determine chain of events
leading to this situation.",
"AlarmPerceivedSeverity": "Major",
"AlarmAdditionalText": "The card in this slot has reset and the media server
cannot establish the reason. The media server deactivates this alarm after a
brief interval.",
"AlarmProbableCause": "306",
"AlarmEventType": "2",
```

```
"AlarmSpecificProblem": "136116",
"AlarmInstance":1
} }
```

Fluentd integration with Containerized Decomposed Media Server for Fault Management is as follows.

1. The Containerized Decomposed Media Server writes the logs to */var/log/fm_messages* file on the OAMP container. The sidecar running on the OAMP container reads this file and redirects the alarms to the stdout.
2. The sidecar log file path is */var/log/containers/*-oamp-0_*_fm-logs-*.log*.

   For example, */var/log/containers/mrf-oamp-0_ns4_fm-logs-3ebce9cfdbfe99b094026ddac488bb8a87dcf125b572b299369200642a0d491a.log*.
3. If Fluentd is configured with the below configuration, the Containerized Decomposed Media Server reads the alarms from the OAMP alarm sidecar file path and sends to the external entities such as output file, kafka, and so on.

NOTE: Ensure to use the proper regular expression pattern in the Fluentd configuration file for alarm re-direction.

Sample Fluentd Configuration File

The following is the sample for Fluentd configuration.

```
# cat fluentd-configmap.yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: fluentd-configmap
  namespace: logging
  labels:
    app: fluentd
data:
  fluent.conf: |
    <source>
      @type tail
//This is the source file from which the alarms are tailed.
path /var/log/containers/*-oamp*fm*

      pos_file /var/log/containers/fluentd-docker.pos
      tag kubernetes.*
      read_from_head true
      emit_unmatched_lines true
      <parse>
//Parsing the JSON content from the path: /var/log/containers/*-oamp*fm*.
        @type json
```

```
time_key time
        time_format %Y-%m-%dT%H:%M:%S.%NZ
        keep_time_key false
        localtime false
      </parse>
    </source>
    <filter kubernetes.var.log.containers.**.log>
      @type parser
//Filters only the Containerized Decomposed Media Server alarms JSON content.
      key_name log
remove_key_name_field true
      <parse>
        @type json
      </parse>
    </filter>
    <match kubernetes.var.log.containers.**.log>
      @type copy
      <store>
        @type file
//This example dumps the alarms to a file. You need to configure the desired
destination in the match section.
        path /var/log/outputAlarmJson
</store>
    </match>
```

Alarms Options in Web GUI

Alarms option of the Fault Management screen allows you to work with active and archived system alarms. When the Alarms option is clicked, it expands to show the following options:

- *Events List Page*
- *Show Alarms Configuration*
- *Configure Alarms*

The Alarms option page has the Manual Update button which updates the alarm summary or the alarm list, depending on which page you have open. If you do not initiate a manual update, the alarms are updated every minute.

Events List Page

The Events List page allows you to view and acknowledge alarms or clear the alarm history.

The Events List lists all the alarms that have occurred on the Containerized Decomposed Media Server. When you log on to the Web GUI, the GUI automatically opens at the Events List, so that you can monitor the status of the system. You can choose to display all alarms, only active alarms, or only unacknowledged alarms.

The information provided for each alarm includes the following:

- Date and time of the event
- Sequence number of the event
- Alarm/SNMP trap identifier
- Severity of the alarm
- Event type of the alarm
- Instance number of the Containerized Decomposed Media Server reporting the alarm. On the Containerized Decomposed Media Server, the instance number is 1 for OAMP and 3 to 22 for active MRFPs.
- Brief description of the alarm.

The Events List is sorted by sequence number, with the most recent alarms appearing at the top of the list. The Events List is updated every 60 seconds for active events and every 120 seconds for all and unacknowledged events, and the time of the most recent update is displayed. Up to a maximum of 300 alarms are maintained in the list. When the Events List is full, alarms are selectively discarded to make room for new events.

Alarm records are discarded depending on the priority level (lowest priority first):

1. Deactivated and acknowledged alarms
2. All deactivated alarms
3. Active but acknowledged alarms
4. Active unacknowledged alarms

You can also manually purge the Events List. Perform the following procedure to view alarms.

View Alarms

The View Alarms page allows you to view active alarms.

To view alarms:

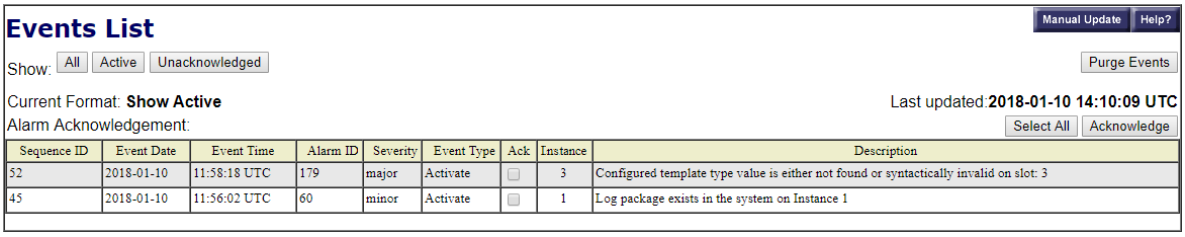
1. Click **Fault Management** > **Alarms** > **Events List**.

   By default, only active alarms display.
2. Do one of the following action in the **Show** label.
   - To view the complete alarm history, click **All**.
   - To view only active alarms, click **Active**.
   - To view only unacknowledged alarms, click **Unacknowledged**.

To acknowledge alarms:

1. Click **Fault Management** > **Alarms** > **Events List**.

   The Events List page displays, showing the list of alarms.



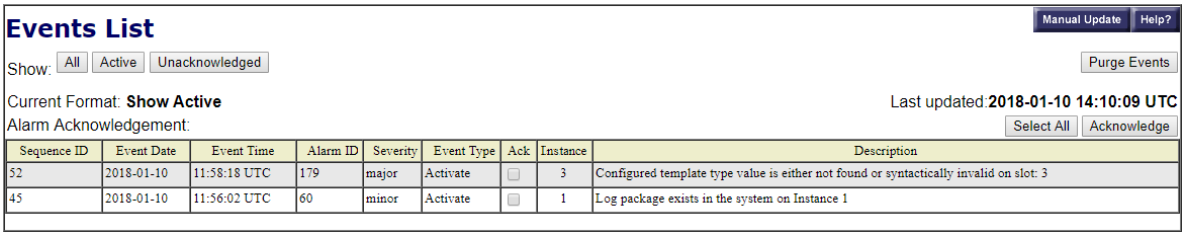
Sequence ID	Event Date	Event Time	Alarm ID	Severity	Event Type	Ack	Instance	Description
52	2018-01-10	11:58:18 UTC	179	major	Activate		3	Configured template type value is either not found or syntactically invalid on slot: 3
45	2018-01-10	11:56:02 UTC	60	minor	Activate		1	Log package exists in the system on Instance 1

2. Do one of the following (this action requires access level 3 or higher):
   - To acknowledge a specific alarm or multiple alarms, select **Ack** checkbox > click **Acknowledge**.
   - To acknowledge all unacknowledged alarms, click **Select All** > **Acknowledge**.

To purge the Events List:

1. Click **Fault Management** > **Alarms** > **Events List**.

   The Events List page displays, showing the list of alarms.



Sequence ID	Event Date	Event Time	Alarm ID	Severity	Event Type	Ack	Instance	Description
52	2018-01-10	11:58:18 UTC	179	major	Activate		3	Configured template type value is either not found or syntactically invalid on slot: 3
45	2018-01-10	11:56:02 UTC	60	minor	Activate		1	Log package exists in the system on Instance 1

2. Click **Purge Events** (this action requires access level 3 or higher).

   All alarms are cleared from the Events list.

   NOTE: The **Purge Events** does not clear the active alarms and the acknowledgments for the active alarms.

Show Alarms Configuration

The Show Alarms Configuration page displays system alarms settings.

To view alarms configuration:

1. Click **Fault Management** > **Alarms** > **Show Alarms Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the alarms configuration information.

Configure Alarms

On the Configure Alarms page, you can set the behavior of configurable alarms.

The following table describes the alarm settings that you can configure.

Table 101. Configurable Alarm Settings

Value	Description
DSP resource alarm: on threshold	Specifies the threshold of DSP resources usage, in percentage. The Containerized Decomposed Media Server raises the *DSP resource* alarm (alarm 106) when this threshold is reached or is exceeded. The supported values are 0 and from 1 to 100, where zero disables this alarm. The default value is 80. Changes to this field take effect immediately.
DSP resource alarm: off hysteresis	Specifies the threshold margin, in percentage, used as hysteresis to prevent vacillations of the *DSP resource* alarm (alarm 106). *DSP resource* usage must fall by this amount[a] below the configured threshold, to clear alarm 106. The supported value ranges from 5 to 100. The default value is 20. Changes to this field take effect immediately.
RTP Packet loss alarm: on threshold	Specifies the threshold of RTP Packet Loss, in percentage. The Containerized Decomposed Media Server raises the *RTP Packet Loss* alarm (alarm 158) when this threshold is reached or is exceeded. The supported values are 0 and from 1 to 100, where zero disables this alarm. The default value is 0. Changes to this field take effect immediately.
RTP Packet loss alarm: off hysteresis	Specifies the threshold margin, in percentage, used as hysteresis to prevent vacillations of the *RTP Packet Loss* alarm (alarm 158). *RTP Packet Loss* alarm must fall by this amount[b] below the configured threshold, to clear alarm 158. The supported value ranges from 0 to 100. The default value is 5. Changes to this field take effect immediately.
SIP response code alarm	Enables or disables triggering of the *SIP response code* alarm (alarm 107) when the Containerized Decomposed Media Server receives particular SIP response codes[c]. The default value is Enabled. Changes to this field take effect immediately.
MSML response code alarm	Enables or disables triggering of the *MSML response code* alarm (alarm 108) when the Containerized Decomposed Media Server sends particular MSML response codes[d]. The default value is Enabled. Changes to this field take effect immediately.
Package version mismatch alarm	Enables or disables the *Required packages or versions are unavailable* alarm (alarm 79) when the required package version are unavailable. The default value is Enabled. Changes to this field take effect immediately.
OS version mismatch alarm	Enables or disables the *Operating system version or distribution not supported* alarm (alarm 78) when the OS version or distribution are not supported. The default value is Enabled. Changes to this field take effect immediately.

Table 101. Configurable Alarm Settings

Value	Description
Enable 3GPP Alarm Format	Enables or disables the 3GPP alarm format to send and clear the alarm traps in SNMPv2c and SNMPv3. The Containerized Decomposed Media Server generates the alarm traps in the 3GPP alarm format or the existing alarm format. The supported values are: • **Enabled.** The Containerized Decomposed Media Server sends alarm traps only in the 3GPP alarm format. • **Disabled.** The Containerized Decomposed Media Server sends alarm traps only in the existing alarm format. The default value is Disabled. Changes to this field take effect immediately. For information on the alarm format, refer to the *SNMP Interface Reference*.
Annlab transcoding failure alarm	Enables or disables the *AnnLab transcoding failure alarm for: Clipname-X, Hostname-Y* (alarm 201)[e], when the AnnLab client failed to generate the transcode clip from the original uploaded clip. The default value is Disabled. Changes to this field take effect immediately.

[a] For example, if DSP Resource Alarm: On Threshold is set to 90% and DSP Resource Alarm: Off Hysteresis to 5%, Alarm 106 turns on if DSP usage reaches 90% or higher of the configured threshold value and clears when the usage falls to 85% or lower of the configured threshold value.

[b] For example, if RTP Packet Loss Alarm: On Threshold is set to 90% and RTP Packet Loss Alarm: Off Hysteresis to 5%, Alarm 158 turns on if RTP Packet Loss Alarm reaches 90% or higher, and subsequently clears when RTP Packet Loss Alarm falls to 85% or lower.

[c] For more information about SIP response codes, refer *to SIP Interface Reference.* For information on *SIP response code alarm* (alarm 107), see *Appendix A, List of Alarms, on page 525*.

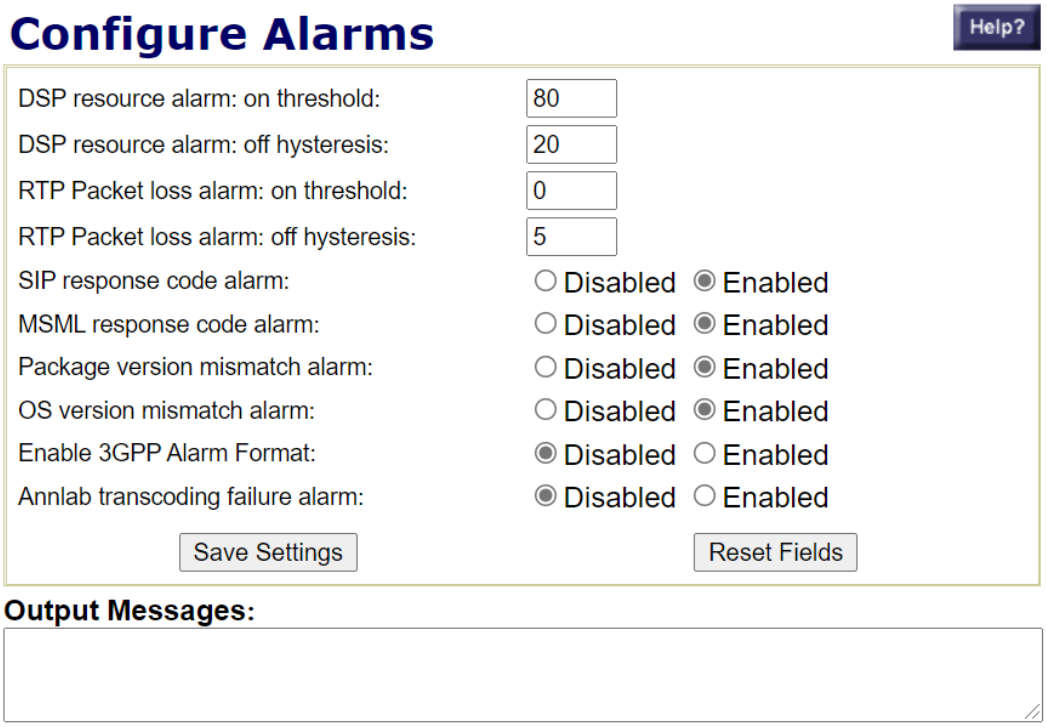
[d] For more information about MSML response codes, refer *to MSML Interface Reference.* For information on *MSML response code alarm* (alarm 108), see *Appendix A, List of Alarms, on page 525*.

[e] For information on the *AnnLab transcoding failure alarm* (alarm 201), see *Appendix A, List of Alarms, on page 525*.

To configure alarms:

1. Click **Fault Management** > **Alarms** > **Configure Alarms**.

The Configure Alarms page displays.



2. Configure the alarms setting information as described in the above table.
3. Click **Save Settings**.

   The change takes effect immediately.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Logs

NOTE: The Containerized Decomposed Media Server also supports logging management activity. For more information, see *Chapter 12, Administration Management, on page 473*.

Significant system events are captured in log messages, which gets saved to an internal file.

Log messages format is as follows:

<PRI>VERSION TIMESTAMP:::date rfc3339 HOSTNAME APP NAME PROCID MSGID STRUCTURED DATA msg

The following example shows a sample set of system log messages.

Sample Syslog Messages

```
<134>1 2020-05-12T09:00:00.533458+00:00 dmrf-localhost-mrfc-1 syssrvr1 15748 -
- : I:syssrvr.cpp:316->Return code from command: 0
```

```
<134>1 2020-05-12T09:00:00.533516+00:00 dmrf-localhost-mrfc-1 syssrvr1 15748 -
- : I:syssrvr.cpp:344->Reply size 5, string:
<134>1 2020-05-12T09:00:00.534333+00:00 dmrf-localhost-mrfc-1 scccp1 15916 - -
: I:sys_srvr_client.c:808->Exit status 0
<133>1 2020-05-12T09:00:00.715443+00:00 dmrf-localhost-mrfc-1 scccp1 15916 - -
: N:platform_info.c:2377->Cloud Type detected
```

About System Logging

The significant factors that can be configured for system log messages are:

- The level of severity reported. This can be different for each syslog module.
- The parts from which the system generates messages.
- The destination to which logs are forwarded. By default, logs are forwarded to internal file .
- The syslog facility to be used for Containerized Decomposed Media Server messages. Log messages are forwarded using the syslog facility.
- Syslogs from all the MRFPs are logged in single syslog file.

System Log Severity

System events generate log messages at different severities, which represent their level of significance for the system. Log severities of events are predefined. However, you can configure which levels of severity are reported. The lower the level of severity specified, the more detail is captured in the logs.

Log severities can be independently set for every facility. When you specify a severity to report, the system reports all log messages of that severity and higher. For example, if you specify a severity of Critical, the system reports all Critical, Alert, and Emergency log messages.

The default level of severity for all facilities is Warning level.

The following table lists the meaning of different system log severities.

Table 102. System Log Severities

Severity	Meaning
Emergency	System is unusable.
Alert	Immediate action is required to prevent the system from becoming unusable. For example an Ethernet link has failed or the Containerized Decomposed Media Server cannot communicate to the NFS server.
Critical	Critical condition exists, such as resource exhaustion. For example, the system is out of memory, or CPU thresholds are being exceeded.
Error	Error condition has occurred. For example a failed system call or a driver error.
Warning	Warns of an event that has the potential to cause an error, such as, invalid parameters passed to a function.
Notice	Normal but significant occurrence, such as an unexpected event.

Table 102. System Log Severities

Severity	Meaning
Information	Reporting of normal conditions as they occur.
Debug	Report events at the trace level of detail.

NOTE: Debug severity level can affect system operation. It should only be used when requested by support personnel.

System Log Modules

The Containerized Decomposed Media Server internal architecture includes a number of modules or major operational subsystems. The following modules produce log messages:

Table 103. System Log Modules

Facility	Description
Control Protocol Engine	Subsystem that processes the call control protocol
VXML Engine	VoiceXML interpreter
Streaming Engine	Responsible for RTP media streaming
SCRM	Responsible for service creation and resource management
OAMP	Responsible for operations, administration, maintenance, and provisioning
Platform	System drivers, utilities, and so on
HCM	HTTP cache manager for caching media files
MSML	Subsystem that processes MSML and MOML messages
MP	Media processing subsystem
Speech Manager	Subsystem that processes MRCP messages
WebRTC	Subsystem responsible for ICE processing

NOTE: Severities can be independently set per module.

System Log Destinations

By default, the System logs are sent to an Internal file, which is the default destination. System logs saved to an internal file can then be saved as a file on an external server in a format that can be read by a simple text editor.

The internal file for system logs has a maximum capacity of 100 MB. When that capacity is reached, older logs get replaced with newer logs.

All system messages are forwarded through a single syslog facility. You can select any facility from **local0** to **local6**.

When using remote server, ensure that your syslog server is configured properly. For information about setting up your syslog server to work with the Containerized Decomposed Media Server, refer *Radisys Special Interfaces Reference*.

Viewing System Logs

The way you view system logs depends on the destination.

If the configured destination is an internal file, use the Retrieve System Log Web GUI page to retrieve the log file and save it as a file on an external server. You can then view the file contents using a simple text editor.

Protocol Logging

The Containerized Decomposed Media Server allows you to can log incoming and outgoing messages for the control protocol, for HTTP messages related to media caching, or for MRCP messages related to ASR or TTS processing.

Protocol logs are stored internally. The **plog.log** and **plog.bak** are the protocol log files, each file shares 100 MB. Up to 200 MB protocol logs can be stored. When the maximum capacity is reached, logs are dropped, oldest first.

When you want to view the protocol log, you can access it through an HTML link. You can read the log using a text editor.

Control protocol log messages contain the following parts:

- Entry number (1 = the first entry after protocol logging is enabled)
- Timestamp, in the format *hh:mm:ss.ss*
- Source IP address and port number
- Destination IP address and port number
- Protocol identifier
- Protocol data

HTTP messages contain the HTTP header only.

The following example shows a sample set of SIP log messages.

Sample SIP Log Messages

```
<<0 21:05:21.589: 176.16.100.36.5060 < 10.0.0.170.50606 (522)>>
INVITE sip:msml@10.2.8.11 SIP/2.0
Via:SIP/2.0/UDP 10.0.0.170:50606
Call-ID: 46D5421F@10.0.0.170:50606
From: <sip:user@10.0.0.170:50606>;tag=1000000-0-19741-10.0.0.170.50606
To: <sip:msml@10.2.8.11:5060>
CSeq: 1 INVITE
Content-Type: application/sdp
Contact: sip:user@10.0.0.170:50606

v=0
o=- 1231232312312312312 123123123123123123 IN IP4 ms.mediaserver.convedia.com
s=Convedia CMS 6000 session
```

```
c=IN IP4 0.0.0.0
t=0 0
m=audio 1234 RTP/AVP 0
a=rtpmap:0 pcmu/8000
a=ptime:20
a=sendrecv
```

Logging Options in Web GUI

The Logs option of the Fault Management screen, you can work with system and protocol logs.

Show System Log Destination Configuration

The Show System Log Destination Configuration page allows you to view the settings for log message reports.

To view system log destination configuration:

1. Click **Fault Management** > **Logs** > **Show System Log Destination Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the system log destination configuration information.

Show System Log Severity Configuration

The Show System Log Severity Configuration page allows you to view the severity settings for log facilities for a given instance or for all instances.

To view system log severity configuration:

1. Click **Fault Management** > **Logs** > **Show System Log Severity Configuration**.
2. Select the **Instance Number** from the drop-down list

   NOTE: Select the drop-down list to view configuration for all the instances.
3. Click **Execute**.

   The system log severity configuration information for the instance displays in the **Output Messages:** box. If you selected all, log severity configuration information displays for every instance.

   Kernel log messages are always sent to the system log, regardless of the level of severity set.

Show Protocol Log Config

The Show Protocol Log Configuration page displays which protocol logging is enabled, CPU threshold, and desired time. You can enable protocol logging for the control protocol (SIP), for HTTP protocol messages associated with media caching, and for MRCP messages associated with ASR or TTS processing.

NOTE: This page is not applicable for non-admin users.

To view protocol log configuration:

1. Click **Fault Management** > **Logs** > **Show Protocol Log Config**.
2. Click **Execute.**

   The **Output Messages:** box specifies whether protocol logging is enabled or not, for control protocol and for HTTP messages associated with media caching.

Configure System Log Destination

On the Configure System Log Destination page, you can change the destination and facility settings for log messages. If no destination is selected, system logging is disabled.

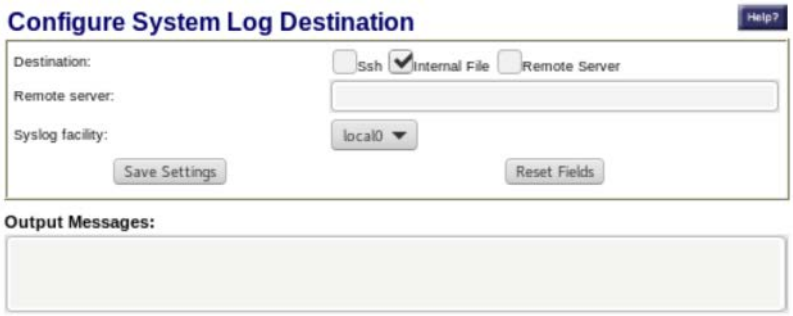
The following table shows the information you can configure the system log destination.

Table 104. Configurable System Log Destination Information

Value	Description
Destination	Indicates the log destination. By default the value is set to Internal File. ***NOTE:*** Ssh and Remote Server are not supported in Containerized Decomposed Media Server.
Remote server	The Fully Qualified Domain Name (FQDN) or IP address of the remote server. ***NOTE:*** This parameter is not supported in Containerized Decomposed Media Server.
Syslog facility	Provides the single syslog facility for the system logs usage. The supported values are: • local0 • local1 • local2 • local3 • local4 • local5 • local6 The default value is local0. Changes to this field take effect immediately.

To modify the system log destination configuration:

1. Click **Fault Management** > **Logs** > **Configure System Log Destination.**



2. Enter the system log destination information described in the above table.
3. Click **Save Settings**.

   The changes take effect immediately and a confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previous saved values.

Configure System Log Severity

On the Configure System Log Severity page, you can change the settings for the severity of message logged for each Containerized Decomposed Media Server module except AnnLab.

To modify system log severity configuration:

1. Click **Fault Management** > **Logs** > **Configure System Log Severity**.

2. Select the **Instance Number** from the drop-down list.

   NOTE: Select the drop-down list to view configuration for all the instances.

3. Do one or more of the following:
   - Select the modules you want to generate log messages. To maximize performance, select **None** for modules that are not of interest.
   - For each module, select one of the severity options. This is the minimum severity the Containerized Decomposed Media Server reports.
4. Click **Save Settings**.

   The changes take place immediately and confirmation message is displayed in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Protocol Log

On the Configure Protocol Log page, you can enable or disable protocol logging for the control protocol (SIP), for HTTP messages associated with media caching or for MRCP messages associated with ASR or TTS processing.

NOTE: Protocol log of the latest enabled instance can be viewed by logging into that particular MRFP pod and by using `trc` command.

The following table shows the protocol log parameters that you can configure.

Table 105. Protocol Log Parameter Settings

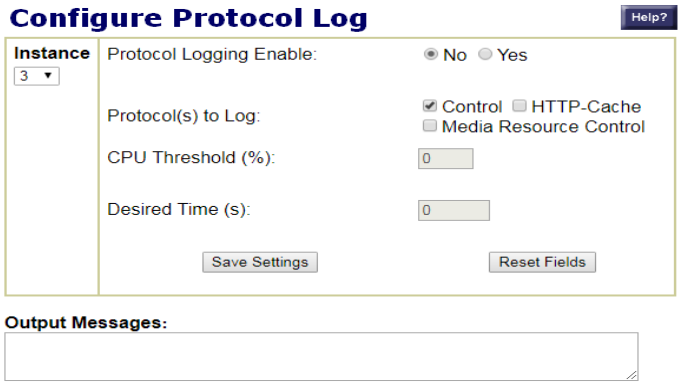
Parameter	Description
Protocol Logging Enable	Enables or disables protocol logging. The supported values are **No** and **Yes**. The default value is No. ***NOTE:*** After the value of **Desired Time** times out, the protocol logging is disabled. That is, the **Protocol Logging Enable** field changes to default state (No). Changes to this field take effect immediately.
Protocol(s) to Log	Specifies which protocol to use for logging. The supported values are: • **Control.** Enable or disable logging for the control protocol (SIP). • **HTTP-Cache.** Enable or disable logging for HTTP messages associated with media caching. • **Media Resource Control.** Enable or disable logging for MRCP messages associated with ASR/TTS processing. The default value is Control. ***NOTE:*** You can enable control protocol, HTTP-Cache, and MRCP logging at the same time. Changes to this field take effect immediately.

Table 105. Protocol Log Parameter Settings

Parameter	Description
CPU Threshold (%)	Specifies the CPU threshold, in percentage. The plog server runs when the current CPU of CP cores is within the configured CPU threshold limit, and stops when the CPU utilization exceeds the configured CPU threshold value. The value range is from 0 to 100. The default value is 0, which indicates the Containerized Decomposed Media Server does not monitor the CPU utilization. ***NOTE:*** This field is non-configurable when **Protocol Logging Enable** is set to No. Changes to this field take effect immediately.
Desired Time (s)	Allows the plog server to run for the configured time, in seconds. The value range is from 0 to 86400. The default value is 0, which indicates the plog server runs forever. ***NOTE:*** This field is non-configurable when **Protocol Logging Enable** is set to No. Changes to this field take effect immediately.

To modify the protocol log configuration:

1. Click **Fault Management** > **Logs** > **Configure Protocol Log**.



2. Select the **Instance Number** from the drop-down list.
3. Enter the protocol log information described in the table above.
4. Click **Save Settings**.

   The changes take effect immediately and confirmation message is displayed in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Retrieve System Log

On the Retrieve System Log page, enables you to retrieve log messages stored in an internal file and save as a file on an external server. The file can be read in a text editor.

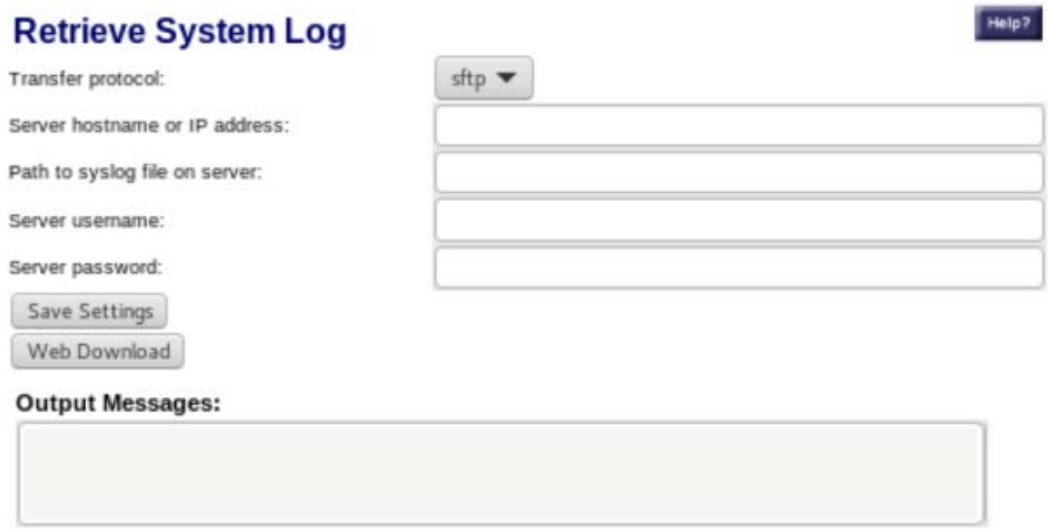
The following table shows the information you must provide to use SFTP to post the system log messages file to a file server. This information is not needed for a Web download.

Table 106. File Transfer Information—Retrieve System Log Messages

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to syslog file on server	The absolute path to syslog file on the remote file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	The username configured on the file server. Supported values are strings of up to 128 characters.
Server password	The password configured on the file server. Supported values are strings of up to 128 characters.

To retrieve system logs and save externally:

1. Click **Fault Management** > **Logs** > **Retrieve System Log**.



2. Enter the required retrieve system log settings described in the above table.
3. Click **Save Settings** to retrieve system log.

   Confirmation message is displayed in the **Output Messages:** box.
4. Click **Web Download** to download the system log retrieved using HTTP through your Web browser.

   For a Web download, use the pop-up window to save the system log file.

Retrieve Protocol Log

On the Retrieve Protocol Log page, you can retrieve the protocol log messages that are posted to an internal file and save as a file on an external server. The file can then be read with a text editor.

The following table describes the information you must provide to use SFTP to post the protocol log messages file to a file server. This information is not needed for a Web download.

Table 107. File Transfer Information—Retrieve Protocol Log Messages

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to protocol log on server	The absolute path to protocol log on the remote file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

NOTE: When the **Password Less Transfer to/from Remote Server** parameter on the *Configure System Security* Web GUI page is enabled, the **Server password** is non-editable.

To retrieve the protocol log and save externally:

1. Click **Fault Management** > **Logs** > **Retrieve Protocol Log**.

2. Enter the required retrieve protocol log settings described in the above table.
3. Click **Save Settings** to retrieve protocol log.

   Confirmation message is displayed in the **Output Messages:** box.
4. Click **Web Download** to download the protocol log retrieved using HTTP through your Web browser.

   For a Web download, use the pop-up window to save the system log file.

Diagnostics

The Containerized Decomposed Media Server allows you to retrieve certain diagnostic information and export it to a file. This file can be submitted to Radisys TAC, to help perform advanced troubleshooting. The information retrieved includes routing information and internal media configuration information. The retrieved files are posted on an external server using SFTP.

NOTE: During the interval when the diagnostics file is being retrieved, service is affected. The service resumes a normal operation after the retrieval operation completes.

You can also configure the Containerized Decomposed Media Server to not automatically reboot when it encounters a fatal software error. This allows retrieval of the Containerized Decomposed Media Server core files, which are generated on unrecoverable software error and maintained in RAM.

The Containerized Decomposed Media Server retains a maximum of five auto log packages. An additional new package generated overwrites the older log package.

Show Fatal Error and Log Package Configuration

The Show Fatal Error and Log Package Configuration page displays the configured behavior of the Containerized Decomposed Media Server when it encounters a fatal software error. You can view how the Containerized Decomposed Media Server is configured to respond if a fatal error occurs:

Whether log packages are automatically transferred when auto-generated and if so, the transfer protocol and SFTP server, which is used as a destination for the package.

To configured behavior on fatal error:

1. Click **Fault Management** > **Diagnostics** > **Show Fatal Error and Log Package Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the settings for fatal error behavior.

Retrieve Diagnostics File

On the Retrieve Diagnostics File page, you can retrieve a diagnostics file from the Containerized Decomposed Media Server and save it to an external server. The file can be submitted to TAC for analysis, to troubleshoot problems.

The following lists the information you must provide to use SFTP to post the diagnostics file to a file server. This information is not needed for a Web download.

Table 108. File Transfer Information—Retrieve Diagnostics File

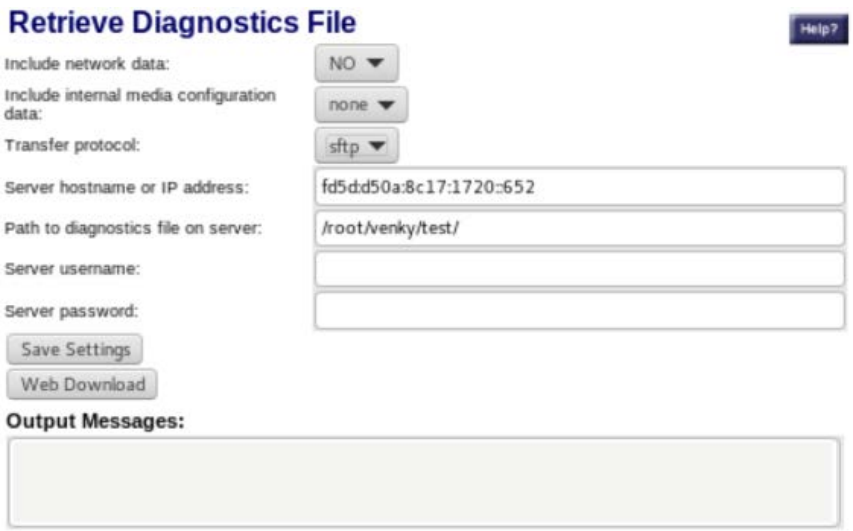
Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".

Table 108. File Transfer Information—Retrieve Diagnostics File

Value	Description
Path to diagnostics file on server	The absolute path to diagnostics file on the remote file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field may not be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

To retrieve diagnostic information and save it externally:

1. Click **Fault Management** > **Diagnostics** > **Retrieve Diagnostics File**.



2. Select the **Include network data** drop-down list as **YES** to include routing table information in the file. To exclude, set it to **NO**.

   NOTE: Currently, the **Include internal media configuration data** field is not implemented. Therefore, always set this field to **NO** when retrieving the diagnostics file.

3. For HTTP, click the **Web Download**. Enter the file transfer information described in the above table.
4. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.

   For a Web download, use the pop-up window to save the diagnostics file.

Configure Log Package Transfer

The Containerized Decomposed Media Server generates a log package containing important diagnostic information, including the core file, if a fatal application error occurs. On the Configure Log Package Transfer page, you can specify whether the Containerized Decomposed Media Server transfers these log packages to an SFTP server after generating them.

If you disable automatic transfer of log packages, the Containerized Decomposed Media Server attempts to save any autogenerated log packages to nonvolatile memory.

The following table describes the information you must provide to use SFTP to automatically post a diagnostics log file to a file server.

Table 109. File Transfer Information—Automatic Log Package Transfer

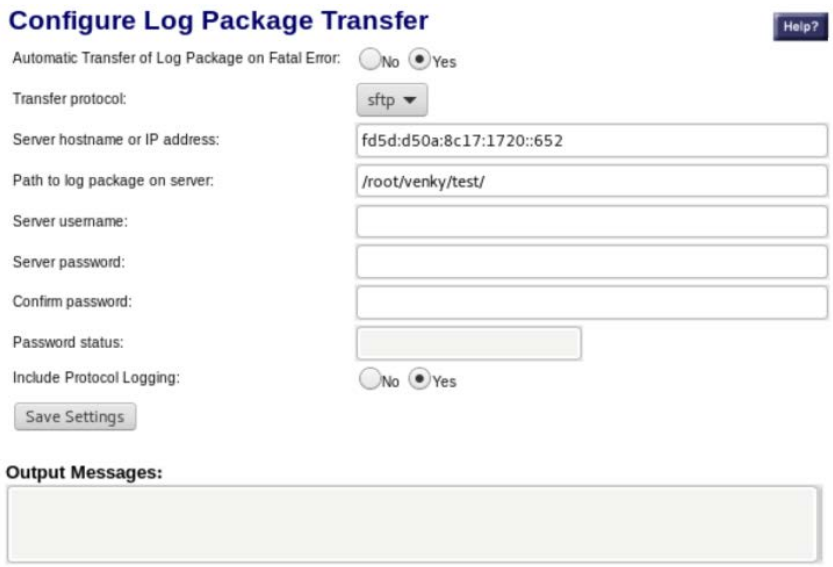
Value	Description
Automatic Transfer of Log Package on Fatal Error	Indicates whether automatically generated log packages are automatically transferred to the file server. • **Yes.** Transfer the log package on fatal application error. • **No.** Do not transfer the log package. The default value is no.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to log package on server	The absolute path to log package on the remote file server. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. Supported values are strings of up to 128 characters.
Server password	The password configured on the file server. Supported values are strings of up to 128 characters.

Table 109. File Transfer Information—Automatic Log Package Transfer

Value	Description
Confirm password	The password configured on the file server. The supported values are strings of up to 128 characters.
Password status	The password status on the file server.
Include Protocol Logging	This option allows the Admin user to enable or disable PLOG packaging in log packages.

To configure transfer for autogenerated log transfers:

1. Click **Fault Management** > **Diagnostics** > **Configure Log Package Transfer**.



2. Enter the log package transfer information as described in the above table.
3. Click **Save Settings**.

   The changes take effect immediately and confirmation message is displayed in the **Output Messages:** box.

Transfer Log Package

On the Transfer Log Package page, you can manually generate a log package. You can also use this page to manually transfer an auto-generated log package that is not transferred.

Log packages reside in an internal format on the Containerized Decomposed Media Server and cannot be accessed until they are transferred to another location.

Log packages generated on demand are transferred when you manually initiate package creation. Auto-generated log packages can be transferred manually (using the Transfer Log Package option), or you can configure the Containerized Decomposed Media Server to automatically transfer auto-generated log packages (using the Configure Log Package Transfer option).

Automatic transfer is to an external file server. Manual transfer can be either by SFTP or HTTP.

The Containerized Decomposed Media Server automatically deletes any user-generated file after transfer, whether the file is successful or not. Auto-generated files are not automatically deleted; you must delete them manually using the Delete Log Package option. (The exception is the SNMP interface, where auto-generated files are automatically deleted after a successful transfer.)

The Containerized Decomposed Media Server retains at most five automatically generated and one user-generated log package. Any newer packages of each type overwrites the older package.

The Containerized Decomposed Media Server uses the following convention for log package file names:

```
<MS host name>_<Date>.<Time>.<package_type>.sl<Instance>.<Seq_num>.gz
```

For example: **ms6scc1_Nov15.1340.swt_package.sl3.1.gz**.

The valid package types are:

- **swt_package.** Created for a software watchdog timeout.
- **sig_package.** Created for process termination due to a signal.
- **usr_package.** Created for a user-generated package.

The following table describes the information you must provide to use SFTP or HTTP to manually post a diagnostics log file to a file server.

Table 110. File Transfer Information—Manual Log Package Transfer

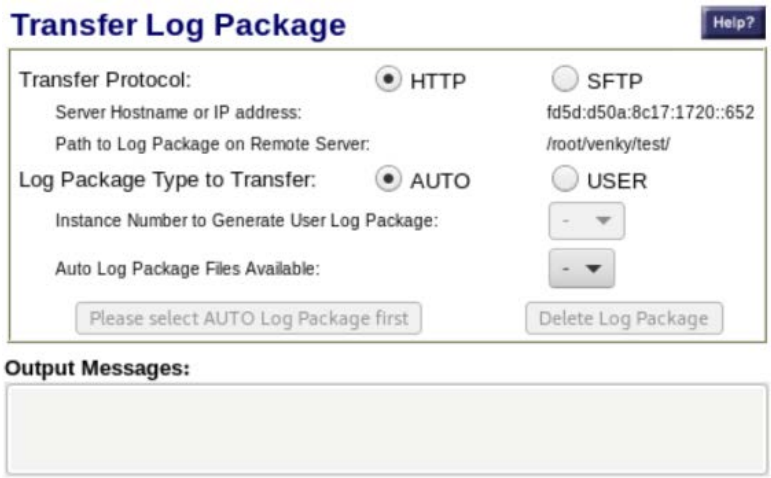
Value	Description
Transfer Protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server Hostname or IP address	The server hostname or the IP address. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". If the automatic log package transfer is set to No in Configure Log Package Transfer page, the then this field is not displayed.

Table 110. File Transfer Information—Manual Log Package Transfer

Value	Description
Path to Log Package on Remote Server	The absolute path to log package on remote server. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". If the automatic log package transfer is set to No in Configure Log Package Transfer page, the then this field is not displayed.
Log Package Type to Transfer	The supported values are: • **AUTO.** Manually transfer the current auto-generated log package. • **USER.** Generate a new log package and transfer it. The default is **AUTO**.
Instance Number to Generate User Log Package	The instance for which you want to generate the log package. The supported values are 1–22. ***NOTE:*** This field is enabled when **USER** is selected in Log Package Type to Transfer.
Auto Log Package Files Available	If there are Auto Log Package files available, then the file names are shown in Drop-down list. The files are ordered by timestamp, with the latest file listed first and maximum of five file names. If no files are available, the default value - is shown.

To transfer a log package:

1. Click **Fault Management** > **Diagnostics** > **Transfer Log Package**.



2. Select the **Transfer Protocol**.
3. Select the **Log Package Type to Transfer**.
   - If you are generating a new (user) log package, select the **Instance Number to Generate User Log Package** drop-down list for which the information is to be collected.
   - If you are transferring auto log package, select the file from **Auto Log Package Files Available** drop-down list.
4. Click **Start Transfer AUTO Log Package**.

   The full text of this button depends on whether you are transferring an autogenerated or a user-generated log package. When started, the **Output Messages** box displays a Transfer initiated message.
   - If the transfer method is SFTP, the file is transferred according to the FTP information specified on the Configure Log Package Transfer page. This information is displayed below the FTP option.
   - If the transfer method is HTTP, a dialog box opens. Specify a destination for the generated file and click **Save**.

   The **Output Messages** box displays the transfer results (either success, or an error message).

Once the request has been submitted, a **Delete** button appears. Depending on whether the log package has been auto-generated or user-generated, this will read **Delete Auto Package** or **Delete User Package**, respectively. However, only the **Delete Auto Package** is enabled; the **Delete User Package** button is disabled. If you click **Delete AUTO Log Package**, it deletes the transfered auto log package.

Delete Log Package

On the Delete Log Package page, you can delete log packages that may remain on the Containerized Decomposed Media Server. You can delete autogenerated and user-generated log packages using this option.

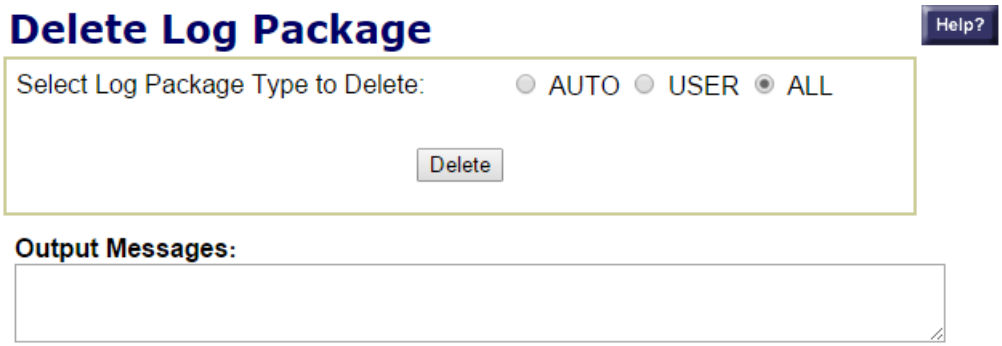
The following table describes the information that you can specify when deleting log packages.

Table 111. Log Package Deletion

Value	Description
Select Log Package Type to Delete	Indicates which log package is to be deleted. The supported options are: • **AUTO.** Deletes the retained auto-generated package. • **USER.** Deletes the retained user-generated package. • **ALL.** Deletes both the auto-generated and the user-generated packages. The default value is **ALL**.

To delete a log package:

1. Click **Fault Management** > **Diagnostics** > **Delete Log Package**.



2. Select the Log Package Type to Delete. Specify whether you want to delete auto-generated packages, user-generated packages, or all packages.
3. Click **Delete**.

   The **Output Messages:** box displays the deletion results (either success, or an error message).

Chapter 11

Performance Management

This chapter describes the features for monitoring the performance of the Containerized Decomposed Media Server.

NOTE: The statistics generated by the Containerized Decomposed Media Server are listed in *Appendix D, List of Statistics, on page 566*.

About Statistics

The Containerized Decomposed Media Server continuously collects information about usage and performance as it operates in a comprehensive set of statistics. At intervals, this information is consolidated and stored in an internal file.

Statistics are collected in intervals of configurable length, starting from 5 to 30 minutes according to the system time. Information is retained for 72 hours (three days). After three days, the oldest interval is discarded when the next interval is added to the file.

When the Containerized Decomposed Media Server is restarted, statistics for all instance are reset, and the statistics file is cleared.

Viewing Statistics

There are several ways to view statistics.

- By using the Web GUI to display a single collection interval from the statistics history.

  The Show Statistics History page lets you view any collection interval from the past 72 hours, so you can investigate system behavior before, during, and after a specific network event. Standard editing keystrokes can be used to copy (**CTRL+C**) and paste (**CTRL+V**) information from the Output Messages box into another document.

  For more information see, *Show Statistics History on page 470*.

- Track Announcements.

  When the announcement service terminates or fails, the Containerized Decomposed Media Server appends the date, time, clip name, and disposition (success or failure) in a new line of a Comma Separated Values (.csv) file. The Containerized Decomposed Media Server appends the clip information for both the port and conference announcements. The date and time format in the *.csv* file is as follows:

  `YYYY-MM-DDTHH:MM:SS`

  where, YYYY is the year, MM is the month, DD is the day of the month, T is the delimiter between date and time, HH is Hours in 24 hour format, MM is minutes, and ss is seconds.

  NOTE: In a multi-clip announcement, all the clip names are logged in the *.csv* file at the end of the announcement.

For each MRFP instance, the Containerized Decomposed Media Server maintains at the most two separate *.csv* files. The *.csv* file are rotated when the size reaches 50 MB or when the reporting interval expires.

- By using the Web GUI to display current values for statistics in real time.

  The Show Real-Time Statistics page lets you to see the current value of statistics and the current active ports. You can also use this option to obtain a snapshot of Containerized Decomposed Media Server activity by clearing values (using the Reset Statistics option), waiting for the desired interval, then displaying statistics using this option. Standard editing keystrokes can be used to copy (**CTRL+C**) and paste (**CTRL+V**) information from the Output Messages box into another document.

  For more information see, *Show Real-Time Statistics on page 471* and *Reset Statistics on page 464*.

- By examining the statistics file.

  To examine the statistics file, you retrieve it using the Retrieve Statistics option, which posts the file to an external server in plain text. This file can be post-processed using a network analysis tool.

  For more information see, *Retrieve Statistics on page 465*. For more information see, *Statistics File in Text Format on page 425*.

- By polling statistics objects from the SNMP interface.

  You can get a real-time report of statistics for the current interval using the SNMP interface. Values for statistics objects can be obtained or reset all at once, or individually for DSPs, for Ethernet port performance, or for the control protocol.

- Through a protocol request or event.

  Protocol-specific statistics, the availability of which depends on the protocol chosen to control the Containerized Decomposed Media Server, may be reported through an event or as a response to a request. The types and usage of these statistics are described in the Containerized Decomposed Media Server Protocol Guides.

Statistics File in Text Format

The statistics file has the following structure:

- *General Header*
- *Slot Header*
- *Group Header*
- *Statistics Data*

General Header

The general header indicates the time when the statistics file is generated and the system startup time.

Example: General Header of the Statistics File

```
# Stats file generated: Mon Mar 24 19:14:15 2014

# Start time: Fri Mar 21 15:48:30 2014
```

Slot Header

The slot header provides the slot number for the set of statistics.

Example: Slot Header of the Statistics File

```
> Slot: 1
```

Group Header

Every individual statistic belong to a group of related statistics. The group header provides the name for the set of statistics in the group. The group name is followed by two lines reporting, respectively, the number of valid and invalid intervals collected within the last 72-hour period. This is followed by the set of timestamps for the intervals within the period, presented as a comma-separated list. In the following example the statistics uses the default 15-minute collection interval.

Example: Group Header of the Statistics File

```
>> Group: System Usage Group
Number of Valid Intervals: 304
Number of Invalid Intervals: 0
Time stamp:,14:00:00,  13:45:00,  13:30:00,  12:15:00,  12:00:00,  11:45:01,
10:45:00,  10:30:00,  10:15:00,  09:15:00,  09:00:00,  08:45:00,  07:45:01,
07:30:01,  07:15:00,  06:30:00,  06:15:00,  06:00:00,  05:15:00,  05:00:00,
04:15:00,  04:00:00,  03:45:00,  03:00:00,  02:45:00,  02:00:00,  01:45:00,
01:00:00,  00:45:00,  00:00:00,  23:45:01,  23:15:00,  23:00:00,  22:15:00,
22:00:01,  21:30:00,  21:15:00,  20:30:00,  20:15:00,  19:45:01,  19:30:01,
19:00:01,  18:45:01,  18:00:00,  17:15:00,  17:00:00,  16:15:00,  15:30:00,
15:15:01,  14:15:00,  14:00:00,  13:45:00,  13:00:00,  12:45:01,  12:30:00,
12:15:00,  12:00:00,  11:45:00,  11:30:00,  11:15:00,  11:00:00,  10:45:00,
10:30:01,  10:15:01,  10:00:00,  09:45:00,  09:30:00,  09:15:01,  09:00:00,
08:45:00,  08:30:00,  08:15:00,  08:00:00,  07:45:00,  07:30:00,  07:15:00,
07:00:01,  06:45:00,  06:30:00,  06:15:00,  06:00:00,  05:45:00,  05:30:00,
```

```
05:15:00,  05:00:01,  04:45:00,  04:30:00,  04:15:00,  04:00:00,  03:45:00,
03:30:00,  03:15:00,  03:00:00,  02:45:01,  02:30:01,  02:15:00,  Total,  Min,
Max,  Avg,
```

Statistics Data

The statistics data section includes lists of comma-separated statistics: a list for each element in the group. Each list starts from the new line and includes the name of the statistic, followed by the data entries plus four entries providing totals. All MRFP and MRFC statistics are present in the single statistics file.

If applicable, an element in a group may have multiple entries. For example, the Containerized Decomposed Media Server has two Ethernet ports per slot, so the **cardstatEthTxErrors** statistic has two entries, one for each Ethernet port.

The data is listed in the same order as in the **Time Elapsed** field; that is, data for the most recent interval is listed first. For example, statistics data listed third in the list is collected over the interval specified third in the **Time Elapsed** field. If there was no statistics data available during an interval the corresponding entry is replaced with a hyphen (-).

Data for statistics that are not reset every interval, for example Ports Created and Ports Deleted in Session Usage Statistics, are displayed as differences from the previous interval.

The last four numbers in the data represent various totals, as follows:

- **Total.** This value is valid only for “counter” type data; it is not valid for statistic that report minimum, maximum, or average values. It represents the accumulative total of all the statistic element since the statistics were last reset or the last reboot.
- **Minimum.** This statistic reports the lowest value (that is, the minimum of all the minimum values) for this statistic element since the statistics were last reset or the last reboot.
- **Maximum.** This statistic reports the highest value (that is, the maximum of all the maximum values) for this statistic element since the statistics were last reset or the last reboot.
- **Average.** This statistic reports the average value for this statistic element since the statistics were last reset or the last reboot.

The average number of ports is calculated as follows.

```
Avg. Num. Of Ports = (N1 * t1 + N2 * t2 + N3 * t3 + ... + Nn * tn) / T

where:

N1, N2, N3, ..., Nn

are the number of ports active when the sample is taken, and

t1, t2, t3, ..., tn
```

```
is the time between each sample, and T is the time since last reset, which is t1
+ t2 + t3 + ... + tn.
```

Note that this statistic does not accurately represent system behavior for systems where traffic bursts are common.

Sample statistics data are shown below.

Example: Sample Statistics Data

```
Max CPU Core Utilization 1:,   100,  100,  87,  99,  100,  90,  99,  100,  100,
100,  100,  100,  100,  93,  94,  100,  99,  99,  98,  100,  100,  100,  98,  98,
100,  96,  100,  100,  96,  98,  14,  100,  100,  100,  100,  97,  97,  100,  100,
100,  100,  100,  100,  100,  100,  100,  100,  100,  100,  100,  100,  100,  38,
38,  32,  39,  31,  29,  29,  42,  28,  39,  28,  28,  32,  36,  38,  39,  37,
43,  39,  33,  30,  38,  38,  33,  36,  36,  43,  37,  29,  30,  32,  34,  38,
28,  39,  30,  39,  38,  30,  28,  42,  33,  29,  39,  -,  0,  100,  13,

Avg CPU Core Utilization 1:,   12,  12,  12,  12,  12,  12,  14,  14,  14,  14,
14,  14,  14,  14,  14,  13,  14,  14,  14,  14,  14,  14,  14,  13,  14,  13,
14,  14,  14,  14,  14,  14,  14,  13,  14,  13,  14,  14,  14,  14,  14,  13,
14,  14,  14,  14,  14,  14,  14,  14,  14,  14,  9,  9,  9,  9,  9,  9,  9,  9,
9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,
9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  9,  -,  0,  29,  7,


Current CPU Core Utilization 1:,   3,  8,  8,  9,  10,  39,  7,  8,  8,  8,  9,
12,  8,  22,  13,  8,  8,  11,  9,  8,  8,  11,  39,  8,  8,  9,  5,  18,  22,
8,  14,  23,  25,  8,  49,  8,  17,  8,  51,  8,  36,  8,  8,  8,  8,  19,  8,
44,  8,  23,  8,  13,  9,  8,  17,  6,  8,  8,  9,  26,  8,  9,  8,  8,  8,  8,
8,  8,  8,  9,  8,  9,  9,  8,  8,  8,  8,  8,  8,  7,  10,  8,  8,  23,  8,  8,
8,  8,  24,  8,  22,  8,  8,  8,  8,  8,  -,  0,  53,  1,
```

Statistics File in XML Format

The Containerized Decomposed Media Server generates the statistics in XML file format as defined in 3GPP TS 32.401, 32.432, and 32.435.

The following is the recommended naming convention for measurement report file as per 3GPP standards.

```
<Type><Startdate>.<Starttime>-[<Enddate>.]<Endtime>[_-<jobId>][_<UniqueId>][_-
_<RC>]
```

where `<Enddate>`, `<jobId>`, `<UniqueId>`, and `<RC>` are optional parameters.

The Containerized Decomposed Media Server generates the measurement report file with the following naming convention.

```
<Type><Year><Month><Date>.<interval start time>-<interval end time>_<Management IP>
```

For example: `A20180725.0745+0000-0750+0000_10.211.1.112`

In every statistics interval, a new XML file is generated, which contains statistics of the last interval. The Containerized Decomposed Media Server can save a maximum of 288 files. When the statistics file rotation begins, the oldest file is replaced by a new file.

The 3GPP XML file path location is */weboam/swms/stats/xml*.

NOTE: XML statistics file generation depends on the XML configuration in the management interface. After reboot, all existing files are deleted.

XML File Content

XML statistics file content is as follows:

- **<measCollecFile>.** Indicates the top-level tag, which identifies the file as a collection of measurement data and includes the namespace of the XML 3GPP standard.
- **<fileheader>.** Indicates the measurement result file header to be inserted in each file. Includes the file `formatversion` attribute with the value **32.435 V14.0**.
- **<filesender>.** Includes the `elementType` attribute, which provides information about the supported Containerized Decomposed Media Server platform.
- **<measData>.** Represents the sequence of zero or more measurement result items contained in the file.
- **<measCollec>.** Includes the `beginTime` attribute and indicates the time stamp in UTC format at the beginning of the interval.
- **<managedElement>.** Includes the `userLabel` and `swVersion` attributes.
  - **userLabel.** Indicates the user defined name for the network element in 3GPP TS 32.622. The string can be empty if it is not configured in the CM applications. Contains the information of the slot from where the data is being collected inside the **<measdata>**.
  - **swVersion.** Indicates the software version defined for the network element in 3GPP TS 32.622. It is an optional parameter that allows post-processing systems to handle vendor specific measurements modified between software versions.
- **<measInfo>.** Indicates the sequence of measurements, values, and related information. It includes a list of measurement types **measTypes** and the corresponding results **measValues**, together with the time stamp **measTimeStamp** and granularity period **granularityPeriod** pertaining to these measurements. Includes the `measInfoId` attribute that holds the statistics group name.
- **<granPeriod>.** Indicates the granularity period of the measurements in seconds.
  - **duration.** Indicates the statistics interval duration in seconds.
  - **endTime.** This tag contains the time stamp that refers to the end of the measurement collection interval (granularity period). The minimum required information within the timestamp is year, month, day, hour, minute, and second.
- **<measType>.** Indicates the list of measurement types for which the analogous list of measurement values **measValues** pertains. Includes the `p` attribute that has sequence number of elements in the corresponding group.

- **<measValue>.** Contains the list of measurement results for the resource being measured. **measValue** includes an identifier of the resource **measObjInstId**, the list of measurement result values **measResults**, and a flag that indicates whether the data is reliable **suspectFlag**. Includes the **measObjLdn** attribute, which holds the slot number information with specific detail of the group or can be blank.
- **<r>.** Includes the **p** attribute, which has sequence number with respect to **p** in the **measType**. This tag holds the actual statistics value.
- **<fileFooter>.** Indicates the end of the XML statistics file.

XML File Sample

The XML statistics file sample is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<measCollecFile
xmlns="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec">
	<fileHeader fileFormatVersion="32.435 V14.0">
		<fileSender elementType="SWMS"/>
		<measCollec beginTime="2018-07-25T07:45:00+0000"/>
	</fileHeader>
	<measData>
		<managedElement userLabel="Slot1" swVersion="1.0.0"/>
		<measInfo measInfoId="CPU Core Group">
			<granPeriod duration="PT300S" endTime="2018-07-
		25T07:50:00+0000"/>
				<measType p="1">Max CPU Core Utilization</measType>
				<measType p="2">Avg CPU Core Utilization</measType>
				<measType p="3">Current CPU Core Utilization</measType>
				<measValue measObjLdn="Slot=1, core=1">
					<r p="1">6</r>
					<r p="2">1</r>
					<r p="3">1</r>
				</measValue>
				<measValue measObjLdn="Slot=1, core=2">
					<r p="1">0</r>
					<r p="2">0</r>
					<r p="3">0</r>
				</measValue>
				<measValue measObjLdn="Slot=1, core=3">
					<r p="1">0</r>
					<r p="2">0</r>
```

```
                <r p="3">0</r>
            </measValue>
            <measValue measObjLdn="Slot=1, core=4">
                <r p="1">0</r>
                <r p="2">0</r>
                <r p="3">0</r>
            </measValue>
            <measValue measObjLdn="Slot=1, core=5">
                <r p="1">0</r>
                <r p="2">0</r>
                <r p="3">0</r>
            </measValue>
            <measValue measObjLdn="Slot=1, core=6">
                <r p="1">0</r>
                <r p="2">0</r>
                <r p="3">0</r>
            </measValue>
            <measValue measObjLdn="Slot=1, core=7">
                <r p="1">0</r>
                <r p="2">0</r>
                <r p="3">0</r>
            </measValue>
        </measInfo>
</measData>
<measData>
<managedElement userLabel="Slot2" swVersion="1.0.0"/>
<measInfo measInfoId="System Usage Group">
        <granPeriod duration="PT300S" endTime="2018-07-
25T07:50:00+0000"/>
            <measType p="1">Card Up Time</measType>
            <measType p="2">Min Free RAM</measType>
            <measType p="3">Current Free RAM</measType>
            <measType p="4">Min Free RAM Drive Space</measType>
            <measType p="5">Avg Free RAM</measType>
            <measType p="6">Min Free System/Process
        Memory</measType>
            <measType p="7">Current Free System/Process
        Memory</measType>
```

```
                <measType p="8">Max Smoothed CPU Utilization</measType>
                <measType p="9">Current Smoothed CPU
            Utilization</measType>
                <measType p="10">Current Free RAM Drive Space</measType>
                <measType p="11">Min Free MPCCP System/Process
            Memory</measType>
                <measType p="12">Current Free MPCCP System/Process
            Memory</measType>
                <measType p="13">Min Free Transient Clip Partition
            Space</measType>
                <measType p="14">Level 2 Cache Enabled Time</measType>
                <measValue measObjLdn="">
                    <r p="1">-</r>
                    <r p="2">-</r>
                    <r p="3">-</r>
                    <r p="4">-</r>
                    <r p="5">-</r>
                    <r p="6">-</r>
                    <r p="7">-</r>
                    <r p="8">-</r>
                    <r p="9">-</r>
                    <r p="10">-</r>
                    <r p="11">-</r>
                    <r p="12">-</r>
                    <r p="13">-</r>
                    <r p="14">-</r>
                </measValue>
            </measInfo>
        </measData>
    <fileFooter>
        <measCollec endTime="2018-07-25T07:50:00+0000"/>
    </fileFooter>
</measCollecFile>
```

Prometheus Support on Performance Management

Prometheus is an open-source systems monitoring and alerting toolkit, which collects metrics from the monitored targets by scraping metrics HTTP and HTTPS endpoints on these targets.

Prometheus stores all data's as time series, that is, the streams of timestamped values belonging to the same metric and the same set of labeled dimensions. Besides stored time series, Prometheus may generate temporary derived time series as the result of queries.

Every time, the series is uniquely identified by its metric name and optional key-value pairs called labels.

The metric name specifies the general feature of a system that is measured.

For example, `Max_Ports`, the maximum number of ports used for G711 during the last statistics interval.

Labels enable the Prometheus's dimensional data model, that is, any given combination of labels for the same metric name identifies a particular dimensional instantiation of that metric. For example, slot value is 3 and the CodecType is G.711.

Changing any label value, including adding or removing a label may create a new time series.

Notation:

```
<metric name>{<label name>=<label value>, ...}
e.g: Max_Ports{slot="3",CodecType="G.711",} 0.0
```

Prometheus support for performance management is applicable only in Containerized Decomposed Media Server.

The Containerized Decomposed Media Server supports either IPv4 or IPv6 based on the management interface and the prometheus must pull the data respectively.

The statistics data are pulled by prometheus from the Containerized Decomposed Media Server at regular intervals.

NOTE:

- The Prometheus gets the last reporting interval statistics from Containerized Decomposed Media Server (not a real time statistics), when it queries for the metrics.
- The least scraping interval at which the statistics can be pulled is 5 minutes.
- The Containerized Decomposed Media Server support the statistics scrapping request only on the http interface.
- When the first statistics reporting interval is not completed in the Containerized Decomposed Media Server, at the sametime, if we get the scrape request from the prometheus, the Containerized Decomposed Media Server response with the 200 OK without the metric information for the pull request.

For example,

 # HELP Min_Free_RAM_Drive_Space. The maximum CPU utilization (%) of the control processor in each statistics collection interval.

```
# TYPE Min_Free_RAM_Drive_Space gauge
Min_Free_RAM_Drive_Space{Slot="1",} 100.0
```

From the metric label, `slot="1"` represents MRFC and the values from 3 to 22 represents MRFP.

Only Containerized Decomposed Media Server slots comes under *Show Instance Status* Web GUI Page are exported at statistics reporting interval.

If the statistics value is `"-"` in case of statistics log file mentioned in the chapter 3 , in prometheus, it is exported as 0.

It is recommended to pull the data by prometheus within the cluster.

We can change the log level of REST API logs inside OAMP pod with the below changes and it takes effect after a minute.

1. Login to OAMP pod.
2. Edit the level in the file */opt/swms/etc/logback-spring-prometheus.xml* with the supported values WARN, ERROR, INFO, and DEBUG.

For example,

```
<logger name="com.radisys.prometheus_client" additivity="false" level="WARN">
```

And logs are in the file */var/log/REST_prometheus.log*.

NOTE: Each metric contains label as a slot, which represents 1 for MRFC and 3 to 22 for MRFP.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Dropped UDP Packets Group	Dropped UDP Packets RX	Dropped_UDP_Packets	{Slot=slot|Type=RX}	Gauge	The number of UDP packets dropped by the control processor IP stack in the receive direction.
Dropped UDP Packets Group	Dropped UDP Packets TX	Dropped_UDP_Packets	{Slot=slot|Type=TX}	Gauge	The number of UDP packets dropped by the control processor IP stack in the transmit direction.
SIP Usage Group	Max Command Rate	Command_Rate	{Slot=slot|Type=Max}	Gauge	The maximum command rate in requests per second, using one second sample periods.
SIP Usage Group	Avg Command Rate	Command_Rate	{Slot=slot|Type=Avg}	Gauge	The average requests rate for the interval in commands per second.
SIP Usage Group	Avg Hold Time	Hold_Time	{Slot=slot|Type=Avg}	Gauge	The average hold time for calls disconnected during the interval.
SIP Usage Group	Max Hold Time	Hold_Time	{Slot=slot|Type=Max}	Gauge	The maximum hold time for calls disconnected during the interval.
SIP Usage Group	Min Hold Time	Hold_Time	{Slot=slot|Type=Min}	Gauge	The minimum hold time for calls disconnected during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
SIP Usage Group	Request Failure Errors (4xx)	Request_Failure_Errors	{Slot=slot|ResponseCode=4xx}	Gauge	Number of 4xx errors.
SIP Usage Group	Request Failure Errors (400)	Request_Failure_Errors	{Slot=slot|ResponseCode=400}	Gauge	Number of 400 errors.
SIP Usage Group	Request Failure Errors (403)	Request_Failure_Errors	{Slot=slot|ResponseCode=403}	Gauge	Number of 403 errors.
SIP Usage Group	Request Failure Errors (404)	Request_Failure_Errors	{Slot=slot|ResponseCode=404}	Gauge	Number of 404 errors.
SIP Usage Group	Request Failure Errors (405)	Request_Failure_Errors	{Slot=slot|ResponseCode=405}	Gauge	Number of 405 errors.
SIP Usage Group	Request Failure Errors (406)	Request_Failure_Errors	{Slot=slot|ResponseCode=406}	Gauge	Number of 406 errors.
SIP Usage Group	Request Failure Errors (408)	Request_Failure_Errors	{Slot=slot|ResponseCode=408}	Gauge	Number of 408 errors.
SIP Usage Group	Request Failure Errors (415)	Request_Failure_Errors	{Slot=slot|ResponseCode=415}	Gauge	Number of 415 errors.
SIP Usage Group	Request Failure Errors (420)	Request_Failure_Errors	{Slot=slot|ResponseCode=420}	Gauge	Number of 420 errors.
SIP Usage Group	Request Failure Errors (422)	Request_Failure_Errors	{Slot=slot|ResponseCode=422}	Gauge	Number of 422 errors.
SIP Usage Group	Request Failure Errors (423)	Request_Failure_Errors	{Slot=slot|ResponseCode=423}	Gauge	Number of 423 errors.
SIP Usage Group	Request Failure Errors (471)	Request_Failure_Errors	{Slot=slot|ResponseCode=471}	Gauge	Number of 471 errors.
SIP Usage Group	Request Failure Errors (480)	Request_Failure_Errors	{Slot=slot|ResponseCode=480}	Gauge	Number of 480 errors.
SIP Usage Group	Request Failure Errors (481)	Request_Failure_Errors	{Slot=slot|ResponseCode=481}	Gauge	Number of 481 errors.
SIP Usage Group	Request Failure Errors (482)	Request_Failure_Errors	{Slot=slot|ResponseCode=482}	Gauge	Number of 482 errors.
SIP Usage Group	Request Failure Errors (483)	Request_Failure_Errors	{Slot=slot|ResponseCode=483}	Gauge	Number of 483 errors.
SIP Usage Group	Request Failure Errors (484)	Request_Failure_Errors	{Slot=slot|ResponseCode=484}	Gauge	Number of 484 errors.
SIP Usage Group	Request Failure Errors (486)	Request_Failure_Errors	{Slot=slot|ResponseCode=486}	Gauge	Number of 486 errors.
SIP Usage Group	Request Failure Errors (487)	Request_Failure_Errors	{Slot=slot|ResponseCode=487}	Gauge	Number of 487 errors.
SIP Usage Group	Request Failure Errors (488)	Request_Failure_Errors	{Slot=slot|ResponseCode=488}	Gauge	Number of 488 errors.
SIP Usage Group	Request Failure Errors (491)	Request_Failure_Errors	{Slot=slot|ResponseCode=491}	Gauge	Number of 491 errors.
SIP Usage Group	Server Failure Errors (5xx)	Server_Failure_Errors	{Slot=slot|ResponseCode=5xx}	Gauge	Number of 5xx errors.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
SIP Usage Group	Server Failure Errors (500)	Server_Failure_Errors	{Slot=slot|ResponseCode=500}	Gauge	Number of 500 errors.
SIP Usage Group	Server Failure Errors (501)	Server_Failure_Errors	{Slot=slot|ResponseCode=501}	Gauge	Number of 501 errors.
SIP Usage Group	Server Failure Errors (503)	Server_Failure_Errors	{Slot=slot|ResponseCode=503}	Gauge	Number of 503 errors.
SIP Usage Group	Server Failure Errors (504)	Server_Failure_Errors	{Slot=slot|ResponseCode=504}	Gauge	Number of 504 errors.
SIP Usage Group	Server Failure Errors (505)	Server_Failure_Errors	{Slot=slot|ResponseCode=505}	Gauge	Number of 505 errors.
SIP Usage Group	Global Failure Errors (6xx)	Global_Failure_Errors	{Slot=slot|ResponseCode=6xx}	Gauge	Number of 6xx errors.
SIP Usage Group	Global Failure Errors (600)	Global_Failure_Errors	{Slot=slot|ResponseCode=600}	Gauge	Number of 600 errors.
SIP Usage Group	Global Failure Errors (603)	Global_Failure_Errors	{Slot=slot|ResponseCode=603}	Gauge	Number of 603 errors.
SIP Usage Group	SIP Packets RX	SIP_Packets	{Slot=slot|Type=RX}	Gauge	The counter value for number of incoming packets.
SIP Usage Group	SIP Packets TX	SIP_Packets	{Slot=slot|Type=TX}	Gauge	The counter value for number of outgoing packets.
SIP Usage Group	Out of Resource Errors	Out_Of_Resource_Errors	{Slot=slot}	Gauge	The number of out of resource errors.
SIP Usage Group	Call Overload Request Rejections	Call_Overload_Request_Rejections	{Slot=slot}	Gauge	The number of call overload events detected.
SIP Usage Group	Service Overload Request Rejections	Service_Overload_Request_Rejections	{Slot=slot}	Gauge	The number of service overload events detected.
SIP Usage Group	Accepted Incoming Priority Calls	Priority_Calls	{Slot=slot|Type=Accepted}	Gauge	The number of SIP invite requests containing an RPH that are accepted by the Media Server.
SIP Usage Group	Established Priority Calls	Priority_Calls	{Slot=slot|Type=Established}	Gauge	The number of SIP invite requests containing an RPH that are established by sending a 200 response to the invite request.
SIP Usage Group	Completed Priority Calls	Priority_Calls	{Slot=slot|Type=Completed}	Gauge	The number of SIP invite requests containing an RPH that are established and subsequently terminated normally.
SIP Usage Group	Priority Out of Resource Errors	Priority_Calls	{Slot=slot|Type=Out_of_Resource_Errors}	Gauge	The number of **out of resource** responses sent for SIP RPH calls.
SIP Usage Group	Priority Timeout Errors	Priority_Calls	{Slot=slot|Type=Timeout_Errors}	Gauge	The number of **timeout** responses sent for SIP RPH calls.
SIP Usage Group	SIP Dropped Msg due Full Serialization Queue	SIP_Dropped_Msg_Due_Full_Serialization_Queue	{Slot=slot}	Gauge	The total number of dropped SIP messages due to full serialization queue.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
SIP Usage Group	Total Sip Ports Deleted Due Rtcp Bye	Total_SIP_Ports_Deleted	{Slot=slot|Type=Due_to_Rtcp_Bye}	Gauge	The total number of SIP ports deleted due to RTCP BYE.
SIP Usage Group	Total Sip Video Ports Deleted DuetoRtcpBye	Total_SIP_Ports_Deleted	{Slot=slot|Type=Due_to_Video_Rtcp_Bye}	Gauge	The total number of SIP video ports deleted due to RTCP BYE.
SIP Usage Group	Total RTCP timeout events generated on SIP audio port	Total_RTCP_Timeout_Events_Generated	{Slot=slot|Type=Audio_Port}	Gauge	The total number of RTCP timeout events generated on SIP audio port.
SIP Usage Group	Total RTCP timeout events generated on SIP video port	Total_RTCP_Timeout_Events_Generated	{Slot=slot|Type=Video_Port}	Gauge	The total number of RTCP timeout events generated on SIP video port.
SIP Usage Group	Total SIP audio ports deleted due toRTCPtimeout	Total_SIP_Ports_Deleted	{Slot=slot|Type=Due_to_Audio_RTCP_timeout}	Gauge	The total number of SIP audio ports deleted due to RTCP timeout event.
SIP Usage Group	Total SIP video ports deleted due toRTCPtimeout	Total_SIP_Ports_Deleted	{Slot=slot|Type=Due_to_Video_RTCP_timeout}	Gauge	The total number of SIP video ports deleted due to RTCP timeout event.
SIP Usage Group	Regular Calls Rejected Due To AccessControl	Regular_Calls_Rejected_Due_To_Access_Control	{Slot=slot}	Gauge	The regular calls rejected due to access control.
SIP Usage Group	Total Priority Calls Received	Priority_Calls	{Slot=slot|Type=Received}	Gauge	The total priority calls received.
SIP Usage Group	Priority Calls Rejected As Priority Management Disabled	Priority_Calls	{Slot=slot|Type=Rejected_As_Priority_Management_Disabled}	Gauge	The priority calls rejected as priority management is disabled.
SIP Usage Group	Priority Calls Accepted As Regular Calls	Priority_Calls	{Slot=slot|Type=Accepted_As_Regular_Calls}	Gauge	The prioruty calls accepted as regular calls.
SIP Usage Group	Total number of TLS calls established	Number_Of_TLS_calls	{Slot=slot|Type=Established}	Gauge	The total number of TLS calls established.
SIP Usage Group	Total number of TLS calls failed	Number_Of_TLS_calls	{Slot=slot|Type=Failed}	Gauge	The total number of TLS calls failed.
ASR/TTS Usage Group	Max TTS Ports	TTS_Ports	{Slot=slot|Type=Max}	Gauge	The maximum number of TTS ports in use at one time during the interval.
ASR/TTS Usage Group	Total TTS Ports	TTS_Ports	{Slot=slot|Type=Total}	Gauge	A running total of the TTS ports created.
ASR/TTS Usage Group	TTS Errors	TTS_Errors	{Slot=slot}	Gauge	The number of errors, including out of resource errors, that occurred on TTS ports during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
ASR/TTS Usage Group	TTS Out of Resource Errors	TTS_Out_Of_Resource_Errors	{Slot=slot}	Gauge	The number of out of resource errors that occurred on TTS ports during the interval.
ASR/TTS Usage Group	Max ASR Ports	ASR_Ports	{Slot=slot|Type=Max}	Gauge	The maximum number of ASR ports in use at one time during the interval.
ASR/TTS Usage Group	Total ASR Ports	ASR_Ports	{Slot=slot|Type=Total}	Gauge	A running total of the ASR ports created.
ASR/TTS Usage Group	ASR Errors	ASR_Errors	{Slot=slot}	Gauge	The number of errors, including out of resource errors, that occurred on ASR ports during the interval.
ASR/TTS Usage Group	ASR Out of Resource Errors	ASR_Out_Of_Resource_Errors	{Slot=slot}	Gauge	The number of out of resource errors that occurred on ASR ports during the interval.
ASR/TTS Usage Group	3xx Errors	ASR_TTS_Connection_Error	{Slot=slot|Type=3xx_Errors}	Gauge	The number of 3xx error responses received on ASR/TTS connections over the interval.
ASR/TTS Usage Group	4xx Errors	ASR_TTS_Connection_Error	{Slot=slot|Type=4xx_Errors}	Gauge	The number of 4xx error responses received on ASR/TTS connections over the interval.
ASR/TTS Usage Group	5xx Errors	ASR_TTS_Connection_Error	{Slot=slot|Type=5xx_Errors}	Gauge	The number of 5xx error responses received on ASR/TTS connections over the interval.
ASR/TTS Usage Group	6xx Errors	ASR_TTS_Connection_Error	{Slot=slot|Type=6xx_Errors}	Gauge	The number of 6xx error responses received on ASR/TTS connections over the interval.
ASR/TTS Usage Group	Total Tts-Ports Deleted Due Rtcp Bye	Ports_Deleted_Due_Rtcp_Bye	{Slot=slot|Type=TTS}	Gauge	The total number of TTS ports deleted due to RTCP BYE.
ASR/TTS Usage Group	Total Asr-Ports Deleted Due Rtcp Bye	Ports_Deleted_Due_Rtcp_Bye	{Slot=slot|Type=ASR}	Gauge	The total number of ASR ports deleted due to RTCP BYE.
ASR/TTS Usage Group	Total Rtsp-Ports Deleted Due Rtcp Bye	Ports_Deleted_Due_Rtcp_Bye	{Slot=slot|Type=RTSP}	Gauge	The total number of RTSP ports deleted due to RTCP BYE.
B2buaUsageGroup	Proxy Dialogs Received	B2BUA_Requests	{Slot=slot|DialogsType=Proxy|Type=Received}	Gauge	The number of proxy dialogs received.
B2buaUsageGroup	Total Proxy Dialogs Received	B2BUA_Requests	{Slot=slot|DialogsType=Proxy|Type=TotalReceived}	Gauge	The total number of proxy dialogs received.
B2buaUsageGroup	B2BUA Dialogs Received	B2BUA_Requests	{Slot=slot|DialogsType=B2BUA|Type=Received}	Gauge	The number of B2BUA dialogs terminated.
B2buaUsageGroup	Total B2BUA Dialogs Received	B2BUA_Requests	{Slot=slot|DialogsType=B2BUA|Type=Total Received}	Gauge	The total number of successful B2BUA dialogs received.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
B2buaUsageGroup	Proxy Dialogs Failed	B2BUA_Requests	{Slot=slot|DialogsType=Proxy|Type=Failed}	Gauge	Number of failed proxy dialogs.
B2buaUsageGroup	B2BUA Dialogs Failed	B2BUA_Requests	{Slot=slot|DialogsType=B2BUA|Type=Failed}	Gauge	Number of failed B2BUA dialogs.
Disk Max Usage Group	Disk Max Usage Root	Disk_Max_Usage	{Slot=slot|DiskType=Root}	Gauge	Disk maximum usage for directory Root.
Disk Max Usage Group	Disk Max Usage Boot	Disk_Max_Usage	{Slot=slot|DiskType=Boot}	Gauge	Disk maximum usage for directory Boot.
Disk Max Usage Group	Disk Max Usage Weboam	Disk_Max_Usage	{Slot=slot|DiskType=Weboam}	Gauge	Disk maximum usage for directory Weboam.
Disk Max Usage Group	Disk Max Usage Home	Disk_Max_Usage	{Slot=slot|DiskType=Home}	Gauge	Disk maximum usage for directory Home.
Disk Max Usage Group	Disk Max Usage Opt	Disk_Max_Usage	{Slot=slot|DiskType=Opt}	Gauge	Disk maximum usage for directory Opt.
Disk Max Usage Group	Disk Max Usage Space	Disk_Max_Usage	{Slot=slot|DiskType=Space}	Gauge	Disk maximum usage for directory Space.
Disk Max Usage Group	Disk Max Usage Usr	Disk_Max_Usage	{Slot=slot|DiskType=Usr}	Gauge	Disk maximum usage for directory Usr.
Disk Max Usage Group	Disk Max Usage Var	Disk_Max_Usage	{Slot=slot|DiskType=Var}	Gauge	Disk maximum usage for directory Var.
Disk Max Usage Group	Disk Max Usage Mnt_Ramdisk	Disk_Max_Usage	{Slot=slot|DiskType=Ramdisk}	Gauge	Disk maximum usage for directory Mnt Ramdisk.
Disk Max Usage Group	Disk Max Usage Mnt	Disk_Max_Usage	{Slot=slot|DiskType=Mnt}	Gauge	Disk maximum usage for directory Mnt
Disk Max Usage Group	Disk Max Usage Dev_Shm	Disk_Max_Usage	{Slot=slot|DiskType=DevShm}	Gauge	Disk maximum usage for directory Dev Shm
Disk Max Usage Group	Disk Max Usage Tmp	Disk_Max_Usage	{Slot=slot|DiskType=Tmp}	Gauge	Disk maximum usage for directory Tmp
Disk Max Usage Group	Disk Max Usage Var_Log	Disk_Max_Usage	{Slot=slot|DiskType=VarLog}	Gauge	Disk maximum usage for directory Var Log
Disk Max Usage Group	Disk Max Usage Var_Log_Audit	Disk_Max_Usage	{Slot=slot|DiskType=VarLogAudit}	Gauge	Disk maximum usage for directory Var Log Audit
Disk Max Usage Group	Disk Max Usage Var_Opt_Swms_Clips	Disk_Max_Usage	{Slot=slot|DiskType=VarOptSwmsClips}	Gauge	Disk maximum usage for directory Var Opt Swms Clip
DSP Usage Group	RTP Packets TX	RTP_Packets	{Slot=slot|Type=TX}	Gauge	The number of RTP packets for all DSPs transmitted during the interval.
DSP Usage Group	RTP Audio Packets TX	RTP_Packets	{Slot=slot|Type=Audio_TX}	Gauge	The number of RTP packets for all audio DSPs transmitted during the interval.
DSP Usage Group	RTP Video Packets TX	RTP_Packets	{Slot=slot|Type=Video_TX}	Gauge	The number of RTP packets for all video DSPs transmitted during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
DSP Usage Group	RTP Packets RX	RTP_Packets	{Slot=slot|Type=RX}	Gauge	The number of RTP packets for all DSPs received during the interval.
DSP Usage Group	RTP Audio Packets RX	RTP_Packets	{Slot=slot|Type=Audio_RX}	Gauge	The number of RTP packets for all audio DSPs received during the interval.
DSP Usage Group	RTP Video Packets RX	RTP_Packets	{Slot=slot|Type=Video_RX}	Gauge	The number of RTP packets for all video DSPs received during the interval.
DSP Usage Group	RTP Packets Lost	RTP_Packets	{Slot=slot|Type=Lost}	Gauge	The number of lost RTP packets for all DSPs during the interval based on RTP sequence number.
DSP Usage Group	RTP Audio Packets Lost	RTP_Packets	{Slot=slot|Type=Audio_Lost}	Gauge	The number of lost RTP packets for audio all DSPs during the interval based on RTP sequence number.
DSP Usage Group	RTP Video Packets Lost	RTP_Packets	{Slot=slot|Type=Video_Lost}	Gauge	The number of lost RTP packets for video in all DSPs during the interval based on RTP sequence number.
DSP Usage Group	RTP Interarrival Jitter	RTP_Interarrival_Jitter	{Slot=slot}	Gauge	The maximum jitter for all DSPs during the interval.
DSP Usage Group	Max DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max}	Gauge	The maximum DSP CPU utilization for all DSPs during the interval.
DSP Usage Group	Avg DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg}	Gauge	The average DSP CPU utilization for all DSPs during the interval.
DSP Usage Group	Max Modeled DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Modeled}	Gauge	The maximum modeled DSP CPU utilization for all DSPs during the interval.
DSP Usage Group	Avg Modeled DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Modeled}	Gauge	The average modeled DSP CPU utilization for all DSPs during the interval.
DSP Usage Group	Max Modeled Audio DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Modeled_Audio}	Gauge	The maximum modeled DSP CPU utilization for all audio DSPs during the interval.
DSP Usage Group	Avg Modeled Audio DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Modeled_Audio}	Gauge	The average modeled DSP CPU utilization for all Audio DSPs during the interval.
DSP Usage Group	Max Actual Audio DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Actual_Audio}	Gauge	The maximum actual DSP CPU utilization for all Audio DSPs during the interval.
DSP Usage Group	Avg Actual Audio DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Actual_Audio}	Gauge	The average actual DSP CPU utilization for all Audio DSPs during the interval.
DSP Usage Group	Max Modeled Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Modeled_Video}	Gauge	The maximum modeled DSP CPU utilization for all video DSPs during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
DSP Usage Group	Avg Modeled Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Modeled_Video}	Gauge	Average Modeled DSP CPU utilization for all Video DSPs during the interval
DSP Usage Group	Max Actual Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Actual_Video}	Gauge	Maximum Actual DSP CPU utilization for all Video DSPs during the interval
DSP Usage Group	Avg Actual Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Actual_Video}	Gauge	Average Actual DSP CPU utilization for all Video DSPs during the interval
DSP Usage Group	Max Modeled HC Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Modeled_HC_Video}	Gauge	Maximum Modeled DSP CPU utilization for all HC DSPs during the interval
DSP Usage Group	Avg Modeled HC Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Modeled_HC_Video}	Gauge	Average Modeled DSP CPU utilization for all HC DSPs during the interval
DSP Usage Group	Max Actual HC Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Max_Actual_HC_Video}	Gauge	Maximum Actual DSP CPU utilization for all HC DSPs during the interval
DSP Usage Group	Avg Actual HC Video DSP CPU Utilization	DSP_CPU_Utilization	{Slot=slot|Type=Avg_Actual_HC_Video}	Gauge	Average Actual DSP CPU utilization for all HC DSPs during the interval
DSP Usage Group	Slipped Cycle Count	Slipped_Cycle_Count	{Slot=slot}	Gauge	Number of slipped cycles during the interval for all audio DSPs
DSP Usage Group	Max DSP HW Packets	Max_DSP_HW_Packets	{Slot=slot}	Gauge	Maximum number of DSP command packets sent for all DSPs
DSP Usage Group	Lost packets recovered using redundant RTP	Lost_Packets_Recovered_Using_Redundant_RTP	{Slot=slot}	Gauge	The number of lost packets recovered using redundant RTP (RFC2198) during the last period for all DSPs
DSP Usage Group	Total Rtcp Bye-Packets Received	Total_Rtcp_Bye_Packets_Received	{Slot=slot}	Gauge	Total number of RTCP BYE packets received for all DSPs
DSP Usage Group	Max Video Encoder Frame Rate Drop Rate	Max_Video_Encoder_Frame_Rate_Drop_Rate	{Slot=slot}	Gauge	The maximum frames drop percentage (Video) during the last period
DSP Usage Group	T.140 Bytes Sent	T140_Bytes_Sent	{Slot=slot}	Gauge	T.140 Bytes sent
DSP Usage Group	T.140 Bytes Received	T140_Bytes_Received	{Slot=slot}	Gauge	T.140 Bytes Received
DSP Usage Group	T.140 Packets Missed not replaceable by redundant T.140 Packets	T140_Packets_Missed_Not_Replaceable_By_Redundant_T140_Packets	{Slot=slot}	Gauge	T.140 packets missed not replaceable by redundant T.140 Packets

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
DSP Usage Group	T.140 Chars Mapped To Apostrophe Chars in TTY streams	T140_Chars_Mapped_To_Apostrophe_Chars_In_TTY_Streams	{Slot=slot}	Gauge	T.140 characters mapped to apostrophe characters in TTY steam
DSP Usage Group	Max Frames Dropped (HC Video)	Max_Frames_Dropped_HC_Video	{Slot=slot}	Gauge	The maximum frames drop percentage (HC Video) during the last period.
DSP Usage Group	Super Slipped Cycle Count (Audio)	Super_Slipped_Cycle_Count	{Slot=slot|Type=Audio}	Gauge	Number of super slipped cycles during the interval for all audio DSPs.
DSP Usage Group	Super Slipped Cycle Count (Video)	Super_Slipped_Cycle_Count	{Slot=slot|Type=Video}	Gauge	Number of super slipped cycles during the interval for all video DSPs.
DSP Usage Group	Super Slipped Cycle Count (HC Video)	Super_Slipped_Cycle_Count	{Slot=slot|Type=HC_Video}	Gauge	Number of super slipped cycles during the interval for all HC video DSPs.
DSP Usage Group	Max Burst Slip Cycles (Audio)	Max_Burst_Slip_Cycles	{Slot=slot|Type=Audio}	Gauge	Maximum burst Cycle received during the interval for audio DSP.
DSP Usage Group	Max Burst Slip Cycles (Video)	Max_Burst_Slip_Cycles	{Slot=slot|Type=Video}	Gauge	Maximum burst Cycle received during the interval for video DSP.
DSP Usage Group	Max Burst Slip Cycles (HC Video)	Max_Burst_Slip_Cycles	{Slot=slot|Type=HC_Video}	Gauge	Maximum burst Cycle received during the interval for HC video DSP.
DSP Usage Group	Burst Slip Cycles Exceed Limit (HC Video)	Burst_Slip_Cycles_Exceed_Limit_HC_Video	{Slot=slot}	Gauge	Total number of times the burst slipped cycle exceeds limit for all HC video DSPs during the reporting interval.
DSP Usage Group	Dropped Video Packets	Dropped_Video_Packets	{Slot=slot}	Gauge	Total number of Dropped Packets for all video DSPs during the reporting interval.
DSP Usage Group	Jitter Buffer Frames Dropped	Jitter_Buffer_Frames_Dropped	{Slot=slot}	Gauge	Total duration (in unit of ms) of audio frames dropped by jitter buffer for all audio DSPs during the reporting interval.
DSP Usage Group	Non Decoded Video Frames	Non_Decoded_Frames	{Slot=slot|Type=Video}	Gauge	Counts the number of video frames that are not decoded for all video DSPs during the reporting interval.
DSP Usage Group	Non Decoded Audio Frames	Non_Decoded_Frames	{Slot=slot|Type=Audio}	Gauge	Counts the duration (in unit of ms) of audio frames that are not decoded by decoder for all audio DSPs during the reporting interval.
DSP Usage Group	Avg Number of Audio Cores Used	Number_of_Cores_Used	{Slot=slot|Type=Avg_Audio}	Gauge	Gives the average number of audio cores used.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
DSP Usage Group	Max Number of Audio Cores Used	Number_of_Cores_Used	{Slot=slot|Type=Max_Audio}	Gauge	Counts the maximum number of audio cores used.
DSP Usage Group	Avg Number of Video Cores Used	Number_of_Cores_Used	{Slot=slot|Type=Avg_Video}	Gauge	Gives the average number of video cores used.
DSP Usage Group	Max Number of Video Cores Used	Number_of_Cores_Used	{Slot=slot|Type=Max_Video}	Gauge	Counts the maximum number of video cores used.
DSP Usage Group	Avg Number of Free Cores	Number_of_Free_Cores	{Slot=slot|Type=Avg}	Gauge	Gives the average number of free cores.
DSP Usage Group	Max Number of Free Cores	Number_of_Free_Cores	{Slot=slot|Type=Max}	Gauge	Counts the maximum number of free cores.
Fax Usage Group	T.38 Faxes Sent	T38_Fax	{Slot=slot|Type=Faxes_Sent}	Gauge	Number of T.38 faxes sent.
Fax Usage Group	T.38 Faxes Received	T38_Fax	{Slot=slot|Type=Faxes_Received}	Gauge	Number of T.38 faxes received.
Fax Usage Group	T.38 Pages Sent	T38_Fax	{Slot=slot|Type=Pages_Sent}	Gauge	Number of T.38 pages sent.
Fax Usage Group	T.38 Pages Received	T38_Fax	{Slot=slot|Type=Pages_Received}	Gauge	Number of T.38 pages received.
Fax Usage Group	T.38 Fax Send Failed	T38_Fax	{Slot=slot|Type=Faxes_Sent_Failed}	Gauge	Number of T.38 fax send failed.
Fax Usage Group	T.38 Fax Received Failed	T38_Fax	{Slot=slot|Type=Faxes_Received_Failed}	Gauge	Number of T.38 fax received failed.
Fax Usage Group	T.38 Retransmissions	T38_Fax	{Slot=slot|Type=Faxes_Retransmissions}	Gauge	Number of T.38 retransmissions.
Fax Usage Group	G.711 Faxes Sent	G711_Fax	{Slot=slot|Type=Faxes_Sent}	Gauge	Number of G.711 faxes sent.
Fax Usage Group	G.711 Faxes Received	G711_Fax	{Slot=slot|Type=Faxes_Received}	Gauge	Number of G.711 faxes received.
Fax Usage Group	G.711 Pages Sent	G711_Fax	{Slot=slot|Type=Pages_Sent}	Gauge	Number of G.711 pages sent.
Fax Usage Group	G.711 Pages Received	G711_Fax	{Slot=slot|Type=Pages_Received}	Gauge	Number of G.711 pages received.
Fax Usage Group	G.711 Fax Send Failed	G711_Fax	{Slot=slot|Type=Faxes_Sent_Failed}	Gauge	Number of G.711 fax send failed.
Fax Usage Group	G.711 Fax Received Failed	G711_Fax	{Slot=slot|Type=Faxes_Received_Failed}	Gauge	Number of G.711 fax received failed.
Fax Usage Group	G.711 Retransmissions	G711_Fax	{Slot=slot|Type=Faxes_Retransmissions}	Gauge	Number of G.711 retransmissions.
HTTP Media Statistics Group	HTTP Clip Requests	HTTP_Clip_Requests	{Slot=slot}	Gauge	The number of audio clips requested from HTTP sources during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
HTTP Media Statistics Group	Cache Hits No Validation	HTTP_Cache_Hits_No_Validation	{Slot=slot}	Gauge	The number of audio clips served from the cache without requiring validation during the interval.
HTTP Media Statistics Group	Cache Hits with Validation	HTTP_Cache_Hits_with_Validation	{Slot=slot}	Gauge	The number of audio clips served from the cache after validation during the interval.
HTTP Media Statistics Group	Cache Misses	HTTP_Cache_Misses	{Slot=slot}	Gauge	The number of audio clips that were retrieved from HTTP servers (cache misses) during the interval.
HTTP Media Statistics Group	Non-Cacheable	HTTP_Non_Cacheable	{Slot=slot}	Gauge	The number of audio clips that were retrieved from HTTP servers that were non-cacheable during the interval.
HTTP Media Statistics Group	Cache Overflows	HTTP_Cache_Overflows	{Slot=slot}	Gauge	The number of clips that could not be played because not enough memory could be made available for the clip in the cache during the interval.
MIKEY Usage Group	MIKEY Initiator Messages Received	MIKEY_Messages	{Slot=slot|Type=Received}	Gauge	Number of MIKEY initiator messages received during the interval.
MIKEY Usage Group	MIKEY Initiator Message Authentication Failures	MIKEY_Messages	{Slot=slot|Type=Authentication_Failure}	Gauge	Number of MIKEY initiator message authentication failures during the interval.
MIKEY Usage Group	MIKEY Initiator Messages Rejected to MIKEY Replay Cache	MIKEY_Messages	{Slot=slot|Type=Rejected_to_MIKEY_Replay_Cache}	Gauge	Number of MIKEY initiator messages rejected to MIKEY replay cache during the interval.
MIKEY Usage Group	MIKEY Response Messages Generated	MIKEY_Messages	{Slot=slot|Type=Response_Generated}	Gauge	Number of MIKEY response messages generated during the interval.
MIKEY Usage Group	MIKEY Error Response Messages Generated	MIKEY_Messages	{Slot=slot|Type=Error_Response_Generated}	Gauge	Number of MIKEY error response messages generated during the interval.
MIKEY Usage Group	MIKEY Verification Response Messages Generated	MIKEY_Messages	{Slot=slot|Type=Verification_Response_Generated}	Gauge	Number of MIKEY verification response messages generated during the interval.
MRFC Stats Group	MrfCtrl SIP message Sent	MrfCtrl_SIP_message	{Slot=slot|Type=Sent}	Gauge	Number of SIP messages sent successfully from MRFC to MRFP.
MRFC Stats Group	MrfCtrl SIP message Received	MrfCtrl_SIP_message	{Slot=slot|Type=Received}	Gauge	Number of SIP messages received successfully from MRFP Invite accepted.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
MRFC Stats Group	MrfCtrl MRFP Failure	MrfCtrl_SIP_message	{Slot=slot|Type=Failed}	Gauge	Number of calls when MRFP is not reachable.
MRFC Stats Group	Annlab Media Files Newly Added	Annlab_Media_Files	{Slot=slot|Type=NewlyAdded}	Gauge	The number of newly created announcement files.
MRFC Stats Group	Annlab Media Files Deleted	Annlab_Media_Files	{Slot=slot|Type=Deleted}	Gauge	the number of announcements that have been removed from the Virtual File System.
MRFC Stats Group	Annlab Media Files updated	Annlab_Media_Files	{Slot=slot|Type=Updated}	Gauge	The number of announcements that have been updated from the Virtual File System.
MRFC Stats Group	Annlab Media Files Provision Error	Annlab_Media_Files	{Slot=slot|Type=ProvisionError}	Gauge	The number of announcements that failed to be created, updated or deleted.
MRFC Stats Group	Annlab Total number of Media Files	Annlab_Media_Files	{Slot=slot|Type=Exists}	Gauge	The total number of media files existing on the VFS at a given time.
MRFC Stats Group	Annlab weight of media files in Koctets	Annlab_Media_Files	{Slot=slot|Type=WeightInKoctets}	Gauge	The disk space occupancy in Kilo Octets (KB) in the entire VFS.
MRFC Stats Group	Annlab Media Files Transfer Succeeded	Annlab_Media_Files	{Slot=slot|Type=TransferSucceeded}	Gauge	Number of successful media file transfers on the clients of the cluster.
MRFC Stats Group	Annlab Media Files Transfer Failed	Annlab_Media_Files	{Slot=slot|Type=TransferFailed}	Gauge	Number of unsuccessful media files transfers on the clients of the cluster.
MRFC Stats Group	MrfCtrl Total number of TLS Calls Established	MrfCtrl_Total_Number_Of_TLS_Calls	{Slot=slot|Type=Established}	Gauge	Total number of TLS Calls Established.
MRFC Stats Group	MrfCtrl Total number of TLS Calls Failed	MrfCtrl_Total_Number_Of_TLS_Calls	{Slot=slot|Type=Failed}	Gauge	Total number of TLS Calls Failed.
MRFP Redundancy Groups	Number of Auto Switchovers	Number_Of_Switchovers	{Slot=slot|RedundancyGroup=Index|Type=Auto}	Gauge	The number of automatic switchovers occurred in a MPC redundancy group for each interval.
MRFP Redundancy Groups	Number of Manual Switchovers	Number_Of_Switchovers	{Slot=slot|RedundancyGroup=Index|Type=Manual}	Gauge	The number of manual switchovers occurred in a MPC redundancy group for each interval.
MSML Usage Group	Total Announcement Requests	Service_Requests	{Slot=slot|ServiceType=Announcement|Type=Total}	Gauge	The total number of accepted MSML announcement requests.
MSML Usage Group	Total Successful Announcement Requests	Service_Requests	{Slot=slot|ServiceType=Announcement|Type=Successful}	Gauge	The total number of successful announcement attempts.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
MSML Usage Group	Total Failed Announcement Requests	Service_Requests	{Slot=slot|ServiceType=Announcement|Type=Failed}	Gauge	The total number of failed MSML announcement requests.
MSML Usage Group	Total Failed Announcement Requests due to All Clips were Skipped	Failed_Announcement_Requests	{Slot=slot|Reason=All_Clips_were_Skipped}	Gauge	The number of announcement requests failed all clips in a multi-clip announcement were skipped because of issues with the clip.
MSML Usage Group	Total Failed Announcement Requests due to Video Issues	Failed_Announcement_Requests	{Slot=slot|Reason=Video_Issues}	Gauge	The number of announcement requests failed because the announcement included video files and an offset or interval attribute existed or the video parameter was changed to higher capability between clips.
MSML Usage Group	Total Failed Announcement Requests due to System Resource Unavailability	Failed_Announcement_Requests	{Slot=slot|Reason=System_Resource_Unavailability}	Gauge	The number of announcement requests failed due to system resource unavailability.
MSML Usage Group	Total Failed Announcement Requests due to File Not Found Error	Failed_Announcement_Requests	{Slot=slot|Reason=File_Not_Found_Error}	Gauge	The number of announcement requests failed due to file not found error.
MSML Usage Group	Total Failed Announcement Requests due to External Server Error	Failed_Announcement_Requests	{Slot=slot|Reason=External_Server_Error}	Gauge	The number of announcement requests failed because the external server returned an error other than Time out, File not found or NFS server down error conditions.
MSML Usage Group	Total Failed Announcement Requests due to Link is Down	Failed_Announcement_Requests	{Slot=slot|Reason=Link_is_Down}	Gauge	The number of announcement requests failed because link to external HTTP or NFS server has failed.
MSML Usage Group	Total Failed Announcement Requests due to Timeout	Failed_Announcement_Requests	{Slot=slot|Reason=Timeout}	Gauge	The number of announcement requests that failed because the external HTTP server is timed out for the reason other than link failure.
MSML Usage Group	Total Failed Announcement Requests due to Speech Server Error	Failed_Announcement_Requests	{Slot=slot|Reason=Speech_Server_Error}	Gauge	The number of announcement requests that failed while a TTS clip is rendered because the external speech server returned an error.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
MSML Usage Group	Total Failed Announcement Requests due to HTTP Cache is Disabled	Failed_Announcement_Requests	{Slot=slot|Reason=HTTP_Cache_is_Disabled}	Gauge	The number of announcement requests that failed because http cache is disabled.
MSML Usage Group	Total Failed Announcement Requests due to Invalid Announcement File	Failed_Announcement_Requests	{Slot=slot|Reason=Invalid_Announcement_File}	Gauge	The number of announcement requests that failed because of Invalid announcement file.
MSML Usage Group	Total Failed Announcement Requests due to Server Timeout Error	Failed_Announcement_Requests	{Slot=slot|Reason=Server_Timeout_Error}	Gauge	Total number of failed announcement requests due to TTS/MRCP server timeout error.
MSML Usage Group	Total Failed Announcement Requests due to Server Connection Error	Failed_Announcement_Requests	{Slot=slot|Reason=Server_Connection_Error}	Gauge	Total number of failed announcement requests due to TTS/MRCP server connection error.
MSML Usage Group	Total Failed Announcement Requests due to Server Internal Error	Failed_Announcement_Requests	{Slot=slot|Reason=Server_Internal_Error}	Gauge	Total number of failed announcement requests due to TTS/MRCP server internal error.
MSML Usage Group	Total Failed Announcement Requests due to Server Authentication Error	Failed_Announcement_Requests	{Slot=slot|Reason=Server_Authentication_Error}	Gauge	Total number of failed announcement requests due to TTS/MRCP server authentication error.
MSML Usage Group	Total Failed Announcement Requests due to Server Overload Error	Failed_Announcement_Requests	{Slot=slot|Reason=Server_Overload_Error}	Gauge	Total number of failed announcement requests due to TTS/MRCP server overload error.
MSML Usage Group	Total Failed Announcement Requests due to Other Reasons	Failed_Announcement_Requests	{Slot=slot|Reason=Other_Reasons}	Gauge	The number of announcement requests that failed because of other reasons.
MSML Usage Group	Total Create Conference Attempt Requests	Service_Requests	{Slot=slot|ServiceType=CreateConference|Type=Total}	Gauge	The total number of attempted MSML <createconference> requests received.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
MSML Usage Group	Total Successful Create Conference Requests	Service_Requests	{Slot=slot|ServiceType=CreateConference|Type=Successful}	Gauge	The total number of successful MSML <createconference> requests.
MSML Usage Group	Total Failed Create Conference Requests	Service_Requests	{Slot=slot|ServiceType=CreateConference|Type=Failed}	Gauge	The total number of failed MSML <createconference> requests.
MSML Usage Group	Total Join Requests between Port and Conference	Service_Requests	{Slot=slot|ServiceType=JoinConference|Type=Total}	Gauge	The total number of attempted MSML <join> requests between port and conference received.
MSML Usage Group	Total Successful Join Requests between Port and Conference	Service_Requests	{Slot=slot|ServiceType=JoinConference|Type=Successful}	Gauge	The total number of successful MSML <join> requests between port and conference.
MSML Usage Group	Total Failed Join Requests between Port and Conference	Service_Requests	{Slot=slot|ServiceType=JoinConference|Type=Failed}	Gauge	The total number of failed MSML <join> requests between port and conference.
Secure RTCP Usage Group	SRTCP Packets with Authentication Failures	SRTCP_Packets_Errors	{Slot=slot|Reason=Authentication_Failures}	Gauge	Number of SRTCP packets with authentication failures.
Secure RTCP Usage Group	SRTCP Packets Dropped Due to SRTCP Replay Cache	SRTCP_Packets_Errors	{Slot=slot|Reason=Dropped_Due_to_SRTP_Replay_Cache}	Gauge	Number of SRTCP packets dropped due to SRTCP replay cache.
Secure RTP Usage Group	SRTP Packets with Authentication Failures	SRTP_Packets_Errors	{Slot=slot|Reason=Authentication_Failures}	Gauge	Number of SRTP packets with authentication failures for all the DSPs.
Secure RTP Usage Group	SRTP Packets Dropped Due to SRTP Replay Cache	SRTP_Packets_Errors	{Slot=slot|Reason=Dropped_Due_to_SRTP_Replay_Cache}	Gauge	Number of SRTP packets dropped due to SRTP replay cache for all the DSPs.
System Usage Group	Card Up Time	Card_Up_Time	{Slot=slot}	Gauge	Counts the number of 10 milliseconds that the system has been running for.
System Usage Group	Min Free RAM	Min_Free_RAM	{Slot=slot}	Gauge	Minimum free system memory (%) of the control processor in each statistics collection interval.
System Usage Group	Current Free RAM	Current_Free_RAM	{Slot=slot}	Gauge	The current free system memory The utilization calculation uses 1-second samples.
System Usage Group	Min Free RAM Drive Space	Min_Free_RAM_Drive_Space	{Slot=slot}	Gauge	The minimum free RAM drive space during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
System Usage Group	Avg Free RAM	Avg_Free_RAM	{Slot=slot}	Gauge	The average free system memory (%) of the control processor in each statistics collection interval.
System Usage Group	Min Free System/Process Memory	Min_Free_System_Process_Memory	{Slot=slot}	Gauge	The minimum system and minimum process memory during the interval.
System Usage Group	Current Free System/Process Memory	Current_Free_System_Process_Memory	{Slot=slot}	Gauge	The current free memory of the system.
System Usage Group	Max Smoothed CPU Utilization	Max_Smoothed_CPU_Utilization	{Slot=slot}	Gauge	The maximum `smoothed` CPU utilization during the interval.
System Usage Group	Current Smoothed CPU Utilization	Current_Smoothed_CPU_Utilization	{Slot=slot}	Gauge	Current `smoothed` CPU utilization.
System Usage Group	Current Free RAM Drive Space	Current_Free_RAM_Drive_Space	{Slot=slot}	Gauge	The current percentage of free space in the rd1 (/ramdisk) partition.
System Usage Group	Min Free MPCCP System/Process Memory	Min_Free_MPCCP_System_Process_Memory	{Slot=slot}	Gauge	The minimum system and current process memory of mpccp.
System Usage Group	Current Free MPCCP System/Process Memory	Current_Free_MPCCP_System_Process_Memory	{Slot=slot}	Gauge	The current process memory of mpccp.
System Usage Group	Min Free Transient Clip Partition Space	Min_Free_Transient_Clip_Partition_Space	{Slot=slot}	Gauge	The minimum percentage of space free in the partition containing transient clips.
System Usage Group	Level 2 Cache Enabled Time	Level2_Cache_Enabled_Time	{Slot=slot}	Gauge	The amount of time in seconds the system is running with the level 2 cache enabled.
VoiceXML Usage Group	Max Active Channels	VXML_Max_Active_Channels	{Slot=slot}	Gauge	Maximum number of active VoiceXML channels for the current statistics interval.
VoiceXML Usage Group	No Channels Session Rejections	VXML_No_Channels_Session_Rejections	{Slot=slot}	Gauge	Number of VoiceXML channels rejected due to no channels available.
VoiceXML Usage Group	Current Active Channels	VXML_Current_Active_Channels	{Slot=slot}	Gauge	Current number of active VoiceXML channels.
VoiceXML Usage Group	Service Overload Session Rejections	VXML_Service_Overload_Session_Rejections	{Slot=slot}	Gauge	Number of VoiceXML channels rejected due to service overload exceeded.
Session Usage Group	Ports Created	Number_Of_Ports	{Slot=slot|Type=Created}	Gauge	The number of ports created since the last reset.
Session Usage Group	Ports Deleted	Number_Of_Ports	{Slot=slot|Type=Deleted}	Gauge	The number of ports deleted since the last reset.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Max Ports Active	Active_Ports	{Slot=slot|Type=Max}	Gauge	The maximum number of ports that have been operational simultaneously, since the last reset.
Session Usage Group	Avg Ports Active	Active_Ports	{Slot=slot|Type=Avg}	Gauge	The average number of ports active since the last reset.
Session Usage Group	Current Ports Active	Active_Ports	{Slot=slot|Type=Current}	Gauge	The number of ports that are currently active.
Session Usage Group	Max Announcements	Max_Service	{Slot=slot|Type=Announcement}	Gauge	The maximum number of announcement services that have been simultaneously active on the Containerized Decomposed Media Server.
Session Usage Group	Max Conferences	Max_Service	{Slot=slot|Type=Conference}	Gauge	The maximum number of Conference Mixes that have been simultaneously active on the Containerized Decomposed Media Server.
Session Usage Group	Max Recordings	Max_Service	{Slot=slot|Type=Recording}	Gauge	The maximum number of recording services that have been simultaneously active on the Containerized Decomposed Media Server.
Session Usage Group	Max DTMF Detectors	Max_Service	{Slot=slot|Type=DTMFDetectors}	Gauge	The maximum number of DTMF Detectors that have been simultaneously active on the Containerized Decomposed Media Server.
Session Usage Group	Max G.711 Ports	Max_Ports	{Slot=slot|CodecType=G.711}	Gauge	The maximum number of ports used for G711 during the last statistics interval.
Session Usage Group	Max G.729 Ports	Max_Ports	{Slot=slot|CodecType=G.729}	Gauge	The maximum number of ports used for G729 during the last statistics interval.
Session Usage Group	Max G.726 Ports	Max_Ports	{Slot=slot|CodecType=G.726}	Gauge	The maximum number of ports used for G726 during the last statistics interval.
Session Usage Group	Max AMR-NB Ports	Max_Ports	{Slot=slot|CodecType=AMR-NB}	Gauge	The maximum number of ports used for AMR during the last statistics interval.
Session Usage Group	Max G.722 Ports	Max_Ports	{Slot=slot|CodecType=G.722}	Gauge	The maximum number of ports used for G722 during the last statistics interval.
Session Usage Group	Max H.263 Ports	Max_Ports	{Slot=slot|CodecType=H.263}	Gauge	The maximum number of ports used for H263 during the last statistics interval.
Session Usage Group	Max H.264 Ports	Max_Ports	{Slot=slot|CodecType=H.264}	Gauge	The maximum number of ports used for H264 during the last statistics interval.
Session Usage Group	Dropped External Announcement Streams	Dropped_External_Announcement_Streams	{Slot=slot}	Gauge	The number of announcement streams dropped due to a timeout or a server error.
Session Usage Group	Dropped External Recording Streams	Dropped_External_Recording_Streams	{Slot=slot}	Gauge	The number of recording streams dropped due to a timeout or a server error.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Current SRTP Ports Allocated	Current_SRTP_Ports_Allocated	{Slot=slot}	Gauge	The current number of SRTP ports allocated.
Session Usage Group	CPA Events	CPA_Events	{Slot=slot}	Gauge	The number of call progress analysis events reported.
Session Usage Group	CP_LIVE_CALL Events	CP_LIVE_CALL_Events	{Slot=slot}	Gauge	The number of CP LIVE CALL events reported.
Session Usage Group	CP_GREETING Events	CP_GREETING_Events	{Slot=slot}	Gauge	The number of CP GREETING events reported.
Session Usage Group	Noisy Line Reports	Noisy_Line_Reports	{Slot=slot}	Gauge	The number of ports that have had noisy line reports.
Session Usage Group	Noisy Line Reports Discarded	Noisy_Line_Reports_Discarded	{Slot=slot}	Gauge	The number of noisy line reports discarded due to insufficient resources.
Session Usage Group	Max NLD Ports Enabled	Max_NLD_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which Noisy Line Detection is enabled during the interval.
Session Usage Group	Max G.711 and G.722 PLC Ports Enabled	Max_G711_and_G722_PLC_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of G.711 and G.726 ports on which Packet Loss Concealment is enabled during the interval.
Session Usage Group	Max PPS Ports Enabled	Max_PPS_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which Per Port Statistics is enabled during the interval.
Session Usage Group	Max NG Ports Enabled	Max_NG_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which Noise Gating is enabled during the interval.
Session Usage Group	Max NR Ports Enabled	Max_NR_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which Noise Reduction is enabled during the interval.
Session Usage Group	Max AEC Ports Enabled	Max_AEC_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which Acoustic Echo Cancellation is enabled during the interval.
Session Usage Group	Max AEC Ports Active	Max_AEC_Ports_Active	{Slot=slot}	Gauge	The maximum number of ports on which Acoustic Echo Cancellation is enabled and active during the interval.
Session Usage Group	Max AEC Ports Resource Limited	Max_AEC_Ports_Resource_Limited	{Slot=slot}	Gauge	The maximum number of ports on which Acoustic Echo Cancellation is enabled and could not be active due to resource limitations during the interval.
Session Usage Group	Max EVRC Ports	Max_Ports	{Slot=slot|CodecType=EVRC}	Gauge	The maximum number of ports used for EVRC0 and EVRC codec during the last statistics interval.
Session Usage Group	Max Auto NR Ports Enabled	Max_Auto_NR_Ports_Enabled	{Slot=slot}	Gauge	The maximum number of ports on which auto Noise Reduction is enabled during the interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Max Auto NR Ports Activated	Max_Auto_NR_Ports_Activated	{Slot=slot}	Gauge	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected and NR turned on.
Session Usage Group	Max NR Ports Resource Limited	Max_NR_Ports_Resource_Limited	{Slot=slot}	Gauge	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected and NR not turned on due to resource limitation.
Session Usage Group	Max NR Ports Config Limited	Max_NR_Ports_Config_Limited	{Slot=slot}	Gauge	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected and NR not turned on due to port limit.
Session Usage Group	Num AEC Monitor Resources Requested	Num_AEC_Monitor_Resources_Requested	{Slot=slot}	Gauge	The number of times a Echo Canceller Monitoring resource is requested.
Session Usage Group	Num AEC Monitor Resources Req Denied	Num_AEC_Monitor_Resources_Req_Denied	{Slot=slot}	Gauge	The number of times a Echo Canceller Monitoring resource is requested and fails to get a resource.
Session Usage Group	Max AEC Monitors in Use	Max_AEC_Monitors_In_Use	{Slot=slot}	Gauge	The maximum number of simultaneous Echo Canceller Monitoring resources are in use.
Session Usage Group	Max EVRCB Ports	Max_Ports	{Slot=slot|CodecType=EVRCB}	Gauge	The maximum number of ports used for EVRCB0 and EVRCB codec during the last statistics interval.
Session Usage Group	NUM Total Full Mix Count	Number_Of_Total_Full_Mix_Count	{Slot=slot}	Gauge	The total number of times that the number of active speakers above the threshold is equal to the number of speakers allowed in the audio mix.
Session Usage Group	Max Full Time Ratio	Max_Full_Time_Ratio	{Slot=slot}	Gauge	Maximum full time ratio.
Session Usage Group	Max T38 Fax Ports	Max_Ports	{Slot=slot|CodecType=T38_Fax}	Gauge	The maximum number of ports used for T38 fax codec during the last period.
Session Usage Group	Max G.711 Fax Ports	Max_Ports	{Slot=slot|CodecType=G.711_Fax}	Gauge	The maximum number of ports used for G711 fax codec during the last period.
Session Usage Group	Max iLBC Ports	Max_Ports	{Slot=slot|CodecType=iLBC}	Gauge	The maximum number of ports used for iLBC codec during the last period.
Session Usage Group	Max Mpeg4V Ports	Max_Ports	{Slot=slot|CodecType=Mpeg4V}	Gauge	The maximum number of ports used for MPEG-4 Visual during the last period.
Session Usage Group	Max VP8 Ports	Max_Ports	{Slot=slot|CodecType=VP8}	Gauge	The maximum number of ports used for VP8 during the last period.
Session Usage Group	Max AMR-WB Ports	Max_Ports	{Slot=slot|CodecType=AMR-WB}	Gauge	The maximum number of ports used for AMR-WB during the last period.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Max Ports T.140	Max_Ports	{Slot=slot|CodecType =T.140}	Gauge	The maximum number of port used for t140.
Session Usage Group	Max Detectors TTY	Max_Detectors_TTY	{Slot=slot}	Gauge	The maximum number of detectors used for tty.
Session Usage Group	Max Opus-NB Ports	Max_Ports	{Slot=slot|CodecType =Opus-NB}	Gauge	The maximum number of ports used for Opus-NB during the last period.
Session Usage Group	Max Opus-WB Ports	Max_Ports	{Slot=slot|CodecType =Opus-WB}	Gauge	The maximum number of ports used for Opus-WB during the last period.
Session Usage Group	Max Evs Ports	Max_Ports	{Slot=slot|CodecType =EVS}	Gauge	The maximum number of ports used for Evs during the last period.
Session Usage Group	Number of times VQE License Exhausted	Number_Of_Times_VQE_License_Exhausted	{Slot=slot}	Gauge	The number of times media port created or modified regardless of VQE license unavailability.
Session Usage Group	Max H.265 Ports	Max_Ports	{Slot=slot|CodecType =H.265}	Gauge	The maximum number of ports used for H265 during the last statistics interval.
Session Usage Group	Max EVRCNW Ports	Max_Ports	{Slot=slot|CodecType =EVRCNW}	Gauge	The maximum number of ports used for EVRCNW0 and EVRCNW codec during the last statistics interval.
Session Usage Group	Total Transcoded Announcement on Audio Ports	Transcoded_Announcement	{Slot=slot|PortType= Audio|Type=Total}	Gauge	The total number of transcoded announcements on audio ports in the reporting interval.
Session Usage Group	Max number of Active Transcoded Announcement on audio ports	Transcoded_Announcement	{Slot=slot|PortType= Audio|Type=MaxActiv e}	Gauge	The max number of transcoded announcements active simultaneously on audio ports in the reporting interval.
Session Usage Group	Total number of transcoded announcement on video ports	Transcoded_Announcement	{Slot=slot|PortType= Video|Type=Total}	Gauge	The total number of transcoded announcements on video ports in the reporting interval.
Session Usage Group	Max number of active transcoded announcement on video ports	Transcoded_Announcement	{Slot=slot|PortType= Video|Type=MaxActiv e}	Gauge	The max number of transcoded announcements active simultaneously on video ports in the reporting interval.
Session Usage Group	Max number of active AMR-WB announcement on AMR ports	Max_Number_Of_Active_Announcements_Ports	{Slot=slot|AnncType= AMR-WB_On_AMR_Port}	Gauge	The maximum number of AMR-WB announcements active simultaneously on AMR ports during the interval.
Session Usage Group	Max number of active AMR announcement on AMR ports	Max_Number_Of_Active_Announcements_Ports	{Slot=slot|AnncType= AMR_On_AMR_Port}	Gauge	The maximum number of AMR announcements active simultaneously on AMR ports during the interval that were transcoded.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Max number of active AMR announcement on AMR-WB ports	Max_Number_Of_Active_Announcements_Ports	{Slot=slot|AnncType=AMR_On_AMR-WB_Port}	Gauge	The maximum number of AMR announcements active simultaneously on AMR-WB ports during the interval.
Session Usage Group	Max number of active AMR-WB announcement on AMR-WB ports	Max_Number_Of_Active_Announcements_Ports	{Slot=slot|AnncType=AMR-WB_On_AMR-WB_Port}	Gauge	The maximum number of AMR-WB announcements active simultaneously on AMR-WB ports during the interval that were transcoded.
Session Usage Group	Total number of PCMA announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=PCMA}	Gauge	Total number of times announcement service was invoked on PCMA ports in the reporting interval.
Session Usage Group	Total number of PCMU announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=PCMU}	Gauge	Total number of times announcement service was invoked on PCMU ports in the reporting interval.
Session Usage Group	Total number of AMR announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=AMR}	Gauge	Total number of times announcement service was invoked on AMR ports in the reporting interval.
Session Usage Group	Total number of AMR-WB announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=AMR-WB}	Gauge	Total number of times announcement service was invoked on AMR-WB ports in the reporting interval.
Session Usage Group	Total number of EVS announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=EVS}	Gauge	Total number of times announcement service was invoked on EVS ports in the reporting interval.
Session Usage Group	Total number of G.722 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=G.722}	Gauge	Total number of times announcement service was invoked on G.722 ports in the reporting interval.
Session Usage Group	Total number of G.729 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=G.729}	Gauge	Total number of times announcement service was invoked on G.729 ports in the reporting interval.
Session Usage Group	Total number of OPUS announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=OPUS}	Gauge	Total number of times announcement service was invoked on OPUS ports in the reporting interval.
Session Usage Group	Total number of EVRC announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=EVRC}	Gauge	Total number of times announcement service was invoked on EVRC ports in the reporting interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Total number of EVRCB announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=EVRCB}	Gauge	Total number of times announcement service was invoked on EVRCB ports in the reporting interval.
Session Usage Group	Total number of EVRCNW announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=EVRCNW}	Gauge	Total number of times announcement service was invoked on EVRCNW ports in the reporting interval.
Session Usage Group	Total number of H.263 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=H.263}	Gauge	Total number of times announcement service was invoked on H.263 ports in the reporting interval.
Session Usage Group	Total number of H.264 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=H.264}	Gauge	Total number of times announcement service was invoked on H.264 ports in the reporting interval.
Session Usage Group	Total number of MPEG-4 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=MPEG4}	Gauge	Total number of times announcement service was invoked on MPEG-4 ports in the reporting interval.
Session Usage Group	Total number of VP8 announcement ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Announcement|CodecType=VP8}	Gauge	Total number of times announcement service was invoked on VP8 ports in the reporting interval.
Session Usage Group	Total number of PCMA recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=PCMA}	Gauge	Total number of times record service was invoked on PCMA ports in the reporting interval.
Session Usage Group	Total number of PCMU recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=PCMU}	Gauge	Total number of times record service was invoked on PCMU ports in the reporting interval.
Session Usage Group	Total number of AMR recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=AMR}	Gauge	Total number of times record service was invoked on AMR ports in the reporting interval.
Session Usage Group	Total number of AMR-WB recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=AMR-WB}	Gauge	Total number of times record service was invoked on AMR-WB ports in the reporting interval.
Session Usage Group	Total number of EVS recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=EVS}	Gauge	Total number of times record service was invoked on EVS ports in the reporting interval.
Session Usage Group	Total number of G.722 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=G.722}	Gauge	Total number of times record service was invoked on G.722 ports in the reporting interval.
Session Usage Group	Total number of G.729 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=G.729}	Gauge	Total number of times record service was invoked on G.729 ports in the reporting interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Total number of OPUS recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=OPUS}	Gauge	Total number of times record service was invoked on OPUS ports in the reporting interval.
Session Usage Group	Total number of EVRC recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=EVRC}	Gauge	Total number of times record service was invoked on EVRC ports in the reporting interval.
Session Usage Group	Total number of EVRCB recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=EVRCB}	Gauge	Total number of EVRCB recording ports in the reporting interval.
Session Usage Group	Total number of EVRCNW recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=EVRCNW}	Gauge	Total number of times record service was invoked on EVRCNW ports in the reporting interval.
Session Usage Group	Total number of H.263 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=H.263}	Gauge	Total number of times record service was invoked on H.263 ports in the reporting interval.
Session Usage Group	Total number of H.264 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=H.264}	Gauge	Total number of times record service was invoked on H.264 ports in the reporting interval.
Session Usage Group	Total number of MPEG-4 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=MPEG4}	Gauge	Total number of times record service was invoked on MPEG-4 ports in the reporting interval.
Session Usage Group	Total number of VP8 recording ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Recording|CodecType=VP8}	Gauge	Total number of times record service was invoked on VP8 ports in the reporting interval.
Session Usage Group	Total number of PCMA conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=PCMA}	Gauge	Total number of times conference service was invoked on PCMA ports in the reporting interval.
Session Usage Group	Total number of PCMU conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=PCMU}	Gauge	Total number of times conference service was invoked on PCMU ports in the reporting interval.
Session Usage Group	Total number of AMR conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=AMR}	Gauge	Total number of times conference service was invoked on AMR ports in the reporting interval.
Session Usage Group	Total number of AMR-WB conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=AMR-WB}	Gauge	Total number of times conference service was invoked on AMR-WB ports in the reporting interval.
Session Usage Group	Total number of EVS conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=EVS}	Gauge	Total number of times conference service was invoked on EVS ports in the reporting interval.
Session Usage Group	Total number of G.722 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=G.722}	Gauge	Total number of times conference service was invoked on G.722 ports in the reporting interval.
Session Usage Group	Total number of G.729 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=G.729}	Gauge	Total number of times conference service was invoked on G.729 ports in the reporting interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Total number of OPUS conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=OPUS}	Gauge	Total number of times conference service was invoked on OPUS ports in the reporting interval.
Session Usage Group	Total number of EVRC conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=EVRC}	Gauge	Total number of times conference service was invoked on EVRC ports in the reporting interval.
Session Usage Group	Total number of EVRCB conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=EVRCB}	Gauge	Total number of times conference service was invoked on EVRCB ports in the reporting interval.
Session Usage Group	Total number of EVRCNW conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=EVRCNW}	Gauge	Total number of times conference service was invoked on EVRCNW ports in the reporting interval.
Session Usage Group	Total number of H.263 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=H.263}	Gauge	Total number of times conference service was invoked on H.263 ports in the reporting interval.
Session Usage Group	Total number of H.264 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=H.264}	Gauge	Total number of times conference service was invoked on H.264 ports in the reporting interval.
Session Usage Group	Total number of MPEG-4 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=MPEG4}	Gauge	Total number of times conference service was invoked on MPEG-4 ports in the reporting interval.
Session Usage Group	Total number of VP8 conference ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Conference|CodecType=VP8}	Gauge	Total number of times conference service was invoked on VP8 ports in the reporting interval.
Session Usage Group	Total number of PCMA transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=PCMA}	Gauge	Total number of Port to Port transcoding sessions established for PCMA ports in the reporting interval.
Session Usage Group	Total number of PCMU transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=PCMU}	Gauge	Total number of Port to Port transcoding sessions established for PCMU ports in the reporting interval.
Session Usage Group	Total number of AMR transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=AMR}	Gauge	Total number of Port to Port transcoding sessions established for AMR ports in the reporting interval.
Session Usage Group	Total number of AMR-WB transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=AMR-WB}	Gauge	Total number of Port to Port transcoding sessions established for AMR-WB ports in the reporting interval.
Session Usage Group	Total number of EVS transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=EVS}	Gauge	Total number of Port to Port transcoding sessions established for EVS ports in the reporting interval.
Session Usage Group	Total number of G.722 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=G.722}	Gauge	Total number of Port to Port transcoding sessions established for G.722 ports in the reporting interval.
Session Usage Group	Total number of G.729 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=G.729}	Gauge	Total number of Port to Port transcoding sessions established for G.729 ports in the reporting interval.

Table 112. Details of Prometheus Metrics

Statistics Group Name	Statistics Name	Metric Name	Label details	Metric Type	Description
Session Usage Group	Total number of OPUS transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=OPUS}	Gauge	Total number of Port to Port transcoding sessions established for OPUS ports in the reporting interval.
Session Usage Group	Total number of EVRC transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=EVRC}	Gauge	Total number of Port to Port transcoding sessions established for EVRC ports in the reporting interval.
Session Usage Group	Total number of EVRCB transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=EVRCB}	Gauge	Total number of Port to Port transcoding sessions established for EVRCB ports in the reporting interval.
Session Usage Group	Total number of EVRCNW transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=EVRCNW}	Gauge	Total number of Port to Port transcoding sessions established for EVRCNW ports in the reporting interval.
Session Usage Group	Total number of H.263 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=H.263}	Gauge	Total number of Port to Port transcoding sessions established for H.263 ports in the reporting interval.
Session Usage Group	Total number of H.264 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=H.264}	Gauge	Total number of Port to Port transcoding sessions established for H.264 ports in the reporting interval.
Session Usage Group	Total number of MPEG-4 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=MPEG4}	Gauge	Total number of Port to Port transcoding sessions established for MPEG-4 ports in the reporting interval.
Session Usage Group	Total number of VP8 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=VP8}	Gauge	Total number of Port to Port transcoding sessions established for VP8 ports in the reporting interval.
Session Usage Group	Total number of T140 transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=T140}	Gauge	Total number of Port to Port transcoding sessions established for T140 ports in the reporting interval.
Session Usage Group	Max Active KWD Sessions	Max_Active_KWD_Sessions	{Slot=slot}	Gauge	Maximum number of keyword detection sessions active simultaneously during the interval. This statistic is reset at the beginning of each interval.
Session Usage Group	Total number of ILBC transcoding ports	Total_Number_Of_Service_Ports	{Slot=slot|ServiceType=Transcoding|CodecType=ILBC}	Gauge	Total number of ILBC transcoding ports.
Session Usage Group	Total Number Of CP_AM_BEEP Events	Total_Number_Of_CP_AM_BEEP_Events	{Slot=slot}	Gauge	Total Number of CP AM BEEP Events.
Session Usage Group	Max Number Of AM_BEEP Session	Max_Number_Of_AM_BEEP_Session	{Slot=slot}	Gauge	Max number of AM Beep Sessions.

NOTE:

YAML and template changes for enabling the feature are listed below:

In *values.yaml* the following fields has to be modified for Prometheus to work.

```
  prometheus:
 isEnabled: false
 scrape: true
 path: "/metrics"
 scheme: "http"
```

where,

- `isEnabled` represents whether the feature needs to be enabled or not.
- `scrape` represents whether the auto discovery has to be enabled and disabled.
- `path` is not advisable to edit, because the changes do not take effect in Containerized Decomposed Media Server.
- `Schema` can be HTTP or HTTPS to scrape the statistics from the OAMP pod.

Apart from this, there is a port for Prometheus for communication purpose.

```
prometheus:
      endpoint: 9090
      nodePort: 30058
```

Port 8091 is reserved for internal Prometheus statistics communication. This port number must not be used for other purpose.

For HTTP

The Prometheus server versions supported for Containerized Decomposed Media Server are 2.18.1 and 2.22. The below mentioned configuration is used during the Prometheus installation for service discovery when Containerized Decomposed Media Server management is IPv4 *(config_map.yaml)*.

```
scrape_configs:
      - job_name: 'prometheus_cdmrf'

        kubernetes_sd_configs:
        - role: pod

relabel_configs:
        - source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_scrape]
          action: keep
          regex: true
        - source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_path]
          action: replace
          target_label: __metrics_path__
```

```
          regex: (.+)
        - source_labels: [__address__,
__meta_kubernetes_pod_annotation_prometheus_io_port]
          action: replace
          regex: ([^:]+)(?::\d+)?;(\d+)
          replacement: $1:$2
          target_label: __address__
        - action: labelmap
          regex: __meta_kubernetes_pod_label_(.+)
        - source_labels: [__meta_kubernetes_namespace]
          action: replace
          target_label: kubernetes_namespace
        - source_labels: [__meta_kubernetes_pod_name]
          action: replace
          target_label: kubernetes_pod_name
```

The Prometheus server versions supported for Containerized Decomposed Media Server are 2.18.1 and 2.22. The below mentioned configuration is used during the Prometheus installation for service discovery when Containerized Decomposed Media Server management is IPv6 *(config_map.yaml)*.

NOTE: Based on the IPv6 address, regex contents need to be modified.

```
scrape_configs:
      - job_name: 'prometheus_cdmrf'

kubernetes_sd_configs:
        - role: pod

relabel_configs:
        - source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_scrape]
          action: keep
          regex: true
        - source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_path]
          action: replace
          target_label: __metrics_path__
          regex: (.+)
        - source_labels:
[__meta_kubernetes_pod_annotation_cni_projectcalico_org_podIPs,
__meta_kubernetes_pod_annotation_prometheus_io_port]
          regex: (.*,)+(\w+::\w+:\w+:\w+:\w+:\w+)(.*)+;(\d+)
          target_label: __address__
          replacement: $2:$4
```

```
    - action: labelmap
      regex: __meta_kubernetes_pod_label_(.+)
    - source_labels: [__meta_kubernetes_namespace]
      action: replace
      target_label: kubernetes_namespace
    - source_labels: [__meta_kubernetes_pod_name]
      action: replace
      target_label: kubernetes_pod_name
```

For HTTPS

The Prometheus server versions supported for Containerized Decomposed Media Server are 2.18.1 and 2.22. The below mentioned configuration is used during the Prometheus installation for service discovery when Containerized Decomposed Media Server management is IPv4 and IPv6 *(config_map.yaml)*.

NOTE: Based on the IPv4 and IPv6 addresses, regex contents need to be modified.

```
scrape_configs:
- job_name: 'prometheus_cdmrf'
kubernetes_sd_configs:
- role: pod
scheme: https
tls_config:
ca_file: '/etc/cert/cacert.pem'
cert_file: '/etc/cert/client_crt.pem'
key_file: '/etc/cert/client_key.pem'
insecure_skip_verify: false

relabel_configs:
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_scrape]
action: keep
regex: true
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_path]
action: replace
target_label: __metrics_path__
regex: (.+)
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_clusterDN,
__meta_kubernetes_pod_annotation_prometheus_io_nodeport]
action: replace
regex: ((([a-zA-Z0-9_]([a-zA-Z0-9\-_]){0,61})?[a-zA-Z0-9]\.)*([a-zA-Z0-9_]([a-
zA-Z0-9\-_]){0,61})?[a-zA-Z0-9]\.?);(\d+)
replacement: $1:$7
target_label: __address__
- action: labelmap
```

```
regex: __meta_kubernetes_pod_label_(.+)
- source_labels: [__meta_kubernetes_namespace]
action: replace
target_label: kubernetes_namespace
- source_labels: [__meta_kubernetes_pod_name]
action: replace
target_label: kubernetes_pod_name
```

NOTE: The cluster DNS must be resolved by Prometheus pod.

The below mentioned configuration is for creating the PV and PVC for Prometheus deployment.

For PV Creation

```
apiVersion: v1
kind: PersistentVolume
metadata:
name: pv-prometheus
spec:
capacity:
storage: 2Gi
accessModes:
- ReadWriteOnce
nfs:
path: /tmp/prometheus
server: 172.27.6.136
persistentVolumeReclaimPolicy: Recycle
storageClassName: nfs
volumeMode: Filesystem
```

For PVC Creation

```
prometheus_pvc.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
name: pv-prometheus
spec:
accessModes:
- ReadWriteOnce
resources:
requests:
storage: 1Gi
storageClassName: nfs
```

The below mentioned configuration is for Prometheus deployment.

```
spec:
hostAliases:
- ip: "172.27.44.229"
hostnames:
- "cdmrf.radisys.com"
containers:
- name: prometheus
image: 172.27.6.92:5000/prometheus:v2.18.1
args:
- "--config.file=/etc/prometheus/prometheus.yml"
- "--storage.tsdb.path=/prometheus/"
ports:
- containerPort: 9090
volumeMounts:
- name: prometheus-config-volume
mountPath: /etc/prometheus/
- name: prometheus-storage-volume
mountPath: /prometheus/
- name: prometheus-cert-volume
mountPath: /etc/cert/
volumes:
- name: prometheus-config-volume
configMap:
defaultMode: 420
name: prometheus-server-conf
- name: prometheus-storage-volume
emptyDir: {}
- name: prometheus-cert-volume
persistentVolumeClaim:
claimName: pv-prometheus
```

The Prometheus server versions supported for Containerized Decomposed Media Server with **Ingress** is 2.34.0. The below mentioned configuration is for HTTP and HTTPS of configmap.

```
relabel_configs:
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_scrape]
action: keep
regex: true
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_scheme]
action: replace
target_label: __scheme__
regex: (https?)
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_path]
```

```
action: replace
target_label: __metrics_path__
regex: (.+)
- source_labels: [__meta_kubernetes_pod_annotation_prometheus_io_clusterDN]
action: replace
target_label: __address__
- action: labelmap
regex: __meta_kubernetes_pod_label_(.+)
- source_labels: [__meta_kubernetes_namespace]
action: replace
target_label: kubernetes_namespace
- source_labels: [__meta_kubernetes_pod_name]
action: replace
target_label: kubernetes_pod_name
```

Web GUI Statistics Options

The Performance Management option of the Web GUI allows you to monitor the performance of the Containerized Decomposed Media Server using statistics.

Reset Statistics

The Reset Statistics page allows you to manually reset counters.

Statistics are automatically reset when the MRFP is restarted. However, you can also manually reset the statistics.

To reset statistics:

1. Click **Performance Management** > **Reset Statistics**.

The Reset Statistics page displays.

2. Select the instance number from the **Instance number** drop-down list.

   The default value is all.

3. Click **Execute.**

   All counters are reset.

   Confirmation message is displayed in the **Output Messages:** box.

Retrieve Statistics

The Retrieve Statistics page allows you to retrieve the announcement statistics along with the statistics file, if TXT or XML format is selected, and save it to an external server. You can retrieve all statistics collected for the past 72 hours (that is, for all intervals), or statistics from the most recent interval collected.

The file is posted in plain text. When you post a file, it overwrites the previous file.

The following table lists the information you must provide to use SFTP to post the statistics file to a file server. This information is not needed for a Web download.

Table 113. File Transfer Information—Retrieve Statistics

Value	Description
Interval	The data is collected or stored in the statistic file as per the configuration of the statistics reporting interval. The supported values: • **All.** The entire data stored in the file. • **Last.** The data stored for last interval in the file. The default value is **All**.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP).
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, the hostname of the file server can be used. Supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".

Table 113. File Transfer Information—Retrieve Statistics

Value	Description
Path to statistics file on server	The absolute path to the statistics on the file server. Supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** • Do not begin the name with "#" or "~". • Pathname must end with /. This field may not be blank.
Server username	The username configured on the file server. Supported values are strings of up to 128 characters.
Server password	The password configured on the file server. Supported values are strings of up to 128 characters.
Announcement Clip Played Count	Allows to retrieve the announcement clip played statistics. When this parameter is selected, the Containerized Decomposed Media Server includes both the current and backup *.csv* files and downloads the files to the local machine when **Web Download** is selected as a *.tar* package. When file transfer is selected, the Containerized Decomposed Media Server transfers the *.csv* files to the remote server as a *.tar* package.
TXT Format	Allows to download the statistics in text file format. By default, this field is enabled.
XML Format	Allows to download statistics in XML file format as a *.tar* package. By default, this field is disabled.
Auto-Transfer of XML Format Statistics	Allows to transfer the 3GPP XML statistics file automatically. By default, this field is disabled. ***NOTE:*** • Only one 3GPP XML statistics file is transfered at a time. • The Containerized Decomposed Media Server transfers the statistics file only from the upcoming reporting interval. Any outstanding 3GPP XML statistics file is not transferred. • The **Interval** field configuration is ignored for 3GPP XML file transfers.

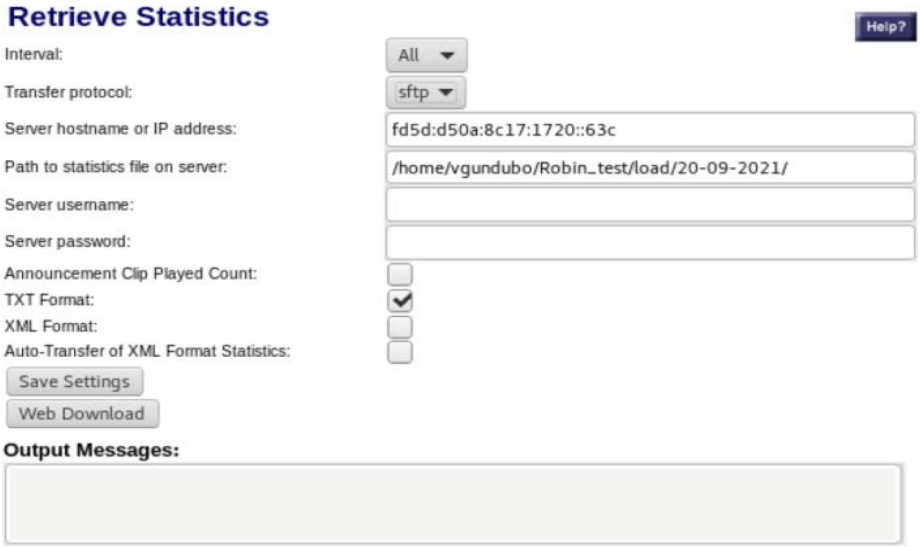
NOTE:

- While retrieving statistics, if **Last** interval is selected, the statistics text file contains the last interval statistics. However, all the generated XML files available from the previous interval are retrieved.
- The statistics file is downloaded as a *.tar* package when,
  - **Announcement Clip Played Count**, **TXT Format**, and **XML Format** options are selected
  - both **Announcement Clip Played Count** and **TXT Format** options are selected
  - both **Announcement Clip Played Count** and **XML Format** options are selected
  - both **TXT Format** and **XML Format** options are selected

To post the statistics file to an external server:

1. Click **Performance Management** > **Retrieve Statistics**.

The Retrieve Statistics page displays.



2. Select the **Interval** option from the drop-down list.
3. Click **Web Download** to save the *.csv* and/or statistic files using HTTP through your Web browser or enter the file transfer information to use the SFTP protocol.

   NOTE: For a Web download, use the pop-up window to save the *.csv* and/or statistic files. The announcement statistics along with the statistics file, if TXT or XML format is selected, is retrieved and stored in the specified location on the file server, overwriting the existing file on the server.
4. Select **TXT Format** or **XML Format**.
5. Select **Auto-Transfer of XML Format Statistics** to transfer 3GPP XML statistics file automatically.
6. Click **Save Settings** to transfer the *.csv* and/or statistic files using the SFTP protocol.

   Confirmation message is displayed in the **Output Messages:** box.

Configure Statistics

The Configure Statistics page allows you to set the statistics reporting interval.

The following table shows the statistics information you can configure for the Containerized Decomposed Media Server.

Table 114. Statistics Configuration

Value	Description
Statistics reporting interval	The reporting interval in minutes, for the Containerized Decomposed Media Server statistics collection. The supported values are: • **5.** Statistics are collected in 5 minute intervals. • **15.** Statistics are collected in 15 minute intervals. • **30.** Statistics are collected in 30 minute intervals. The default value is 15. The changes to this field require an OAMP pod restart to take effect.
Enable Announcement Clip Played Count	Enables or disables announcement clip played count on a instance. At the end of an announcement, the Containerized Decomposed Media Server writes the announcement URIs in the *.csv* file along with the date, time, clip name, and disposition (success or failure) in the *.csv* file, when the announcement service terminates or fails. The supported values are: • **Enabled.** The Containerized Decomposed Media Server appends the clip information in the *.csv* file for both the port and conference announcements. • **Disabled.** The Containerized Decomposed Media Server does not append the clip information. The default value is Disabled. This parameter does not require a restart and takes effect on the next announcement request.
Enable 3gpp XML Format	Enables or disables statistics in the 3GPP XML file format. The supported values are: • Enabled • Disabled The default value is Disabled. This parameter does not require a restart to take effect.
Delete 3gpp XML (After Successful Transfer)	Allows to delete the XML statistics after a successful transfer. By default this field is unchecked. This parameter does not require a restart to take effect.

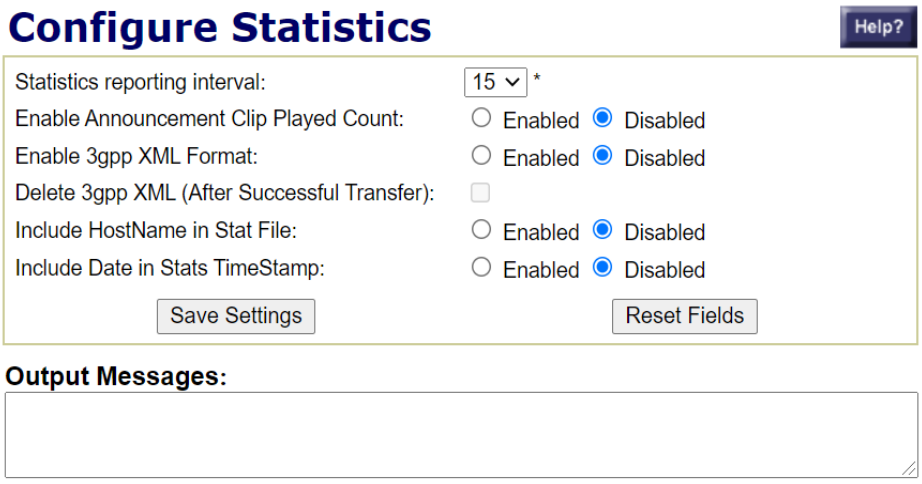
Table 114. Statistics Configuration

Value	Description
Include HostName in Stat File	Enables or disables the Containerized Decomposed Media Server to include the hostname in the filename of the statistic file, which is retrieved from the management interface. The supported values are: • **Enabled.** The Containerized Decomposed Media Server includes the hostname in the statistic filename retrieved through web download or sftp on to the remote server. • **Disabled.** The Containerized Decomposed Media Server does not include the hostname in the statistic filename. ***NOTE:*** • If the hostname of the Containerized Decomposed Media Server is changed, the Containerized Decomposed Media Server includes the new hostname in the statistic filename after the restart. • The hostname is the OAMP pod hostname for the statistics file. The default value is Disabled. This parameter does not require a restart to take effect.
Include Date in Stats TimeStamp	Enables or disables the Containerized Decomposed Media Server to include the month and date in timestamp in the statistics file. The supported values are: • **Enabled.** The Containerized Decomposed Media Server includes the month, date, and time in timestamp in the statistics file. • **Disabled.** The Containerized Decomposed Media Server includes only timestamp in the statistics file. The default value is Disabled. This parameter does not require a reboot to take effect.

To set the statistics reporting interval:

1. Click **Performance Management** > **Configure Statistics**.

The Configure Statistics page displays.



2. Enter the information described in the above table.
3. Click **Save Settings**.

   The changes require reboot to take effect and a confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values

Show High Watermarks

The Show High Watermarks page displays the high watermarks for licensed entities (for example, codecs).

To view high watermarks:

1. Click **Performance Management** > **Show High Watermarks**.

   The Show High Watermarks page displays.
2. Click **Execute**.

   The high watermarks for the licensed codecs are displayed in the **Output Messages:** box.

Show Statistics Configuration

The Show Statistics Configuration page displays the statistics configuration settings for the Containerized Decomposed Media Server.

To view statistics configuration:

1. Click **Performance Management** > **Show Statistics Configuration**.
2. Click **Execute**.

   The statistics configuration displays in the **Output Messages:** box.

Show Statistics History

The Show Statistics History page displays the statistics for any collection interval over the past 72 hours, if statistics were collected for that interval. The Containerized Decomposed Media Server shows the statistics collected only since the most recent restart. The statistics displayed in the Web GUI are a subset of all statistics collected by the Containerized Decomposed Media Server.

To view statistics for an interval in the last 72 hours:

1. Click **Performance Management** > **Show Statistics History**.
2. Select the **Instance number** from the drop-down list.
3. Specify the collection interval you want to view.

   The interval begins with the time you select, and ends 5, 15, or 30 minutes later.

4. Click **Execute**.

   The statistics for the selected interval are listed in the **Output Messages:** box.

   NOTE: Use standard editing procedures to copy (**Ctrl+C**) and paste (**Ctrl+V**) information from the Output Messages box into a document.

Show Real-Time Statistics

The Show Real-Time Statistics page lets you see the current value of statistics and the current active ports. For statistics such as averages and maximums, the value shown is the real-time value of the interval in progress. For counters, the value shown is the cumulative value since the last time the Containerized Decomposed Media Server was reset. The statistics displayed in the Web GUI are a subset of all statistics collected by the Containerized Decomposed Media Server.

To view real-time statistics:

1. Click **Performance Management** > **Show Real-Time Statistics**.
2. Select the **Instance number** from the drop-down list.
3. Click **Execute**.

   The statistics are listed in the **Output Messages:** box.
4. If required, use standard editing keystrokes to copy (**Ctrl+C**) and paste (**Ctrl+V**) information from the **Output Messages:** box into another document.

   When diagnosing problems, you may want to isolate statistics around a particular network event. You can use the following procedure to take a snapshot of the Containerized Decomposed Media Server activity.

To snapshot activity in the Web GUI:

1. Clear the values in the current interval using the Reset Statistics page.
2. Wait for the desired amount of time.
3. Use the Show Real-Time Statistics page to display the values since reset. The values for the interval are displayed in the **Output Messages:** box.
4. If required, use standard editing keystrokes to copy (**Ctrl+C**) and paste (**Ctrl+V**) information from the **Output Messages:** box into another document.

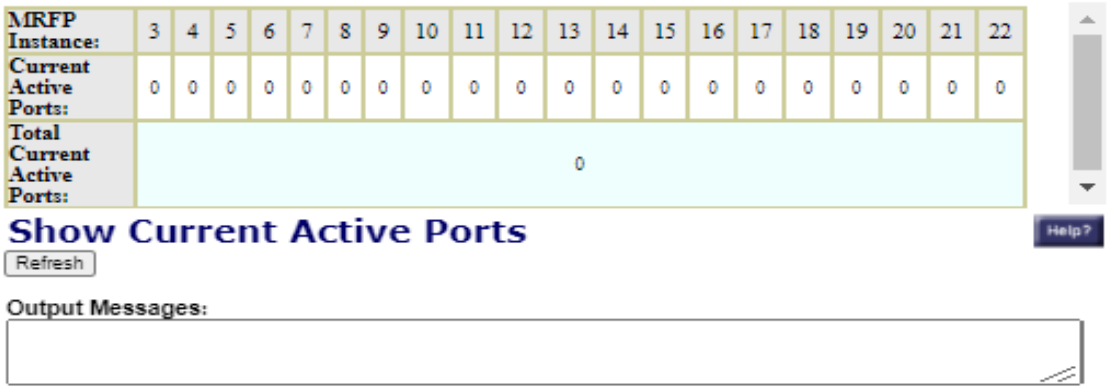
Show Current Active Ports

The Show Current Active Ports page displays the current active ports per MRFP. It also displays the total number of active ports for all MRFPs.

To view current active ports:

1. Click **Performance Management** > **Show Current Active Ports**.

   The Show Current Active Ports page displays.



MRFP Instance:	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Current Active Ports:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total Current Active Ports:	0																			

Show Current Active Ports

Help?

Refresh

Output Messages:

2. Click **Refresh** to see the latest active ports values.

   The **Output Messages:** box displays the active port refresh status.

Administration Management

This chapter describes how to manage user information and customize the Web-based management interface.

The administration options allow you to manage user accounts and customize the Web-based management interface.

User Accounts

The following table shows the different accounts the Containerized Decomposed Media Server supports and the access each has to its management interfaces.

Table 115. User Accounts' Access to Interfaces

Account Type		NETCONF	Management Interface Access	
	SAML		Web	SNMP
Operating System User: **webadmin** for Web GUI/SAML **snmpadmin** for SNMP **swmsadmin** for NETCONF (default password = convedia)	Y	Y (OAMP)	Y (OAMP only)	Y (OAMP only)
Operating System User: **root** (default password = ChangeMe)	—	—	—	—
SNMP User	—	—	—	Y (OAMP only)
Locally Provisioned User	Y	—	Y (OAMP only)	—
NETCONF Users	—	Y (MRFCtrl and OAMP)	—	—
LDAP Users	—	N	Y	—

The Containerized Decomposed Media Server runs all its application processes with non-root privilege (swmsadmin) except WebRTC and keepalived daemon process.

Valid User Names

Locally provisioned User IDs must be between 6 and 64 alphanumeric characters. No two User IDs can be identical. User IDs can include printable ASCII characters 0x20 through 0x7E, with the exception of 0x22 (“), 0x27 (‘), 0x3A (:), and 0x23 (#). User IDs are case-sensitive.

NOTE: Locally Provisioned users, OS users, and LDAP users can have the same username.

Valid Passwords

The Containerized Decomposed Media Server enforces rules on users of locally provisioned accounts when configuring passwords through its management interface. Two sets of such password rules are supported: basic and complex. After one of these sets is configured for the Containerized Decomposed Media Server, all new passwords must meet the level of complexity to be accepted as valid for the account.

When the Containerized Decomposed Media Server is configured to require basic complexity for new passwords, the following rules apply.

- For web user, the password must be between 6 and 64 alphanumeric characters.
- Passwords can include printable ASCII characters 0x20 through 0x7E.
- Passwords are case-sensitive.

When the Containerized Decomposed Media Server is configured to require complex new passwords, the following rules apply:

- For web user, the password must be between 8 and 64 alphanumeric characters.
- Passwords can include printable ASCII characters 0x20 through 0x7E and contains at least one uppercase alphabetic character (A-Z), one lowercase alphabetic character (a-z), and one a special character (for example an underscore (_)).
- Must not contain the account’s username.
- Are case-sensitive.
- Must not match with previous four old passwords.

  NOTE:

  - All the non-CLI users on the Containerized Decomposed Media Server must use SHA-512. However, any existing passwords in database continue to be MD5, and you need to re-configure the passwords for the changes to take effect.
  - The database persistent password are encrypted with AES-256.
  - Same user names under Locally Provisioned users and OS user can have different passwords.

Along with the above specified rules, the new password must also follow the default rules provided by **`pam_cracklib.so`** module.

- The `Cracklib` routine is called to verify if the password is part of a dictionary.
- If the password is not a part of the dictionary, perform the following steps.
  - **Palindrome.** Verifies if the new password is a palindrome.

- **Case Change Only.** Verifies if the new password is the old password with only a change of case.
- **Similar.** Verifies if the new password is similar to the old password. This is controlled by `difok` argument. The `difok` argument is a number of character change (inserts, removals, or replacements) between old and the new password that are required to accept the new password. This defaults to 5 changes.
- **Simple.** Verifies if the new password is simple. This is controlled by `minlen`, `maxclassrepeat`, `dcredit`, `ucredit`, `lcredit`, and `ocredit` arguments.
- **Rotated.** Verifies if the new password is a rotated version of the old password.
- **Same consecutive characters.** Verifies for the same consecutive characters. This is an optional step.
- **Too long monotonic character sequence.** Verifies for long monotonic character sequence. This is an optional step.
- **Contains user name.** Verifies the password contains the user name in some form. This is an optional step.

Access Levels (Hierarchical Permissions)

The Containerized Decomposed Media Server supports creating hierarchical accounts such that not every user is permitted the full range of configurations and actions that can be performed on the system. For example, you can allow some users to only read configuration data that other users are allowed to set. Support for hierarchical permissions differs for the various management interfaces and types of accounts:

- The Web-based management interface supports hierarchical permissions based on defined access levels
- The SNMP interface supports SNMPv3 user management

For the Web-based management interface, the Containerized Decomposed Media Server supports setting hierarchical permissions based on four access levels: 1, 2, 3, and 4. User accounts configured for any one of these access levels can perform only actions permitted to that level.

The Containerized Decomposed Media Server supports assigning an access level to locally provisioned and LDAP managed user accounts. The operating system admin user account always retains the highest level access. For information on the different LDAP access level configuration, see *Configure User Authentication on page 480*.

The highest access level is 1, meaning an account with level 1 access is permitted to perform actions that may be restricted for accounts with lower access levels. An account with access level *n* is permitted all the actions of lower access accounts, that is, an account with access level 2 can perform all actions requiring access level 2, 3, and 4.

The following table describes the access level required for an account to be permitted to perform the different actions available to the Containerized Decomposed Media Server Web-based management interface.

Table 116. Permissions for Each Access Level

Permitted Action	Minimum Access Level
All (that is, full read and write permissions for all configurations)	1
• Read and configure users	1
• Configure password aging[a]	1
• Retrieve the management activity log	1
• Change configuration data	2
• Backup and restore actions	2
• Reset statistics	3
• Retrieve log packages	3
• Acknowledge alarms	3
• Read configuration data	4
• Change account password[a]	4
• Retrieve a reduced version of the management activity log	4

[a] The Containerized Decomposed Media Server does not manage the LDAP user password policy and does not support the LDAP users from changing their password through the Web GUI or SSH.

Management Activity Logging

Management activities generate log messages at different severities, which represent their level of significance for the system. Log severities of events are predefined. However, you can configure the level of detail that is reported in log messages by specifying the level of severity that is reported. The lower the level of severity specified, the more detail is captured in the logs.

When you specify a severity to report, the system understands that as the *minimum* severity to report, and it reports all log messages of that severity and higher. For example, if you specify a severity of Information, the system reports all Notice and Information log messages.

The default level of severity for all management activities is None (management activities are not logged).

Management activities are logged alternately to two local files. When the file currently being written to accumulates 100 KB of log messages, the Containerized Decomposed Media Server closes that file and begins overwriting the log messages in the alternate file.

The management activity logs contains the username (admin or access level1 user) that is used for the operations such as **Create New User**, **Set Username**, **Set Password**, **Set Access Level/Password Aging**, **Reactivate User**, **Force User Password Expiry**, **Delete User**.

Administration Options

The sub options under the administration option are discussed below.

Change Password

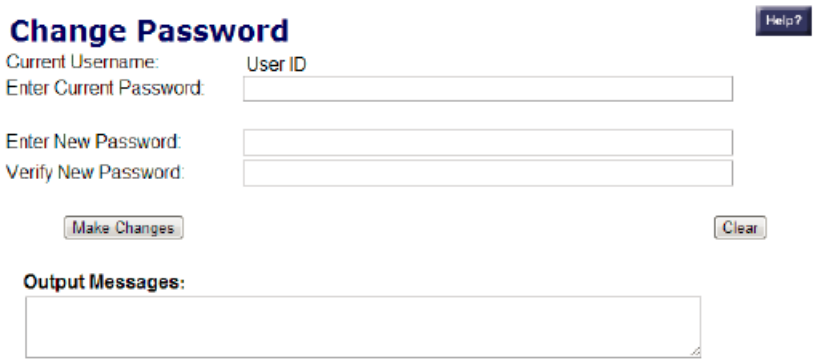
The Change Password page allows you to change the password of the local provisioned users.

The rules governing valid user names and passwords are described under *User Accounts on page 473*.

To change the account password:

1. Click **Administration** > **Change Password**.

   The Change Password page displays.



2. Enter the password of the account in the **Enter Current Password** field.
3. Enter the new password of the account in the **Enter New Password** field.
4. Confirm the new password of the account in the **Verify New Password** field.
5. Click **Make Changes** to change the password.

   The changes take immediate effect and a confirmation message displays in the **Output Messages:** box.
6. Optionally, click **Clear** to clear all the input fields.

Show Authentication Configuration

The Show Authentication Configuration page displays the user authentication configured for the Containerized Decomposed Media Server.

To view the authentication configuration:

1. Click **Administration** > **Show Authentication Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the authentication configuration information.

Show Password Complexity Configuration

The Show Password Complexity Configuration page displays the setting the password complexity (Basic or Complex) for the Web users.

To view the password complexity setting:

1. Click **Administration** > **Show Password Complexity Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the password complexity configuration information.

Show Users

The Show Users page displays the provisional user information configured on the Containerized Decomposed Media Server.

NOTE: This feature is accessible only by Level 1 users.

To view provisioned users:

1. Click **Administration** > **Show Users**.

   The Show Users page displays.

2. Select Yes or No in **Show enabled users only**.
3. Enter the username in the **Username** field.

   NOTE: If the field is left blank, the details of all the usernames are listed in the **Output Messages:** box.
4. Check the **Detailed users Information** check box to fetch the following provisional user (Web GUI) information.
   - **Username.** Displays the user name of the account.
   - **User Creation Date.** Displays the date and time when the user account was created.
   - **User Expiry Date.** Displays the expiry date of the user account. There is no expiry date for the users, therefore this value is set as **forever**.
   - **User Current Status.** Displays the current status of the user.
   - **User Last Login Time.** Displays the date and time when the user last logged in.
   - **User Type.** Displays the user type. The user type is **WebOam**.

5. Click **Execute**.

   The **Output Messages:** box displays the provisioned users information.
6. Optionally, click **Clear** to clear all the input fields.

Show HTTP Server Configuration

The Show HTTP Server Configuration page displays the HTTP and HTTPS settings on the Containerized Decomposed Media Server.

NOTE: This page is not applicable for non-cloud mode.

To view the HTTP server configuration information:

1. Click **Administration** > **Show HTTP Server Configuration**.
2. Click **Execute**.

   The **Output Messages:** box displays the HTTP and HTTPS configuration information.

Show Management Activity Log Configuration

The Show Management Activity Log Configuration page displays the settings for logging the management activity.

To view the configuration information for logging management activity:

1. Click **Administration** > **Show Management Activity Log Configuration**.
2. Click **Execute.**

   The **Output Messages:** box displays the logging settings information.

Show SANE Configuration

The Show SANE Configuration page displays the SAML Authenticated Network Element (SANE) configuration of the Containerized Decomposed Media Server. The information displayed on this page is set on the Configure SANE page.

To view the SAML information:

1. Click **Administration** > **Show SANE Configuration**.

   The Show SANE Configuration page displays.
2. Click **Execute**.

   The Security Assertion Markup Language (SAML) information is displayed in the **Output Messages:** box.

Configure User Authentication

On the Configure User Authentication page, you can configure the user authentication information for the Containerized Decomposed Media Server.

The following table shows the user authentication information that can be configured.

Table 117. User Authentication Information

Value	Description
Order of Authentication	The order in which the Containerized Decomposed Media Server attempts to authenticate users. The supported values are: • **Local Only.** The Containerized Decomposed Media Server attempts to authenticate users only locally. • **Local then Remote Authentication Protocol.** The Containerized Decomposed Media Server attempts to authenticate users locally; if local authentication fails, the Containerized Decomposed Media Server attempts to authenticate on the remote authentication server. • **Remote Authentication Protocol then Local.** The Containerized Decomposed Media Server attempts to authenticate users on the remote authentication server; if authentication on the server fails, the Containerized Decomposed Media Server attempts to authenticate locally. The default value is Local Only. The change takes effect immediately.
Remote Authentication Protocol	The authentication protocol used for remote communications. The supported value is LDAP. The Containerized Decomposed Media Server communicates with a remote server using the Lightweight Directory Access Protocol (LDAP) authentication protocol. The change takes effect immediately.
LDAP Authentication Mode	Mandatory. The Containerized Decomposed Media Server enables only the Web GUI login to support the LDAP authentication. The change takes effect immediately.
LDAP Server Parameters	
Server Type	Mandatory. The type of LDAP server that the Containerized Decomposed Media Server uses. The supported values are: • **OpenLDAP.** The open LDAP server. • **Active Directory.** The Active Directory (AD) customized for a Microsoft product suite. The default value is OpenLDAP. The change takes effect immediately.
Server Name or IP Address	Mandatory. The IP address of the LDAP serve if DNS is used, you can enter a server hostname of up to 63 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". The change takes effect immediately.

Table 117. User Authentication Information

Value	Description
Authentication Port	Mandatory. The authentication (TCP) port at which the OpenLDAP server is listening for connections. The supported values are 1 to 65535. The default value is 389. ***NOTE:*** The AD server supports port number 636 for encrypted connection and port number 389 for non-encrypted connection. The change takes effect immediately.
Secure LDAP using TLS	Mandatory. Enables or disables the TLS for secure communication between the Containerized Decomposed Media Server (LDAP client) and LDAP servers. The supported values are: • **Enabled.** Set the **Authentication Port** to TLS enabled port configured at the LDAP server. • **Disabled.** Set the **Authentication Port** to TLS disabled port configured at the LDAP server. ***NOTE:*** The default TLS enabled port at the LDAP server is 636. The default value is Disabled. Changes to this field take effect immediately.
Base DN	Mandatory. The base distinguished name (DN) identifies the entry in the directory from which the LDAP clients initiate a search. The base DN is often referred to as the search base. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. The change takes effect immediately.
Admin Bind DN	Mandatory. The DN of the administrator. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-=,space) The default value is blank. The change takes effect immediately.
Admin Bind Password	Mandatory. The password for the administrator bind DN. The supported values are strings of a maximum of 63 characters. The default value is blank. The change takes effect immediately.

Table 117. User Authentication Information

Value	Description
User Search DN	Optional. Allows to search the user from the configured DN. If this value is not set, the user search starts from the configured base DN. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. ***NOTE:*** When an incorrect value is configured in this field, it results in a login failure. The change takes effect immediately.
User Search Scope	Allows to search the user based on the defined scope. The supported values are: • **Single Level.** Allows to search up to one level below the user DN. • **Whole Subtree.** Allows to search the entire subtree below the user DN. The default value is Whole Subtree. The change takes effect immediately.
User Search Filter	Optional. Defines the LDAP filter used to identify the users according to search criteria in the search request. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (()=*~|&.@-_space) The default value is blank. ***NOTE:*** When an incorrect value is configured in this field, it results in a login failure. The change takes effect immediately.
User ID Attribute	Optional. The attribute represents the user's unique ID. The supported values are strings of a maximum of 31 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) The default value is blank. For AD server, the value is *sAMAccountName/name/cn/givenName* and for OpenLDAP server, the value is *uid/cn*. If this value is not configured, the AD server uses the **sAMAccountName** attribute, and OpenLDAP server uses the **uid** attribute. The change takes effect immediately.
User Member Attribute	This attribute contains all the group distinguished names (DNs) of which the user entry is a member. The default value is memberOf. This field is not user-configurable.

Table 117. User Authentication Information

Value	Description
Group Search DN	Optional. Allows to search the group from the configured DN. If this value is not set, the group search starts from the configured base DN. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_- space) The default value is blank. ***NOTE:*** When an incorrect value is configured in this field, it results in a login failure. The change takes effect immediately.
Group Search Scope	Allows to search the group based on the defined scope. The supported values are: • **Single Level.** Allows to search up to one level below the group DN. • **Whole Subtree.** Allows to search the entire subtree below the group DN. The default value is Whole Subtree. The change takes effect immediately.
Group Search Filter	Optional. Defines the criteria that are used to identify the groups in the search request. The supported values are strings of a maximum of 127 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (()=*~|&.@-_space) The default value is blank. ***NOTE:*** When an incorrect value is configured in this field, it results in a login failure. The change takes effect immediately.
Group Member Attribute	Optional. The group membership attribute contains values that reference groups to which this entry belongs. If UserA belongs to GroupA, the value of the memberOf attribute of UserA must contain the distinguished name of GroupA. The group entries include member attribute values specifying the group member in distinguished names. The supported values are strings of a maximum of 31 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) The default value is blank. The change takes effect immediately.

Table 117. User Authentication Information

Value	Description
Access Level 1 Allowed Group List	Sets the access level 1 for the configured LDAP group list. The maximum supported length is of 255 characters, where the maximum length of each group name is of 64 characters and the groups are separated by a comma. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. When entering the value, you must provide only the group name and exclude the domain name. For example, if the LDAP group name is *group1@example.com*, enter the value as **group1**. The change takes effect immediately.
Access Level 2 Allowed Group List	Sets the access level 2 for the configured LDAP group list. The maximum supported length is of 255 characters, where the maximum length of each group name is of 64 characters and the groups are separated by a comma. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. When entering the value, you must provide only the group name and exclude the domain name. For example, if the LDAP group name is *group2@example.com*, enter the value as **group2**. The change takes effect immediately.

Table 117. User Authentication Information

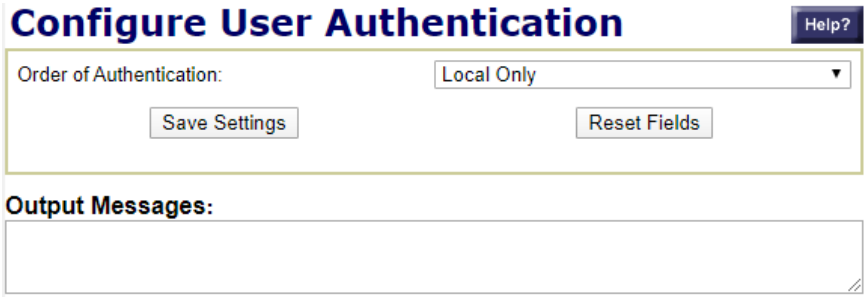
Value	Description
Access Level 3 Allowed Group List	Sets the access level 3 for the configured LDAP group list. The maximum supported length is of 255 characters, where the maximum length of each group name is of 64 characters and the groups are separated by a comma. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. When entering the value, you must provide only the group name and exclude the domain name. For example, if the LDAP group name is *group3@example.com*, enter the value as **group3**. The change takes effect immediately.
Access Level 4 Allowed Group List	Sets the access level 4 for the configured LDAP group list. The maximum supported length is of 255 characters, where the maximum length of each group name is of 64 characters and the groups are separated by a comma. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (_-space) The default value is blank. When entering the value, you must provide only the group name and exclude the domain name. For example, if the LDAP group name is *group4@example.com*, enter the value as **group4**. The change takes effect immediately.

NOTE:

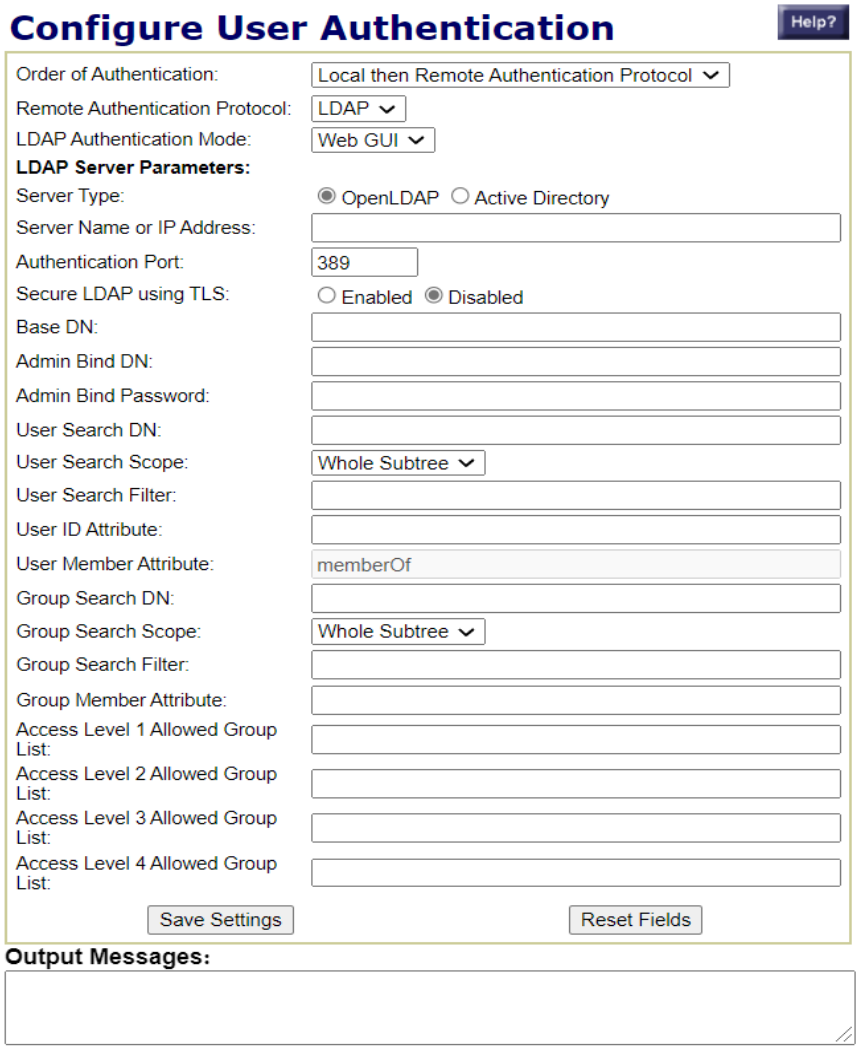
- Any one of the four access levels must be set. For information on permissions of each access level, see Table 116.
- If the same group name is configured in multiple levels, the LDAP considers the highest level of access.
- Ensure to provide correct values for the LDAP configurations in the Containerized Decomposed Media Server Web GUI as configured in the LDAP server; otherwise, the Containerized Decomposed Media Server fails the authentication and authorization.

To configure user authentication:

1. Click **Administration** > **Configure User Authentication.**
   The Configure User Authentication page displays.



   The Configure User Authentication page displays when the **Remote Authentication Protocol** is selected as LDAP. The default screen that is displayed is blank, but the sample screen that is displayed below has filled in information.



2. Enter the authentication parameters information described in above table.
3. Click **Save Settings**.

   The authentication configuration is set. The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to default values.

Configure Password Parameters

On the Configure Password Parameters page, you can manage the configuration of password parameters on the Containerized Decomposed Media Server for locally provisioned user accounts as described in the following table.

Password aging information you can configure

The following table shows the password parameters that can be configured.

Table 118. Password Parameters Information

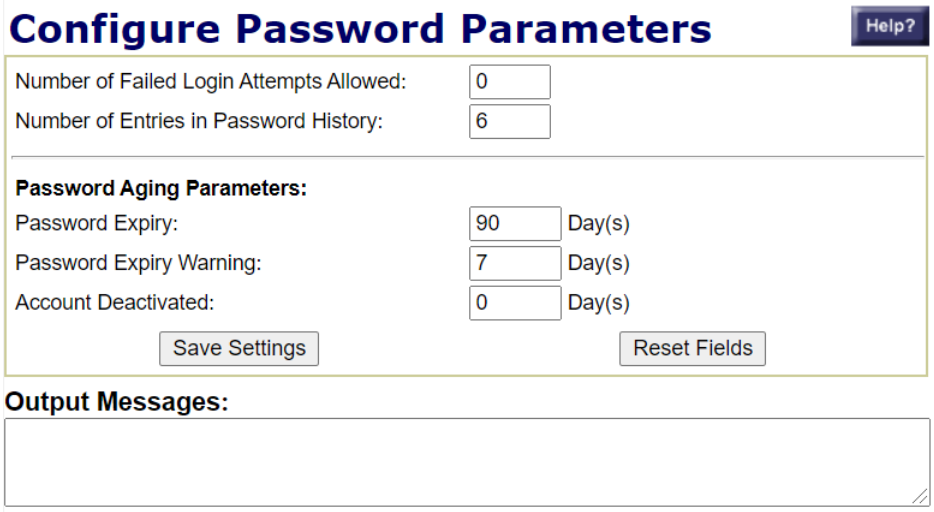
Value	Description
Number of Failed Login Attempts Allowed	The number of unsuccessful login attempts, counted from the previous successful login, the Containerized Decomposed Media Server allows before deactivating the account. The range is 0 to 20, where 0 does not restrict the number of failed login attempts. The default is 0. The change takes effect immediately.
Number of Entries in Password History	The number of previous passwords the Containerized Decomposed Media Server retains and blocks from being reused on the account. Range is 0 to 12, where 0 allows the user to reuse the account current password (and 1 disallows only the current password). The default is 1. The change takes effect immediately.
Password Expiry	The number of days, for which a new password remains valid. The range is 1 to 365 (one year). The default is 90 (about 3 months). ***NOTE:*** If password is not changed within 30 days of its expiry, the account is locked and login is denied. The change takes effect immediately.
Password Expiry Warning	The number of days before expiration that a notice is sent. The range is 0 to 365 (one year). The default is 7 (one week). The change takes effect immediately.
Account Deactivated	The number of days following an account password expiration during which the Containerized Decomposed Media Server allows the account user to log in and then enforces a change of password as a condition to allow further actions. The range is 0 to 365 (one year). The default is 0. The change takes effect immediately.

NOTE: The **Password Expiry**, **Password Expiry Warning**, **Account Deactivated** are the password aging parameters.

To configure password parameters:

1. Click **Administration** > **Configure Password Parameters**.

   The Configure Password Parameters page displays.



2. Enter the password parameters described in the above table.
3. Click **Save Settings**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Password Complexity

On the Configure Password Complexity page, you can set the complexity level (basic or complex) that the Containerized Decomposed Media Server requires for the Web users.

Password Complexity Levels for Web users:

The Containerized Decomposed Media Server enforces rules on web user accounts when configuring passwords through its management interface. The two sets of password rules supported are:

- Basic
- Complex

When one of these sets is configured for the Containerized Decomposed Media Server, all new passwords must meet that level of complexity to be accepted as valid for the account.

When the Containerized Decomposed Media Server is configured to require basic complexity for new passwords, the following rules apply:

- Passwords must be between 6 and 64 alphanumeric characters in length excluding a NULL terminator.
- Passwords can include printable ASCII characters 0x20 through 0x7E.

- Passwords are case-sensitive.

When the Containerized Decomposed Media Server is configured to require complex new passwords, the following rules apply:

- Passwords must be between 8 and 64 alphanumeric characters.
- Passwords can include printable ASCII characters 0x20 through 0x7E, with the exception of 0x22 (“) and 0x27 (‘). Passwords must contain at least one alphabetic character (a–z, A–Z), one a numeric character (0–9), and one a special character (example, an underscore, “_”).
- Password must not contain the account username.
- Passwords are case-sensitive.

Following table lists some behavioral changes for Basic and Complex password rules for web users.

Behavior	Password Rule	
	Basic	Complex
Default password change forced	No	Yes
Minimum days between password change	NA	7 days
Validity of password	99999 days	90 days[a]
Restrict password reuse	No	Yes

[a] If password is not changed within 30 days of its expiry, the account is locked and login is denied.

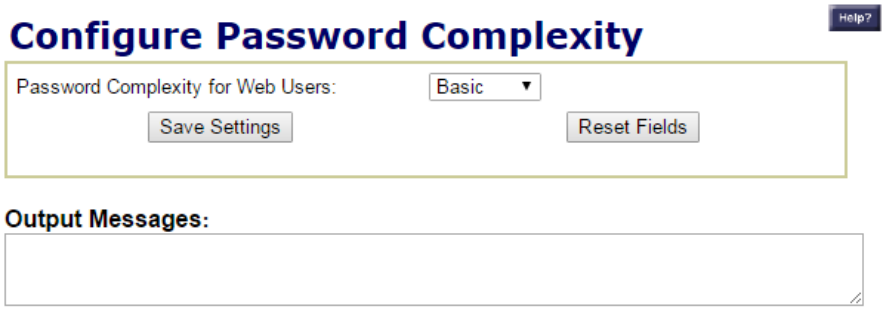
NOTE: For configuring the password rules for Complex, refer to *Configure Password Parameters on page 487*.

The rules governing valid user names and passwords are described under *User Accounts on page 473*.

To configure the password complexity:

1. Click **Administration** > **Configure Password Complexity**.

The Configure Password Complexity page displays.



2. Select the preferred complexity level for the Web users in the **Password Complexity for Web Users** list.

3. Click **Save Settings**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.

4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Configure Local Provisioned Users

On the Configure Local Provisioned Users page, you can provision and configure the Containerized Decomposed Media Server local user accounts as described in the following table.

NOTE: This page allows you to create a local provisioned user with swmsadmin. However, Radisys recommends not to create a local provisioned user with swmsadmin.

The rules governing valid user names and passwords are described under *User Accounts on page 473*.

The following table shows the parameters that can be configured for locally provisioned users.

Table 119. Local Provisioned User Information

Value	Description
Username	The user ID for the account to be configured or provisioned. Valid values are the existing user IDs and **Create New User**, which allows for the provisioning of a new local account. When an existing Username is selected, the following information is shown for that account. • **Set Status.** Whether the account is enabled • **Set Access Level.** The access level configured for the account • **Set Password.** change the account password • **Set Access Level/Password Aging.** Set the account access level and verify whether password aging is enabled for the account. When enabled the status (active or expired) is also shown • **Reactivate User.** Reactivate the user configuration • **Forced User Expiry.** Force users to change passwords to enhance security • **Delete User.** Delete existing user configuration • **Password Aging.** whether password aging is enabled for the account. When enabled, the status (active or expired) is also shown The default is to provision a new account. Changes to this field take effect immediately.
Configuration Option	When an existing Username is selected, you can change the following options for the existing user: • **Set Status.** Default option. To enable or disable the user status. • **Set Username.** To change the existing username. • **Set Password.** To change the existing password. • **Set Access Level/Password Aging.** To change the existing access level and change the password aging status. • **Reactivate User.** To reactivate the existing user. • **Force User Expiry.** To expire the existing user account forcefully. • **Delete User.** To delete the existing user account.

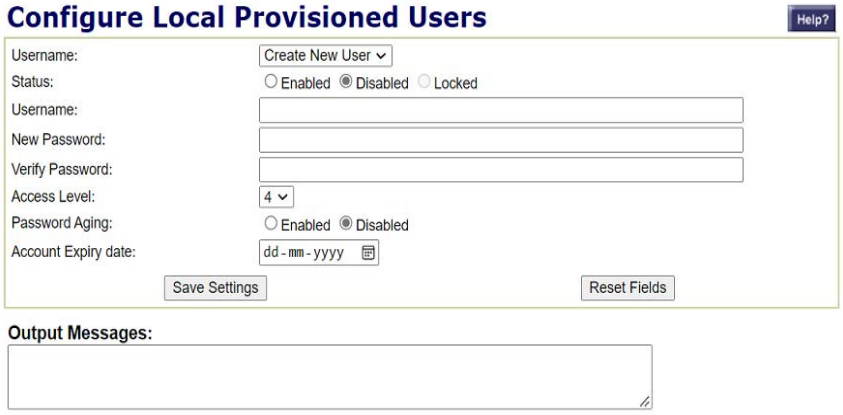
Table 119. Local Provisioned User Information

Value	Description
User Summary	User Summary information is shown for an existing account: • **Status.** Whether the account is enabled • **Access Level.** The access level configured for the account • **Password Aging.** Whether password aging is enabled for the account. When enabled the status (active or expired) is also shown.
Status	Enables or disables the user account. The supported values are: • **Enabled.** Enables the account. • **Disabled.** Disables the account. • **Locked.** Displays the user status. The default value is Disabled. The change takes effect immediately.
Username	Sets the account User ID. The supported values are strings that follow the rules for valid User IDs. The default value is blank. The change takes effect immediately.
New Password	Sets the account password. The supported values are strings that follow the rules for valid passwords for local accounts. The default is blank. The change takes effect immediately.
Verify Password	To set the account password, the string set in the Password field should be repeated correctly. The supported values are strings that follow the rules for valid passwords for local accounts. The default is blank. The change takes effect immediately.
Access Level	Sets the account access level. The range is 1 (read and write access to all configurations) to 4 (minimal access). The default is 4. The change takes effect immediately.
Password Aging	Enables or disables password aging for this account. The supported values are: • **Enabled.** Enables password aging for the account. • **Disabled.** Disables password aging for the account. The default is Disabled. The change takes effect immediately.
Account Expiry date	Optional. Sets the account expiry date in **dd - mm - yyyy** format for the user account. When the user whose account is expired tries to log in, the Containerized Decomposed Media Server restricts the user login attempt and logs the expired user login activity in the management log file. ***NOTE:*** • If the account expiry date is not set, the user account never expires. • If the account is expired, the admin can reactivate the account by modifying the **Status** and **Account Expiry date**. The change takes effect immediately.

To configure local users:

1. Click **Administration** > **Configure Local Provisioned Users**.

The Configure Local Provisioned Users page displays.



2. Select an existing account to configure or **Create New User** to provision a new account.
3. For existing accounts, enter the account information described in the above table.
4. Click **Save Settings**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.
5. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

To create shared account user

To create a **swmsadmin** or equivalent shared user account, perform the following steps.

1. Click **Administration** > **Configure Local Provisioned Users**.
2. Select **Create New User** to provision a new account.
3. Provide a **Username**.
4. Provide **New Password** and **Verify Password**.
5. Select the **Access Level** as 1.
6. Click **Save Settings**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.

Configure Web Interface

On the Configure Web Interface page, you can specify how long a management session can remain idle before the session is closed and the user is logged off.

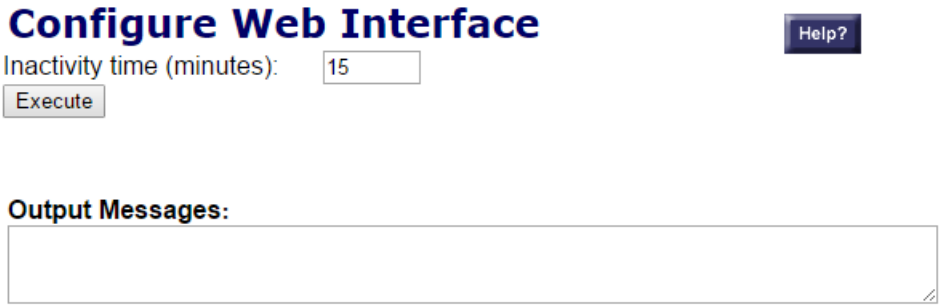
By default, the idle timeout interval is 15 minutes. You can configure any interval in minutes up to a maximum of 9999 minutes. Specifying 0 allows a management session to remain idle indefinitely without being closed.

NOTE: If you set the session to stay open forever, ensure to log off to end your session. If you end your session by closing the browser without logging off, and the GUI is set to stay open indefinitely, the Containerized Decomposed Media Server still keeps the session open. Because only 10 administrative user sessions can be in progress at one time, users might not be able to log on to the GUI again, until the Containerized Decomposed Media Server is reset.

To configure the GUI idle timeout interval:

1. Click **Administration** > **Configure Web Interface**.

The Configure Web Interface page displays.



2. Enter the number of minutes a session is to remain idle before it is closed, in the **Inactivity time (minutes):** field. If you enter 0 as the value, the GUI does not time out.
3. Click **Execute**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.

Configure HTTP Server

On the Configure HTTP Server page, you can manage HTTP and HTTPS for the Web-based management interface.

For information on for fetching the TLS announcements or making recordings to remote web servers or Containerized Decomposed Media Server, see *Manage Certificates* Web GUI page.

NOTE: This page is not applicable for non-cloud mode.

HTTPS enhances security through the following means:

- Protecting the transferred data from eavesdropping

  To protect the data, the server encrypts it using a private key unique to the server. The server public key is used to decrypt the data.
- Verifying the server identity

  To verify the server identity, a trusted certificate authority (CA) digitally signs the server certificate (or if third-party verification is not required, the server administrator self-signs it).

The Containerized Decomposed Media Server supports both a pre-installed key and certificate and the provisioning of a key and certificate.

Provisioning SSL certificates and Keys

The Containerized Decomposed Media Server supports the provisioning of an SSL key and certificate. The supported format for both SSL private key and certificate is x509 ASCII PEM Base64 encoded format. Provisioning of the key and certificate can be done through the Web-based management interface or through the operating system **scp** (Secure CoPy) command.

For security, the Containerized Decomposed Media Server does not back up provisioned SSL certificates and private keys to a remote server when performing backup operations.

To use scp to directly copy a key and certificate on the platform

The file name and path, where the key and certificate must be stored, are determined by the SSL Certificate and SSL Certificate-Key File directives in the httpd SSL configuration file. The Red Hat OS sets the default httpd SSL configuration file as /etc/httpd/conf.d/ssl.conf.

In stand-alone operational mode, when using the **scp** method, the SSL certificate and private key must be copied to the following destination file name and path:

- **SSL certificate.** /opt/swms/etc/provisioned_ssl_server.crt
- **SSL private key.** /opt/swms/etc/provisioned_ssl_server.key

  NOTE: For stand-alone operational mode, if the Web-based management interface has been used to provision SSL certificate and private key, Web-provisioned files overwrite the copied files upon the next restart. This is because SSL certificates and keys provisioned through the management interface are saved as /var/opt/swms/www/ssl/provisioned_ssl_server.crt and /var/opt/swms/www/ssl/provisioned_ssl_server.key and then copied to the /opt/swms/etc/ directory upon restart. To prevent the copied files from being overwritten, delete the files under the /var/opt/swms/www/ssl/ directory.

To login to the Web-based management interface and enabling HTTPS:

- For unsecure HTTP use
  - **http:**//*<AnyKubernetesHostIp>:<NodePortHttp>/swms*
- For HTTP over SSL (HTTPS) use
  - **https:**//*<AnyKubernetesHostIp>:<NodePortHttps>/swms*

The following table shows the HTTPS parameters that can be configured.

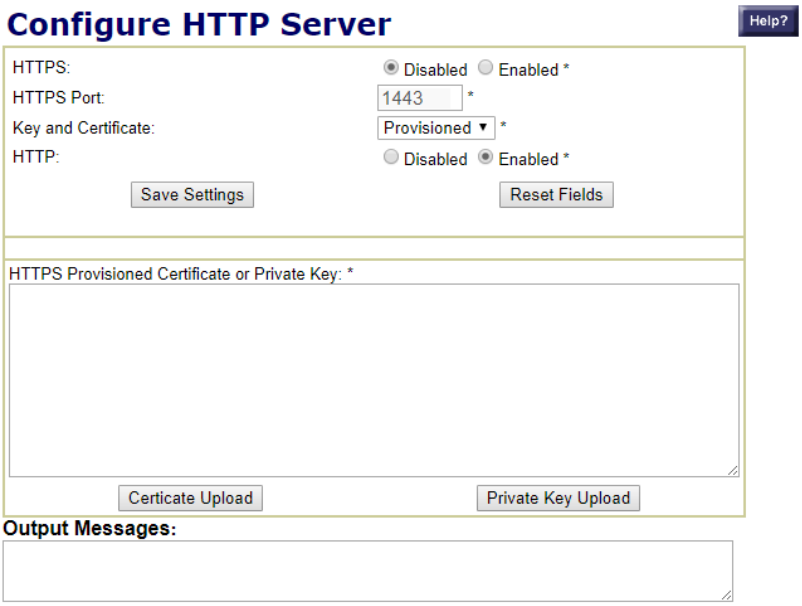
Table 120. HTTP Server Information

Value	Description
HTTPS	Enables or disables HTTP over SSL. The supported values are: • **Enabled.** Enables HTTPS. • **Disabled.** Disables HTTPS. ***NOTE:*** Configure TLS versions (1.0, 1.1, or 1.2) and **Preferred Cipher List** from the *Configure TLS* Web GUI to configure the required cipher suites. The default is Disabled. Changes to this field require an OAMP pod restart to take effect.
HTTPS Port	Port number to be used for HTTPS. This field is non-editable.
Key and Certificate	Specifies whether to use a provisioned key and certificate or the installed default. The supported values are: • **Default.** Selects the installed key and certificate. • **Provisioned.** Selects to use a provisioned key and certificate. ***NOTE:*** If the **extCert** (Certificate Manager) field is enabled in the *values.yaml* file, the supported value is Default. By default the Containerized Decomposed Media Server uses a provisioned key and certificate. Changes to this field require an OAMP pod restart to take effect.
HTTP	Enables or disables HTTP for the Web GUI and Annlab server. The supported values are: • **Enabled.** Enables HTTP. • **Disabled.** Disables HTTP. The default is Enabled. ***NOTE:*** • When this parameter is enabled, the AnnLab server listens on HTTP for receiving the REST APIs. • When this parameter is disabled, the AnnLab server does not listen on HTTP for receiving the REST APIs. Changes to this field require an OAMP pod restart to take effect.
HTTPS Provisioned Certificate or Private Key	Sets the certificate or key. The supported values are strings of maximum 4096 characters. To configure a Certificate or Private Key with more than 4096 characters, use *Manage Certificates* Web GUI page. The default value is blank. Changes to this field require an OAMP pod restart to take effect. ***NOTE:*** While deploying the Containerized Decomposed Media Server, if the **extCert** (Certificate Manager) field is enabled in the *values.yaml* file, the **HTTPS Provisioned Certificate or Private Key** parameter is not applicable. For more information on **extCert** parameter, refer *Containerized Decomposed Media Server Installation Guide*.

To configure the HTTP server:

1. Click **Administration** > **Configure HTTP Server**.

The Configure HTTP Server page displays.



2. Enter the information described in the above table and click **Save Settings**.

   The HTTPS or HTTP server configuration is set. The changes require a reboot or restart to take effect. When the changes are made, a confirmation message displays in the **Output Messages:** box.

3. Optionally, click **Reset Fields** to reset the changes made to the default values.

To upload SSL provisioned certificate and private key:

NOTE: If you select the **Key and Certificate** field value as **Provisioned**, follow this procedure.

1. Enter the certificate or private key message in the **HTTPS Provisioned Certificate or Private Key** field.
2. Click **Certificate Upload** or **Private Key Upload**.

   The SSL certificate or Private Key is uploaded. The changes require a reboot or restart to take effect.

Configure Management Activity Log

On the Configure Management Activity Log page, you can configure the management activity log and save it to a remote server.

For more information, see *Management Activity Logging on page 476*.

The following table shows the meanings of different log severities for management activities.

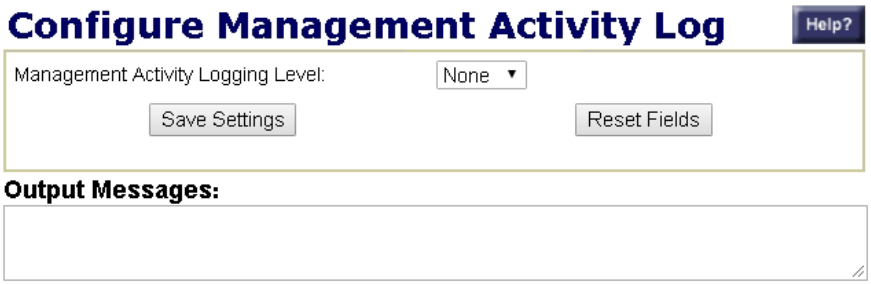
Table 121. Management Activities Log Severities

Severity	Meaning
None	No logging. This is the default value.
Info	A log severity of Information reports, in addition to the events reported under Notice severity, the changing of configuration parameters set through the Containerized Decomposed Media Server management interfaces.
Notice	A log severity of Notice reports occurrences of logging in, logging out, unsuccessful information, and change in management activities of the Containerized Decomposed Media Server management interfaces.

To configure logging severity:

1. Click **Administration** > **Configure Management Activity Log**.

The Configure Management Activity Log page displays.



2. Select the preferred severity for logging management activities in the **Management Activity Logging Level:** list.
   - **None.** No logging (this is the default)
   - **Info.** Logging at a severity level of Information
   - **Notice.** Logging at a severity level of Notice
3. Click **Save Settings**.

   The changes take effect immediately. When the change is done, a confirmation message displays in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to default values.

Retrieve Management Activity Log

On the Retrieve Management Activity Log page, you can retrieve the log file for management activity and save the file to a remote server or allow download using HTTP without user information. It also allows automatic transfer of the management activity log to the remote server. The management log file name is in the format of filename.$hostname.$timestamp, during auto transfer.

NOTE: When management activity log is retrieved though the Retrieve Management Activity Log page, the actual usernames are replaced with `<uname>` and the web client IP addresses are replaced with `<IPAddress>`.

For more information, see *Management Activity Logging on page 476*.

The following table describes the information that you must provide to use SFTP to post the management activities log file to a file server. This information is not needed for a Web download.

Table 122. File Transfer Information—Retrieve Management Activities Log

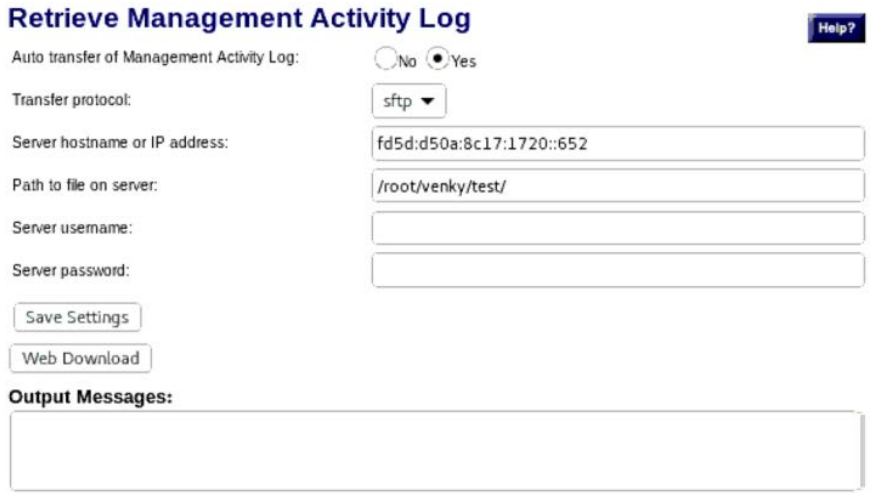
Value	Description
Auto transfer of Management Activity Log	The auto transfer of the management activity log to the remote server. The supported values are: • **Yes.** automatic transfer of management log is enabled • **No.** automatic transfer of management log is disabled The default value is No.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to file on server	The absolute path on the remote file server, where the management activities log messages file is to be saved. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank. ***NOTE:*** If the management log is a directory, append a slash ("/") in the remote server path.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.

NOTE: If auto transfer is enabled, the management activity log is transferred automatically to the remote server configured, after it reaches 100 KB and log rotation is attempted.

To retrieve the log file for management activity log:

1. Click **Administration** > **Retrieve Management Activity Log**.

The Retrieve Management Activity Log page displays.



2. For HTTP, click **Web Download**. For SFTP, enter the file transfer information described in the table.
3. Click **Save Settings**.

   For a Web download, use the pop-up window to save the log file.

Retrieve Management Activity Log (With Usernames)

On the Retrieve Management Activity Log (With Usernames) page, you can retrieve the management activity log file, including usernames, web client IP address, and save the file to a remote server or allow download using HTTP. It also allows to automatically transfer the management activity log to the remote server. The management log file name is in the format of filename.$hostname.$timestamp, during auto transfer.

For more information, see *Management Activity Logging on page 476*.

NOTE: This page is exactly the same as *Retrieve Management Activity Log* page except that the content of the activity log includes usernames and web client IP address. This page is available only for level1 users.

The following table describes the information that you must provide to use SFTP to post the management activities log file to a file server. This information is not needed for a Web download.

Table 123. File Transfer Information—Retrieve Management Activity Log (With Usernames)

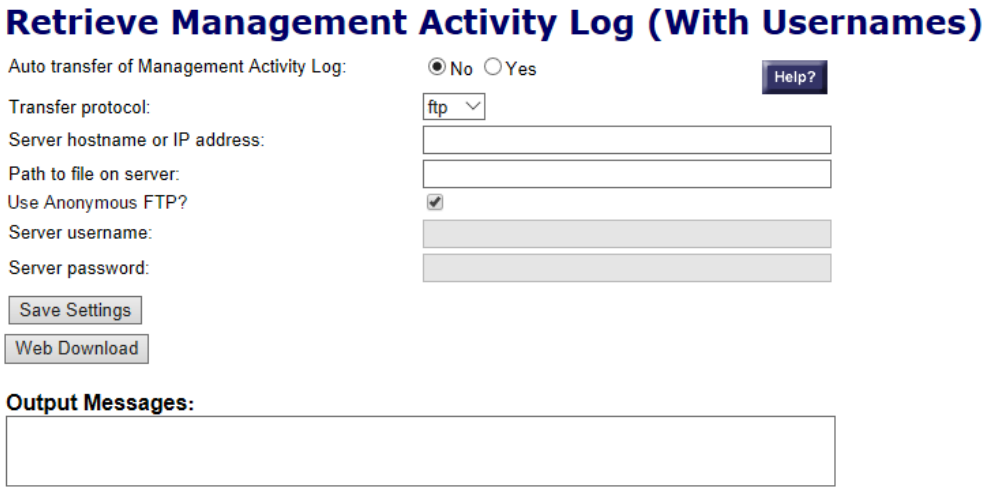
Value	Description
Auto transfer of Management Activity Log	The auto transfer of the management activity log to the remote server. The supported values are: • **Yes.** automatic transfer of management log is enabled • **No.** automatic transfer of management log is disabled The default value is No.
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to file on server	The absolute path on the file server, where the management activities log messages file is to be saved. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank. ***NOTE:*** If the management log is a directory, append a slash (“/”) in the remote server path.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters.

NOTE: If auto transfer is enabled, the management activity log is transferred automatically to the remote server configured, after it reaches 100 KB and log rotation is attempted.

To retrieve the log file for management activity log:

1. Click **Administration** > **Retrieve Management Activity Log (With Usernames)**.

   The Retrieve Management Activity Log (With Usernames) page displays.



2. For HTTP, click **Web Download**. For SFTP, enter the file transfer information described in the above table.
3. Click **Save Settings**.

   For a Web download, use the pop-up window to save the log file.

   Confirmation message is displayed in the **Output Messages:** box.

Backup User Database

The Backup User Database page allows you to back up the Containerized Decomposed Media Server locally provisioned users and their configuration by saving the user database to a file server.

The following table describe the information you must provide to use SFTP to back up the user database to a file server. This information is not needed for a Web download.

Table 124. File Transfer Information—Backup User Database

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to user database file on server	The absolute path on the file server, where the user database backup file is to be saved. The supported values are strings of up to 256 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank
Server username	The username configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.

To backup the user database:

1. Click **Administration** > **Backup User Database**.

The Backup User Database page displays.

2. For HTTP, click **Web Download**. For SFTP, enter the file transfer information described in the above table.
3. Click **Save Settings**.

   For a Web download, use the pop-up window to save the backup file.

   Confirmation message is displayed in the **Output Messages:** box.

Restore User Database

On the Restore User Database page, you can restore the Containerized Decomposed Media Servers locally provisioned users and their configuration from a previously saved database file on a file server.

The following table shows the information you must provide to use SFTP to restore the locally provisioned users and their configurations from a user database previously saved on a file server. This information is not needed for a Web download.

Table 125. File Transfer Information—Restore User Database

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6 of the file server. For DNS, use the hostname of the file server. The supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~".
Path to user database on server	The absolute path on the file server, where the user database backup file is located. The supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank.
Server username	The username configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.
Server password	The password configured on the file server. The supported values are strings of up to 128 characters. Changes to this field take effect immediately.

To restore user database and their configurations from a saved database file:

1. Click **Administration** > **Restore User Database**.

The Restore User Database page displays.

2. Enter the restore user database information described in the table.
3. Click **Save Settings**.

   The user database of the Containerized Decomposed Media Server is restored and is displayed in the **Output Messages:** box.

Configure SANE

The Configure SANE page allows you to configure the SAML Authenticated Network Element (SANE). The Containerized Decomposed Media Server Web GUI supports user authentication using Security Assertion Markup Language (SAML) 2.0 standards to provide single sign-on (SSO) functionalities.

The following table shows the SAML parameters that you can configure.

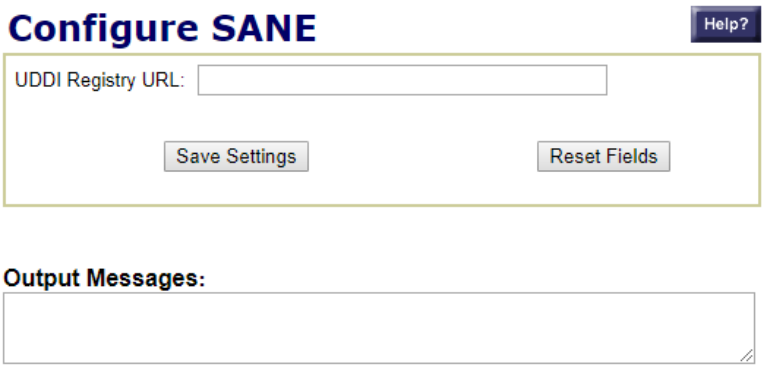
Table 126. SAML Information

Option	Description
UDDI Registry URL	Allows you to configure the UDDI register URL. The UDDI registry is a Simple Object Access Protocol (SOAP) web service that SAML provides to keep track of all the available services. The supported values are strings of a maximum of 255 characters. Changes to this field take effect from the next SAML assertion request.

To configure the SAML information:

1. Click **Administration** > **Configure SANE**.

The Configure SANE page displays.



2. Enter the **UDDI Registry URL**.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.
4. Optionally, click **Reset Fields** to reset the changes made to the previously saved values.

Retrieve Users

The Retrieve Users page allows you to retrieve the user information from the Containerized Decomposed Media Server in a *.csv* file and web downloaded file is transfered to an external remote server. The file can be read in a text editor.

NOTE: This feature is accessible only by Level 1 users.

The following table describes the information that you must provide to use SFTP to post the management activities log file to a file server. This information is not required for a Web download.

Table 127. File Transfer Information—Retrieve Users

Value	Description
Transfer protocol	The transfer protocol used for communicating with the file server is Secure File Transfer Protocol (SFTP). Changes to this field take effect immediately.

Table 127. File Transfer Information—Retrieve Users

Value	Description
Server hostname or IP address	The IP address, in dotted quad format for IPv4 or the supported notations for IPv6, of the file server. For DNS, the hostname of the file server can be used. Supported values are strings of up to 80 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". Changes to this field take effect immediately.
Path to retrieve users on server	The absolute path on the remote file server, where the user information is to be saved. Supported values are strings of up to 128 characters. Allowed set of characters is. • uppercase alphabetic characters (A-Z) • lowercase alphabetic characters (a-z) • numeric characters (0-9) • special characters (/#.-_@=+%:~) ***NOTE:*** Do not begin the name with "#" or "~". This field cannot be blank. Changes to this field take effect immediately.
Server username	The username configured on the file server. Supported values are strings of up to 128 characters. Changes to this field take effect immediately.
Server password	The password configured on the file server. Supported values are strings of up to 128 characters. Changes to this field take effect immediately.

To retrieve user information:

1. Click **Administration** > **Retrieve Users**.

   The Retrieve Users page displays.

2. Configure the retrieve user information as described in the above table.
3. Click **Save Settings**.

   Confirmation message is displayed in the **Output Messages:** box.

   For a Web download, use the pop-up window to save the user information in a *.csv* file and transfer the downloaded file to the remote server.

MRFC Configuration

This chapter describes the MRFC configuration for Containerized Decomposed Media Server.

MRFC is configured manually in the configuration files and cannot be changed through the management interface. As MRFC configuration does not synchronize automatically. MRFC configured manually on both the active and standby MRFC. Table 128 lists the MRFC configuration parameters. These parameters requires a reboot. However, you can configure the MRFCtrl and AnnLab parameters during the instantiation. For procedure on how to configure, refer to the *Containerized Decomposed Media Server Installation Guide*.

After changing the configuration parameters, the following switchover is required.

- Parameters in *sipproxysubsystem.ini* file, require MRFC switchover
- Parameters in *annlabservercfg.properties* file, require MNGT switchover
- Parameters in *mrfctrl.cfg* file, require MRFC switchover

Other than the parameters listed in Table 128, there are additional parameters present in the configuration files. Radisys recommends not to change these additional parameters.

Table 128. MRFC Configuration Parameters

Parameter Name	Description
DscpAutoAnswer [General]	The Differentiated Services Code Point (DSCP) mirroring. The supported values are: • 0. Configured DSCP value is used. • 1. Takes precedence over received DSCP value from the requests. The default value is 0. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
DscpValue [General]	The outgoing SIP messages are marked with the entered DSCP. Instructs the system to create the SIP network sockets with DSCP options. The value range is from 0 to 63. The default value is 26 (AF31). ***NOTE:*** If DscpValue is not configured, the value is considers as zero. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
MaxOtgUDPReqSize [SIP-TX]	The maximum size in bytes, of a SIP request message sent over the UDP. The SIP request that is larger than this size is sent over the TCP. The value range is from 1024 to 65535. The default value is 4096. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
MaxOtgUDPReqSizeForIpv6 [SIP-TX]	The maximum size in bytes, of a SIP request message sent over the UDP for an IPv6 address type. The SIP request that is larger than this size is sent over the TCP. The value range is from 1024 to 65535. The default value is 4096. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.

Table 128. MRFC Configuration Parameters

Parameter Name	Description
setTcpDscpVal [SIPTCP]	Sets the configured DSCP value for SIP over TCP. The supported values are: • **0.** Sets the **DnsDscpValue** to 46 (0x2E). • **1.** Sets the **DnsDscpValue** to 32 (0x20) for TCP connection. The default value is 0. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns1Server1 [SIPDNS]	The pool1 primary Domain Name Server (DNS) IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns1Server2 [SIPDNS]	The pool1 secondary DNS IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns1Server3 [SIPDNS]	The pool1 tertiary DNS IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
DnsSweepTimeout [SIPDNS]	The DNS sweep timer in seconds. It scans the local cache and removes the expired DNS records. The value range is from 250 to 500. The default value is 300. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns2Server1 [SIPDNS]	The pool2 primary DNS IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns2Server2 [SIPDNS]	The pool2 secondary DNS IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
Dns2Server3 [SIPDNS]	The pool2 tertiary DNS IP address of the destination host. An IP address is in dotted quad format for IPv4 or the supported notations for IPv6. The supported values are: • IPv4=0.0.0.0 • IPv6=[0::0] Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.

Table 128. MRFC Configuration Parameters

Parameter Name	Description

DnsDscpValue
[SIPDNS]
	Instructs the system to create the SIP network sockets for DNS queries with DSCP options.
	• For UDP transport, the outgoing DNS messages are marked with the entered DSCP value. The value range is from 0 to 63. The default value is 26.
	• For TCP transport, the outgoing DNS messages are marked with the DSCP value 32 or 46.
	  • The value of **DnsDscpValue** is 46, when **setTcpDscpVal** is set to 0.
	  • The value of **DnsDscpValue** is 32, when **setTcpDscpVal** is set to 1.
	The default value is 46 (AF31).
	NOTE: If DscpValue is not configured, the value is considered as zero.
	Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.

sipDomain1	The first accepted "external" SIP domain. This is used to check the invite sipdomain. Configuration file is */opt/AVPOP/cfg/modules/aliases.ini*.
sipDomain2	The second accepted "external" SIP domain. This is used to check the invite sipdomain. This is an optional parameter, but mandatory for dual stack mode. Configuration file is */opt/AVPOP/cfg/modules/aliases.ini*.
TlsSupport [SIPTLS]	Enables or disables the TLS feature. The supported values are: • **0.** Disables the TLS feature. • **1.** Enables the TLS feature. The default value is 0. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
MaxNbrConn [SIPTLS]	The maximum number of TLS connections allowed at a time. The data type is integer. The default value is 100. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
TlsConnTimer [SIPTLS]	The default value for TLS connection cyclic timer in milliseconds. The data type is integer. The default value is 3600000. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
certfile [SIPTLS]	The local certificate path for TLS handshake. The data type is string. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
keyfile [SIPTLS]	The local key file path for TLS handshake. The data type is string. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
cafile [SIPTLS]	The Certificate Authority (CA) file path for TLS handshake. The CA file is used to validate the received server certificates during TLS handshake. The data type is string. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
PeerAuth [SIPTLS]	Enables peer authentication through IP validation. The data type is boolean. The supported values are: • **1.** true • **0.** false The default value is 0. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.

Table 128. MRFC Configuration Parameters

Parameter Name	Description
IPv4ValidationList [SIPTLS]	Allows to configure a list of IPv4 addresses that are verified at the server to authenticate the client certificates. The IPv4 addresses are represented as comma-separated values. When the MRFC acts as a server for SSL connection, the TLS connections are allowed only from the configured IP addresses. The data type is string. The default value is ' '. ***NOTE:*** This can be configured only when **PeerAuth** is enabled. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
IPv6ValidationList [SIPTLS]	Allows to configure a list of IPv6 addresses that are verified at the server to authenticate the client certificates. The IPv6 addresses are represented as comma-separated values. When the MRFC acts as a server for SSL connection, the TLS connections are allowed only from the configured IP addresses. The data type is string. The default value is ' '. ***NOTE:*** This can be configured only when **PeerAuth** is enabled. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
PreferredCipherList [SIPTLS]	Allows to configure a list of cipher suites that are preferred for the TLS connection. The data type is string. The default value is ' '. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
ecdhe_curve [SIPTLS]	Allows to set the Elliptic-curve Diffie–Hellman (ECDHE) curve. The data type is string. The default value is ' '. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
setTcpDscpVal [SIPTLS]	Sets the configured DSCP value for SIP over TLS. The data type is boolean. The supported values are: • **0.** Sets the **DnsDscpValue** to 46 (0x2E). • **1.** Sets the **DnsDscpValue** to 32 (0x20) for TLS connection. The default value is 0. Configuration file is */opt/AVPOP/mrfctrl/current/bin/ini/sipproxysubsystem.ini*.
client.timeout	The period, in ms, in which the AnnLab server disconnects if there is no heartbeat from the AnnLab client. The data type is integer. The default value is 10000. Configuration file is */opt/swms/cfg/modules/annlabservercfg.properties*.
Method [Load_Balancing]	Specifies the load balancing methods for forwarding the initial SIP INVITE requests to the select MRFPs. The supported values are: • **ROUND_ROBIN.** MRFC distributes the incoming calls on MRFPs in a round-robin method, without considering a load on the individual MRFP. • **DYNAMIC_FEEDBACK.** When Dynamic-Feedback method is enabled, MRFPs report their current resource utilization to MRFC at regular intervals through the `SIP REGISTER` request. MRFC uses this information to evaluate the resource utilization for each MRFP, bucketizes the MRFPs, and routes the new incoming call on MRFPs. The default value is Round-Robin. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
Slab1 [Load_Balancing]	Indicates the maximum threshold value configured for bucket1, in percentage. The supported value is from 0 to 100. The default value is 40. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.

Table 128. MRFC Configuration Parameters

Parameter Name	Description
Slab2 [Load_Balancing]	Indicates the maximum threshold value configured for bucket2, in percentage. The supported value is from 0 to 100. The default value is 60. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
Slab3 [Load_Balancing]	Indicates the maximum threshold value configured for bucket3, in percentage. The supported value is from 0 to 100. The default value is 80. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
Enable503	Defines the replacment of *503 Service Unavailable* response code with *404 Not Found* response code after each restart of MRFCtrl for a period of time. The data type is boolean. The supported values are: • **1.** true • **0.** false The default value is 0. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
Enable503_timer	Defines the timer, in seconds, that must pass before the feature activation expires. This timer is refreshed after each MRFCtrl restart. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
errorCodeNoMRFP	Defines the error code that is returned when the MRFP is unavailable for SIP INVITE messages. When the MRFP is unavailable, this error code is used for the SIP OPTIONS irrespective of **Enable503** value. ***NOTE:*** For SIP INVITE, this parameter is applicable when **Enable503** is set to false. The data type is integer. The supported value is from 400 to 699. The default value is 404. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.
errorCodeNoMRFPOptions	Defines the error code that is returned when all the MRFPs are unavailable for SIP OPTIONS messages. The data type is integer. The supported value is from 400 to 699. As this parameter is commented, there is no default value. ***NOTE:*** If this parameter is not defined in the file, the parameter must be manually added for it to work. Configuration file is */opt/AVPOP/cfg/modules/mrfctrl.cfg*.

NOTE: The slab values must be in incremental order, that is, **Slab3** value must be greater than **Slab2** and **Slab1** value, and **Slab2** value must be greater than **Slab1** value.

JSON File Configuration

AnnLab output transcoding files are controlled using the JSON file.

The Containerized Decomposed Media Server provides a configuration JSON file (txConfig.json) on MRFC, at */opt/swms/cfg/modules/txConfig.json*. Changes in this configuration file are synchronized automatically with each MRFP after restart. The *txConfig.json* file is modified to select the list of desired generated clips. The specific sections of the codec formats in the JSON file can be removed or modified to reduce offline transcoding time and disk space requirements.

Sample JSON file

```
{
    "TranscodeList": [
      {
                "CodecName": "PCM",
                "Comment": "S16LE",
                "Bitrate": [ "pcm" ],
                "Samplerate": [ 8000, 16000, 32000 ],
                "Channels": [ 1 ],
                "FileExtn": "pcm"
      },
      {
                "CodecName": "AMR",
                "Comment": "AMR NB",
                "Bitrate": [ "Mode0", "Mode1", "Mode2", "Mode3", "Mode4",
                "Mode5", "Mode6", "Mode7" ],
                "Samplerate": [ 8000 ],
                "Channels": [ 1 ],
                "FileExtn": "3gp"
      },
      {
                "CodecName": "AMRWB",
                "Comment": "AMR-WB",
                "Bitrate": [ "Mode0", "Mode1", "Mode2", "Mode3", "Mode4",
                "Mode5", "Mode6", "Mode7", "Mode8" ],
                "Samplerate": [ 16000 ],
                "Channels": [ 1 ],
                "FileExtn": "3gp"
      },
      {
                "CodecName": "G711U",
                "Comment": "ULAW",
                "Bitrate": [ "pcm" ],
                "Samplerate": [ 8000 ],
                "Channels": [ 1 ],
                "FileExtn": "wav"
      },
      {
                "CodecName": "G711A",
                "Comment": "ALAW",
                "Bitrate": [ "pcm" ],
                "Samplerate": [ 8000 ],
                "Channels": [ 1 ],
                "FileExtn": "wav"
```

```
},
{
        "CodecName": "G722",
        "Comment": "G722",
        "Bitrate": [ "pcm" ],
        "Samplerate": [ 16000 ],
        "Channels": [ 1 ],
        "FileExtn": "wav"
},
{
        "CodecName": "G729",
        "Comment": "G729",
        "Bitrate": [ "pcm" ],
        "Samplerate": [ 8000 ],
        "Channels": [ 1 ],
        "FileExtn": "wav"
},
{
        "CodecName": "EVS",
        "Comment": "BW_NB",
        "Bitrate": [ "BR_5_9", "BR_7_2", "BR_8_0", "BR_9_6", "BR_13_2",
        "BR_16_4", "BR_24_4" ],
        "Samplerate": [ 8000 ],
        "Channels": [ 1 ],
        "FileExtn": "evs"
},
{
        "CodecName": "EVS",
        "Comment": "BW_WB",
        "Bitrate": [ "BR_5_9", "BR_7_2", "BR_8_0", "BR_9_6", "BR_13_2",
        "BR_16_4", "BR_24_4", "BR_32_0", "BR_48_0", "BR_64_0",
        "BR_96_0", "BR_128_0" ],
        "Samplerate": [ 16000 ],
        "Channels": [ 1 ],
        "FileExtn": "evs"
},
{
        "CodecName": "EVS",
        "Comment": "BW_SWB",
        "Bitrate": [ "BR_9_6", "BR_13_2", "BR_16_4", "BR_24_4",
        "BR_32_0", "BR_48_0", "BR_64_0", "BR_96_0", "BR_128_0" ],
        "Samplerate": [ 32000 ],
        "Channels": [ 1 ],
        "FileExtn": "evs"
},
```

```
        {
                "CodecName": "EVSIO",
                "Comment": "EVS-IO",
                "Bitrate": [ "Mode0", "Mode1", "Mode2", "Mode3", "Mode4",
                "Mode5", "Mode6", "Mode7", "Mode8" ],
                "Samplerate": [ 16000 ],
                "Channels": [ 1 ],
                "FileExtn": "evs"
        }
      ]
   }
```

To change the transcoder options:

The number of offline transcoding clips generated for a single clip is very high; therefore, the Containerized Decomposed Media Server provides an option to configure only the required codecs.

NOTE: The transcoding JSON file must not be changed frequently.

1. Edit the *txConfig.json* file placed in MRFC, at */opt/swms/cfg/modules/txConfig.json*.
2. Delete the supported codecs or bitrates based on your requirements.

   When deleting the supported codec and bitrates, ensure the following.
   - Do not remove the PCM entries from the JSON file.
   - Do not add any unsupported codec formats in the JSON file.
   - Arbitrary bitrates are not supported; you must include only the specified bitrates as per the JSON file.
   - You must include only the supported sample rate (8000, 16000, and 32000).
   - You must follow the JSON format as the JSON file is sensitive for **Tab**, **,**, **{ }**, and **New_line**.
   - The Containerized Decomposed Media Server supports mono (number of channels is 1).
3. Save the *txConfig.json*.
4. Restart the MRFP.

MNGT Tool

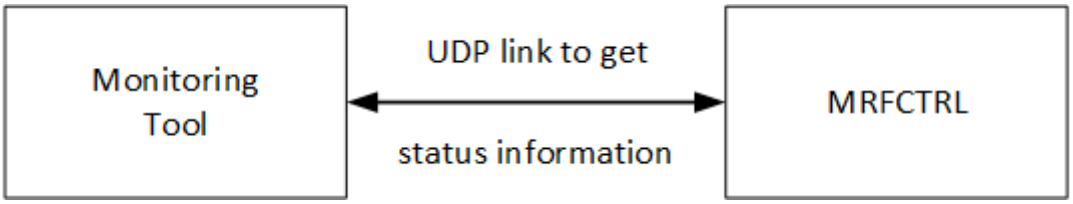
This chapter provides the information on monitoring (MNGT) tool.

MRFCtrl Monitoring

The MRFCtrl is a control process delivered with a monitoring tool. MRFCtrl allows `swmsuser` to retrieve the dynamic state information relative to MRFPs (capabilities of the MNGT tool). For example, the MNGT tool command **`mngttool mrfctrl`** lists all the conferences created on the Containerized Decomposed Media Server.

The MNGT tool is used to verify the registered MRFPs.

Figure 28. MRFCtrl Monitoring



The monitoring tool provides the following features.

- Dumps the capabilities registration table
- Dumps the aliases table
- Dumps the list of physical MRFPs, supporting conferencing and MRFPs current state
- Dumps the list of conferences for each MRFP and their current state
- Stops the MRFCtrl
- Configures the trace levels for the MRFCtrl component at run time
- Directs call functionality

MNGT Tool Commands

The MNGT tool command `mngttool mrfctrl`, lists all the conferences created on the Containerized Decomposed Media Server.

Table 129 lists the functionality of MNGT tool commands.

Table 129. MNGT Tool Commands and Functionalities

MNGT Tool Commands	Functionalities
`help`	Lists all the available commands in the MNGT tool.
`get aliases`	Dumps the aliases table.
`get capabilities table`	Dumps the capabilities of the registration table.
`get conference hosts`	Dumps the list of all physical MRFP supporting conferences and MRFP current state.

Table 129. MNGT Tool Commands and Functionalities

MNGT Tool Commands	Functionalities
`get conferences list`	Dumps the list of conferences for each MRFP and MRFP current state.
`get trace mask`	Obtains the MRFCTRL log level.
`get buckets`	Obtains the MRFP presence in the buckets. This is applicable for Containerized Decomposed Media Server load balancing method.
`remove mrfp <ip>`	Removes MRFP for the MRFC.
`set trace rotate`	Rotates the trace file.
`set trace mask <level>`	Configures the MRFCTRL log level. See *Traces Interface* for detail description of these commands.
`Selection Interface`	Used for directing calls feature. See *Selection Interface* for detail description of these commands.

Access MNGT Tool

The following commands are used to access the MNGT tool.

```
[root@master-1 ~]# kubectl exec -it mrfctrl-0  -- /bin/bash
[root@mrfctrl-0 /]# su - swmsuser
-bash-4.2$  /opt/AVPOP/mpm/4.5.0-03/etc/mngttool mrfctrl
mngt> <Provide the MNGT tool commands>
```

For example: `mngt> get capabilities table`

Call Interface

The following are the call interface commands.

```
get aliases
get capabilities table
get invite rate
get conference hosts
get conferences list
remove mrfp <ip>
```

NOTE: The commands `get aliases` and `get invite rate` are not applicable in the Containerized Decomposed Media Server.

Traces Interface

The following are the trace interface commands.

```
set trace rotate
get trace mask
set trace mask <level>
   INFO_LEVEL          0x000004
   ERROR_LEVEL         0x000008
   WARNING_LEVEL       0x000100
```

```
CONF_LEVEL          0x000400
STATISTIC_LEVEL     0x200000
```

Selection Interface

The following are the selection interface commands.

```
get selection
set selection call <criteria>
set selection conf <Conference Id>
set selection mrfp <IP address of MRFP>
set selection duration <minutes>
set selection number <number>
set selection terminate
set selection call steering <enable/disable>
```

Call Steering

The call steering selection criteria is configured through the MNGT tool using the following command.

```
set selection call steering <enable/disable>
```

The default value is disable.

Based on the call steering criteria set in the MNGT tool and SIP load balancing method configured in the management interface, the MRFCtrl forwards the calls to the specific MRFP. If the call steering criteria do not match with the particular MRFP, the MRFCtrl does not forward the calls to that MRFP; instead, MRFCtrl forwards the calls to the next available MRFP.

Stop MRFCTRL Process

The following command is used to stop the MRFCtrl process.

```
mngt> stop
```

Examples

The following example shows the execution of get conferences list command.

```
mngt> get conferences list
HOSTNAME: 192.168.234.221
Number of conferences = 1
-------------------------------------------------------------
capability Name | language  | conference Name  |  status   |
-------------------------------------------------------------
Msml            |  Msml     |  conference1     |   alive   |
-------------------------------------------------------------
END
mngt>
```

The following example shows the execution of get buckets command.

```
mngt> get buckets
--------------------------------------------------------------------------------
            Bucket ID           |                    Hosts
--------------------------------+-----------------------------------------
            Bucket 0            | 10.214.4.50
                                | 10.214.4.49
--------------------------------+-----------------------------------------
            Bucket 1            | Bucket EMPTY
--------------------------------+-----------------------------------------
            Bucket 2            | Bucket EMPTY
--------------------------------+-----------------------------------------
            Bucket 3            | Bucket EMPTY
--------------------------------+-----------------------------------------
END
mngt>
```

Directing Calls Feature

Directing calls feature allows to configure the MRFCtrl to forward some identified calls or conferences to a specific MRFP. Only NETANN and MSCML conferences are redirected to the specified MRFP. This feature routes the particular call or conference on a desired MRFP.

This feature is used only in lab testing and not for production environment.

NOTE:

- This feature is not applicable for MSML conference or the **sip:monitor** service context.
- Call can be directed to only one MRFP at a given time.

MRFC Configuration using MNGT Tool

MRFCtrl forwards the call or conference to the selected MRFP based on the following criteria.

- For a call, criteria is present in `From` or `P-Asserted-Identity` SIP header.
- For the conferences, criteria contains conference name.

Different criteria for call and conferences can be set at a time. Following commands are used for adding a criteria in the MNGT tool.

```
# mngttool mrfctrl
mngt> set selection call <string criteria>
mngt> set selection conf <Conference Id>
```

One or more criteria can be specified in the `set selection` command. When multiple criteria are specified in a `set selection` command, the multiple criteria are considered to be logically OR'd together and the MRFCtrl matches to any one of the specified criteria.

For example, `set selection call criteria1 critera2 criteria3` or `set selection conf criteria1 critera2 criteria3`

- Following are the commands when * criteria is used.

  ```
  # mngttool mrfctrl
  mngt> set selection call *
  mngt> set selection conf *
  ```

  All the incoming calls or conferences are forwarded in * criteria commands.
- The MRFCtrl provides an option to steer calls to an MRFP only when the criteria match. The MRFP does not receive other calls. This option is enabled through the **steering** parameter. The default setting for this option is disabled.

  ```
  # mngttool mrfctrl
  mngt> set selection call steering enable
  ```
- Execute the following command to add the selected MRFP.

  ```
  # mngttool mrfctrl
  mngt> set selection mrfp <IP address of MRFP>
  ```

  where the IP address format is IPv4 or IPv6. If the command is inactive, the Containerized Decomposed Media Server rejects the command with the message `No active selection`.

  ```
  # mngttool mrfctrl
  mngt> set selection mrfp <IP address of MRFP>
  ```
- If `<string criteria>` or `<Conference Id>` is matched, the MRFCtrl directs the call or conference exclusively to targeted MRFP.
- If `<string criteria>` or `<Conference Id>` is not matched, the MRFCtrl balances the calls or conferences across all of the available MRFPs. The available MRFPs list can include the targeted MRFP.

Duration of Selection

The duration for selection is limited with the following parameters.

- **Duration.** Represents the number of minutes (m) after the current time (t). After the expiration date (t +m), the selection becomes inactive. The duration value is unlimited. Following are the duration of selection commands.

  ```
  # mngttool mrfctrl
  mngt> set selection duration <minutes>
  ```
- **Number.** Represents the number of calls forwarded. Number is used for several criteria and cannot be greater than five.

  ```
  # mngttool mrfctrl
  mngt> set selection number <number of call forwarded>
  ```

  For example, two calls from the first MDN (A@radisys.com) and three calls from the second MDN (B@radisys.com) are forwarded and other calls are rejected. Because the total number of calls are limited to five.

If both call and conference criteria are set, the total number is shared between the call and the conference. For example, two calls from the MDN (A@radisys.com) and three conferences from conference criteria are forwarded and other calls and conferences are rejected. Because the total number of calls and conferences are five.

If the **duration** and the **number** are not set in the selection, only one call or conference is forwarded and the selection is removed.

Selection Termination

The following command is used to remove the selection.

```
# mngttool mrfctrl
mngt> set selection terminate
```

Additional Commands

Following are the additional MNGT commands.

The `get selection` command allows you to know about the active selection. Following is the sample for `get selection` command.

```
# mngttool mrfctrl
mngt> get selection
MRFP: 192.168.213.130
Duration: 4 call(s)
Duration: end at 04/08/15;05:53:42 PM
Selection Call :
bob@radisys
alice@radisys
Selection MSCML/NETANN Conf :
confid001
confid200
```

In the above example, the **`Duration: end at <time>`** indicates that the **duration** parameter is set. The syntax varies if the **number** parameter is set and the syntax is:

```
Duration: X calls
```

If the selection is inactive, the MNGT tool displays `No active selection` message.

```
# mngttool mrfctrl
mngt> get selection
No active selection
```

The **`help`** command provides the available commands in the MNGT tool that are allowed for MRFP.

```
# mngttool mrfctrl
mngt> help
SELECTION INTERFACE :
   get selection
```

```
set selection call <criteria>
set selection conf <Conference Id>
set selection mrfp <IP address of MRFP>
set selection duration <minutes>
set selection number <number>
set selection terminate
set selection call steering <enable/disable>
```

Examples

Forward the first incoming call or conference to the selected MRFP

```
# mngttool mrfctrl
mngt> set selection *
mngt> set selection mrfp 192.168.213.130
```

Forward the first incoming call or conference to the selected MRFP with two criteria and a limited duration of 10 minutes

```
# mngttool mrfctrl
mngt> set selection call john@radisys.com
mngt> set selection call brenda@radisys.com
mngt> set selection conf confId001
mngt> set selection conf confId200
mngt> set selection duration 10
mngt> set selection mrfp 192.168.213.130
```

Forward the first incoming call or conference to the selected MRFP with two criteria and number of calls forwarded to 5

```
# mngttool mrfctrl
mngt> set selection call john@radisys.com
mngt> set selection call brenda@radisys.com
mngt> set selection conf confId001
mngt> set selection conf confId200
mngt> set selection number 5
mngt> set selection mrfp 192.168.213.130
```

PART 3: APPENDICES

Appendix A

List of Alarms

This appendix lists the alarms generated by the Containerized Decomposed Media Server.

The Containerized Decomposed Media Server SNMP traps and alarms are shared across all platforms of the Containerized Decomposed Media Server family of products.

On the Containerized Decomposed Media Server, terms such as firmware must be understood as referring to software.

System Alarms

The following table describes the system alarms. Alarms are sorted first by severity and then by alarm ID number.

Table 130. Critical Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
Critical Alarms					
45	Resource usage exceeded service overload threshold on slot X	Resource usage below service overload threshold for the past minute on slot X	Critical	MRFP	The Containerized Decomposed Media Server is in a service overload situation. This alarm indicates that the Containerized Decomposed Media Server now starts rejecting all new calls and all service requests on existing calls (except those that free resources, like delete requests). This alarm is cleared when resource levels drop below threshold for at least one minute. Possible causes: • The Containerized Decomposed Media Server has exceeded either a CPU usage threshold or a memory usage threshold. • The Containerized Decomposed Media Server reached the call overload threshold and began rejecting new calls, but the overload continued to increase. Recommended actions: • Lower the call overload threshold so that the Containerized Decomposed Media Server does not reach a service overload condition. • Optimize applications to maximize Containerized Decomposed Media Server capacity. (See *Radisys Special Interfaces Reference* for guidelines.) • Increase capacity of the Containerized Decomposed Media Server by adding more hardware. • Verify that the RAM drive size is set appropriately for your application. For applications that do not involve internal recordings, the RAM drive should be set to the minimum size. • If using either NFS or HTTP announcements, change to using internal announcements, which typically provides higher capacity. • Use a control agent that implements load balancing and can redirect failed calls to another Containerized Decomposed Media Server. • Use a control agent that implements an algorithm for reducing the load on an Containerized Decomposed Media Server when it reaches an overload condition.
47	The system is in service overload situation continuously on slot X	Overload reboot alarm cleared on startup on slot X	Critical	MRFP	The Containerized Decomposed Media Server is in a service overload situation for so long, it is automatically rebooted. This alarm is cleared after a brief interval. Possible cause: • Refer to the causes for Service overload condition. Recommended action: • Reduce the possibility that the Containerized Decomposed Media Server reaches a service overload condition.

Table 130. Critical Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
73	Network interface is down: *device name*	Network interface link restored.	Critical	MRFC or MRFP	The Containerized Decomposed Media Server has found the link status of network interface 1 is an Ethernet or bonded Ethernet interface and is inoperable or the interface is not configured for use. This alarm is cleared when the link status becomes operational. Recommended actions: • Ensure that the port on the switch and the port on the Containerized Decomposed Media Server are configured identically. • Verify Ethernet cabling. • Verify the Ethernet connections on network interface 1.
74	Network interface is down: *device name*	Network interface link restored.	Critical	MRFC or MRFP	The Containerized Decomposed Media Server has found the link status of network interface 2 is an Ethernet or bonded Ethernet interface and is inoperable. This alarm is cleared when the link status becomes operational or the interface is not configured for use. Recommended actions: • Ensure that the port on the switch and the port on the Containerized Decomposed Media Server are configured identically. • Verify Ethernet cabling. • Verify the Ethernet connections on network interface 2.
75	Network interface is down: *device name*	Network interface link restored.	Critical	MRFC or MRFP	The Containerized Decomposed Media Server has found the link status of network interface 3 is an Ethernet or bonded Ethernet interface and is inoperable. This alarm is cleared when the link status becomes operational or the interface is not configured for use. Recommended actions: • Ensure that the port on the switch and the port on the Containerized Decomposed Media Server are configured identically. • Verify Ethernet cabling. • Verify the Ethernet connections on network interface 3.
80	The node license key is invalid.	The node license key is valid.	Critical	MRFC	The license file entered for this platform is incorrect. This alarm is cleared when a valid license file is entered. Recommended action: • Recommended action is to contact TAC, for valid instance license.
83	MRFP redundancy is unavailable for group X	Alarm cleared	Critical	MRFP	The alarm is generated when the MRFP redundancy group does not have an online standby MRFP. This alarm is cleared when either there is an online standby MRFP in the redundancy group or the redundancy group no longer exist. Recommended action: • Ensure that the instance in the MRFP designated as the standby is present and in service operation mode.

Table 130. Critical Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
84	MRFP heartbeat failure detected on slot X	Alarm cleared	Critical	MRFP	The alarm is generated when the Containerized Decomposed Media Server has detected a heartbeat failure on MRFP instance. This alarm is cleared when heartbeat is re-established or the MRFP instance is no longer in a redundancy group. Recommended action is none.
90	Failed to connect to all ASR servers on slot X	Connection is established with an ASR server on slot X	Critical	MRFP	A connection failure has occurred with every configured ASR server. This alarm is cleared if the Containerized Decomposed Media Server is shut down, all ASR servers are disabled through configuration, or a response to the Containerized Decomposed Media Server heartbeat request is received from one of the disconnected ASR servers. Recommended action is to verify that the servers are operating normally, that the servers have been configured properly, and that the network communication can be established between the Containerized Decomposed Media Server and each ASR server.
92	Failed to connect to all TTS servers on slot X	Connection is established with a TTS server on slot X	Critical	MRFP	A connection failure has occurred with every configured TTS server. This alarm is cleared if the MRFP is shut down, all TTS servers are disabled through configuration, or a response to the Containerized Decomposed Media Server heartbeat request is received from one of the disconnected TTS servers. Recommended action is to verify that the servers are operating normally, that the servers have been configured properly, and that the network communication can be established between the Containerized Decomposed Media Server and each TTS server.
98	Software timeout limit exceeded on slot X	Alarm cleared on slot X	Critical	MRFP	An excessive number of soft watchdog timeouts (SWTs) have been detected on one of the MRFPs. This alarm is automatically cleared. Recommended action it to terminate all connections on the MRFP, take the MRFP out of service, and contact TAC.
101	Network interface failed to initialize: <*device name*>	Alarm cleared	Critical	MRFC or MRFP	The Containerized Decomposed Media Server has detected that a network interface is failed to initialize. This alarm is cleared on reboot. Recommended action: Check that the network configuration is valid.
149	Network Interface is Down: <device name>	Network interface link restored	Critical	MRFP	The MRFP detects that the network interface 4 is an Ethernet or bonded Ethernet interface and is inoperable. This alarm is cleared when the link status becomes operational or the interface is not configured for use. Recommended action is to check that the network cable is in good working condition and is securely connected at each end.

Table 130. Critical Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
174	Containerized Decomposed Media Server Controller SipProxysubsystem configuration failed on host: X where X is hostname of the Containerized Decomposed Media Server instance	Alarm cleared	Critical	MRFCtrl	This alarm is generated due to incorrect configuration of *SipProxysubsystem* or when the MRFC *SipProxysubsystem* configuration fails. This alarm is cleared when the configuration of *SipProxysubsystem* is correct. Possible cause: MRFC *SipProxysubsystem* configuration failure. Recommended action: Verify the logs at */var/log/AVPOP/mrfctrl.log* to find out the reason for failure.
175	Containerized Decomposed Media Server Controller configuration failed on host: X where X is hostname of the Containerized Decomposed Media Server instance	Alarm cleared	Critical	MRFCtrl	This alarm is generated when the MRFC configuration fails. This alarm is cleared when the MRFC configuration is successful. Possible causes: • MRFC configuration failure. • Startup error when reading or analyzing the configuration file. Recommended action: Verify the logs at */var/log/AVPOP/mrfctrl.log* to find out the reason for failure.
176	Containerized Decomposed Media Server controller failed to retrieve hostname on host: X where X is hostname of the Containerized Decomposed Media Server instance	Alarm cleared	Critical	MRFCtrl	This alarm is generated when the MRFC configuration fails to retrieve the hostname. Hostname is not found through the name service (*/etc/hosts*). This alarm is cleared when the MRFC configuration to retrieve the hostname is successful. Possible cause: MRFC configuration failure to retrieve the hostname. Recommended actions: • Verify the configuration file at */var/log/AVPOP/mrfctrl.log*. • Verify the configuration file and */etc/hosts*.
177	Containerized Decomposed Media Server Controller UDP port initialization failed on host: X where X is hostname of the Containerized Decomposed Media Server instance	Alarm cleared	Critical	MRFCtrl	This alarm is generated when the MRFC startup error is observed during the UDP port initialization. This alarm is cleared when the MRFC startup error is cleared. Possible causes: • MRFC startup error is observed during the UDP port initialization. • *mrfctrlmngt* port or *SipSPApiPort* allocation failure. • Service is unavailable. Recommended actions: • Verify the logs at */var/log/AVPOP/mrfctrl.log* to find out the reason for failure. The failure reason can be *mrfctrlmngt* port or *SipSPApi-Port* allocation failure. • Verify the UDP ports used in the configuration files. Verify the */etc/services*.

Table 130. Critical Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
178	MRFP registration failed or missing from host: X, IP-Y where X is the instance number of MRFP where Y is the control IP address of MRFP	Alarm cleared	Critical	MRFP	This alarm is generated when the MRFP host is removed. This alarm is cleared when the MRFP host is added. Possible causes: • MRFP host is removed. • Host is unregistered. Recommended actions: • Verify the configuration at */opt/AVPOP/cfg/modules* file. Verify the capabilities table with *mngttool* (`mngttool mrfctrl`).
187	Exceeded critical threshold level for X X: resource usage	Alarm cleared for X X: resource usage	Critical	MRFP	This alarm is used for priority call management. This alarm is raised if the resource usage exceeds above the critical threshold value for CPU usage, memory usage, media interface bandwidth usage, media interface packet loss, disk usage, actual DSP usage, and modeled DSP usage. This alarm is cleared when resource usage falls below or equal to the critical threshold value (hysteresis is applicable). Recommended actions: • **CPU usage.** Check the CP cores and call rate. Reduce the call rate if it exceeds the call limit. • **Memory usage.** Check the process utilization and reduce it. • **Bandwidth usage and packet loss.** Check the load on the media interface and reduce the call rate if exceeds the call limit. • **Modeled and actual DSP.** Monitor the usage of DSP cores and increase the DSP cores. • **Disk usage.** Check the disk usage of the particular partition and clean the partition.
202	Certificates are Renewed: X X: subsystem (SipOverTls, AnnouncementRecording, VXML, DTLS, LDAP, SAML, AnnLab, HTTPS, Prometheus, and AnnLabClnt)	Alarm Cleared: X X: subsystem (SipOverTls, AnnouncementRecording, VXML, DTLS, LDAP, SAML, AnnLab, HTTPS, Prometheus, and AnnLabClnt)	Critical	OAMP	This alarm is generated when the certificates are renewed by the cert-manager. This alarm is cleared when renewed certificates are loaded. Recommended actions: Refer to *Containerized Decomposed Media Server Installation Guide*.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
Major Alarms					
3	Configuration file was corrupt or not present	Valid configuration file found	Major	MRFC	The configuration file was not found, or was found to be corrupted on startup. This alarm is not deactivated until the next reboot. Recommended actions: • Reconfigure. • If this does not resolve the condition, contact TAC.
5	Failed mounting an external file server X	Mount failure alarm is cleared for external file server: X	Major	MRFP	The Containerized Decomposed Media Server was unable to mount the specified external NFS server. This alarm is not cleared until the next reboot. Possible causes: • External NFS server is unreachable. • Permissions on NFS directory are not correct. • The path to the mount point is not correct. • NFS server IP address or hostname is incorrect. • NFS mount point configuration was successfully changed during runtime, but the mount subsequently failed. Recommended actions: • Check connectivity to the external NFS server. • Check file permissions on the NFS server. • Check NFS configuration settings. • If the Containerized Decomposed Media Server failed to mount the mount point, reset the Containerized Decomposed Media Server.
16	Cause of the last reboot is unknown on slot X	Alarm cleared on slot X	Major	MRFC or MRFP	The Containerized Decomposed Media Server has reset and cannot establish the reason. The Containerized Decomposed Media Server clears this alarm after a brief interval. Recommended actions: • Check the alarms leading up to the reboot. • Check the system logs for the period before this alarm, to determine the chain of events leading to this situation.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
17	Cause of the last reboot was a watchdog timeout on slot X	Alarm cleared on slot X	Major	MRFC or MRFP	The Containerized Decomposed Media Server reboot due to a watchdog timeout. This alarm is auto cleared. Recommended actions: The reboot clears the diagnostic information for this event. Prepare for another occurrence as follows: • To provide a history that leads up to this failure condition, enable system logging. • To capture the final system messages at the time of failure, enable console logging. • If core files are being lost on reboot, disable reboot on fatal error. Collect any log packages that are generated and submit them to TAC.
18	Reboot due to exception for process: xxx	Alarm cleared on slot X	Major	MRFC or MRFP	The Containerized Decomposed Media Server reboots due to an exception. The related process name and the exception name are given as part of the alarm text. This alarm is auto cleared. Recommended actions: The reboot clears the diagnostic information for this event. Prepare for another occurrence as follows: • To provide a history that leads up to this failure condition, enable system logging. • To capture the final system messages at the time of failure, enable console logging. • If core files are being lost on reboot, disable reboot on fatal error. Collect any log packages that are generated and submit them to TAC.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
34	Error saving audio segment configuration to disk	Audio segment configuration status restored	Major	MRFC	A failure occurred while writing the audio segment configuration file to RAM or to disk. This alarm is not cleared until the next reboot. Possible causes: • The audio segment configuration file is not a valid XML file. • The audio segment file contains parse errors. • The Flash disk is full or corrupted. • The file name is configured through the configuration restore, but the file is not present in the system. Recommended actions: • Use an XML utility (such as XMLSpy) to check your audio segment configuration file against the XML schema for audio segment configuration. The schema is available from the Radisys Web site. • Retrieve the audio segment errors file and check it for parse errors. • Check the capacity of the Flash disk. If the disk is full, delete unnecessary files. • If the disk is still full or corrupted, contact TAC.
41	The upgrade operation has failed. Current firmware version: X.Y.Z.	Alarm cleared	Major	MRFC	The upgrade utility has failed to upgrade Data Base. This alarm is automatically cleared. Possible cause: The upgrade utility is an internal component that performs any data conversions necessary to ensure that the structure of configuration data is consistent with the software. An occurrence of this alarm means that the upgrade utility encountered problems trying to convert data, and the configuration database may not be as expected. The specification configuration problem depends on the versions of the configuration database and the software respectively. Recommended action: • Currently, the upgrade utility is used to restore the configuration. Check NFS mount point configuration. If necessary, restore the configuration.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
43	HTTP cache overflow on slot X	Alarm cleared on slot X	Major	MRFP	The capacity of the HTTP media cache has been exceeded. This alarm is cleared after five minutes without a cache overflow condition. Possible cause: • The cache is too small for the size and number of clips being cached. Recommended actions: • Reduce the number of clips being cached. • Only cache clips that are used frequently. • Only cache smaller clips. (The Containerized Decomposed Media Server determines which clips can be cached based on the HTTP header.)
44	Resource usage exceeded call overload threshold on slot X	Resource usage below call overload threshold for the past minute on slot X	Major	MRFP	The Containerized Decomposed Media Server is in a call overload situation. This alarm indicates that the Containerized Decomposed Media Server executes the protocol-appropriate behavior for this condition. For most protocols, this means rejecting new calls while this alarm is active. This alarm is cleared when resource levels drop below threshold for at least 1 minute. Possible cause: The Containerized Decomposed Media Server has exceeded either a CPU or a memory usage threshold. This is caused either by the number or the type of calls being processed. Recommended actions: • Optimize applications to maximize Containerized Decomposed Media Server capacity. (See *Radisys Special Interfaces Reference* for guidelines.) • Increase capacity of the Containerized Decomposed Media Server by adding more hardware. • If using either NFS or HTTP announcements, change to using internal announcements, as this typically provides higher capacity. • Use a control agent that implements load balancing and can redirect failed calls to another Containerized Decomposed Media Server. • Use a control agent that implements an algorithm for reducing the load on an Containerized Decomposed Media Server when it reaches an overload condition.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
46	RAM disk drive usage exceeded threshold on slot X	RAM disk usage below threshold for the past minute on slot X	Major	MRFP	The alarm is generated when RAM disk usage has exceeded the threshold level. This alarm is cleared when the RAM disk usage drops below the threshold level for at least a minute. Possible cause: Transient recordings have filled up the disk. Recommended action: Clear the unwanted files off the disk.
48	The last reboot was caused by overload protection on slot X	Alarm cleared on slot X	Major	MRFP	The Containerized Decomposed Media Server in this slot has rebooted due to overload protection. The Containerized Decomposed Media Server clears this alarm after a brief interval. Possible cause: Refer to the causes for service overload condition. Recommended action: • Reduce the possibility that the Containerized Decomposed Media Server reaches a service overload condition.
49	Failed to get health check response from external file server: X	Health check alarm cleared for external file server: X	Major	MRFP	The NFS server X failed the health check and is currently unavailable. This alarm is cleared when the NFS server becomes available again. Possible cause: • External NFS server is unreachable. Recommended action: Check connectivity to the external NFS server.
64	HTTP server timeout. <*Server name*> <*timeout period in ms*>	Alarm is cleared on slot X	Major	MRFP	An HTTP timeout occurred when accessing an external HTTP server to play/record media. The Containerized Decomposed Media Server clears this alarm after a brief interval. Recommended actions: • Verify that the HTTP server exists and is reachable at this location. If it is, consider enabling HTTP caching for media. • Check network connections.
88	Automatic switchover: <*switchover detail*> where *switchover detail indicates* MRFP is now standby	Alarm cleared	Major	MRFP	This alarm is generated in the Containerized Decomposed Media Server initiated switchover and the formerly active MRFP in the redundancy group is now a standby. This alarm is generated only for MRFPs that belong to an MRFP redundancy group. This alarm is automatically cleared after a brief interval. Recommended action: None

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
89	Failed to connect to ASR server X	Alarm cleared for ASR server X	Major	MRFP	A connection failure has occurred while communicating with an enabled ASR server. This alarm is cleared if the Containerized Decomposed Media Server is shut down, the ASR server is disabled through configuration, or a response to the Containerized Decomposed Media Server heartbeat request is received from the disconnected ASR server. Recommended action: • Verify that the server is operating normally, that the server has been configured properly, and that the network communication can be established between the Containerized Decomposed Media Server and the ASR server.
91	Failed to connect to TTS server X	Alarm cleared for TTS server X	Major	MRFP	A connection failure has occurred while communicating with an enabled TTS server. This alarm is cleared if the Containerized Decomposed Media Server is shut down, the TTS server is disabled through configuration, or a response to the Containerized Decomposed Media Server heartbeat request is received from the disconnected TTS server. • Verify that the server is operating normally, that the server has been configured properly, and that the network communication can be established between the Containerized Decomposed Media Server and the TTS server.
100	AEC provisioning exceeds maximum capacity on slot X	Alarm cleared on slot X	Major	MRFP	The number of resources provisioned for AEC exceed the maximum capacity of the instance. This alarm is raised when the number of resources specified for monitoring or canceling acoustic echo is too high. This alarm is cleared when resource provisioning for AEC is reduced to a level at or below the capacity of the card. Recommended action: • Reduce the provisioned resources for AEC.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
103	MS allocated cores exceeds capacity	Alarm cleared	Major	MRFP	The Containerized Decomposed Media Server has detected that the number of CPU cores allocated to the Containerized Decomposed Media Server is higher than the number of cores detected on the system. This alarm is cleared on reboot if the number of allocated cores does not exceed the number of detected cores. Recommended actions: • Check that the number of cores allocated to the Containerized Decomposed Media Server do not exceed the cores on the platform. • Check that the first core allocated to the Containerized Decomposed Media Server plus the number of cores allocated to the Containerized Decomposed Media Server do not exceed the cores on the platform. • Check that the number of VoiceXML cores plus DSP cores is at least two less than the number of cores allocated for MRFP. • Check that the number of cores detected by the Containerized Decomposed Media Server is the expected number of cores in the system for MRFP.
106	DSP resource alarm: <*variable text*> where <*variable text*> specifies the actual resource that has trigger the alarm	Alarm cleared on slot X	Major	MRFP	The Containerized Decomposed Media Server has detected that the configured threshold for DSP modeled resource usage has been exceeded. This alarm is cleared when DSP modeled resource usage drops below the configured threshold by at least the configured value of the hysteresis. Recommended actions: • Optimize applications to maximize Containerized Decomposed Media Server capacity. • Increase capacity of the Containerized Decomposed Media Server by upgrading hardware. • Reduce the load on the Containerized Decomposed Media Server.
109	Duplicate IPv6 address on port N <*IPv6 address*>	Alarm cleared on slot X	Major	MRFC or MRFP	The IP Version 6 address is a duplicate of that set on another interface or another instance. The Containerized Decomposed Media Server clears this condition when the Containerized Decomposed Media Server boots up with no duplicated IPv6 addresses. Recommended action: • Check the IP addresses settings in the network settings and ensure that they are correct.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
111	MPC booted with mismatch firmware on slot X	Alarm cleared on slot X	Major	MRFC	An MRFP has booted up with a firmware version different from the OAMP pod firmware version. This alarm is cleared when the MRFP boots up with a firmware version that matches the OAMP pod firmware version. Recommended action: • Verify that the firmware versions match. If the versions match, reboot the MRFP; if not, upgrade the system.
151	Failed to add route(s) on slot S	Alarm cleared on Slot S	Major	MRFC or MRFP	Failed to add the route configured in the OAMP during the Containerized Decomposed Media Server start-up. This alarm is cleared when the network routes are modified and the Containerized Decomposed Media Server is rebooted on which this alarm is raised. Recommended actions: • Reconfigure network routes • Check the connectivity with the route gateway

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
152	Resource Server offline: X where X is FQDN of the Resource Server. ***NOTE:*** If the alarm is already raised for FQDN X and FQDN is changed from X to Y, the existing alarm for FQDN X is cleared and a new alarm is raised for FQDN Y, even if the resource server is still offline.	Resource Server offline alarm cleared: X where X is FQDN of the Resource Server. ***NOTE:*** If the alarm is already raised for FQDN X: • Change the FQDN from X to Y, then in case of clear alarm for this Resource Server, clear trigger description will have the new FQDN Y. • Change the FQDN from X to "", then in case of clear alarm for this Resource Server, clear trigger description will have default behavior of clear alarm (may have slot information or "")	Major	MRFP	The alarm is generated when: • Load balancing is disabled and the health status of both primary and secondary instances of a resource server is dead for valid FQDN. • Load balancing is enabled and the health status of all four instances (primary, secondary, third, and fourth) of a resource server are dead for valid FQDN. This alarm is cleared when: • Load balancing is disabled and either of the primary or secondary instance of the valid RS is alive. That is, RS status is online. • Load balancing is enabled and if any of the four instances (primary, secondary, third, or fourth) of the valid RS is alive. That is, RS status is online. • RS FQDN is set to "". Recommended action: Check the Resource Server on the remote side.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
153	Minimum hardware configuration has not met. Reason:	Alarm cleared	Major	MRFP	The platform hardware configuration does not meet the minimum requirements. This alarm is cleared when the platform's hardware configuration meets the minimum recommended requirements and after a reboot. Possible cause: • The platform's hardware configuration does not meet the minimum recommended requirements. • If any of the partition except `/home` does not meet 95% of the minimum size criteria or if the total disk space is less than 30 GB. • If the available space of each partition except `/boot` and `/home` is less than 90% of the recommended space. Recommended actions: Check whether the following hardware configurations are met with the minimum requirements for the Containerized Decomposed Media Server. • CPU type • Number of cores • Processor speed • RAM • Hard drive size • Cache size • Disk partition table • CPU frequency • Ethernet interface type
155	License expired	Alarm cleared	Major	MRFC	The alarm is generated when the license expires. This alarm is cleared when the new license file is installed with more time limit. Recommended actions: • Check the license expiry date • Install new license file with more validity

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
157	Port limit hit for Y feature	Alarm cleared for Y feature	Major	MRFC	The alarm is generated when the current port usage hits the specified limit for Y feature. Y is one of the feature defined in the license file which license is obtained. ***NOTE:*** When bundle license is configured, the available bundle license for a given codec-A can reduce when a port with a different codec-B consumes the bundle license. As a result, this alarm for codec-A can be raised even though ports are not being created for codec-A. This alarm is cleared when the any one of the following condition is met. • Port usage reaches below 20 percent of the block limit for Y feature. • When new license file is installed with more limit or unlimited ports for Y feature Recommended actions: • Check license port limit for Y feature • Install license File with more port limits
158	RTP Packet loss alarm: <*variable text*> where variable text is RTP packet loss rate	Alarm cleared on Slot X	Major	MRFP	This alarm is generated when the RTP packet loss exceeds the configured RTP Packet loss threshold. This alarm is auto cleared. Recommended actions: • Check the network bandwidth or packet loss. • Increase capacity of the Containerized Decomposed Media Server by upgrading hardware. • Reduce the load on the Containerized Decomposed Media Server.
170	Scheduled backup operation failed on slot X	Alarm cleared on Slot X	Major	MRFC	This alarm is generated when a scheduled backup operation has failed. This alarm is cleared on the next successful scheduled backup. Possible causes: • Remote FTP server is not reachable due to a network issue or internal error. • Remote FTP server details are not configured properly. • The user authentication has failed or there is no write permission on the FTP server. Recommended actions: • Check that the remote FTP server address and user credentials are configured properly in the Containerized Decomposed Media Server. • Verify that the remote FTP server is running and the server is reachable from the Containerized Decomposed Media Server.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
172	Annlab remote server sync failed on host: X where X is hostname of the MRFC instance	Alarm cleared on host X	Major	OAMP	This alarm is generated when the AnnLab remote server fails to synchronize with the local server. This alarm is not cleared automatically. To clear this alarm, execute the `ClearAnnlabAlarm` script in the path */opt/swms/bin/* as follows: `ClearAnnlabAlarm.sh <alarmId to clear> <instance id>` where • <alarmId to clear> indicates the alarm ID to be cleared. • <instance id> indicates the Decomposed Media Server instance, which can be all or instance number. Possible causes: • **localServerToBeSync** is missing. Recommended actions: • Verify the log file in */var/log/AVPOP/annlabserver.log.* • Verify whether the **localServerToBeSync** parameter is present at */opt/swms/cfg/modules/annlabservercfg.properties.* • Check the */opt/swms/exec/synchroCluster* script to verify what commands were executed.
173	Failed to synchronize AnnLab client on host: X where X is hostname of the MRFP instance	Alarm cleared on host X	Major	MRFC	This alarm is generated when the Decomposed Media Server tries to synchronize with an AnnLab client or host is unreachable. This alarm is not cleared automatically. To clear this alarm, execute the `ClearAnnlabAlarm` script in the path */opt/swms/bin/* as follows: `ClearAnnlabAlarm.sh <alarmId to clear> <instance id>` where • <alarmId to clear> indicates the alarm ID to be cleared. • <instance id> indicates the Decomposed Media Server instance, which can be all or instance number. Possible cause: Error is observed when the Decomposed Media Server tries to synchronize with an AnnLab client or host Recommended action: Verify the log file at */var/log/swms/annlabclient.log*.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
179	A configured template type value on slot X is either not found or is syntactically invalid	Alarm cleared on Slot X	Major	MRFC	This alarm is generated when one or more values configured in the **Template Type** field of the CPV layout template table are invalid or not configured. This alarm is cleared when all the values configured in the CPV layout template table are valid after reboot. Possible causes: • One or more pre-defined template names configured are unsupported. • One or more referred SMIL files are not provisioned in the Containerized Decomposed Media Server. • One or more referred SMIL files are syntactically invalid. Recommended action: • Ensure that all the values configured in the CPV layout template table are valid.
186	Disk max usage exceeded threshold on partition	Alarm cleared on Slot X	Major	MRFC and MRFP	This alarm is generated when the maximum disk usage exceeds the threshold value on the following partitions. /root/, /boot/, /weboam/, /home/, /opt/, /space/, /usr/, /var/, /mnt/ramdisk/, /mnt/, /dev/shm/, /tmp/, /var/log/, /var/log/audit/, and /var/opt/swms/clips/ This alarm is cleared when the disk usage value is 5% less than the configured threshold value. ***NOTE:*** • If threshold value is set to 0, the existing alarms are cleared and no new alarms are raised. • If threshold value is set from 1 to 4, the existing alarms are cleared, if the threshold value reaches 0. Recommended action: Check the disk usage of the particular partition and clean the partition.

Table 131. Major Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
188	Exceeded major threshold level for X X: resource usage	Alarm cleared for X X: resource usage	Major	MRFP	This alarm is used for priority call management. This alarm is raised if the resource usage exceeds above the major threshold value for CPU usage, memory usage, media interface bandwidth usage, media interface packet loss, disk usage, actual DSP usage, and modeled DSP usage. This alarm is cleared when resource usage falls below or equal to the major threshold value. (hysteresis is applicable). Recommended action: • **CPU usage.** Check the CP cores and call rate. Reduce the call rate if it exceeds the call limit. • **Memory usage.** Check the process utilization and reduce it. • **Bandwidth usage and packet loss.** Check the load on the media interface and reduce the call rate if exceeds the call limit. • **Modeled and actual DSP.** Monitor the usage of DSP cores and increase the DSP cores. • **Disk usage.** Check the disk usage of the particular partition and clean the partition.
192	No connection with LDAP server X X: IP or hostname	Alarm cleared for X	Major	MRFC	This alarm is generated when a connection failure has occurred in communicating with the LDAP server. This alarm is automatically cleared when LDAP server is reachable. Possible causes: • LDAP IP or host is unreachable. • The configured IP address is incorrect. • The configured port number is incorrect. Recommended actions: • Verify that the LDAP server information is correctly configured on the Containerized Decomposed Media Server. • Check that DNS is working. • Check the connectivity between the LDAP server and the Containerized Decomposed Media Server. • Check whether LDAP server is listening to the configured port number.
193	DRI library initialization failed for languages: X where X is the name of the failed DRI languages. For example, en_US, en_IND, and so on.	Alarm cleared for instance X	Major	MRFP	This alarm is generated when MRFP fails to load at least one of the DRI library languages. This alarm is cleared after loading the DRI language library successfully on the next MRFP reboot. Possible cause: • When the configured DRI library loading fails. • The Containerized Decomposed Media Server fails the variable announcement calls for the failed DRI library language. Recommended action: Reboot the impacted MRFPs.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
Minor Alarms					
14	No connection with NTP server X	Connection re-established with NTP server X	Minor	MRFC	The Containerized Decomposed Media Server is unable to establish a connection with an NTP server, or the connection has failed. This alarm is cleared when the connection is re-established. Possible causes: • The IP address for the NTP server is incorrect, or the hostname cannot be resolved. • The NTP server has lost connectivity to the network. Recommended actions: • Check NTP configuration for the Containerized Decomposed Media Server. • Ensure that DNS is working correctly on your network. • Check the connectivity between the Containerized Decomposed Media Server and the NTP server.
15	No connection with DNS	Connection re-established with DNS	Minor	MRFC or MRFP	The Containerized Decomposed Media Server is unable to establish a connection with the DNS server, or the connection has failed. This alarm is cleared when the connection is re-established. Possible causes: • The IP address for the DNS server is incorrect, or the hostname cannot be resolved. • The DNS server has lost connectivity to the network. Recommended actions: • Check the DNS configuration for the Containerized Decomposed Media Server. • Check the connectivity between the DNS server and the Containerized Decomposed Media Server. • Check the DNS servers specified. • Check the hostname configured.
19	Last reboot was user-initiated on slot X	Alarm cleared on slot X	Minor	MRFP	An operator has initiated a restart of the Containerized Decomposed Media Server. The Containerized Decomposed Media Server clears this alarm after a brief interval. Recommended action is none.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
60	Log package exists in the system on slot X	No log package exists in the flash on slot X	Minor	MRFC	There are one or more log packages in the flash. Possible cause: Log package(s) are generated as a result of a system crash and/or user request. Recommended action: Transfer the log package(s) using either FTP or Web and the log package(s) will be deleted automatically after the transfer. This will prevent newly generated log package files from overwriting existing ones.
63	ICMP error: <*variable text*> where <*variable text*> is address:port:destination unreachable /packet too big	Alarm cleared on slot X	Minor	MRFP	An ICMP/ICMPv6 Destination Unreachable message or an ICMPv6 Packet Too Big error is detected. The Containerized Decomposed Media Server has sent RTP packets to an unreachable address and port a.b.c.d:pppp (IPv4) a.b.c.d.e.f.g.h:pppp (IPv6) or received an ICMP Packet Too Big error message. The Containerized Decomposed Media Server clears this alarm after a brief interval. Recommended actions: • Verify that IP addresses are valid. • Check configuration of video MTU for Packet Too Big error messages. • Check network connections.
65	Dropped audio stream due to: XXX where XXX is either no media	Alarm cleared on slot X	Minor	MRFP	The streaming engine dropped an audio stream due to no media during a play buffer overrun during a record. The Containerized Decomposed Media Server clears this alarm after a brief interval. Possible causes: The streaming engine drops an audio stream due to one of the following: • No media during a play • Buffer overrun during a record Recommended action: • If HTTP is being used, consider enabling caching. • If NFS is being used, consider using faster servers.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
70	Network interface below 100BASE-T full duplex: *device name*	Network interface restored to at least 100BASE-T full duplex	Minor	MRFC or MRFP	This alarm is generated when Network interface 1 is Ethernet interface running below 100BASE-T full duplex. This alarm is cleared if the link becomes 100 full duplex or the interface is not configured for use. This alarm is not activated for bonded interfaces. Recommended actions: • Check that the network switch is capable of operating at least 100BASE-T full duplex. • Check that the network switch and the Containerized Decomposed Media Server have consistent link configurations. • Check that the network cable is in good working condition and is securely connected at each end.
71	Network interface below 100BASE-T full duplex: *device name*	Network interface restored to at least 100BASE-T full duplex	Minor	MRFC or MRFP	This alarm is generated when Network interface 2 is Ethernet interface running below 100BASE-T full duplex. This alarm is cleared if the link becomes 100 full duplex or the interface is not configured for use. This alarm is not activated for bonded interfaces. Recommended actions: • Check that the network switch is capable of operating at least 100BASE-T full duplex. • Check that the network switch and the Containerized Decomposed Media Server have consistent link configurations. • Check that the network cable is in good working condition and is securely connected at each end.
72	Network interface below 100BASE-T full duplex: *device name*	Network interface restored to at least 100BASE-T full duplex	Minor	MRFC or MRFP	This alarm is generated when Network interface 3 is Ethernet interface running below 100BASE-T full duplex. This alarm is cleared if the link becomes 100 full duplex or the interface is not configured for use. This alarm is not activated for bonded interfaces. Recommended actions: • Check that the network switch is capable of operating at least 100BASE-T full duplex. • Check that the network switch and the Containerized Decomposed Media Server have consistent link configurations. • Check that the network cable is in good working condition and is securely connected at each end.
76	Clip partition disk usage threshold exceeded	Alarm cleared	Minor	MRFP	The disk space used in the partition allocated to transient clips has exceeded the configured threshold for over a minute. This alarm is cleared when disk space used for transient clips drops below the threshold. Recommended action: • Delete unnecessary files from the partition allocated to transient files.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
86	User-initiated switchover: <switchover details> where <switchover details> indicates MRFP X is now standby	Alarm cleared	Minor	MRFP	This alarm is generated in a user initiated switchover and the formerly active MRFP in the redundancy group is now a standby. This alarm is generated only for MRFPs that belong to an MRFP redundancy group. This alarm is automatically cleared after a brief interval. Recommended action: None.
97	Software timeout detected on slot X	Alarm cleared on slot X	Minor	MRFP	A soft watchdog timeout (SWT) has been detected on one of the MRFPs. The Containerized Decomposed Media Server clears this alarm after a brief interval. Recommended action: • Terminate all connections on the MRFP, take the MRFP out of service, and contact TAC.
107	SIP response code alarm: <*variable text* > where variable text is specified to contain the actual response code that triggered the alarm and the SIP call agent	Alarm cleared on slot X	Minor	MRFC or MRFP	This alarm is generated when the Containerized Decomposed Media Server SIP interface receives the SIP response code 400 (Bad Request) or 408 (Request Timeout). The Containerized Decomposed Media Server clears this condition after a brief interval. Recommended action: • This is an informational alarm that highlights the occurrence of specific protocol response codes. The recommended action is dependent on the actual response code and the circumstance under which it occurred.
108	MSML response code alarm: <*variable text* > where variable text is specified to contain the actual response code that triggered the alarm and the requester identification	Alarm cleared on slot X	Minor	MRFP	The Containerized Decomposed Media Server MSML interface has sent MSML response code 400, Bad Request, 401 Unknown Element, 402, Unsupported Element, 406, Unknown Attribute, or 407, Unsupported Attribute. The Containerized Decomposed Media Server clears this condition after a brief interval. Recommended action: • This is an informational alarm that highlights the occurrence of specific protocol response codes. The recommended action is dependent on the actual response code and the circumstance under which it occurred.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
148	Network Interface 4 Below 100BT Full Duplex: <*device name*>	Network interface is restored to at least 100BASE-T full duplex	Minor	MRFP	The Containerized Decomposed Media Server detects that the network interface 4 is an Ethernet interface running below 100BASE-T full duplex. This alarm is cleared when the link goes down, the link status becomes 100BASE-T full duplex or the interface is not configured for use. This alarm is not activated for bonded interfaces. Recommended actions: • Check whether the network switch is capable of operating at least 100BASE-T full duplex. • Check whether the network switch and Containerized Decomposed Media Server have consistent link configurations. • Check whether the network cable is in good working condition and is securely connected at each end.
154	License will expire in X days	Alarm cleared	Minor	MRFC	The alarm is generated starting from X days at 12 am until the license expires. X is the license warning threshold configurable in OAMP (from 0 to 30 days). The alarm is cleared before and the same alarm is raised at the beginning of next day.The last instance of this alarm (license will expire in 1 day), is generated before the *License expired* alarm is raised. This alarm is cleared when: • The license validity of the instance is expired • Valid license file is installed and license validity is valid • New warning alarm is going to be raised with new X number of days Recommended actions: • Check license expiry date • Install valid license file with enough TimeLimit

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
156	Port limit warning for Y feature	Alarm cleared for Y features	Minor	MRFC	The alarm is generated when the current port usage of Y feature is increased to warning threshold limit for the corresponding feature in the license file. Y is one of the feature defined in the license file which license is obtained. ***NOTE:*** When bundle license is configured, the available bundle license for a given codec-A can reduce when a port with a different codec-B consumes the bundle license. As a result, this alarm for codec-A can be raised even though ports are not being created for codec-A. The alarm is cleared when any one of the following conditions are met. • The current port usage is below 20 percent of the warning threshold limit for Y feature. • The current port usage reaches Block-Limit for Y feature and "Port limit hit for Y feature" alarm is raised. • When new license is installed with more limit or unlimited ports for Y feature. Recommended actions: • Check license port limit for Y feature • Install license file with more port limits before blocking limit is reached
159	Auto transfer of management activity log failed to host: <variable text> where variable text is remote IP or host name	Alarm cleared on host X where X is remote host IP	Minor	MRFC	This alarm is generated when automatic transfer of management activity log to the configured remote host fails. This alarm is cleared when • The remote host is reachable and auto transfer is attempted. • Auto transfer is disabled. Recommended actions: • Verify the remote host is configured and make it reachable. • Configure the remote host which is reachable.
171	AnnLab client is disconnected on host: X. where X is hostname of the Containerized Decomposed Media Server instance	Alarm cleared	Minor	MRFC	This alarm is generated when the AnnLab client is disconnected. This alarm is cleared when the AnnLab client is connected. Possible cause: `PingHost` requests are not sent from the AnnLab client to the AnnLab server. Recommended action: On the AnnLab client Containerized Decomposed Media Server, verify whether the `PingHost` request log is present in the AnnLab server at */var/log/AVPOP/annlabserver.log*.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
189	Exceeded minor threshold level for X X: resource usage	Alarm cleared for X X: resource usage	Minor	MRFP	This alarm is used for priority call management. This alarm is raised if the resource usage exceeds above the minor threshold value for CPU usage, memory usage, media interface bandwidth usage, media interface packet loss, disk usage, actual DSP usage, and modeled DSP usage. This alarm is cleared when resource usage falls below or equal to the minor threshold value. (hysteresis is applicable). Recommended action: • **CPU usage.** Check the CP cores and call rate. Reduce the call rate if it exceeds the call limit. • **Memory usage.** Check the process utilization and reduce it. • **Bandwidth usage and packet loss.** Check the load on the media interface and reduce the call rate if exceeds the call limit. • **Modeled and actual DSP.** Monitor the usage of DSP cores and increase the DSP cores. • **Disk usage.** Check the disk usage of the particular partition and clean the partition.

190	Test Alarm Triggered	Test Alarm Cleared	Minor	MRFC	This alarm is generated to test the integration at the Operations Support Systems (OSS) without any service impact.
					This alarm is generated by executing the following CLI command at */opt/swms/bin*.
					`./testAlarm.sh -r`
					This alarm is cleared by executing the following command at */opt/swms/bin*.
					`./testAlarm.sh -c`
					Execute the following command at */opt/swms/bin* to retrieve the alarm status.
					`./testAlarm.sh -g`
					Execute the following command at */opt/swms/bin* to view the help options.
					`./testAlarm.sh -h`
					Recommended action:
					Clear the alarm manually by executing the following command at */opt/swms/bin*.
					`./testAlarm.sh -c`

196	NFS server is slow: <variable text> Where <variable text> is NFS Server IP	NFS server slow alarm is cleared: <variable text> Where <variable text> is NFS Server IP	Minor	MRFC	This alarm is generated when the NFS operations are failed due to the slow NFS Server. This alarm is auto-cleared. Recommended action is none.

Table 132. Minor Alarms

Alarm ID	Active Trigger Description	Clear Trigger Description	Severity	Event Source	Description and Recommended Action
200	Scaling operation started on Instance: MRFPX Y. where X is the instance number where Y is the Auto ScaleIn/ScaleOut Manual ScaleIn/ScaleOut	Scaling operation finished on Instance: MRFPX where X is the instance number	Minor	MRFP	This alarm is generated when any MRFP instance is scaled-in or scaled-out. The scale-in and scale-out operation can be either auto or manual. This alarm is automatically cleared. Possible Cause: When the MRFP instance is scaled-in or scaled-out. Recommended action is none.
201	AnnLab transcoding failure alarm for: Clipname-X, Hostname-Y where, X is the clip name and Y is the Hostname	AnnLab transcoding failure alarm cleared for: Clipname-X, Hostname-Y where, X is the clip name and Y is the Hostname	Minor	MRFP	This alarm is generated when the AnnLab transcoding of a clip X is failed on host Y. This alarm is auto-cleared. Recommended action: Verify the uploaded clip is in the correct format. Possible cause: Uploaded clip transcoding fails due to, • file I/O operations failure. • mismatch between file header and file format. • file header corruption. • bitstream corruption. • interrupted exceptions. • file permissions failure. ***NOTE:*** • An alarm is raised only on the single MRPF, even if other MRFPs encounters transcoding failure issue. • Only one alarm is raised per uploaded file.

Kafka Alarm Formats

This appendix gives the information about Kafka alarm formats.

Table 133 provides the information about the JSON header and the description.

Table 133. JSON header for Kafka Broker

Rakuten Example	Containerized Decomposed Media Server Example	Description
"alarmCode":"EID_PROGRAM_MINOR_TERM"	Raise: "alarmCode":"170_Raise" Clear: "alarmCode":"170_Clear"	The Containerized Decomposed Media Server updates the common value for all the instances of the particular alarm . The raise and clear events of the fault have different values.
"alarmId":"131"	Raise: "alarmId":"17234567_Raise" Clear: "alarmId":"17234567_Clear"	The Containerized Decomposed Media Server updates the instance ID of the fault. The raise and clear events have different values.
"alarmName":"EID_PROGRAM_MINOR_TERM"	Raise: "alarmName":"Scheduled backup or auto transfer of Stats file failed on slot 1" Clear: "alarmName":"Alarm Cleared on Slot 1"	The Containerized Decomposed Media Server updates the alarm description as per the Web GUI or SNMP trap. The raise and clear events of the fault have different values.
"eventTime":"1599565125"	"eventTime":"1599565125"	The Containerized Decomposed Media Server updates the alarm event time in the Epoch time format.
“uhn”:”<podHostName>”	“uhn”:”cdmrf-oamp-0”	The Containerized Decomposed Media Server updates the OAMP POD hostname. ***NOTE:*** If the alarm is for the MRFP and MRFCtrl, the POD name is the same as the OAMP POD. The raise and clear events have the same value.
"managedObject":”2"	"managedObject":”XXXX-YYYY-ZZZZ"	The Containerized Decomposed Media Server labels `managedObject` defined in the Helm chart. The raise and clear events have the same value. ***NOTE:*** Applicable only for robin.io
"cnfc_uuid":"<CNFC_UUID>“	"cnfc_uuid":" XXXX-YYYY-ZZZZ“	The Containerized Decomposed Media Server labels `cnfc_uuid` defined in the Helm chart. The raise and clear events have the same value. ***NOTE:*** Applicable only for robin.io
"pod_uuid":"<POD_UUID>”	"pod_uuid":"42db696d-f553-42e6-8054-4016293002cc”	The Containerized Decomposed Media Server updates the POD UUID. The raise and clear events have the same value. ***NOTE:*** The POD UUID have the same value even after the POD restarts.

Table 133. JSON header for Kafka Broker

Rakuten Example	Containerized Decomposed Media Server Example	Description
"probableCause":"Minor program has been terminated."	"probableCause":"Remote FTP server is not reachable due to network issue or internal error. Remote FTP server details are not set properly. The user authentication failed or no write permission on FTP server."	The Containerized Decomposed Media Server updates the trigger condition for the alarm. The raise and clear events have the same value.
"severity":"Minor“	Raise: "severity":"Minor“ Clear: "severity":"Clear“	The Containerized Decomposed Media Server updates the alarm severity like Critical, Major, Minor, and Clear. The alarm raised has Critical, Major and Minor, whereas the clear alarm has Clear.
"equipmentSubId":"/nsID/test001/componentID“	"equipmentSubId":"OAMP“	Provides the information of subprocess or the application ID raising the alarm in the POD. The raise and clear events have the same value.
"productType":“mOne"	"productType":“CDMRF"	The Containerized Decomposed Media Server updates the product name as Containerized Decomposed Media Server. The raise and clear events have the same value.
"additionalText":"0"	"additionalText":"A scheduled backup operation has failed. "	The Containerized Decomposed Media Server updates the alarm additional text, corresponding to the additional information for that alarm. The raise and clear events have the same value.
"applicationId":"IMG"	"applicationId":"OAMP"	The Containerized Decomposed Media Server updates the microservice name. The raise and clear events have same value.
"correlationId":”717”	"correlationId":”1”	The Containerized Decomposed Media Server updates the correlation ID as the alarm identifier for raise and clear. The raise and clear events have the same value even after the POD restarts.

"eventType":"TYPE_PROCESSING_ERROR"	"eventType":communicationsAlarm"	The Containerized Decomposed Media Server updates the alarm 3GPP event type in the following string format.
		`unknown,`
		`communicationsAlarm`
		`environmentalAlarm,`
		`equipmentAlarm,`
		`processingErrorAlarm,`
		`qualityOfServiceAlarm, integrityViolation, operationalViolation, physicalViolation,`
		`securityViolation,`
		`timeDomainViolation`
		The raise and clear events have the same value.

"moduleName":"PM"	"moduleName":"FM"	The Containerized Decomposed Media Server updates as Fault Management (FM) module. The raise and clear events have the same value.

Table 133. JSON header for Kafka Broker

Rakuten Example	Containerized Decomposed Media Server Example	Description
"podId":"0-9.mavenir1.com,10.2.63.58",	“podId":"oamp-0"	The Containerized Decomposed Media Server updates the OAMP POD name. The raise and clear events have the same value.
"repairAction":"PM restarts the minor program automatically."	"repairAction":"Check the remote FTP server address and user credentials are set properly in MRF. Verify that the remote FTP service is running and the server is reachable from MRF."	The Containerized Decomposed Media Server updates the alarm recommended action for the specific alarm. The raise and clear events have the same value.
"specificProblem":"Minor program has been terminated (manually or due to internal reasons) system will try to restore it automatically.“	"specificProblem":"A scheduled backup operation has failed. “	The Containerized Decomposed Media Server updates the alarm with additional text corresponding to the additional information for the specific alarm. The raise and clear events have the same value.
"name":"CUSTOMEVENT"	"name":""	The Containerized Decomposed Media Server updates it as empty. The raise and clear events have the same value.
"namespace":"urn:mavenir:mavenir-custom-event"	"namespace":"default"	The Containerized Decomposed Media Server updates the namespace of the POD. The raise and clear events have the same value.

Example


```
{"header":{"alarmCode":"19_Raise","alarmId":"190000113_Raise","alarmName":"Last
reboot was user-initiated on Instance
1","eventTime":"1630990608267809","uhn":"cdmrf-oamp-
0","managedObject":"zac_61","cnfc_uuid":"zac_61","pod_uuid":"4dcef80e-9fed-
4da4-952a-96b0fa5fe3b0","probableCause":"Operator initiates a card
reset.","severity":"Minor","equipmentSubId":"OAMP"},"body":{"productType":"CDMR
F","additionalText":"An operator has initiated a restart of the card/instance in
this slot. The media server deactivates this alarm after a brief
interval.","applicationId":"OAMP","correlationId":"112","eventType":"processing
ErrorAlarm","moduleName":"FM","podId":"cdmrf-oamp-
0","repairAction":"None.","specificProblem":"An operator has initiated a
restart of the card/instance in this slot. The media server deactivates this
alarm after a brief interval.","name":"","namespace":"ns1"}}
```

```
{"header":{"alarmCode":"19_Clear","alarmId":"190000113_Clear","alarmName":"Alar
m cleared on Instance 1","eventTime":"1630990608569471","uhn":"cdmrf-oamp-
0","managedObject":"zac_61","cnfc_uuid":"zac_61","pod_uuid":"4dcef80e-9fed-
4da4-952a-96b0fa5fe3b0","probableCause":"Operator initiates a card
reset.","severity":"Clear","equipmentSubId":"OAMP"},"body":{"productType":"CDMR
F","additionalText":"An operator has initiated a restart of the card/instance in
this slot. The media server deactivates this alarm after a brief
interval.","applicationId":"OAMP","correlationId":"112","eventType":"processing
ErrorAlarm","moduleName":"FM","podId":"cdmrf-oamp-
0","repairAction":"None.","specificProblem":"An operator has initiated a
restart of the card/instance in this slot. The media server deactivates this
alarm after a brief interval.","name":"","namespace":"ns1"}}
```

NOTE: Verification is done from Kafka broker through the `kafka-console-consumer.sh` command.

```
kafka-console-consumer.sh --bootstrap-server localhost:9092 --topic topic --
property key.deserializer:
org.apache.kafka.common.serialization.StringDeserializer value-
deserializer:org.springframework.kafka.support.serialization.JsonDeserializer
```

Generic Alarm Template Formats

This appendix provides the information about the generic alarm template formats.

Table 134 provides the information about the variable elements and are case sensitive.

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
ALARM_SEQUENCE_ID	1	This defines the alarm sequence ID. It is an integer from 1 to 2147483647, and for every raise or clear event, the alarm sequence ID is incremented.
ALARM_EVENT_TYPE_ACTIVATE_DEACTIVATE	Activate	This defines the state of the alarm in string format. The supported values are: • Activate for raise alarm • Deactivate for clear alarm
ALARM_ID	190	This defines the alarm ID in integer format. More than one alarm is supported in Containerized Decomposed Media Server.
ALARM_INSTANCE_ID	190000	This defines the alarm instance ID. It is an integer from 1 to 2147483647. For the same alarm, the instance ID gets incremented, and both alarm raise and alarm clear have the same values.
ALARM_TEXT	Test Alarm Triggered	This defines the alarm text in string format. Both the raise and clear have different content.
ALARM_SEVERITY_STRING	Minor	This defines the alarm severity in string format. The supported values are Critical, Major, Minor, Cleared, and Indeterminate.
ALARM_SEVERITY_ENUM	2	This defines the alarm severity in integer format. The supported values are: • indeterminate • critical • major • minor • warning • cleared
ALARM_EVENT_TIME	2022-05-11 19:40:03 IST	This defines the alarm time stamp in %Y-%m-%d %T %Z format.
ALARM_EVENT_TIME_EPOC_FORMAT	1.63099E+15	This defines the alarm event time in EPOC format.
ALARM_SLOT_NUMBER	1	This defines the Containerized Decomposed Media Server instance number in integer format. The supported values are from 1 to 22.
ALARM_SYSTEM_DN	SLOT-SCC1	This defines the slot in system format. It is a string. The supported values are SLOT-SCC1, SLOT-SCC2, SLOT-MPC3...SLOT-MPC22.

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
ALARM_SPECIFIC_PROBLEM_ENUM	136101	This defines the alarm specific problem in enum value based on the alarm ID. It is an integer. The supported values are 136101 to 136202.
ALARM_ADDITIONAL_TEXT	This alarm is used for testing	This defines the alarm additional text in string format.
ALARM_PROBABLE_CAUSE_ENUM	0.	This defines probable cause for the alarm enum value based on alarm ID. The following values are defined in 3GPP. • indeterminate (0) • alarmIndicationSignal (1) • callSetupFailure (2) • degradedSignalM3100 (3) • farEndReceiverFailure (4) • framingErrorM3100 (5) • lossOfFrame (6) • lossOfPointer (7) • lossOfSignal (8) • payloadTypeMismatch (9) • transmissionError (10) • remoteAlarmInterface (11) • excessiveBitErrorRate (12) • pathTraceMismatch (13) • unavailable (14) • signalLabelMismatch (15) • lossOfMultiFrame (16) • communicationsReceiveFailure (17) • communicationsTransmitFailure (18) • modulationFailure (19) • demodulationFailure (20) • backPlaneFailure (51) • dataSetProblem (52) • equipmentIdentifierDuplication (53) • externalDeviceProblem (54) • lineCardProblem (55) • multiplexerProblemM3100 (56) • neIdentifierDuplication (57) • powerProblemM3100 (58) • processorProblemM3100 (59) • protectionPathFailure (60) • receiverFailureM3100 (61) • replaceableUnitMissing (62)

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
		• replaceableUnitTypeMismatch (63) • synchronisationSourceMismatch (64) • terminalProblem (65) • timingProblemM3100 (66) • transmitterFailureM3100 (67) • trunkCardProblem (68) • replaceableUnitProblem (69) • realTimeClockFailure(70) • protectionMechanismFailure (81) • protectionResourceFailure (82) • airCompressorFailure (101) • airConditioningFailure (102) • airDryerFailure (103) • batteryDischarging (104) • batteryFailure (105) • commericalPowerFailure (106) • coolingFanFailure (107) • engineFailure (108) • fireDetectorFailure (109) • fuseFailure (110) • generatorFailure (111) • lowBatteryThreshold (112) • pumpFailureM3100 (113) • rectifierFailure (114) • rectifierHighVoltage (115) • rectifierLowFVoltage (116) • ventilationSystemFailure (117) • enclosureDoorOpenM3100 (118) • explosiveGas (119) • fire (120) • flood (121) • highHumidity (122) • highTemperature (123) • highWind (124) • iceBuildUp (125) • intrusionDetection (126) • lowFuel (127) • lowHumidity (128) • lowCablePressure (129)

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
		• lowTemperature (130) • lowWater (131) • smoke (132) • toxicGas (133) • externalPointFailure (136) • storageCapacityProblemM3100 (151) • memoryMismatch (152) • corruptDataM3100 (153) • outOfCpuCycles (154) • softwareEnvironmentProblem (155) • softwareDownloadFailure (156) • lossOfRealTime (157) • reInitialized (158) • excessiveErrorRate (203) • adapterError (301) • applicationSubsystemFailure (302) • bandwidthReduction (303) • communicationProtocolError (305) • communicationSubsystemFailure (306) • configurationOrCustomizingError (307) • congestion (308) • cpuCyclesLimitExceeded (310) • dataSetOrModemError (311) • dtedceInterfaceError (313) • equipmentMalfunction (315) • excessiveVibration (316) • fileError (317) • heatingOrVentilationOrCoolingSystemProblem (321) • humidityUnacceptable (322) • inputOutputDeviceError (323) • inputdeviceError (324) • lanError (325) • leakDetection (326) • localNodeTransmissionError (327) • materialSupplyExhausted (330) • outOfMemory (332) • outputDeviceError (333) • performanceDegraded (334) • pressureUnacceptable (336)

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
		• queueSizeExceeded (339) • receiveFailure (340) • remoteNodeTransmissionError (342) • resourceAtOrNearingCapacity (343) • responseTimeExcessive (344) • retransmissionRateExcessive (345) • softwareError (346) • softwareProgramAbnormallyTerminated (347) • softwareProgramError (348) • temperatureUnacceptable (350) • thresholdCrossed (351) • toxicLeakDetected (353) • transmitFailure (354) • underlyingResourceUnavailable (356) • versionMismatch (357) • aBisToBtsInterfaceFailure (501) • aBisToTrxInterfaceFailure (502) • antennaProblem (503) • batteryBreakdown (504) • batteryChargingFault (505) • clockSynchronisationProblem (506) • combinerProblem (507) • diskProblem (508) • excessiveReceiverTemperature (510) • excessiveTransmitterOutputPower (511) • excessiveTransmitterTemperature (512) • frequencyHoppingDegraded (513) • frequencyHoppingFailure (514) • frequencyRedefinitionFailed (515) • lineInterfaceFailure (516) • linkFailure (517) • lossOfSynchronisation (518) • lostRedundancy (519) • mainsBreakdownWithBatteryBackup (520) • mainsBreakdownWithoutBatteryBackup (521) • powerSupplyFailure (522) • receiverAntennaFault (523) • receiverMulticouplerFailure (525) • reducedTransmitterOutputPower (526)

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
		• signalQualityEvaluationFault (527) • timeslotHardwareFailure (528) • transceiverProblem (529) • transcoderProblem (530) • transcoderOrRateAdapterProblem (531) • transmitterAntennaFailure (532) • transmitterAntennaNotAdjusted (533) • transmitterLowVoltageOrCurrent (535) • transmitterOffFrequency (536) • databaseInconsistency (537) • fileSystemCallUnsuccessful (538) • inputParameterOutOfRange (539) • invalidParameter (540) • invalidPointer (541) • messageNotExpected (542) • messageNotInitialised (543) • messageOutOfSequence (544) • systemCallUnsuccessful (545) • timeoutExpired (546) • variableOutOfRange (547) • watchDogTimerExpired (548) • coolingSystemFailure (549) • externalEquipmentFailure (550) • externalPowerSupplyFailure (551) • externalTransmissionDeviceFailure (552) • reducedAlarmReporting (561) • reducedEventReporting (562) • recucedLoggingCapability (563) • systemResourcesOverload (564) • broadcastChannelFailure (565) • callEstablishmentError (566) • invalidMessageReceived (567) • invalidMsuReceived (568) • lapdLinkProtocolFailure (569) • localAlarmIndication (570) • remoteAlarmIndication (571) • routingFailure (572) • ss7ProtocolFailure (573) • transmissionFailure (574)

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
ALARM_PROBABLE_CAUSE_ENUM	0	• authenticationFailure (701) • breachOfConfidentiality (702) • cableTamper (703) • delayedInformation (704) • denialOfService (705) • duplicateInformation (706) • informationMissing (707) • informationModificationDetected (708) • informationOutOfSequence (709) • keyExpired (711) • nonRepudiationFailure (712) • outOfHoursActivity (713) • outOfHoursService (714) • proceduralError (715) • unauthorizedAccessAttempt (716) • unexpectedInformation (717) • unspecifiedReason (718)
ALARM_EVENT_TYPE_ENUM	1	This defines the alarm event type in enum value based on alarm ID. The supported values are: • unknown (0) • communicationsAlarm (2) • environmentalAlarm (3) • equipmentAlarm (4) • processingErrorAlarm (10) • qualityOfServiceAlarm (11) • integrityViolation (5) • operationalViolation (8) • physicalViolation (9) • securityViolation (13) • timeDomainViolation (15)
ALARM_CORRELATION_ID	1	This defines the alarm correlation ID. Both raise and the clear has same ID and gets incremented for every next alarm. It is an integer ranging from 1 to 2147483647.
ALARM_TRIGGER_REASON	Execute the script `testAlarm.sh` in the Containerized Decomposed Media Server along with the argument -r.	This defines the alarm trigger condition for the alarm.

Table 134. Variable Elements for Generic Alarm Template Formats

Variables	Example	Comments
ALARM_CLEARING_MECHANISM	Go to the location where the script `testAlarm.sh` is present in the Containerized Decomposed Media Server and execute the script.	This defines the alarm clearing mechanism for the alarm.
POD_HOST_NAME	mrf-oamp-0.	This defines the pod hostname.
POD_UID	d640a845-9339-4d79-aa96-23587b44c6c5.	This defines the pod UID.
POD_NAMESPACE	OAMP.	This defines the pod namespace.
POD_CNFC_UUID	XXXX-YYYY-ZZZZ.	This defines the CNFC_UUID, configured by the user. ***NOTE:*** Applicable only for Robin platform.
POD_NAME	mrf-oamp-0.	This defines the name of the pod.

Example

In the *values.yaml* file,

alarmTemplate:

isEnabled: true

alarmRaiseTemplate: "{ \"alarmSequenceId\" : <ALARM_SEQUENCE_ID>, \"alarmEventType\" : \"<ALARM_EVENT_TYPE_ACTIVATE_DEACTIVATE>\", \"alarmId\": <ALARM_ID>, \"alarmInstanceId\" : <ALARM_INSTANCE_ID>, \"alarmText\" : \"<ALARM_TEXT>\", \"alarmSeverityString\" : \"<ALARM_SEVERITY_STRING>\", \"alarmSeverityEnum\" : <ALARM_SEVERITY_ENUM>, \"AlarmEventTime\" : \"<ALARM_EVENT_TIME>\", \"alarmEventTimeEpoch\" : <ALARM_EVENT_TIME_EPOC_FORMAT>, \"alarmSlotNum\" : <ALARM_SLOT_NUMBER>, \"alarmSystemDN\" : \"<ALARM_SYSTEM_DN>\", \"alarmSpecificProblemEnum\" : <ALARM_SPECIFIC_PROBLEM_ENUM>, \"alarmAdditionalText\" : \"<ALARM_ADDITIONAL_TEXT>\", \"alarmProbableCauseEnum\" : <ALARM_PROBABLE_CAUSE_ENUM>, \"alarmEventTypeEnum\" : <ALARM_EVENT_TYPE_ENUM>, \"alarmCorrelationId\" : <ALARM_CORRELATION_ID>, \"alarmTriggerReason\" : \"<ALARM_TRIGGER_REASON>\", \"alarmClearingMechanism\" : \"<ALARM_CLEARING_MECHANISM>\", \"podHostName\" : \"<POD_HOST_NAME>\", \"podUuid\" : \"<POD_UID>\", \"podNamespace\" : \"<POD_NAMESPACE>\", \"podName\" : \"<POD_NAME>\" }"

alarmClearTemplate: "{ \"alarmSequenceId\" : <ALARM_SEQUENCE_ID>, \"alarmEventType\" : \"<ALARM_EVENT_TYPE_ACTIVATE_DEACTIVATE>\", \"alarmId\": <ALARM_ID>, \"alarmInstanceId\" : <ALARM_INSTANCE_ID>, \"alarmText\" : \"<ALARM_TEXT>\", \"alarmSeverityString\" : \"<ALARM_SEVERITY_STRING>\", \"alarmSeverityEnum\" : <ALARM_SEVERITY_ENUM>, \"AlarmEventTime\" : \"<ALARM_EVENT_TIME>\", \"alarmEventTimeEpoch\" : <ALARM_EVENT_TIME_EPOC_FORMAT>, \"alarmSlotNum\" : <ALARM_SLOT_NUMBER>, \"alarmSystemDN\" : \"<ALARM_SYSTEM_DN>\", \"alarmSpecificProblemEnum\" : <ALARM_SPECIFIC_PROBLEM_ENUM>, \"alarmAdditionalText\" :

\"<ALARM_ADDITIONAL_TEXT>\", \"alarmProbableCauseEnum\" : <ALARM_PROBABLE_CAUSE_ENUM>, \"alarmEventTypeEnum\" : <ALARM_EVENT_TYPE_ENUM>, \"alarmCorrelationId\" : <ALARM_CORRELATION_ID>, \"alarmTriggerReason\" : \"<ALARM_TRIGGER_REASON>\", \"alarmClearingMechanism\" : \"<ALARM_CLEARING_MECHANISM>\", \"podHostName\" : \"<POD_HOST_NAME>\", \"podUuid\" : \"<POD_UID>\", \"podNamespace\" : \"<POD_NAMESPACE>\", \"podName\" : \"<POD_NAME>\" }"

NOTE:

- The template can be modified, and the user has to ensure that the template has the correct JSON syntax.
- Double quotes have to be given before and after <>, if the variable part is a string.
- Update the variable part with double quotes.

  For example,

  "<MY_VARIABLE>"

  Here, <MY_VARIABLE> is replaced with the actual content or empty.

  (or) "MY_VARIABLE".

  Here, the content remains same.
- If any modification is needed after deployment, Containerized Decomposed Media Server pod has to be redeployed.
- If **enableFM** and **generic alarm template format** parameters are enabled, both JSON content uses the same sidecar.

Appendix D

List of Statistics

This appendix lists the statistics generated by the Containerized Decomposed Media Server.

Most statistics can be retrieved from the Containerized Decomposed Media Server and posted to an external server or obtained using the SNMP interface. Only a subset of the statistics is displayed in the Web GUI. Additionally, control protocols can have protocol-specific statistics.

The following statistics are presented.

- *System Usage Group*
- *Session Usage Group*
- *SIP Usage Group*
- *DSP Usage Group*
- *Dropped UDP Packets Group*
- *HTTP Media Statistics Group*
- *VoiceXML Usage Group*
- *CPU Core Group*
- *ASR/TTS Usage Group*
- *Fax Usage Group*
- *MRFC Stats Group*
- *Disk Max Usage Group*
- *MSML Usage Group*

System Usage Group

Table 135 shows system usage statistics generated for both MRFC and MRFP by the Containerized Decomposed Media Server.

Table 135. System Usage Group

Name	Description
Card Up Time	Time since last reset in units of 10 milliseconds. This statistic is cumulative.
Min Free RAM	Minimum free system memory for all 1 second samples during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Current Free RAM	Minimum free system memory during the interval, expressed as a percentage. This statistic is not reset.
Avg Free RAM	Average free system memory over all 1 second samples within the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Min Free RAM Drive Space	Minimum free RAM drive space during the interval, expressed as a percentage. 1 second samples during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Min Free System/Process Memory	Minimum free system plus the minimum free process memory for all 1 second samples during the interval, expressed as a percentage. This element is used for overload protection calculation. This statistic is reset at the beginning of each interval.
Current Free System/Process Memory	Current free system plus free process memory, expressed as a percentage. This is a snapshot of usage during the last second. This element is used for overload protection calculation. This statistic is not reset.
Min Free MPCCP System/Process Memory	Minimum free system plus the minimum free memory for the MPCCP process for all 1 second samples during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Current Free MPCCP System/Process Memory	Current free system plus memory for the MPCCP process, with sample rate as 1 second is expressed as a percentage. This is a snapshot of usage during the last second. This element is used for overload protection calculation. This statistic is not reset.
Min Free Transient Clip Partition Space	Minimum free space in the partition that contains transient clips, expressed as a percentage. Measured once per second. This statistic is not reset.

Session Usage Group

When per-codec statistics are generated, the Containerized Decomposed Media Server increments the counter for the codec the first time it sends or receives an RTP packet of that type on a port. In these counters, the Containerized Decomposed Media Server does not count G.729 or G.711 encoders used for Transcoding announcements and recordings. For example, if the Containerized Decomposed Media Server plays a G.729 announcement to a G.711 port, then the Max Ports Active G.711=1 and the Max Ports Active G.729=0.

If the Containerized Decomposed Media Server receives an RTP packet of a different type on an existing port (mid-call codec change) it behaves as follows:

- Decrements the counter for the original codec type
- Increments the counter for the new codec type

Table 136 shows session usage statistics generated for each MRFP in the Containerized Decomposed Media Server. An entry is generated for each Ethernet port on the MRFP.

Table 136. Session Usage Group

Name	Description
Ports Created	Number of media ports created since the last reset. This statistic is reset at the beginning of each interval.
Ports Deleted	Number of media ports deleted since the last reset. This statistic is reset at the beginning of each interval.
Max Ports Active	Maximum number of ports active simultaneously during the interval. This statistic is updated each time a port becomes operational. This statistic is reset at the beginning of each interval.
Avg Ports Active	Average number of ports active simultaneously during the interval. This is a time-weighted average that includes all ports active during the interval: • Ports created prior to reporting interval • Ports created during reporting interval • Ports deleted during reporting interval For example for a 15 minutes interval, if there are 200 ports active for 14 minutes, 100 ports that were active for the entire interval (that is, the ports created before the interval and still active when the interval ended), and 300 ports active for 1 minute, the weighted average = 14/15 * 200 + 1* 100 + 1/15*300 = 306. This statistic is recalculated at the beginning of each interval.
Current Ports Active	Current number of ports active. This statistic is updated when a port is created or deleted. This is a snapshot of port usage. This statistic is not reset.
Max Announcements	Maximum number of announcement services that are simultaneously active on the Containerized Decomposed Media Server. This statistic is updated when an announcement service is created. Note that for multimedia announcements, two services are created: one for audio and one for video. This statistic is reset at the beginning of each interval.
Max Conferences	Maximum number of conference mixes that are simultaneously active on the Containerized Decomposed Media Server. This statistic is updated when a conference mix is created. Note that for multimedia conferences, two conference mixes are created: one for audio and one for video. This statistic is reset at the beginning of each interval.
Max Recordings	Maximum number of recording services that are simultaneously active during the interval. This statistic is updated when a recording service is created. Note that for multimedia recordings, two recording services are created: one for audio and one for video. This statistic is reset at the beginning of each interval.
Max DTMF Detectors	Maximum number of DTMF detectors that are simultaneously active during the interval. This statistic is updated when a DTMF detection service is enabled. Note that where a port has both in-band and RFC 2833 detection active, this is only counted as just DTMF detection service. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Max G.711 Ports	The maximum number of G.711 ports used during the interval. This statistic is reset at the beginning of each interval.
Max G.722 Ports	The maximum number of G.722 ports used during the interval. This statistic is reset at the beginning of each interval.
Max G.729 Ports	The maximum number of G.729 ports used during the interval. This statistic is reset at the beginning of each interval.
Max AMR-NB Ports	The maximum number of ports used for AMR during the last statistics interval. This statistic is reset at the beginning of each interval.
Max AMR-WB Ports	The maximum number of ports used for AMR-WB during the last statistics interval. This statistic is reset at the beginning of each interval.
Max EVRC Ports	The maximum number of ports used for EVRC0 and EVRC during the last statistics interval. This statistic is reset at the beginning of each interval.
Max EVRCB Ports	The maximum number of ports used for EVRCB0 and EVRCB during the last statistics interval. This statistic is reset at the beginning of each interval.
Max EVRCNW Ports	The maximum number of ports used for EVRNW0 and EVRCNW during the last statistics interval. This statistic is reset at the beginning of each interval.
Max Opus-NB Ports	The maximum number of ports used for Opus-NB during the last statistics interval. This statistic is reset at the beginning of each interval.
Max Opus-WB Ports	The maximum number of ports used for Opus-WB during the last statistics interval. This statistic is reset at the beginning of each interval.
Max Evs Ports	The maximum number of ports used for EVS during the last statistics interval. This statistic is reset at the beginning of each interval.
Max VP8 Ports	The maximum number of ports used for VP8 during the last statistics interval. This statistic is reset at the beginning of each interval.
Max H.265 Ports	The maximum number of ports used for H.265 during the last statistics interval.
Max Ports T.140	The maximum number of ports used for T.140. This statistic is reset at the beginning of each interval.
Max Detectors TTY	The maximum number of detectors used for tty. This statistic is reset at the beginning of each interval.
CP_LIVE_CALL Events	The number of call progress LIVE_CALL events reported. This statistic is not reset.
CP_GREETING Events	The number of call progress GREETING events reported. This statistic is not reset.
Noisy Line Reports	The number of ports that have had one or more noisy-line reports. This statistic is not reset.
Noisy Line Reports Discarded	The number of noisy-line reports discarded due to insufficient resources. This statistic is not reset.
Max NLD Ports Enabled	The maximum number of ports on which noisy-line detection is enabled during the interval. This statistic is reset at the beginning of each interval.
Max G.711 and G.722 PLC Ports Enabled	The maximum number of G.711 (ITU G.711 Appendix 1) and G.722 (ITU G.722 Appendix IV) ports on which packet loss concealment are enabled during the interval. This statistic is reset at the beginning of each interval.
Max PPS Ports Enabled	The maximum number of ports on which per-port statistics are enabled during the interval. This statistic is reset at the beginning of each interval.
Max NG Ports Enabled	The maximum number of ports on which noise gating is enabled during the interval. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Max NR Ports Enabled	The maximum number of ports on which noise reduction is enabled during the interval. This statistic is reset at the beginning of each interval.
Max AEC Ports Enabled	The maximum number of ports on which acoustic echo cancellation is enabled during the interval. This statistic is reset at the beginning of each interval.
Max AEC Ports Active	The maximum number of ports on which acoustic echo cancellation is enabled and active during the interval. This statistic is reset at the beginning of each interval.
Max AEC Ports Resource Limited	The maximum number of ports on which acoustic echo cancellation is enabled and must have been active but could not be activated due to limited resources during the interval. This statistic is reset at the beginning of each interval.
Max Auto NR Ports Enabled	The maximum number of ports on which auto Noise Reduction is enabled during the interval. This statistic is reset at the beginning of each interval.
Max Auto NR Ports Activated	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected, and NR turned on. This statistic is reset at the beginning of each interval.
Max NR Ports Resource Limited	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected, and NR not turned on due to resource limitation. This statistic is reset at the beginning of each interval.
Max NR Ports Config Limited	The maximum number of ports on which auto Noise Reduction is enabled during the interval and noise detected, and NR not turned on due to port limit.This statistic is reset at the beginning of each interval.
Num AEC Monitor Resources Requested	The number of times an Echo Canceler Monitoring resource is requested. This statistic is reset at the beginning of each interval.
Num AEC Monitor Resources Req Denied	The number of times an Echo Canceler Monitoring resource is requested and fails to get a resource. This statistic is reset at the beginning of each interval.
Max AEC Monitors in Use	The maximum number of simultaneous Echo Canceler Monitoring resources are in use. This statistic is reset at the beginning of each interval.
NUM Total Full Mix Count	The total number of times in which the number of active speakers with energy levels above a specified threshold is equal to the maximum allowed speakers.This statistic is reset at the beginning of each interval.
Max Full Time Ratio	The maximum ratio, found across all conferences on the Containerized Decomposed Media Server during the interval, between the time a conference was full (that is, its active speakers with energy levels above a specified threshold equaled the maximum allowed speakers) to the total time of the conference. This statistic is reset at the beginning of each interval.
Max T38 Fax Ports	The maximum number of ports used forT.38 fax codec during the interval. This statistic is reset at the beginning of each interval.
Max G.711 Fax Ports	The maximum number of ports used for G.711 fax codec during the last period. This statistic is reset at the beginning of each interval.
Number of times VQE License Exhausted	The number of calls established on the Containerized Decomposed Media Server when a VQE license is exhausted but the codec license is available.

Table 136. Session Usage Group

Name	Description
Total Transcoded Announcement on Audio Ports	The total number of transcoded announcements on the audio ports in the reporting interval. This counter is incremented when a announcement clip played on the port is transcoded. For multi-clip and variable announcements, this counter is updated for each clip that was transcoded. For NFS or internal location iterative announcements, this counter is incremented only once for each clip. For HTTP announcements, this counter is incremented for each clip and iteration. This statistic is reset at the beginning of each interval.
Max number of Active Transcoded Announcement on audio ports	The maximum number of transcoded announcements simultaneously active on the audio ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of transcoded announcement on video ports	The total number of transcoded announcements on the video ports in the reporting interval. This counter is incremented when an announcement clip played on the port is transcoded. For multi-clip announcements, this counter is updated for each clip that was transcoded. For iterative announcements, this counter is incremented only once for each clip. This statistic is reset at the beginning of each interval.
Max number of Active Transcoded Announcement on video ports	The maximum number of transcoded announcements simultaneously active on the video ports in the reporting interval. This statistic is reset at the beginning of each interval.
Max number of active AMR-WB announcement on AMR ports	The maximum number of AMR-WB announcements simultaneously active on the AMR ports during the interval. These announcements are always transcoded. This statistic is reset at the beginning of each interval.
Max number of active AMR announcement on AMR ports	The maximum number of active AMR announcements on the AMR ports during the interval that were transcoded. This counter is not updated for bypass announcement. This statistic is reset at the beginning of each interval.
Max number of active AMR announcement on AMR-WB ports	The maximum number of AMR announcements simultaneously active on the AMR-WB ports during the interval. These announcements are always transcoded. This statistic is reset at the beginning of each interval.
Max number of active AMR-WB announcement on AMR-WB ports	The maximum number of active AMR-WB announcements simultaneously active on the AMR-WB ports during the interval that were transcoded. This counter is not updated for bypass announcement. This statistic is reset at the beginning of each interval.
Total number of PCMA announcement ports	Total number of times the announcement service was invoked on PCMA ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of PCMU announcement ports	Total number of times the announcement service was invoked on PCMU ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of AMR announcement ports	Total number of times the announcement service was invoked on AMR ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Total number of AMR-WB announcement ports	Total number of times the announcement service was invoked on AMR-WB ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of EVS announcement ports	Total number of times the announcement service was invoked on EVS ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of G.722 announcement ports	Total number of times the announcement service was invoked on G.722 ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of G.729 announcement ports	Total number of times the announcement service was invoked on G.729 ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of OPUS announcement ports	Total number of times the announcement service was invoked on Opus ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of EVRC announcement ports	Total number of times the announcement service was invoked on EVRC ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of EVRCB announcement ports	Total number of times the announcement service was invoked on EVRCB ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of EVRCNW announcement ports	Total number of times the announcement service was invoked on EVRCNW ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of H.264 announcement ports	Total number of times the announcement service was invoked on H.264 ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Total number of VP8 announcement ports	Total number of times the announcement service was invoked on VP8 ports in the reporting interval. This includes bypass and transcoded announcements. Multi-clip, variable clip, and iterative announcements are considered as a single announcement and this counter is updated only once. This statistic is reset at the beginning of each interval.
Total number of PCMA recording ports	Total number of times the record service was invoked on PCMA ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of PCMU recording ports	Total number of times the record service was invoked on PCMU ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of AMR recording ports	Total number of times the record service was invoked on AMR ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of AMR-WB recording ports	Total number of times the record service was invoked on AMR-WB ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of EVS recording ports	Total number of times the record service was invoked on EVS ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of G.722 recording ports	Total number of times the record service was invoked on G.722 ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of G.729 recording ports	Total number of times the record service was invoked on G.729 ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of OPUS recording ports	Total number of times the record service was invoked on Opus ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of EVRC recording ports	Total number of times the record service was invoked on EVRC ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of EVRCB recording ports	Total number of times the record service was invoked on EVRCB ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of EVRCNW recording ports	Total number of times the record service was invoked on EVRCNW ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of H.264 recording ports	Total number of times the record service was invoked on H.264 ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of VP8 recording ports	Total number of times the record service was invoked on VP8 ports in the reporting interval. This includes bypass and transcoded recordings. This statistic is reset at the beginning of each interval.
Total number of PCMA conference ports	Total number of times the conference service was invoked on PCMA ports in the reporting interval. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Total number of PCMU conference ports	Total number of times the conference service was invoked on PCMU ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of AMR conference ports	Total number of times the conference service was invoked on AMR ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of AMR-WB conference ports	Total number of times the conference service was invoked on AMR-WB ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVS conference ports	Total number of times the conference service was invoked on EVS ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of G.722 conference ports	Total number of times the conference service was invoked on G.722 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of G.729 conference ports	Total number of times the conference service was invoked on G.729 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of OPUS conference ports	Total number of times the conference service was invoked on Opus ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRC conference ports	Total number of times the conference service was invoked on EVRC ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRCB conference ports	Total number of times the conference service was invoked on EVRCB ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRCNW conference ports	Total number of times the conference service was invoked on EVRCNW ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of H.264 conference ports	Total number of times the conference service was invoked on H.264 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of VP8 conference ports	Total number of times the conference service was invoked on VP8 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of PCMA transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for PCMA ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of PCMU transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for PCMU ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of AMR transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for AMR ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of AMR-WB transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for AMR-WB ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVS transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for EVS ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of G.722 transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for G.722 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of G.729 transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for G.729 ports in the reporting interval. This statistic is reset at the beginning of each interval.

Table 136. Session Usage Group

Name	Description
Total number of OPUS transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for Opus ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRC transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for EVRC ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRCB transcoding ports	TTotal number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for EVRCB ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of EVRCNW transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for EVRCNW ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of H.264 transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for H.264 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of VP8 transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for VP8 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of T140 transcoding ports	Total number of port-to-port transcoding sessions (MSML port-to-port session, B2BUA call, or `sip:tc` call) established for T.140 ports in the reporting interval. This statistic is reset at the beginning of each interval.
Max Active KWD Sessions	Maximum number of keyword detection sessions simultaneously active during the interval. This statistic is reset at the beginning of each interval.
Total Number Of CP_AM_BEEP Events	Total number of CP_AM_BEEP events detected in each reporting cycle in the OAMP statistics. This statistic is reset at the beginning of each interval.
Max Number Of AM_BEEP Session	Maximum number of AM Beep Detection sessions enabled in each reporting cycle in the OAMP statistics. This statistic is reset at the beginning of each interval.

SIP Usage Group

Table 137 shows SIP statistics generated by the MRFP

Table 137. SIP Usage Group

Name	Description
Max Command Rate	Maximum number of SIP requests in commands per second, in 1-second sample periods. This number includes only requests received by the Containerized Decomposed Media Server; it does not include responses received. This statistic is reset at the beginning of each interval.
Avg Command Rate	Average number of SIP requests in commands per second, for all 1-second sample periods. This number includes only requests received by the Containerized Decomposed Media Server; it does not include responses received. This statistic is reset at the beginning of each interval.

Name	Description
Avg Hold Time	Average hold time for calls during the interval. The hold time of a call starts when the connection is successfully created and stops, when the connection is deleted. This statistic is reset at the beginning of each interval. The unit of average hold time is second.
Max Hold Time	Maximum hold time for calls during the interval. The hold time of a call starts when the connection is successfully created and stops when the connection is deleted. This statistic is reset at the beginning of each interval. The unit of maximum hold time is second.
Min Hold Time	Minimum hold time for calls during the interval. The hold time of a call starts when the connection is successfully created and stops when the connection is deleted. This statistic is reset at the beginning of each interval. The unit of minimum hold time is second.
Request Failure Errors (4xx)	The number of 4xx errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (400)	The number of 400 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (404)	The number of 404 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (403)	The number of 403 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (405)	The number of 405 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (406)	The number of 406 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (408)	The number of 408 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (415)	The number of 415 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.

Name	Description
Request Failure Errors (420)	The number of 420 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (422)	The number of 422 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (423)	The number of 423 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (471)	The number of 471 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (480)	The number of 480 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (481)	The number of 481 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.

Name	Description
Request Failure Errors (482)	The number of 482 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (483)	The number of 483 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (484)	The number of 484 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (486)	The number of 486 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (487)	The number of 487 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (488)	The number of 488 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Request Failure Errors (491)	The number of 491 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (5xx)	The number of 5xx errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (500)	The number of 500 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (501)	The number of 501 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (503)	The number of 503 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (504)	The number of 504 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Server Failure Errors (505)	The number of 505 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Global Failure Errors (6xx)	The number of 6xx errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Global Failure Errors (600)	The number of 600 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
Global Failure Errors (603)	The number of 603 errors sent by the Containerized Decomposed Media Server during the interval. This statistic is reset.
SIP Packets RX	The total number of packets received during the interval. This statistic is reset.
SIP Packets TX	The total number of packets transmitted during the interval. This statistic is reset.
Out of Resource Errors	The number of out-of-resource errors received during the interval. This statistic is the sum of 486 and 503 responses that includes Call Overload Request Rejections and Service Overload Request Rejections statistics. This statistic is not reset.
Call Overload Request Rejections	The number of call overload events detected during the interval. In this case, new calls (INVITE requests) are rejected, but existing calls are still processed. This statistic is not reset.
Service Overload Request Rejections	The number of service overload events detected during the interval. In this case, all service requests except call deletion (INFO, OPTIONS, and re-INVITE requests) are rejected. This statistic is not reset.

Name	Description
Accepted Incoming Priority Calls	The number of SIP INVITE requests containing a SIP Resource Priority Header (RPH) that are accepted by the Containerized Decomposed Media Server. Calls are accepted when they are processed or added to the RPH call queue. This statistic is not reset.
Current Priority Calls in Queue	The number of SIP calls waiting in the RPH call queue. This statistic is not reset. ***NOTE:*** This statistic is available only on the SNMP interface and the *Show Real-Time Statistics* Web GUI page. It is neither added to the statistic file nor displayed on the *Show Statistics History* Web GUI page.
Established Priority Calls	The number of SIP INVITE requests containing an RPH that are established by sending a 200 response to the invite request. This statistic is not reset.
Completed Priority Calls	The number of SIP INVITE requests containing an RPH that are established and subsequently terminated normally. This statistic is not reset.
Priority Out of Resource Errors	The number of out-of-resource responses sent for SIP RPH calls. This response is sent for each incoming call that the Containerized Decomposed Media Server fails to handle due to a lack of resources. This statistic is not reset.
Priority Timeout Errors	The number of timeout responses sent for SIP RPH calls. This response is sent for each incoming call that the Containerized Decomposed Media Server rejects after it has remained too long in the RPH call queue This statistic is not reset.
SIP Dropped Msg due Full Serialization Queue	The total number of SIP messages dropped because the serialization queue was full. This statistic is not reset.
Total Sip Ports Deleted Due Rtcp Bye	The total number of SIP ports deleted because RTCP BYEs were received. This statistic is not reset.
Total Sip Video Ports Deleted Due to Rtcp Bye	The total number of SIP video ports deleted because RTCP BYEs were received. This statistic is not reset.
Total RTCP timeout events generated on SIP audio port	The total number of RTCP timeout events generated on SIP audio port. This statistic is not reset.
Total RTCP timeout events generated on SIP video port	The total number of RTCP timeout events generated on SIP video port. This statistic is not reset.
Total SIP audio ports deleted due to RTCP timeout	The total number of SIP audio ports deleted due to RTCP timeout event. This statistic is not reset.
Total SIP video ports deleted due to RTCP timeout	The total number of SIP video ports deleted due to RTCP timeout event. This statistic is not reset.
Regular Calls Rejected Due To Access Control	The regular calls rejected due to the access control. This statistic is not reset.
Total Priority Calls Received	The total number of priority calls received. This statistic is not reset.
Priority Calls Rejected As priority Management Disabled	The priority calls rejected due to priority management disabled. This statistic is not reset.
Priority Calls Accepted As Regular Calls	The priority calls accepted as the regular calls. This statistic is not reset.
Total number of TLS calls established	The total number of SIP-TLS calls established in the reporting interval. This statistic is reset at the beginning of each interval.
Total number of TLS calls failed	The total number of SIP-TLS calls failed in the reporting interval. This statistic is reset at the beginning of each interval.

Name	Description
Average conference hold time	The average hold time for conferences created in MSML, MSCML, and Netann conference service contexts. The unit of average conference hold time is second. In MSML conference, the Containerized Decomposed Media Server measures the time between `<createconferencce>` and `<destroyconference>` request. Also, the Containerized Decomposed Media Server updates the counter when the conference object is destroyed implicitly due to **delete-when=no-media** and **delete-when=no-control**. In `<destroyconference>` request, the Containerized Decomposed Media Server updates the counter when the conference is deleted, not when a mixer is destroyed. In the MSCML conference, the Containerized Decomposed Media Server measures the time between the created and deleted conference control leg and updates the statistics accordingly. In the Netann conference, the Containerized Decomposed Media Server measures the time since the first participant call-leg was created till the last participant call-leg is deleted. This statistic is reset at the beginning of each interval.
Average participants per conference	The average participants per conference created in MSML, MSCML, and Netann conference service contexts. In MSML, the participant `<join>` or `<unjoin>` and port delete. For MSCML and Netann conference, the SIP-BYE on the port is considered for the calculation. This statistic is reset at the beginning of each interval.

NOTE: The 4xx and 5xx error code statistics such as 400, 404, 405, 483, 505, and so on, are not incremented when the Containerized Decomposed Media Server SIP stack rejects the INVITE with these error codes. However, these statistics are incremented when the Containerized Decomposed Media Server application generates these error response codes.

DSP Usage Group

Table 138 shows DSP statistics generated by the MRFP.

NOTE: HC core configuration is deprecated. Hence, the HC video core statistics are by default set to 0. However, the HC video profile/levels are still supported.

Table 138. DSP Usage Group

Name	Description
RTP Packets TX	Number of RTP packets for all DSPs transmitted during the interval. This statistic is not reset.
RTP Audio Packets TX	Number of RTP packets for all audio DSPs transmitted during the interval. This statistic is not reset.
RTP Video Packets TX	Number of RTP packets for all video DSPs transmitted during the interval. This statistic is not reset.
RTP Packets RX	Number of RTP packets for all DSPs received during the interval. This statistic is not reset.
RTP Audio Packets RX	Number of RTP packets for all audio DSPs received during the interval. This statistic is not reset.

Table 138. DSP Usage Group

Name	Description
RTP Video Packets RX	Number of RTP packets for all video DSPs received during the interval. This statistic is not reset.
RTP Packets Lost	Number of lost RTP packets for all DSPs during the interval based on RTP sequence number. This statistic is not reset.
RTP Audio Packets Lost	Number of lost RTP packets for all audio DSPs during the interval based on RTP sequence number. This statistic is not reset.
RTP Video Packets Lost	Number of lost RTP packets for all video DSPs during the interval based on RTP sequence number. This statistic is not reset.
RTP Interarrival Jitter	Maximum jitter for all DSPs during the interval. This statistic is reset at the beginning of each interval.
Max DSP CPU Utilization	Maximum DSP CPU utilization for all the DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg DSP CPU Utilization	Average DSP CPU utilization for all the DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Slipped Cycle Count	The number of times the DSP is unable to complete processing of the audio frame during the processing window allocated for each DSP. For the busiest audio DSP, the success criteria for any load or functional test includes checking, that the slip cycles are not more than 90 per DSP core in a 15 min interval. This statistic is reset at the beginning of each interval.
Max DSP HW Packets	Maximum number of DSP command packets sent for all the DSPs. This statistic is not reset.
Max Modeled DSP CPU Utilization	Maximum modeled DSP CPU utilization for all the DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Modeled DSP CPU Utilization	Average modeled DSP CPU utilization for all the DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Max Modeled Audio DSP CPU Utilization	Maximum modeled DSP CPU utilization for all the audio DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Modeled Audio DSP CPU Utilization	Average modeled DSP CPU utilization for all the audio DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Max Actual Audio DSP CPU Utilization	Maximum actual DSP CPU utilization for all the audio DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Actual Audio DSP CPU Utilization	Average actual DSP CPU utilization for all the audio DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Max Modeled Video DSP CPU Utilization	Maximum modeled DSP CPU utilization for all the video DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Modeled Video DSP CPU Utilization	Average modeled DSP CPU utilization for all the video DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Max Actual Video DSP CPU Utilization	Maximum actual DSP CPU utilization for all the video DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Actual Video DSP CPU Utilization	Average actual DSP CPU utilization for all the video DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Max Modeled HC Video DSP CPU Utilization	Maximum modeled DSP CPU utilization for all the HC DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Modeled HC Video DSP CPU Utilization	Average modeled DSP CPU utilization for all the HC DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.

Table 138. DSP Usage Group

Name	Description
Max Actual HC Video DSP CPU Utilization	Maximum actual DSP CPU utilization for all the HC DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg Actual HC Video DSP CPU Utilization	Average Actual DSP CPU utilization for all the HC DSPs during the interval, expressed as a percentage. This statistic is reset at the beginning of each interval.
Total Rtcp Bye-Packets Received	Total number of RTCP BYE packets received. This statistic is not reset.
Lost packets recovered using redundant RTP	The number of lost packets recovered using redundant RTP (RFC2198) during the last period. This statistic is reset at the beginning of each interval.
Max Video Encoder Frame Rate Drop Rate	The maximum frames drop percentage (Video) during the last period. This statistic is reset at the beginning of each interval.
Max Frames Dropped (HC Video)	The maximum frames drop percentage (HC Video) during the last period. This statistic is reset at the beginning of each interval.
Super Slipped Cycle Count (Audio)	This statistic counts the number of times an audio DSP is unable to complete processing in a 90 ms window. The audio cores must not contain any super slip cycles. This statistic is reset at the beginning of each interval.
T.140 Bytes Sent	T.140 characters sent. This statistic is reset at the beginning of each interval.
T.140 Bytes Received	T.140 characters received. This statistic is reset at the beginning of each interval.
T.140 Packets Missed not replaceable by redundant T.140 Packets	T.140 packets missed not replaceable by redundant T.140 Packets. This statistic is reset at the beginning of each interval.
T.140 Chars Mapped To Apostrophe Chars in TTY streams	T.140 characters mapped to apostrophe characters in TTY stream. This statistic is reset at the beginning of each interval.
Super Slipped Cycle Count (Video)	***NOTE:*** Processing load for Video packets is uneven as compared to processing load for Audio packets. Video DSPs may take 30 ms or more to process video frames. Therefore, it is not possible to state that there are no slip cycles on video DSPs. For this reason the concept of Super Slipped cycles was introduced. This statistic counts the number of times a Video DSP is unable to complete processing of video packet in 90 ms. For the busiest video DSP, the success criteria for any load or functional test includes checking, that the super slip cycles are not more than 90 per DSP core in a 15 min interval. This statistic is reset at the beginning of each interval.
Super Slipped Cycle Count (HC Video)	This statistic counts the number of times an HC video DSP is unable to complete the processing of HC video packet in 95 ms. The HC video is defined based on the “Burst Slip Cycle Exceed Limit”. This statistic is reset at the beginning of each interval.
Max Burst Slip Cycles (Audio)	Maximum number of contiguous slip cycles incurred by an audio DSP during the interval. This statistic is reset at the beginning of each interval.
Max Burst Slip Cycles (Video)	Maximum number of contiguous slip cycles incurred by a video DSP during the interval. For example, if a DSP core never incurred more than 5 slip cycles, this stat is set to 5. This statistic is reset at the beginning of each interval.

Table 138. DSP Usage Group

Name	Description
Max Burst Slip Cycles (HC Video)	Maximum number of contiguous slip cycles incurred by an HC video DSP during the interval. For example, if an HC video DSP core never incurred more than 5 slip cycles, this stat is set to 5 This statistic is reset at the beginning of each interval.
Burst Slip Cycles Exceed Limit (HC Video)	Tracks the number of times the burst slip cycles exceed 50 for all HC video DSPs during the reporting interval. Statistic increments by one, for each block of 50 consecutive slipped cycles for the busiest HC video DSP. For an HC video DSP, a new OAMP statistic that counts the number of times the burst slip cycle exceeds 50 (refer MaxBurstSlipCycle) is supported. The counter must not be more than 11 in any 15 min interval. This statistic is reset at the beginning of each interval.
Dropped Video Packets	Total number of Dropped Packets for all video DSPs during the reporting interval. This statistic is reset at the beginning of each interval.
Jitter Buffer Frames Dropped	Total duration of audio frames dropped by jitter buffer for all audio DSPs during the reporting interval. This statistic is reset at the beginning of each interval.
Non Decoded Video Frames	Counts the number of video frames that are not decoded for all video DSPs during the reporting interval. This statistic is reset at the beginning of each interval.
Non Decoded Audio Frames	Counts the duration (in unit of milliseconds) of audio frames that are not decoded by the decoder for all audio DSPs during the reporting interval. This statistic is computed only for the Opus decoder. The Opus decoder may not decode a frame, if its sampling frequency or the number of channels is higher than what is configured. This statistic is reset at the beginning of each interval.

Dropped UDP Packets Group

Table 139 shows dropped UDP packet statistic generated by the MRFC and MRFP.

Table 139. Dropped UDP Packets Group

Name	Description
Dropped UDP Packets RX	Number of UDP packets dropped by the control processor in the receive direction. This count does not include UDP packets dropped outside the instance, RTP packets dropped (which are also UDP packets, but which are handled by specialized hardware), or other sources of packet loss (for example, hardware buffer overflow), as those are captured by other counters. This statistic is not reset.
Dropped UDP Packets TX	UDP packets dropped by the control processor in the transmit direction. This count does not include UDP packets dropped outside the instance, RTP packets dropped (which are also UDP packets, but which are handled by specialized hardware), or other sources of packet loss (for example hardware buffer overflow), as those are captured by other counters. This statistic is not reset.

HTTP Media Statistics Group

Table 140 shows statistics generated by the MRFP for caching media from HTTP servers. These statistics are applicable only when HTTP media operation mode is configured as cache mode.

Table 140. HTTP Media Statistics Group

Name	Description
HTTP Clip Requests	The number of media clips during the interval requested from HTTP sources. This statistic is not reset.
Cache Hits No Validation	The number of media clips served from the cache during the interval without requiring validation (cache hits). This statistic is not reset.
Cache Hits With Validation	The number of media clips during the interval served from the cache after validation. This statistic is not reset.
Cache Misses	The number of media clips during the interval that had to be retrieved from HTTP servers (cache misses). This statistic is not reset.
Non-Cacheable	The number of media clips during the interval that were retrieved from HTTP servers and were marked as “non-cacheable”. This statistic is not reset.
Cache Overflows	The number of media clips that could not be played because enough memory was not available for the clip in the cache. This statistic is not reset.

VoiceXML Usage Group

Table 141 shows VoiceXML statistics generated by the MRFP.

Table 141. VoiceXML Usage Group

Name	Description
Max Active Channels	Maximum number of VoiceXML channels active simultaneously during the interval. This statistic is updated each time a channel becomes operational. This statistic is reset during the interval.
No Channels Session Rejections	Number of VoiceXML sessions rejected due to a lack of available channels. This statistic is not reset.
Current Active Channels	Current number of VoiceXML channels active. This statistic is updated when a channel is created or deleted. This is a snapshot of channel usage. This statistic is not reset.
Service Overload Session Rejections	The number of VoiceXML sessions rejected due to a service overload condition. This statistic is not reset.

CPU Core Group

Table 142 shows CPU statistics generated by the Containerized Decomposed Media Server. An entry is generated for each MRFC and MRFP.

Table 142. CPU Core Group

Name	Description
Max CPU Core Utilization	Peak CPU utilization of the control processor during the interval using 1 second sample periods, expressed as a percentage. This statistic is reset at the beginning of each interval.
Avg CPU Core Utilization	Average CPU utilization of the control processor during the interval using 1 second sample periods, expressed as a percentage. This statistic is reset at the beginning of each interval.
Current CPU Core Utilization	Current CPU utilization of the control processor, expressed as a percentage. This is a snapshot of usage during the last second. Reset does not apply.

MRFP Redundancy Groups

Table 143 shows MRFP redundancy statistics generated by the Decomposed Media Server.

Table 143. MRFP Redundancy Groups

Name	Description
Number of Auto Switchovers	Number of automatic switchover occurred in an MRFP redundancy group. This statistic is not reset.
Number of Manual Switchovers	Number of manual switchover occurred in an MRFP redundancy group. This statistic is not reset.

ASR/TTS Usage Group

Table 144 describes the ASRs and TTS statistics generated by the MRFP.

Table 144. ASR/TTS Usage Group

Name	Description
Max TTS Ports	The maximum number of TTS ports in use at one time during the interval. This statistic is reset at the beginning of each interval.
Total TTS Ports	A running total of the TTS ports created. This statistic is not reset.
TTS Errors	The number of errors, including out of resource errors, that occurred on TTS ports. This includes errors that occur while the connection is being established or torn down. This statistic is not reset.
TTS Out of Resource Errors	The number of out of resource errors that occurred on TTS ports. This statistic is not reset.
Max ASR Ports	The maximum number of ASR ports in use at one time during the interval. This statistic is reset at the beginning of each interval.
Total ASR Ports	A running total of the ASR ports created. This statistic is not reset.
ASR Errors	The number of errors, including out of resource errors, that occurred on ASR ports. This includes errors that occur while the connection is being established or torn down. This statistic is not reset.

Table 144. ASR/TTS Usage Group

Name	Description
ASR Out of Resource Errors	The number of out of resource errors that occurred on ASR ports. This statistic is not reset.
3xx Errors	The number of 3xx error responses received on ASR and TTS connections. This statistic is not reset.
4xx Errors	The number of 4xx error responses received on ASR and TTS connections. This statistic is not reset.
5xx Errors	The number of 5xx error responses received on ASR and TTS connections. This statistic is not reset.
6xx Errors	The number of 6xx error responses received on ASR and TTS connections. This statistic is not reset.
Total Tts-Ports Deleted Due Rtcp Bye	Total number of TTS ports deleted due to RTCP BYE. This statistic is not reset.
Total Asr-Ports Deleted Due Rtcp Bye	Total number of ASR ports deleted due to RTCP BYE. This statistic is not reset.
Total Rtsp-Ports Deleted Due Rtcp Bye	Total number of RTSP ports deleted due to RTCP BYE. This statistic is not reset.

Fax Usage Group

Table 145 describes the fax statistics generated by the MRFP.

Table 145. Fax Usage Group

Name	Description
T.38 Faxes Sent	The number of T.38 faxes sent. This statistic is reset at the beginning of each interval.
T.38 Faxes Received	The number of T.38 faxes received. This statistic is reset at the beginning of each interval.
T.38 Pages Sent	The number of T.38 fax pages sent. This statistic is reset at the beginning of each interval.
T.38 Pages Received	The number of T.38 fax pages received. This statistic is reset at the beginning of each interval.
T.38 Fax Send Failed	The number of T.38 faxes failed in sending. This statistic is reset at the beginning of each interval.
T.38 Fax Received Failed	The number of T.38 faxes failed in receiving. This statistic is reset at the beginning of each interval.
T.38 Retransmissions	The number of T.38 fax retransmissions sent. This statistic is reset at the beginning of each interval.
G.711 Faxes Sent	The number of G.711 faxes sent. This statistic is reset at the beginning of each interval.
G.711 Faxes Received	The number of G.711 faxes received. This statistic is reset at the beginning of each interval.
G.711 Pages Sent	The number of G.711 fax pages sent. This statistic is reset at the beginning of each interval.
G.711 Pages Received	The number of G.711 fax pages received. This statistic is reset at the beginning of each interval.
G.711 Fax Send Failed	The number of G.711 faxes failed in sending. This statistic is reset at the beginning of each interval.
G.711 Fax Received Failed	The number of G.711 faxes failed in receiving. This statistic is reset at the beginning of each interval.
G.711 Retransmissions	The number of G.711 fax retransmissions sent. This statistic is reset at the beginning of each interval.

MRFC Stats Group

Table 146 shows the statistics generated by the MRFCtrl and OAMP Pods.

Table 146. MRFC Statistics Group

Name	Description
MrfCtrl SIP message Sent	The number of SIP messages sent successfully from MRFC to MRFP. This statistic is reset at the beginning of each interval.
MrfCtrl SIP message Received	The number of SIP messages received successfully from MRFP INVITE accepted. This statistic is reset at the beginning of each interval.
MrfCtrl MRFP Failure	The number of calls failed when MRFP is not reachable. This statistic is reset at the beginning of each interval.
Annlab Media Files Newly added	The number of newly created announcement files. This statistic is reset at the beginning of each interval.
Annlab Media Files Deleted	The number of announcements that are removed from the Virtual File System (VFS). This statistic is reset at the beginning of each interval.
Annlab Media Files updated	The number of announcements that are updated from the VFS. This statistic is reset at the beginning of each interval.
Annlab Media Files Provision Error	The number of announcements that failed to be created, updated, or deleted. This statistic is reset at the beginning of each interval.
Annlab Total number of Media Files	The total number of media files exists on the VFS at a given time. This statistic is not reset.
Annlab weight of media files in Koctets	The disk space occupancy in VFS in units of Kilo Octets (KB). This statistic is not reset.
Annlab Media Files Transfer Succeeded	The number of successful media file transfered on the clients of the cluster. This statistic is reset at the beginning of each interval.
Annlab Media Files Transfer Failed	The number of unsuccessful media file transfered on the clients of the cluster. This statistic is reset at the beginning of each interval.
MrfCtrl Total number of TLS Calls Established	The total number of TLS calls established. This statistic is reset at the beginning of each interval.
MrfCtrl Total number of TLS Calls Failed	The total number of failed TLS calls. This statistic is reset at the beginning of each interval.

Disk Max Usage Group

Table 147 shows the disk maximum usage statistics generated by the Containerized Decomposed Media Server.

Table 147. Disk Max Usage Group

Name	Description
Disk Max Usage Root	The disk maximum usage for `Root` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Boot	The disk maximum usage for `Boot` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Weboam	The disk maximum usage for `Weboam` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Home	The disk maximum usage for `Home` directory partition. This statistic is reset at the beginning of each interval.

Table 147. Disk Max Usage Group

Name	Description
Disk Max Usage Opt	The disk maximum usage for `Opt` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Space	The disk maximum usage for `Space` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Usr	The disk maximum usage for `Usr` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Var	The disk maximum usage for `Var` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Mnt_Ramdisk	The disk maximum usage for `Mnt_Ramdisk` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Mnt	The disk maximum usage for `Mnt` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Dev_Shm	The disk maximum usage for `Dev_Shm` (shared memory) directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Tmp	The disk maximum usage for `Tmp` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Var_Log	The disk maximum usage for `Var_Log` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Var_Log_Audit	The disk maximum usage for `Var_Log_Audit` directory partition. This statistic is reset at the beginning of each interval.
Disk Max Usage Var_Opt_Swms_Clips	The disk maximum usage for `Var_Opt_Swms_Clip` directory partition. This statistic is reset at the beginning of each interval.

MSML Usage Group

Table 148 shows the MSML usage statistics generated by the Containerized Decomposed Media Server.

Table 148. MSML Usage Group

Name	Description
Total Announcement Requests	The total number of accepted MSML announcement requests. This statistic is reset at the beginning of each interval.
Total Successful Announcement Requests	The total number of successful announcement attempts. The announcement attempt includes: • Successful completion of play operation • Barged play operation • Partial completion of multi-clip play operation because some clips were skipped due to clip issues • Terminated announcements either by sending `<dialogend>` or on receiving BYE • The existing `<play>` is overridden by another `<play>` request using override=true This statistic is reset at the beginning of each interval.

Table 148. MSML Usage Group

Name	Description
Total Failed Announcement Requests	The total number of failed MSML announcement requests. This counter is a sum of the following statistics values. • Total Failed Announcement Requests • Total Failed Announcement Requests due to All Clips were Skipped • Total Failed Announcement Requests due to Video Issues • Total Failed Announcement Requests due to System Resource Unavailability • Total Failed Announcement Requests due to File Not Found Error • Total Failed Announcement Requests due to External Server Error • Total Failed Announcement Requests due to Link Is Down • Total Failed Announcement Requests due to Timeout • Total Failed Announcement Requests due to Speech Server Error • Total Failed Announcement Requests due to HTTP Cache is Disabled • Total Failed Announcement Requests due to Invalid Announcement File • Total Failed Announcement Requests due to Other Reasons This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to All Clips were Skipped	The total number of announcement requests failed because of skipping the clips in the multi-clip announcement due to the clip issues. This counter corresponds to the **play.failed.all-skipped** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to Video Issues	The total number of announcement requests failed because the announcement included video files, an offset, an interval attribute existed, or the video parameter was changed to higher capability between the clips. This counter corresponds to the **play.failed.video** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to System Resource Unavailability	The total number of announcement requests failed because of the unavailability of system resources. This counter corresponds to the **play.failed.noresource** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to File Not Found Error	The total number of announcement requests failed because of file not found error. This counter corresponds to the **play.failed.file-not-found** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to External Server Error	The total number of announcement requests failed because the external server returned an error other than the timeout, File not found, or NFS server down error conditions. This counter corresponds to the **play.failed.ext-server-error** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to Link Is Down	The total number of announcement requests failed because the link to the external HTTP or NFS server has failed. This counter corresponds to the **play.failed.mpc-link-down** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to Timeout	The total number of announcement requests failed because the external HTTP server times out for a reason other than link failure. This counter corresponds to the **play.failed.timeout** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.

Table 148. MSML Usage Group

Name	Description
Total Failed Announcement Requests due to Speech Server Error	The total number of announcement requests failed while rendering the TTS clip because the external speech server returned an error. This counter corresponds to the **play.failed.speech-server-error** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to HTTP Cache is Disabled	The total number of announcement requests failed because of disabling the HTTP cache. This counter corresponds to the **play.failed.no-http-cache** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to Invalid Announcement File	The total number of announcement requests that failed because of invalid announcement file. This counter corresponds to the **play.failed.invalid-file** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Failed Announcement Requests due to Other Reasons	The total number of announcement requests failed because of other reasons. This counter corresponds to the **play.failed** MSML response that the Containerized Decomposed Media Server generates. This statistic is reset at the beginning of each interval.
Total Create Conference Attempt Requests	The total number of attempted MSML `<createconference>` requests received. This statistic is reset at the beginning of each interval.
Total Successful Create Conference Requests	The total number of successful MSML `<createconference>` requests. This statistic is reset at the beginning of each interval.
Total Failed Create Conference Requests	The total number of failed MSML `<createconference>` requests. This statistic is reset at the beginning of each interval.
Total Join Requests between Port and Conference	The total number of attempted MSML `<join>` requests between port and conference received. This statistic is reset at the beginning of each interval.
Total Successful Join Requests between Port and Conference	The total number of successful MSML `<join>` requests between port and conference. This statistic is reset at the beginning of each interval.
Total Failed Join Requests between Port and Conference	The total number of failed MSML `<join>` requests between port and conference. This statistic is reset at the beginning of each interval.

Statistics - Not Supported

The Containerized Decomposed Media Server does not support the following statistics.

- B2buaUsageGroup
  - B2BUA Dialogs Failed
  - B2BUA Dialogs Received
  - Proxy Dialogs Failed
  - Proxy Dialogs Received
  - Total B2BUA Dialogs Received
  - Total Proxy Dialogs Received

- Ethernet Statistics Group
  - Ethernet RX Errors
  - Ethernet TX Errors
- MIKEY Usage Group
  - MIKEY Error Response Messages Generated
  - MIKEY Initiator Message Authentication Failures
  - MIKEY Initiator Messages Received
  - MIKEY Initiator Messages Rejected to MIKEY Replay Cache
  - MIKEY Response Messages Generated
  - MIKEY Verification Response Messages Generated
- System Usage Group
  - Current Smoothed CPU Utilization
  - Max Smoothed CPU Utilization
  - Level 2 Cache Enabled Time
  - Current Free RAM Drive Space
- Secure RTP Usage Group
  - SRTP Packets with Authentication Failures
  - SRTP Packets Dropped Due to SRTP Replay Cache
- Session Usage Group
  - Dropped External Announcement Streams
  - Dropped External Recording Streams
  - Max G.723 Ports
  - Max G.726 Ports
  - Total number of ILBC transcoding ports
  - Max iLBC Ports
  - Max H.263 Ports
  - Max Mpeg4V Ports
  - Max H.265 Ports
  - CPA Events
  - Current SRTP Ports Allocated
  - Total number of H.263 announcement ports
  - Total number of MPEG-4 announcement ports
  - Total number of H.263 recording ports
  - Total number of MPEG-4 recording ports
  - Total number of H.263 conference ports
  - Total number of MPEG-4 conference ports
  - Total number of H.263 transcoding ports

    - Total number of MPEG-4 transcoding ports
    - Max Active KWD Sessions
- Secure RTCP Usage Group
    - SRTCP Packets with Authentication Failures
    - SRTCP Packets Dropped Due to SRTCP Replay Cache

Codecs

This appendix describes the Containerized Decomposed Media Server support for codecs.

Codec Terminology and Support

The following section provides an overview of some codec terminology and describes the available codecs support for the Containerized Decomposed Media Server functions.

NOTE:

- Comfort Noise with payload type 13 is explained in *Comfort Noise on page 594*.
- The Containerized Decomposed Media Server terminates a multi-clip announcement that starts in bypass and changes the codec type. This is valid for all audio and video codecs.

Audio Codecs

The Containerized Decomposed Media Server supports narrowband and wideband codecs.

- **Narrowband.** Codecs are usually defined as 300 to 3400 Hz with a sample rate of 8 KHz.
- **Wideband.** Codecs are usually defined as 50 to 7000 Hz with a sample rate of 16 KHz.

NOTE: Opus also supports medium band with 12 KHz sample rate, super wideband with 24 KHz sample rate, and fullband at 48 KHz sample rate on incoming Opus streams.

Waveform or Source

Speech codecs generally fall into two main categories: waveform coders and source coders.

Waveform coders are typically simple and have low compression ratios (usually 4 or less). G.711 is a narrowband and G.722 is a wide-band audio waveform codec. Waveform coders try to reproduce a signal waveform without knowledge of the signal's source. These coders, which include a-law, m-law, DPCM, and ADPCM typically encode on a sample-by-sample basis. The frame size for a waveform codec can be any multiple of one sample (A sample is 1 byte or 125 microseconds for µ-law and a-law). However, for computational efficiency, larger frames sizes such as 80 bytes (10 ms) are used.

Source coders are more complicated than waveform codecs and have higher compression ratios (typically 16 or more). Source coders, which include EVRC0, EVRCB0, G.729, and AMR use information about the source of the signal, generally assumed to be speech, to achieve higher compression ratios. Instead of coding the waveform directly, source coders create a model of the source and then send the parameters of the model. The speech model tends to change rather slowly—on the order of about 10 milliseconds—so source coders require at least 10 milliseconds or more of speech before they can begin coding. G.729 has a frame size of 10 bytes (10 ms) and AMR frame sizes vary from a low of 12 bytes for mode 1 to 31 bytes for mode 8. A comfort noise frame is even smaller at 4 bytes. The AMR frame length is 20 ms.

Codec Parameters

The following parameters are used in describing codecs.

- **Sample rate.** The rate at which the media is sampled.
- **Clock rate.** The rate at which time stamps are incremented.
- **Frame size.** The minimum number of samples required before coding can take place.
- **Packetization interval.** The time interval between RTP packets (an integer multiple of the minimum frame size).
- **Bitrate.** The rate at which the RTP packets are transferred.
- **Number of Channels.** The number of channels codec can transmit within a single stream. This is available only in Opus codec.
- **FEC.** The forward error correction. This is available only in Opus codec.
- **CBR/VBR.** The Constant or Variable Bitrate. This is available only in Opus codec.
- **Bandwidth.** The audio bandwidth. This is available only in Opus codec.
- **Silence Suppression.** Reduces the bitrate during silence or background noise.
- **Payload Type ID.** Indicates the RTP Payload types for audio and video codecs.

Video codecs have the following additional parameters.

- **Picture size.** The number of pixels for each picture; for example, CIF (352x288), QCIF (176x144), 4CIF (704x576), 480p (720x480), 720p (1280x720), QVGA (320x240), or VGA (640x480).
- **Minimum picture interval.** The minimum number of frame periods between consecutive pictures.
- **Bitrate.** The number of bits that are processed per unit of time.
- **Profiles.** The targeted specific classes of applications.
- **Levels.** The specified set of constraints that indicate a degree of required decoder performance for a profile.

Functionality

The following features are associated with the Containerized Decomposed Media Server use of codecs.

- *Comfort Noise*
- *DTMF*
- *Packet Loss Concealment*
- *Silence Suppression*
- *Transcode Bypass*

Comfort Noise

Comfort noise (CN) is an estimate of the background noise and is inserted during silence suppression. Comfort noise produces a more natural effect during silence suppression than using pure silence. Codecs that support this feature insert comfort noise during periods when no packets are received. This requires that the codec first receive a comfort noise packet, also known as a Silence Insertion Descriptor (SID). The comfort noise frame contains an estimate of the background noise. It is transmitted immediately upon entering silence suppression and then periodically if the character of the background noise changes.

DTMF

The Containerized Decomposed Media Server provides the following DTMF functions.

- **Generation.** In-band and out-of-band (RFC 2833 and RFC 4733)
- **Detection.** In-band and out-of-band (RFC 2833 and RFC 4733)
- **Clamping.** Removal of in-band DTMF tones once detected rather than filtering DTMF tones. The time to detect can leave a small residual DTMF signal 10 - 25 ms or so.
- **Pass-through.** Relaying DTMF to SIP netann and MSML conference participants. The DTMF digits pass-through are transcoded in SIP netann and MSML conference with the audio and are translated to the correct DTMF type (RFC 2833 or in-band) for each port that receives the audio. The Containerized Decomposed Media Server does not support sending long telephone events and truncate any long events that it sends at the maximum RFC 2833 length of 3 seconds (8 kHz RTP clock), 3 seconds (16 kHz RTP clock), or 1 seconds (48 kHz RTP clock). For regular DTMF Detection, all received events are processed immediately on reception. For DTMF pass-through, the events are buffered and passed through according to each digit duration.

  NOTE:

  - In-band detection and clamping are not very reliable for high compression codecs such as G.729. AMR, AMR-WB, EVRC, EVRCB, or Opus. The Containerized Decomposed Media Server supports buffering a maximum of 30 events. These events can be received in a single packet or in multiple packets.
  - The Containerized Decomposed Media Server ignores telephone events with a zero duration as specified by RFC 4733.

Packet Loss Concealment

Packet Loss Concealment (PLC) can be used to improve the quality of a received RTP stream in the presence of lost packets or excessive jitter. PLC for audio streams consists of predicting the audio in the missing packet based on the previously received audio. Codecs such as G.729, AMR, AMR-WB, EVS, EVRC, EVRCB, and Opus have built-in PLC and it is enabled all the time. It has to be specially enabled for G.711 and G.722 through management interface.

Silence Suppression

The Containerized Decomposed Media Server supports the following methods of silence suppression.

- codec-based silence suppression
- RTP silence suppression

The Containerized Decomposed Media Server performs silence suppression in the encoder for all codecs. Codecs like G.729, EVS, EVRC, EVRCB, AMR, and AMR-WB have built-in silence suppression. G.711 does not have built-in support and require an additional resources for VAD and comfort noise. For G.711 and G.722 codecs, a separate payload type is required for CN and the encoder needs to allocate additional VAD resources. For more information see *Chapter 2, Silence Suppression, on page 40*.

Transcode Bypass

Transcoding allows the Containerized Decomposed Media Server to bridge participants using different codecs and/or different bit rates. Media from a conference participant is automatically transcoded from the original format to the format needed to stream to the other connection. In addition, any clip (for example, an announcement) stored in any of the supported file formats can be played to an endpoint of any codec type. For example, transcoding enables mobile video phones and fixed line video terminals to communicate with one another independent of their respective capabilities (screen size, minimum picture interval, and bit rate).

The Containerized Decomposed Media Server can transcode between all supported audio and video codecs. Transcoding is applied automatically in all audio processing functions for all supported audio unless transcode bypass is enabled through the Containerized Decomposed Media Server management interface. The Containerized Decomposed Media Server supports video port-to-port transcoding between two video ports or between same video codec and other video codec (for example: H.264 constrained baseline profile at level 1.0 to 3.1).

For video codecs (H.264), transcoding and rate matching are supported only for profile/level picture size, bit rate, and only in continuous presence conferencing (including announcements and recordings to a continuous presence conference).

The video component of Voice Activated Switching (VAS) conferencing, VAS port recordings, and VAS announcements is not transcoded; instead, all participants of a VAS conference must use the same video codec and parameters. The text and icon overlay feature transcodes H.264 announcements in order to mix in text and images, but rejects announcements if the codec and picture size do not match those negotiated for the connection.

Transcoding is performed automatically, unless transcode bypass is enabled through the Containerized Decomposed Media Server management interface. Note that transcoding is quite resource-intensive and can affect capacity. In addition, transcoding can degrade the quality of media compressed using the G.729 codec. If audio transcoding is not required for your application, consider disabling it using the transcode bypass feature.

AMR

Adaptive Multi Rate (AMR) is a codec optimized for speech, adapted by 3GPP, and widely used for GSM. It uses Algebraic code excited linear prediction (ACELP), VAD, Discontinuous Transmission (DTX), and CN detection. Containerized Decomposed Media Server supports receiving following AMR payload formats: RFC 4867. The Containerized Decomposed Media Server can receive maximum of 240 ms of packetization interval of AMR packets[1]. But Containerized Decomposed Media Server can only send out AMR packets with 80 ms packetization and no RTP redundancy (RFC 4867 redundancy).

NOTE: The Containerized Decomposed Media Server supports maximum 11 redundancy frames for AMR.

AMR is a narrow-band audio frame (source) codec. RFC 2198 redundancy is supported for up to five redundant frames. RFC 4867 redundancy and RFC 2198 redundancy are mutually exclusive.

Table 149 summarizes AMR parameters.

Table 149. AMR Parameters

Parameter	AMR
A/V	Audio
Bit Rate	12.2, 10.2, 7.95, 7.40, 6.70, 5.90, 5.15, 4.75 kbps
Clock Rate	8 kHz
Frame Size	20 ms
Packetization	20, 40, 60, 80 ms
Payload Type ID	Dynamic
Sample Rate	8 kHz

Supported Functionality

Table 150 summarizes the Containerized Decomposed Media Server functions supported for AMR.

Table 150. AMR Supported Functions

Function	Support
Automatic Gain Control (AGC)	Yes
Announcements/Recordings Format	Yes
Comfort Noise	Yes
Dual Tone Multi Frequency (DTMF)[a]	Yes
fmtp Parameters[b]	Yes
Packet Loss Concealment (PLC)	Yes
Silence Suppression	Built-in
Transcode Bypass[c]	Yes
Transcoding Supported	Yes
Noise Gating (NG)	Yes

1. To support 240 ms packetization jitter size must be equal to or greater than 240 ms.

Table 150. AMR Supported Functions

Function	Support
Noisy-Line Detection (NLD)	Yes
Noise Line Detection (NLD)	Yes
Acoustic Echo Cancellation (AEC)	Yes
Noise Reduction (NR)	Yes

[a] Although in-band DTMF detection is supported, performance is poor and the success rate is lower than other codecs. Telephone events (RFC 2833) is the recommend DTMF type for this codec.

[b] See the SDP section of the Containerized Decomposed Media Server protocol guide.

[c] Note that when an AMR announcement is being played with transcode bypass enabled, the transmitted frame types are determined by the announcement file.

RFC 4867 Support

Table 151 summarizes the Containerized Decomposed Media Server support for RFC 4867.

Table 151. RFC 4867 Support

RFC4867		Containerized Decomposed Media Server Support	
Feature	**Specification**	**Receive**	**Transmit**
Bandwidth Efficient Mode	Required	Yes	Yes
Octet Aligned Mode	Required	Yes	Yes
Codec Mode Request (CMR)	Required for receive	Yes	Yes. Always uses 15 (no mode change).
Interleaving	Optional	—	—
Frame CRC	Optional	—	—
Robust Sort Ordering	Optional	—	—
Redundant Frames	Required[a]	Yes	—
Multiple Channels	Optional	—	—
Unequal Error Protection (UEP)/ Unequal Error Detection (UED)	Optional	—	—
RTP Marker bit (M) for start of speech	Required[b]	Yes	—
Forward Error Correction (FEC)	Optional	—	—

[a] Use first frame received. (***NOTE***: RFC 4867 recommends using the highest mode received but redundant frames are typically the same mode.)

[b] Supported as define in RFC 3550.

Usage Guidelines

The Containerized Decomposed Media Server supports mid-call codec change from wideband to narrowband or from narrowband to wideband.

AMR-WB

Adaptive Multi-Rate Wide-Band (AMR-WB) is a codec optimized for speech, adapted by 3GPP, and widely used for GSM. It makes use of ACELP, VAD, DTX, and CN detection based on the specifications of RFC 4867. Containerized Decomposed Media Server can receive up to 240 ms of packetization interval of AMR-WB packets[1]. But Containerized Decomposed Media Server can only send out AMR-WB packets with 80 ms packetization and no RTP redundancy (RFC 4867 redundancy).

The Containerized Decomposed Media Server supports receiving AMR or AMR-WB packets containing up to 80 ms of primary media regardless of the negotiation of the time parameter or the setting of the OAMP packetization value.

NOTE: The Containerized Decomposed Media Server supports maximum 11 redundancy frames for AMR.

AMR-WB is a wide-band audio frame (source) codec. RFC 2198 redundancy is supported for up to 5 levels. RFC 2198 redundancy and RFC 4867 redundancy are mutually exclusive.

Table 152 summarizes AMR-WB parameters.

Table 152. AMR-WB Parameters

Parameter	AMR-WB
A/V	Audio
Bit Rate	6.60, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05 and 23.85 kbps
Clock Rate	16 kHz
Frame Size	20 ms
Packetization	20, 40, 60, 80 ms
Payload Type ID	Dynamic
Sample Rate	16 kHz

Supported Functionality

Table 153 summarizes the Containerized Decomposed Media Server functions supported for AMR-WB.

Table 153. AMR-WB Supported Functions

Function	Support
AGC	Yes
Announcements/Recordings Format	Yes
Comfort Noise	Yes
DTMF[a]	Yes
fmtp Parameters[b]	Yes
PLC	Yes
Silence Suppression	Yes, Built-in.
Transcode Bypass[c]	Yes

1. To support 240 ms packetization jitter size must be equal to or greater than 240 ms.

Table 153. AMR-WB Supported Functions

Function	Support
Transcoding Supported	Yes
NG	Yes
NLD	Yes
AEC	Yes
NR	Yes

[a] Although in-band DTMF detection is supported, performance is poor and the success rate is lower than other codecs.

[b] See the SDP section of your Containerized Decomposed Media Server protocol guide.

[c] Note that when an AMR announcement is being played with transcode bypass enabled, the transmitted frame types are determined by the announcement file.

EVRC, EVRCB, and EVRC-NW

Enhanced Variable Rate Coder (EVRC) is a real-time implementation of the 3GPP2 standardized vocoder. EVRC audio codec is widely used for cellular telephony in CDMA networks and VoIP applications. Following are the versions of the EVRC codec family as defined by the 3GPP2 and supported by the Containerized Decomposed Media Server.

- Original EVRC codec (also referred as EVRC-A)
- Improved higher quality, higher complexity codec (EVRC-B)
- EVRC Narrowband and Wideband version (EVRC-NW)

EVRC and EVRC-B are narrowband audio frame (source) codecs whereas EVRC-NW negotiates both narrowband and wideband audio frame (source) codecs.

The Containerized Decomposed Media Server supports the original EVRC (EVRC-A), EVRC-B, and EVRC-NW codecs as defined in the 3GPP2 C.S0014 v3.0 and the RFC 4788.

- The Containerized Decomposed Media Server supports the EVRC-A codec, as per the 3GPP2 C.S0014-A service option 3, and header free format with codec mode name EVRC0 as defined in the RFC 3558.
- The Containerized Decomposed Media Server supports the EVRC-B codec, as per the 3GPP2 C.S0014-B service option 68, and header free format with codec mode name EVRCB0 as defined in the RFC 5188 and RFC 3558.
- The Containerized Decomposed Media Server supports the EVRC-NW codec, as per the 3GPP2 C.S0014-D service option 73, and header free format with codec mode name EVRCNW0 as defined in the RFC 6884 and RFC 3558.

Table 154 summarizes the EVRC codec family parameters supported by the Containerized Decomposed Media Server.

Table 154. EVRC Parameters

Parameter	Support
A/V	Audio
Codec version	As per the 3GPP2 C.S0014 v3.0. The individual speech Service Options (SO) are. • EVRC: 3GPP2 C.S0014-A SO3 • EVRC-B: 3GPP2 C.S0014-B SO68 • EVRC-NW: 3GPP2 C.S0014-D SO73
Codec Mode	• Header Free format: EVRC0, EVRCB0, and EVRCNW0 • Interleaved or Bundled format: EVRC, EVRCB, and EVRCNW
Bandwidth	• Narrowband • Wideband ***NOTE:*** The Containerized Decomposed Media Server considers EVRC-NW mode 0 and EVRC-NW0 mode 0 as wideband codec regardless of whether a narrowband or wideband mode is negotiated. For more information, refer to the Table 160.
Bit Rate	Variable Supports a maximum of 8.55 kbps
Channel	Mono
Clock Rate	• EVRC, EVRC-B: 8,000 Hz • EVRC-NW: 16,000 Hz
Frame Size	20 ms
Packetization	• 20 when negotiating in header free format. For example, EVRC0, EVRCB0, and EVRCNW0 • 20, 40, 60, and 80 ms when negotiating in interleaved or bundled format. For example, EVRC, EVRCB, and EVRCNW
Payload Type ID	Dynamic (96-127)

Supported Functionality

Table 155 summarizes the Containerized Decomposed Media Server functions supported for EVRC codec family.

Table 155. EVRC Supported Functions

Function	Support
AGC	Yes
Announcements/Recordings Format	Announcements only ***NOTE:*** The EVRC-NW codec does not support 3G2 file format presently. Hence, the Containerized Decomposed Media Server does not support 3G2 announcement clips format for EVRC-NW codec.
Announcement Bypass	Yes ***NOTE:*** • The Containerized Decomposed Media Server does not support codec bypass of EVRC-B 3G2 clips to an EVRC-NW port. • When an announcement is being played with transcode bypass enabled, the transmitted frame types are determined by the announcement file.

Table 155. EVRC Supported Functions

Function	Support
Discontinuous Transmission (DTX)	Yes, in-built DTX
DTMF[a]	Yes
fmtp Parameters	Yes. Refer to the *SIP Interface Reference*.
PLC	Yes
Silence Suppression	Yes
Voice Quality Enhancing (VQE)	Yes, except R-factor.

[a] Although in-band DTMF detection is supported, performance is poor and the success rate is lower than other codecs.

RFC Support

The RFC 3558 defines the header-free and interleaved/bundled formats supported for EVRC. The RFC 4788, RFC 5188 adds support for EVRCB whereas the RFC 6884 adds support for EVRC-NW codec.

EVRC supports full rate, half rate, and eighth rate, as shown in Table 157. Quarter-rate frames are used only with EVRC-B. Blank and erasure frames are not transmitted over RTP. Erasure frames are used internally by the decoder to indicate frames lost in transmission. Blank frames are used internally by the encoder during silence suppression.

EVRC codec family supports full rate (1), half rate (1/2), and eighth rate (1/8), as shown in Table 157. Quarter-rate (1/4) frames are used only with EVRC-B. Blank and erasure frames are not transmitted over RTP. Erasure frames are used internally by the decoder to indicate frames lost in transmission. Blank frames are used internally by the encoder during silence suppression.

EVRC has several codec-specific profiles defined in RFC 4788: EVRC, EVRC0. The Containerized Decomposed Media Server supports both header-free (EVRC0, EVRCB0, EVRCNW0) and interleaved or bundled (EVRC, EVRCB, EVRCNW) formats. Mode negotiation is not supported by the Containerized Decomposed Media Server because it is configurable through the management interface.

Table 156. EVRC Family Formats

Format	Header	Multiple Frames (Bundling)	Mode Requests	Interleaving	SDP CodecNames
Header Free	No	No	No	No	EVRC0 EVRCB0 EVRCNW0
Interleaved/Bundled	Yes	Yes	Yes	No	EVRC EVRCB EVRCNW

The EVRC header-free format is the simplest format and contains single frame only. In the header-free format, the RTP payload consists of a single 20-millisecond EVRC frame of type 4, 3, or 1, as defined in the Table 155, and 4 modes defined in the Table 157.

Table 157 lists the bit rates of EVRC frame types.

Table 157. EVRC Frame Types

Frame Type (ToC)	Rate	Frame Size
0	Blank (Null)	0 bit (not transmitted)
1	Eighth rate (1/8)	2 bytes (16 bits)
2	Quarter rate (1/4)	5 bytes (40 bits) ***NOTE:*** Applicable for EVRC-B and EVRC-NW only.
3	Half rate (1/2)	10 bytes (80 bits)
4	Full rate (1)	22 bytes (171 bits; 5 padded at end with zeros)
5	Erasure	0 bit (not transmitted)

The EVRC interleaved/bundled format contains a header with a mode request and Table of Contents (ToC) containing the frame type for each frame in the packet.

Operating Modes

The EVRC (also known as EVRC-A) codec has five defined modes and two non-variable modes.

Table 158. EVRC Operating Modes

Mode	Fraction of Rate 1	Packets Set to	Mode Description
	Rate 1	Rate 1/2	
Rate Reduction Mode 0	1	0	Rate is set solely by the encoder to 1 frame.
Rate Reduction Mode 1	3/4	1/4	Changes 25% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 2	1/2	1/2	Changes 50% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 3	1/4	3/4	Changes 75% of the rate 1 frames to rate 1/2.
Rate Reduction Mode 4	0	1	Changes all of the rate 1 frames to rate 1/2.
Non-Variable Modes:			
Fixed Full Rate	—	—	Radisys proprietary non-variable full rate.
Fixed Half Rate	—	—	Radisys proprietary non-variable half rate.

The EVRC-B codec has eighth defined modes and two non-variable modes.

Table 159. EVRC-B Operating Modes

Mode	Average Source Encoding bit-rate [kbps]	Mode Description
Rate Reduction Mode 0	8.3	No quarter rate frames.
Rate Reduction Mode 1	7.57	
Rate Reduction Mode 2	6.64	
Rate Reduction Mode 3	6.18	
Rate Reduction Mode 4	5.82	
Rate Reduction Mode 5	5.45	
Rate Reduction Mode 6	5.08	
Rate Reduction Mode 7	4.0	Half rate max, no quarter rate frames
Non-Variable Modes:		
Fixed Full Rate 8	8.8	Non-variable full rate
Fixed Half Rate 9	4.0	Non-variable half rate

The EVRC-NW codec has eighth defined modes.

Table 160. EVRC-NW Operating Modes

Mode	Average Source Encoding bit-rate [kbps]	Compatible Mode	Mode Description
Rate Reduction Mode 0	7.5		Mode 0 is wideband mode only.
Rate Reduction Mode 1	8.3	0	
Rate Reduction Mode 2	6.64	2	
Rate Reduction Mode 3	6.18	3	
Rate Reduction Mode 4	5.82	4	
Rate Reduction Mode 5	5.45	5	
Rate Reduction Mode 6	5.08	6	
Rate Reduction Mode 7	4.0	7	Half rate max

Usage Guidelines

The Containerized Decomposed Media Server supports all audio features on EVRC, EVRC-B, and EVRC-NW RTP ports for all service contexts.

The Containerized Decomposed Media Server supports transcode bypass when playing EVRC 3G2 clips to a header-free or interleaved or bundled format on EVRC port. Only the 3GPP2 container file format is supported and the file extension must be **.3g2** (case-insensitive). The Containerized Decomposed Media Server does not support the **evrc** file format as defined in the RFC 4788.

The Containerized Decomposed Media Server supports TTY and DTMF features of EVRC decoders and does not support optional TTY, noise reduction, signaling, and DTMF features of EVRC, EVRC-B, and EVRC-NW encoders.

The Containerized Decomposed Media Server negotiates the SDP parameters (silencesupp, dtxmax, dtxmin, and hangover) for silence suppression as per the RFC 4788 for both header-free and interleaved/bundled formats on EVRC, EVRC-NW, and EVRC-B ports. For EVRC and EVRC-B codecs, the SDP clock rate is 8 kHz and for EVRC-NW, the SDP clock rate is 16 kHz. The Containerized Decomposed Media Server can play external NFS or internal EVRC announcements to connections or conferences through the MSML 1.1 interface. EVRC announcements can be audio-only, video-only, or multimedia. As with other codecs, the use of EVRC is enabled or disabled by configuring the preferred codec list using the management interface.

EVS

Enhanced Voice Services (EVS) a multi-rate audio codec which is also referred as Full HD Voice. The EVS audio codec is designed for VoIP applications, standardized by 3GPP, and optimized for VoLTE (as per IR.92 specification). The EVS codec provides enhanced audio experience and higher speech coding efficiency for narrowband, wideband, and super wideband speech services. The EVS codec can seamlessly switch between speech and music codecs as per the incoming signal and also provide enhanced quality for mixed content and music in conversational applications; for example, in-call music. EVS provides improved compression efficiency at all rates and improved audio quality over AMR-NB and AMR-WB at similar rates. EVS also has backward compatibility to AMR-WB and enables seamless integration of EVS into existing AMR-WB services.

The Containerized Decomposed Media Server supports the following EVS codec features.

- **Primary mode.** EVS Primary Mode has 11 fixed bit rates, one variable bitrate, and the Containerized Decomposed Media Server supports NB, WB, and SWB bandwidths. EVS codec supports a large bit rate range starting from 5.9 to 128 kbps. Source controlled variable rate mode (SC-VBR) switches between the fixed bitrates of 7.2 and 8.0 kbps and a special lower bitrate of 2.8 kbps used to achieve an average bitrate of 5.9 kbps. In Containerized Decomposed Media Server, the EVS Channel aware mode (13.2 kbps, wideband and SWB) is supported for both ingress and egress directions. Channel aware mode adds redundancy to the EVS frames and reduces packet loss at the receiver end. When either SWB or NB-SWB are negotiated for send or receive direction, the Containerized Decomposed Media Server treats the stream as SWB in that direction.

  NOTE: An EVS port is considered a SWB port, if the SDP negotiated send or receive bandwidth is SWB or NB-SWB, otherwise the EVS port is considered as a wideband port.

- **AMR-WB IO (inter-operable) mode.** EVS AMR-WB IO (inter-operable) mode is compatible with AMR-WB and includes all 9 AMR-WB bitrates (including AMR-WB SID frames) ranging from 6.6 to 23.85 kbps.

  NOTE: Although EVS AMR-WB IO mode has backward compatibility with AMR-WB codec, the RTP bit stream is not compatible and is formatted using the EVS format rather than RFC 4867. The Containerized Decomposed Media Server negotiates with AMR-WB codec when AMR-WB RTP compatibility is required.

The EVS codec can start either Primary or AMR-WB IO mode and switches between the modes at any time. The Containerized Decomposed Media Server supports both the modes and an `evs-mode-switch` parameter is used to determine the initial mode. Both EVS Primary and AMR-WB IO mode supports silence suppression with Voice Activity Detection (VAD), Discontinuous Transmission (DTX), and Comfort Noise Generation (CNG) through Silence Insertion Descriptors (SID) frames. Silence suppression for EVS operates in variable and fixed bitrate modes. For bitrates below 24.4 kbps, the transmission is stopped during silent intervals. For bitrates above 24.4 kbps, EVS uses a less aggressive mode by sending SID frames during silent intervals. This is because EVS functions like any other speech codec at lower bitrates but changes operation at higher bitrates, which would typically be used for higher quality operation.

The Containerized Decomposed Media Server supports all VQE features (NR, NG, NLD, AEC except R-Factor) for EVS NB, EVS WB, and EVS AMR-WB IO ports. However, the Containerized Decomposed Media Server does not support VQE features for EVS SWB ports.

The following table summarizes the EVS parameters supported by Containerized Decomposed Media Server.

Parameters	Support
A/V	Audio
Codec version	Floating point version 14.0.0 (3GPP TS 26.443).
Mode	EVS Primary mode and AMR-WB IO mode
Bandwidth	• Narrowband (NB): 4 kHz • Wideband (WB): 8 kHz • NB-WB (Only for EVS Primary mode) • Super Wideband (SWB): 16 kHz • NB-SWB

Bit Rate	• Primary mode
	  • Fixed Bitrate: 7.2, 8.0, 9.6, 13.2, 13.2 (with Channel Aware), 16.4, 24.4, 32.0, 48.0, 64.0, 96.0, 128.0 kbps
	  • Variable Bitrate: 5.9 kbps
	  NOTE:
	  • EVS Primary mode supports narrowband (up to 24.4 kbps), wideband (up to 128.0 kbps), and super wideband (up to 128.0 kbps).
	  • Super wideband supports at a minimum bitrate of 9.6 kbps.
	• AMR-WB IO mode
	  • Fixed Bitrate: 6.6, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05, 23.85 kbps
	For RX and TX, the supported Bitrate is a maximum of 128 kbps.
	NOTE: The appropriate bitrate range is supported as per the negotiated bandwidth. If no bandwidths are compatible then the Containerized Decomposed Media Server lowers the bitrate before negotiation. If no bitrates and bandwidths are compatible then the Containerized Decomposed Media Server rejects the offer.

Channel	Mono (for TX and RX)
RTP Clock Rate	16000
Frame Size	20 ms
Packetization	20, 40, 60, and 80 ms The default packetization interval is 20 ms.
Payload Type ID	Dynamic (0-127)
Sample Rate	• Narrowband (NB): 8 kHz • Wideband (WB): 16 kHz • Super Wideband (SWB): 32 kHz For RX and TX, the supported sampling rate is 8, 16 and 32 kHz.

Supported Functionality

The following table summarizes the functions supported by Containerized Decomposed Media Server.

Functions	Support
Announcements/Recordings Format	Yes, the Containerized Decomposed Media Server supports playback of EVS announcement clips for all services. EVS recording is not supported.
Announcement Bypass	Yes, when clip and port properties are matched, EVS announcement gets transcode bypassed. The Containerized Decomposed Media Server supports playback of AMR-WB clips over EVS port
Channel Aware Mode	Yes, the Containerized Decomposed Media Server continues to encode channel aware FEC data in the egress direction irrespective of whether EVS JBM is enabled or disabled, based on the user channel aware Forward Error Correction (FEC) offset preference.
Comfort Noise Generation (CNG)	Yes
Discontinuous Transmission (DTX)	Yes
DTMF[a]	Yes
fmtp Parameters	Yes, Optional. The Containerized Decomposed Media Server receives both compact and header-full EVS packets regardless of the fmtp parameter value. For more information, refer to *Chapter 6: SDP Profile* in the *SIP Interface Reference*.
Jitter Buffer Management (JBM)	Yes. EVS JBM as per 3GPP TS 26.448.
Silence Suppression	Yes
PLC	Yes
Voice Activity Detection (VAD)	Yes
Voice Quality Enhancing (VQE)	Yes (except R-factor). However, VQE for super wideband is not supported.

[a] EVS is unreliable for in-band DTMF at low bitrates.

NOTE: In a multi-clip transcode bypass announcement, there is a possibility of hearing a glitch (less than 20 ms) on the user end when the announcement transitions from one clip to the other clip. During transition, the EVS stream packets core-type information (for example ACELP, TCX, HQ-MDCT, and so on) of the first frame of a new announcement clip cannot match with the core-type information of the last frame of the previous announcement clip. This may cause the decoder to momentarily produce a glitch. To avoid this glitch, you may use transcode announcement instead of bypass announcement.

The Containerized Decomposed Media Server supports the EVS codec in all SIP service contexts. Table 161 provides supported EVS features in the service contexts:

Table 161. EVS Codec Features Versus Service Contexts

Media Feature	SIP Netann Announcement (sip:annc)	SIP Netann Conference (sip:conf)	SIP/MSML (sip:msml)	SIP Conf (sip:conf)	SIP IVR (sip:ivr)	SIP/VXML (sip:dialog)
Audio port-to-port transcoding	NA	NA	Y	NA	NA	NA
Audio announcement	Y	NA	Y	Y	Y	Y
Audio conference	NA	Y	Y	Y	Y	NA
Audio recording	NA	NA	NA	NA	NA	NA
Audio RTP relay	NA	NA	NA	NA	NA	NA
AEC (EVS NB, EVS WB, and EVS AMR-WB I/O ports)	NA	Y	Y	Y	Y	NA
NR (EVS NB, EVS WB, and EVS AMR-WB I/O ports)	NA	Y	Y	Y	Y	Y
NG (EVS NB, EVS WB, and EVS AMR-WB I/O ports)	NA	Y	Y	Y	Y	Y
NLD (EVS NB, EVS WB, and EVS AMR-WB I/O ports)	NA	NA	Y	NA	NA	NA
PLC	NA	Y	Y	Y	Y	Y
DTMF detection and generation	NA	NA	Y[a]	Y	Y	Y
DTMF Pass-through	NA	Y	NA	Y	Y	NA
AGC	NA	NA	NA	NA	NA	NA
Silence Suppression	Y	Y	Y	Y	Y	Y
Fax tone (CED and CEG) detection	NA	NA	Y	NA	NA	Y
ASR/TTS	NA	NA	Y	NA	NA	Y
CPA/AMD	NA	NA	Y	NA	NA	NA
Sets and Variables	NA	NA	Y	Y	Y	Y

[a] In-band DTMF detection and generation is supported in EVS codec. But it is not reliable for lower EVS bitrates.

G.711

G.711 codecs are based on the ITU-T Recommendation G.711 for Pulse Code Modulation (PCM) of Voice Frequencies. G.711 includes two similar codecs:

- µ-law (PCMU)
- a-law (PCMA)

G.711 is a narrow-band audio waveform codec. It also supports dynamic payload type.

Table 162 summarizes G.711 µ-law parameters.

Table 162. G.711 µ-law Parameters

Parameter	G.711 µ-law
A/V	Audio
Bit Rate	64 kbps
Clock Rate	8 kHz
Minimum Frame Size	1 sample
Packetization	5, 10, 20, 30, 40, 50 ms
Payload Type ID	Dynamic
Sample Rate	8 kHz

Table 163 summarizes G.711 a-law parameters.

Table 163. G.711 a-law Parameters

Parameter	G.711 a-law
A/V	Audio
Bit Rate	64 kbps
Clock Rate	8 kHz
Packetization	5, 10, 20, 30, 40, 50 ms
Payload Type ID	Dynamic
Sample Rate	8 kHz

Supported Functionality

Table 164 summarizes the Containerized Decomposed Media Server functions supported for G.711.

Table 164. G.711 Supported Functions

Function	Support
AGC	Yes
Announcements/Recordings Format	Yes
Comfort Noise[a]	The Containerized Decomposed Media Server supports G.711 Appendix 2
DTMF	Yes
fmtp Parameters	Yes
PLC[b]	The Containerized Decomposed Media Server supports G.711 Appendix 1.
Silence Suppression[c]	Yes

Table 164. G.711 Supported Functions

Function	Support
Transcode Bypass	Yes
NG	Yes
NLD	Yes
AEC	Yes
NR	Yes

[a] Comfort Noise is negotiated separately and requires additional resources (VAD).

[b] You can configure this function using the Containerized Decomposed Media Server Web GUI or SNMP and requires additional resources (VAD).

[c] Silence suppression is not built-in and requires additional resources (VAD).

Usage Guidelines

The Containerized Decomposed Media Server supports mid-call codec change from wideband to narrowband or from narrowband to wideband.

G.722

The G.722 codec is based on the ITU-T Recommendation G.722 7 kHz Audio Coding within 64kb/s. This codec uses Adaptive Differential Pulse-Code Modulation (ADPCM) for data sampled at 16 kHz for superior audio quality to narrowband codecs.

G.722 is a wide-band audio waveform codec. It also supports dynamic payload type. G.722 has a 16 kHz sample rate but uses an 8 kHz RTP timestamp clock.

Table 165 summarizes the G.722 codec parameters.

Table 165. G.722 Parameters

Parameter	G.722
A/V	Audio
Bit Rate	64 kbps
Clock Rate	16 kHz
Minimum Frame Size	1 sample (62.5 microseconds), 5 ms frames (internal)
Packetization	5,10, 20, 30, 40, 50 ms
Payload Type ID	Dynamic
Sample Rate	16 kHz

Supported Functionality

Table 166 summarizes the Containerized Decomposed Media Server functions supported for the G.722 codec.

Table 166. G.722 Supported Functions

Function	Support
AGC	Yes
VQE	Yes
Announcements/Recordings Format	No
Comfort Noise	Yes
DTMF	Yes
fmtp Parameters	No
PLC[a]	Yes, the Containerized Decomposed Media Server supports ITU G.722 Appendix IV.
Silence Suppression	Yes (receive only).
NG	Yes
NLD	Yes
AEC	Yes
NR	Yes
R-factor	Yes

[a] The Containerized Decomposed Media Server supports G.722 PLC for all the protocols and service contexts except transcode bypass.

Usage Guidelines

The Containerized Decomposed Media Server supports mid-call codec change from wideband to narrowband or from narrowband to wideband.

G.729

The G.729 codec is based on the ITU-T Recommendation G.729 Coding of Speech at 8 kb/s using Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP). This codec is designed to use a data derived from an analog signal filtered as per recommendation G.712, sampled at 8 kHz, and converted to 16-bit linear PCM.

G.729 is a narrow-band audio frame (source) codec. It also supports dynamic payload type.

The Containerized Decomposed Media Server supports Annexes A and B. Annex C defines a floating point implementation of G.729 which is compatible with the fixed point implementation defined in the main standard. In the Containerized Decomposed Media Server it is a fixed point implementation of G.729 A and B, but it is compatible with Annex C. Annex A is complexity reduced from the main G.729 specification (and so has slightly poorer audio quality). Annex B specifies the silence suppression (dtx) and comfort noise generation (cng).

Table 167 summarizes the G.729 codec parameters.

Table 167. G.729 Parameters

Parameter	G.729
A/V	Audio
Bit Rate	8 kbps
Clock Rate	8 kHz
Minimum Frame Size	10 ms
Packetization	10, 20, 30, 40, 50 ms
Payload Type ID	Dynamic
Sample Rate	8 kHz

Supported Functionality

Table 168 summarizes the Containerized Decomposed Media Server functions supported for the G.729 codec.

Table 168. G.729 Supported Functions

Function	Support
AGC	Yes
Announcements/Recordings Format	Yes
Comfort Noise[a]	Yes
DTMF[b]	Yes
fmtp Parameters[c]	Yes
PLC	Yes
Silence Suppression[d]	Yes
Transcode Bypass	Yes
NG	Yes
NLD	Yes
AEC	Yes
NR	Yes

[a] Reception is always supported; generation is supported for Annex B. Silence suppression must be enabled as well.

[b] Although in-band DTMF detection is supported, performance is poor and the success rate is lower than other codecs.

[c] See the SDP section of the Containerized Decomposed Media Server protocol guide.

[d] The Containerized Decomposed Media Server supports Annex B silence suppression. G.729 always uses the built-in annex b silence suppression even when Annex B is not negotiated. In this case, it does not send the comfort noise packets.

Usage Guidelines

The Containerized Decomposed Media Server supports mid-call codec change from wideband to narrowband or from narrowband to wideband.

Opus

Opus is a lossy audio compression format developed by IETF and made especially suitable for interactive real-time applications over the Internet. The WebRTC client supports Opus codec. Table 169 summarizes the Opus parameters.

Table 169. Opus Support

RFC 6716 Features	Opus
A/V	Audio
Bit Rate	Constant and Variable Bit Rate
Channels	Mono and Stereo[a]
Sample Rate	• NB - 8 kHz • MB - 12 kHz • WB - 16 kHz • SWB - 24 kHz • FB - 48 kHz
Payload Type ID	Dynamic
Bitrates	6 kbps to 510 kbps
Frame size	5, 10, and 20 ms
Packetization	20 ms
Bandwidth[b]	• NB - 4 kHz • MB - 6 kHz • WB - 8 kHz • SWB - 12 kHz • FB - 20 kHz

[a] Stereo channel is only supported for receiving and is mixed to mono for using in the Containerized Decomposed Media Server.

[b] The Containerized Decomposed Media Server supports receiving any of NB, MB, WB, SWB, or FB. For sending, Containerized Decomposed Media Server sample rate converts to either NB or WB: below 16kHz, sample rate 8kHz is used; 16kHz or above, Containerized Decomposed Media Server uses 16kHz sample rate.

NOTE: It is recommended that the Opus ports are negotiated with RFC 2833 for DTMF events.

Supported Functionality

Table 170 summarizes the Containerized Decomposed Media Server functions supported for the Opus.

Table 170. Opus Supported Functions

Functions	Support
Codec version	1.1
Mode	RX: SILK-only | CELT-only | Hybrid TX: SILK-only | CELT-only
Sampling rate	RX: 8000 | 12000 | 16000 | 24000 | 48000 Hz TX: 8000 | 16000 Hz

Table 170. Opus Supported Functions

Functions	Support
Channel number	RX: stereo | mono TX: mono
Bitrate	RX: 6-510 kbps TX: 8-12 kbps (for NB port) or 16-20 kbps (for WB port)
Bitrate operation mode	VBR | CBR
Packetization	20 ms
Frame size	RX: 5 | 10 | 20 ms TX: 20 ms
DTX	Yes
PLC	Yes
NLD	Yes
NR	Yes
AEC	Yes
In-band FEC[a]	No

[a] The Containerized Decomposed Media Server supports receiving an Opus stream with FEC, however FEC is ignored.

Table 171 provides supported Opus features in the service contexts.

Table 171. Opus Codec Features Versus Service Contexts

Media Feature	SIP Netann Announcement (sip:annc)	SIP Netann Conference (sip:conf)	SIP/MSML (sip:msml)	SIP/VXML (sip:dialog)
Audio port-to-port transcoding	NA	NA	Y	NA
Audio announcement	Y	NA	Y	Y
Audio conference	NA	Y	Y	NA
Audio recording	NA	NA	Y	Y
Audio RTP relay	NA	NA	NA	NA
AEC	NA	Y	Y	NA
NR	NA	Y	Y	Y
NG	NA	Y	Y	Y
NLD	NA	NA	Y	NA
PLC	NA	Y	Y	Y
DTMF detection and generation	NA	NA	Y	Y
DTMF Pass-through	NA	Y	Y	NA
AGC	NA	NA	Y	NA
Silence Suppression	Y	Y	Y	Y
tone (CED and CEG) detection	NA	NA	Y	Y
ASR/TTS	NA	NA	Y	Y
CPA/AMD	NA	NA	Y	NA

Mid-call Audio Codec Change

The Containerized Decomposed Media Server supports mid-call audio codec change between a narrowband and wideband codec in all service contexts such as VXML, SIP netann, and MSML.

The Containerized Decomposed Media Server supports all VQE features for narrowband and wideband ports on VQE supported codecs. The Containerized Decomposed Media Server supports mid-call change between narrowband and wideband codecs for a port with VQE features enabled as long as the sufficient resources are available for the mid-call change. If the AEC and/or NR features are enabled in the management interface, the Containerized Decomposed Media Server enables the AEC/NR features on the audio ports, after changing the codec type from wideband to narrowband or narrowband to wideband during the mid-call.

The Containerized Decomposed Media Server renegotiates the silence suppression and PLC features during the mid-call codec change, depending on the new codec type and management interface setting, after the mid-call change.

NOTE: PLC is supported for G.711 or G.722 codec and by default disabled in management interface. For G.711 or G.722, PLC should be enabled only if it is enabled in the management interface. For other codecs, PLC is a codec built-in feature and should be always enabled.

The following media processing features are enabled or disabled on the audio port:

- Noise Gating
- DTMF Pass-through
- Automatic Gain Control (AGC)

H.264

H.264 is a video codec based on the ITU-T Recommendation H.264 Advanced Video Coding for Generic Audiovisual Services. This codec was developed in response to the growing need for higher compression. It is also known as MPEG-4 ISO Part 10.

H.264 levels place restrictions on buffer memory, bit rate, decoded frame size, processing rate in macroblocks per second, number of video objects, and so on.

For H.264 codec, the Containerized Decomposed Media Server supports constrained baseline profile only. However, the Containerized Decomposed Media Server accepts either baseline or Constrained baseline in the offer, but returns constrained baseline in the answer. The constrained baseline profile supports almost all the baseline profile features except error resilience feature. The Containerized Decomposed Media Server supports Constrained baseline profile when sending SDP (offer/answer) and I-frame (SPS) for H.264 codec. It supports Constrained baseline profile level 1, 1b, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1 H.264 RTP formatted in accordance with RFC 6184 (previously RFC 3984) with packetization-mode 0 and 1.

H.264 supports packetization modes 0 and 1. H.264 packetization modes are part of the RTP formatting. Mode 0 requires that H.264 NAL Units (Network Abstraction Layer) be sent in separate single NAL unit packets. Mode 1 permits single NAL unit packet as well as fragmenting NAL units across multiple packets or aggregating multiply NAL units to a single packet. The Containerized Decomposed Media Server supports receiving all three packet types but sending only the first 2.

H.264 supports other profiles, such as main or high profile, but the standard requires that all terminals support the constrained baseline. Similarly terminals may support modes other than 0 and 1 but RFC 6184 requires support of mode 0.

Table 172 summarizes the H.264 codec parameters.

Table 172. H.264 Parameters

Parameter	H.264
A/V	Video
Clock Rate	90 KHz
Profile	Constrained Baseline
Level	1, 1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1.
Bandwidth	20-4000
Payload Type ID	Dynamic
Picture Size[a]	Upto 720p based on the levels
Video Bit Rates	Upto 4000 kbps
Video Encoder Bitrate Mode	Constant bit rate (CBR)[b]

[a] The support of the picture size is based on levels. The level specifies the maximum number of macroblocks (MBs). For example, for level 3, 396 MBs (16x16 pixels) are supported. Based on your requirement, you can arrange 396 MBs to give CIF (352x288) or 288x352 or 340x240, or QCIF (176*144). Anything up to including the maximum number of MBs is supported by a level.

[b] When creating H.264 encoder on Containerized Decomposed Media Server, the Containerized Decomposed Media Server sets video encoder bitrate mode to CBR.

Table 173 indicates H.264 codec levels.

Table 173. H.264 Codec Parameters

H.264 Level	Maximum Frame Rate MB/s	Maximum Resolution	Maximum Media Bandwidth kbps	Typical Picture Sizes and Maximum Frame Rate	HC Video
1	1485	99	64	sQCIF 128x96 30.9 fps QCIF 176x144 15 fps	No
1b	1485	99	128	sQCIF 128x96 30.9 fps QCIF 176x144 15 fps	No
1.1	3000	396	192	QCIF 176x144 30.3 fps QVGA 320x240 10 fps CIF 352x288 7.5 fps	No
1.2	6000	396	384	QVGA 320x240 20 fps CIF 352x288 15.2 fps	No
1.3	11880	396	768	QVGA 320x240 36 fps CIF 352x288 30 fps	No

Table 173. H.264 Codec Parameters

H.264 Level	Maximum Frame Rate MB/s	Maximum Resolution	Maximum Media Bandwidth kbps	Typical Picture Sizes and Maximum Frame Rate	HC Video
2	11880	396	2000	QVGA 320x240 36 fps CIF 352x288 30 fps	No
2.1	19800	792	4000	HHR NTSC 352x480 30 fps HHR PAL 352x576 25 fps	Yes
2.2	20250	1620	4000	HHR NTSC 352x480 30.7 fps HHR PAL 352x576 25.6 fps D1 NTSC 720x480 15 fps D1 PAL 720x576 12.5 fps 4CIF 704x576 12.8 fps	Yes
3	40500	1620	4000	D1 NTSC 720x480 30 fps D1 PAL 720x576 25 fps 4CIF 704x576 25.6 fps	Yes
3.1	108000	3600	4000	720p30 1280x720 30 fps	Yes

Supported Functionality

Table 174 summarizes the Containerized Decomposed Media Server functions supported for the H.264 codec.

Table 174. H.264 Supported Functions

Function	Support
Announcements/Recordings Format	Yes
Continuous Presence Conference	Yes
fmtp Parameters[a]	Yes
Port to Port Transcoding	Yes
Text Overlay	Yes
Transcode Bypass	Yes
Icon Overlay	Yes
VAS Conference	Yes
Packet Loss Concealment	Yes

[a] See the SDP section of the *SIP Interface Reference*.

RFC 6184 Support

Table 175 summarizes the Containerized Decomposed Media Server support for RFC 6184.

Table 175. RFC 6184 Support

RFC 6184 Feature	Containerized Decomposed Media Server Support
Single NAL Unit Mode (mode 0)	Yes
Non-Interleaved Mode (mode 2)	—
Interleaved Mode (mode 3)	—
In-Band Parameter Sets	Yes
Out-of-Band Parameter Sets (sprop-parameter-sets)	—

VP8

VP8 codec is a video codec, which has a highly efficient video compression technology.

Table 176 summarizes the VP8 parameters.

Table 176. VP8 Support

RFC 6386 Feature	VP8
A/V	Video
Clock Rate	90 KHz
Picture Size	QCIF, 180p, CIF, 360p, 480p (640x480 and 720x480), 720p
Payload Value	Dynamic
Video Bit Rates	20 to 2000 kbps
Frame rate	30fps (hard-coded)
Frame size[a] (unit of macroblock)	99, 225, 396, 900, 1200, 1350, 3600

[a] Frame size is configurable using the Containerized Decomposed Media Server Web GUI and cannot be negotiated using SDP.

Table 177 indicates VP8 codec levels.

Table 177. VP8 Codec Parameters

VP8 Frame Size (in macroblock)	Parameters for VP8 Load Calibration	HC Video
99	QCIF (176x144) @ 30fps, 64 kbps	No
225	180p (320x180) @ 30fps, 100 kbps	No
396 (default)	CIF (352x288) @ 30 fps, 768 kbps	No
900	360p (640x360) @ 30fps, 1 Mbps	No
1200	480p (640x480) @ 30fps, 2 Mbps	No
1350	480p (720x480) @ 30fps, 2 Mbps	No
3600	720p (1280x720) @ 30fps, 2 Mbps	Yes

Supported Functionality

Table 178 summarizes the Containerized Decomposed Media Server functions supported for the VP8.

Table 178. VP8 Supported Functions

Functions	Support
Announcements/Recordings format[a]	No
Continuous Presence Conference	Yes
fmtp Parameters	Yes
Text Overlay	Yes
Icon Overlay	Yes
VAS Conference	Yes
Transcode Bypass[b]	Yes
Port-to-port Transcode	Yes
PLC	Yes

[a] VP8 does not support announcement and recording format. You can play announcements and record to VP8 ports, however they need to be transcoded from a supported codec type.

[b] VP8 supports transcode bypass except announcements and recordings.

H.265

H.265 is known as High Efficiency Video Codec (HEVC). It is also known as MPEG-H Part 2. This codec was developed by ITU and ISO/IEC.

For the H.265 codec, the Containerized Decomposed Media Server supports main profile levels 1, 2, 2.1, 3, and 3.1. The Containerized Decomposed Media Server sends and receives the H.265 single stream single transport (SRST) RTP streams as specified in RFC 7798. The Containerized Decomposed Media Server discards the H.265 RTP streams with levels higher than the SDP negotiated value.

The Containerized Decomposed Media Server receives Single NAL unit packet, Aggregation Packet (AP), and Fragmentation Unit (FU) H.265 RTP packet types, and discards H.265 PAyload Content Information (PACI) packets. The Supplemental Enhancement Information (SEI) NALs are passed through the Containerized Decomposed Media Server without any modification. However, the Containerized Decomposed Media Server discards the Fragmented(FU) SEI NALS.

The Containerized Decomposed Media Server does not support receiving IP fragmented H.265 RTP packets. The Containerized Decomposed Media Server sends H.265 RTP streams using either single NAL or fragmented packets. Single NAL packets are used if an H.265 NAL matches with the configured video MTU size RTP payload in the management interface, otherwise fragmentation packets are used. The Containerized Decomposed Media Server does not support sending H.265 aggregated packets or PACI packets. The Containerized Decomposed Media Server does not support transcoded VAS on H.265.

Table 179 summarizes the H.265 codec parameters.

Table 179. H.265 Parameters

Parameter	H.265
A/V	Video
Clock Rate	90 KHz
Profile	Main
Level	1, 2, 2.1, 3, and 3.1
Bandwidth	20-4000
Frame Rate	Maximum of 30 fps
Payload Type ID	Dynamic
Picture Size	Upto 720p based on the levels
Video Bit Rates	Upto 4000 kbps
RTP transmission mode	Single RTP Stream on a Single Transport (SRST)

Table 180 indicates H.265 codec levels for encoding in the Containerized Decomposed Media Server.

Table 180. H.265 Codec Parameters

H.265 Level	Maximum Frame Rate pixels/s[a]	Max Picture Size pixels	Maximum Bandwidth kbps	Typical Picture Sizes and Maximum Frame Rate
1	552,960	36,864	128	128×96@33.7 176×144@15.0
2	3,686,400	122,880	1,500	176×144@100.0 352×288@30.0
2.1	7,372,800	245,760	3,000	352×288@60.0 640×360@30.0
3	16,588,800	552,960	4000	640×360@67.5 720×576@37.5 960×540@30.0
3.1	33,177,600	983,040	4000	720×576@75.0 960×540@60.0 1280×720@33.7

[a] On the Egress, the Containerized Decomposed Media Server always limits the frame rate to 30 fps and caps the bitrates to 4000 kbps.

Supported Functionality

Table 181 summarizes the Containerized Decomposed Media Server functions supported for the H.265 codec.

Table 181. H.265 Supported Functions

Function	Support
Announcements/Recordings Format	No
Continuous Presence Conference	No
fmtp Parameters[a]	Yes

Table 181. H.265 Supported Functions

Function	Support
Port to Port Transcoding	No
Text Overlay	No
Transcode Bypass	Yes
Icon Overlay	No
VAS Conference	Yes
Error Concealment	No

[a] See the SDP section of the *SIP Interface Reference*.

Mid-Call Changes on Video Port

The Containerized Decomposed Media Server supports mid-call changes (using SIP re-INVITE or UPDATE) on video ports. Mid-call changes include modification in the following:

- Session parameter
- Codec parameter
- Codec

Table 182 provides information on supported mid-call changes for different service contexts.

Table 182. Mid-call Video Changes on Supported Service Contexts

Mid-call Video Port Change	CP Video Conference	VAS Conf	No Service or Idle (For MSML/VXML)	Video Annc	Video Recording
IP address	Y	Y	Y	Y	N
IP address version (v4 <-> v6)	N	N	N	Y	N
port number	Y	Y	Y	Y	N
payload number	Y	Y	Y	Y	N
RTP direction mode	Y	Y	Y	Y	N
AVP <-> AVPF[a]	Y	N	Y	Y	N
RTCP-PLI (on <-> off)	Y	N	Y	Y	N
RTCP-FIR (on<->off)	Y	N	Y	Y	N
RTCP-TMMBR (on<->off)	Y	N	Y	Y	N
CVO (on<->off)	Y	Y	Y	Y	Y
codec type (non-HC <-> non-HC)	Y	N	Y	Y	N
codec type (non-HC <-> HC)	Y	N	Y	Y	N
codec type (HC <-> HC)	Y	N	Y	Y	N
H.264 profile-level	Y	N	Y	Y	N
H.264 bandwidth	Y	Y (if within allowed tolerance)	Y	Y	N
H.264 packetization mode (0<->1)	Y	N	Y	Y	N

Table 182. Mid-call Video Changes on Supported Service Contexts

Mid-call Video Port Change	CP Video Conference	VAS Conf	No Service or Idle (For MSML/VXML)	Video Annc	Video Recording
VP8 bandwidth	Y	Y (if within allowed tolerance)	Y	Y	N
Transcode <-> Transcode-Bypass	NA	NA	NA	Y[b]	NA

[a] For AVP <-> AVPF, mid-call changes are supported until there is no change in RTCP-FB capability on the port.

[b] The mid-call change that switches from transcode to transcode-bypass and transcode-bypass to transcode may result in some user experience.

T.140

T.140 is a text-based codec defined by RFC 4103 that is used for transmitting text on a separate RTP session.

As per RFC 4103, the Containerized Decomposed Media Server transcodes T.140 that is received over an RTP stream by using the **text/t140** payload format to TTY encoded in all supported codecs. The transcoding works in the reverse direction as well.

This feature enables TTY-capable devices to interact with emergency services in PSTN and CDMA UEs.

Table 183 summarizes the T.140 codec parameters.

Table 183. T.140 Parameters

Parameter	T.140
cps	1 to 30 characters per second
Buffer Size	100 to 500 ms

Supported Functionality

Table 184 summarizes the Containerized Decomposed Media Server support for the T.140 codec function.

Table 184. T.140 Supported Functions

Function	Support
RFC 4117 sip:tc context	Yes

TTY

TTY devices transmit characters using a 45.45 bps Baudot code. Each bit has a nominal duration of 22 ms and a character consists of 1 start bit, 5 data bits, and 1.5 stop bits; totally 7.5 data bits per character. Therefore it can allow for transmitting up to a maximum of 6 TTY characters per second. The code uses a carrier-less, binary FSK signaling scheme. A mark, or 1, is transmitted with a 1400 Hz tone. The space, or 0, is transmitted with an 1800 Hz tone.

With 5 data bits, the Baudot code is only capable of 32 different characters, which is not enough to represent the alphabet, numbers, and punctuation. This problem is remedied by introducing “shift” characters that change the way the receiving TTY device interprets the 5 data bits. There exists the letters shift character (31) and the figures shift character (27). Following the letters shift character, the receiving TTY device interprets the 5-bit code using the letters library, which consists of letters of the alphabet. The figures library contains numbers, punctuation, and special characters.

The TTY PCM tones can be coded in any of the formats like G.711 (a-law and µ-law), G.722, G.729, AMR, and AMR-WB. However, since lossy compression techniques like G.729, AMR and AMR-WB are not reliable for pure tones like TTY/T140, it is best to use TTY tones with G.711 (a-law and µ-law) codec.

IPv6 Supported Notations

This appendix describes the supported notations for IP Version 6.

For more information about the Containerized Decomposed Media Server support for IPv6, refer *Special Interfaces Reference*.

The Containerized Decomposed Media Server supports all the notations for entering IPv6 addresses.

- **Standard Notation.** Represents the address as eight 16-bit hexadecimal words in fields separated by colons (":"). Each field must contain at least one hexadecimal digit. Leading zeros can be omitted.
  Examples of the standard notation are.

  `FEDC:BA98:0332:0000:CF8A:000C:2154:7313` Upper case long notation with prefix 0

  `fedc:ba98:0332:0000:cf8a:000c:2154:7313` Lower case long notation with prefix 0

  `FEDC:BA98:332:0000:0000:CF8A:2154:7313` Upper case long notation

  `fedc:ba98:332:0000:0000:cf8a:2154:7313` Lower case long notation

- **Compressed Notation.** Represents a contiguous group of zero fields within the IPv6 address using a double colon ("::"). Only one contiguous group of zero fields per address can be represented in this way.
  Examples of the compressed notation are.

  `FEDC:BA98:332:0:CF8A:C:2154:7313` Upper case long notation without prefix 0

  `fedc:ba98:332:0:cf8a:c:2154:7313` Lower case long notation without prefix 0

  `FEDC:BA98:332::CF8A:2154:7313` Upper case compressed short notation

  `fedc:ba98:332::cf8a:2154:7313` Lower case compressed short notation

  Examples of the standard and compressed notation are.

```
Standard notation:          Compressed notation:
1762:0:0:0:0:B03:1:AF18     1762::B03:1:AF18
FF01:0:0:0:CA:0:0:2         FF01::CA:0:0:2
0:0:0:0:0:0:0:1             ::1
0:0:0:0:0:0:0:0             ::
```

Traffic on Interfaces

This appendix describes the traffic on interfaces. Interfaces are predefined and there is no provision to configure and map these interfaces.

Table 1. Traffic on Interfaces

Interface	Network Protocol or Application	IP Version
Management	HTTP (web)	IPv4 or IPv6
	SNMP	
	NETCONF	
	SFTP	
	DNS	
	Syslog or logpkg on external server	
	Alarms external server	
	Statistics external server	
	Clips provisioning	
Control	DNS	
	SIP	
	MSML 1.1	
	MSCML	
	VoiceXML	
	MRCP (RTSP, ASR, and TTS (Signaling))	
	ICMP	
Media	DNS	
	RTP or SRTP	
	RTCP or SRTCP	
	HTTP streaming (for announcement or recording)	
	ICMP	
	RTSP, ASR, and TTS (RTP)	
	HTTP (for VXML document fetch)	
	UDPTL (for T.38 fax port)	

Automated Task

This appendix describes the automated tasks provided by the Containerized Decomposed Media Server.

Containerized Decomposed Media Server Backup and Restore Script

The automated script provided with the release package allows you to perform the automatic backup or restore operations using the SNMP interface.

External Server

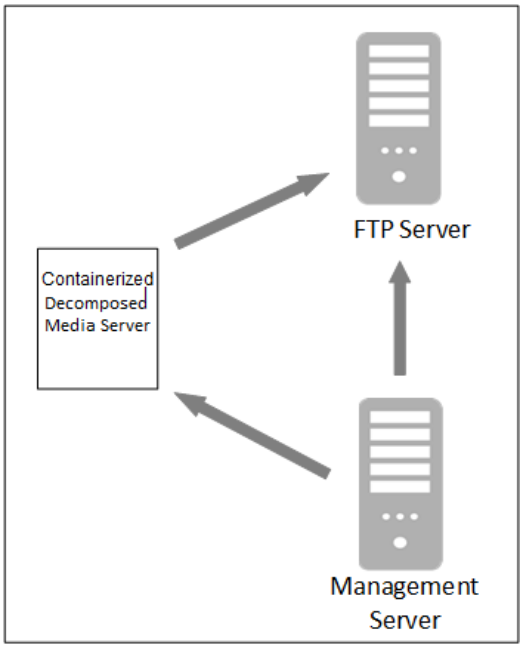
The **`mrfBackupRestore.sh`** script allows you to perform the automatic backup or restore operations on an external server using the SNMP interface.

Prerequisites

- **cURL (version 7.19.7 or above).** The cURL must be installed on the system and is used to perform the transfer operations with the file server using the SFTP protocol.
- **Net-SNMP.** The Net-SNMP must be installed on the system and is used to perform SNMP GET/SET operations with Containerized Decomposed Media Server.

The script works in the following scenarios.

- When the FTP server and Management server are different (as shown in the figure).



  - The FTP server supports SFTP protocol
  - The Containerized Decomposed Media Server backup or restore script is executed from the management server
  - The backup and restore server type settings specified in the **.cfg** file is set to REMOTE (`BKP_RSTR_SERVER_TYPE=REMOTE`)
- When the FTP and Management servers are the same.
  - The Decomposed Media Server backup or restore script is executed from the management server
  - The backup and restore server type settings specified in the ***.cfg*** file is set to LOCAL (`BKP_RSTR_SERVER_TYPE=LOCAL`)

Before performing the backup or restore operation, the script uses **SWMRF_MGMT_IP** setting to perform backup or restore operation.

NOTE: To execute the backup or restore script from the management server when passwordless file transfer is enabled in the Containerized Decomposed Media Server, you must

- enable the passwordless file transfer from Containerized Decomposed Media Server to the FTP server and from the management server to the FTP server.
- copy the local public key of the remote server for file transfer from Decomposed Media Server to the FTP server and from the management server to the FTP server.

To execute the script

Execute the following command for backup or restore operation.

```
mrfBackupRestore.sh -c <config file>
```

The **`mrfBackupRestore.sh`** script allows you to perform the backup or restore operation for the Containerized Decomposed Media Server based on configuration provided in the `<config file>`.

The script additionally provides command line options to override some of the settings from the ***.cfg*** file without modifying the ***.cfg*** file. The following are the syntax for backup and restore options.

- **`mrfBackupRestore.sh [--backup <full|config>] -c <config file> [backup path]`**
- **`mrfBackupRestore.sh [--restore <full|config>] -c <config file> <restore path>`**

Table 2 lists the CLI options for the backup and restore script.

Table 2. CLI Options for Backup and Restore Script

CLI Options	Description
backup	Performs the backup. If specified in the command line, it overrides the BKP_RSTR_OPTION and BKP_RSTR_ACTION settings in the config file.
restore	Performs the restore. If specified in the command line, it overrides the BKP_RSTR_OPTION and BKP_RSTR_ACTION in the config file.
full	Performs the full backup or restore, which includes backing up or restoring the Containerized Decomposed Media Server configuration and all the clips loaded on the Decomposed Media Server.

CLI Options	Description
config	Performs the backup or restore of the Containerized Decomposed Media Server configuration.
[backup path]	Absolute path of backup location. If specified, it overrides the FILE_PATH setting in the configuration file. If [backup path] is specified, no automatic timestamp based folder is created and the backup is performed directly in the [backup path] provided.
<restore path>	Absolute path of the Containerized Decomposed Media Server backup folder on the FTP_SERVER from where the restore must be performed. This parameter overrides the RSTR_FILE_PATH setting in the config file. Full restore or the configuration restore results in the Containerized Decomposed Media Server reboot.

Backup Operation

Following is the backup operation.

1. The script uses the USERNAME, PASSWORD, and PROTOCOL specified in the `<config file>` to log into the FTP_SERVER.
2. Creates a new timestamp directory under the FILE_PATH setting.

   The timestamp folder has the following naming convention.
   `<BKP_RSTR_MRF_ID>_<FULL|CFG>_BKP_YYYYMMDD_HHMMSS`

   NOTE: If the INCLUDE_HOSTNAME is enabled, the Decomposed Media Server creates a subfolder **cfg_backup_<Containerized Decomposed Media Server hostname>** or **fbr_backup_<Decomposed Media Server hostname>** inside *<BKP_RSTR_MRF_ID>_<FULL|CFG>_BKP_YYYYMMDD_HHMMSS* folder and the *back-up_config.ms* or full backup files are placed in this folder.
3. After creating the timestamp directory, the script sets the full path of the timestamp directory, USERNAME, PASSWORD, FTP_SERVER, PROTOCOL, and USE_ANON in the Decomposed Media Server using `SNMP SET` command.
4. The script starts the backup operation.

Restore Operation

Following is the restore operation.

1. The script uses the USERNAME, PASSWORD, and PROTOCOL specified in the `<config file>` to log into the FTP_SERVER and verifies the validity of the specified RSTR_FILE_PATH.
2. If the specified path is valid, the script sets RSTR_FILE_PATH, FTP_SERVER, USERNAME, PASSWORD, PROTOCOL, and USE_ANON in the Containerized Decomposed Media Server using `SNMP SET` command.
3. The script starts the restore operation.

NOTE:

- In case of any backup or restore operation failure, the script attempts the operation after the lapse of the time specified in the RETRY_DELAY. The script retries any backup or restore operation for the specified number of times in the MAX_BKP_RSTR_RETRY.
- If the INCLUDE_HOSTNAME is enabled, the complete path until the subfolder must be provided for the restore operation.

Logs

The **`mrfBackupRestore.sh`** script stores the status of the backup and restore operation in a log file created in the directory specified in BKP_RSTR_LOG_PATH. If BKP_RSTR_LOG_PATH is not specified, the log file is created under the current directory. The created log file is of the form `<BKP_RSTR_MRF_ID>_bkpRstr.log`.

For more information refer `README.txt` file provided along with the release package.

Containerized Decomposed Media Server

The **`mrfbackuprestore_v1.sh`** script allows you to perform the automatic backup or restore operations on the Containerized Decomposed Media Server using the SNMP interface.

NOTE: Only `swmsadmin` users are allowed to modify the **.cfg** file.

The **`mrfbackuprestore_v1.sh`** script is stored in ***/opt/swms/bin*** location.

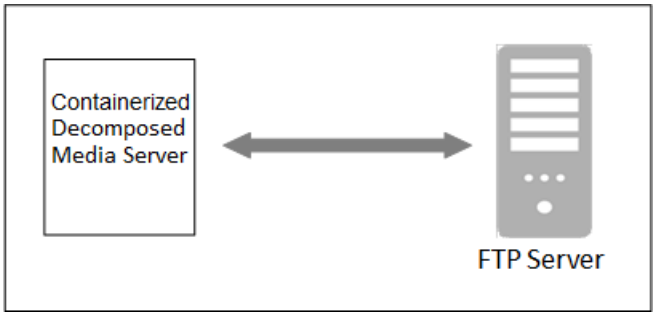
Prerequisites

cURL (version 7.19.7 or above). The cURL must be installed on the system and is used to perform the transfer operations with the file server using the SFTP protocol.

The script works as follows:

- The FTP server supports SFTP protocols
- The Containerized Decomposed Media Server runs the backup or restore script
- The backup and restore server type settings specified in the **.cfg** file is set to REMOTE (`BKP_RSTR_SERVER_TYPE=REMOTE`)

  NOTE: The backup and restore server type does not support LOCAL server type.



Before performing the backup or restore operation, the script uses **SWMRF_MGMT_IP** setting to perform backup or restore operation.

NOTE: When the passwordless file transfer is enabled, the local public key of the remote server for the file transfer must be configured in the Containerized Decomposed Media Server and the **PASSWORD** field entry in the .cfg file is not mandatory.

To execute the script

Execute the following command for backup or restore operation.

```
mrfbackuprestore_v1.sh -c <config file>
```

The **`mrfbackuprestore_v1.sh`** script allows you to perform the backup or restore operation for the Containerized Decomposed Media Server based on configuration provided in the `<config file>`.

The script additionally provides command line options to override some of the settings from the ***.cfg*** file without modifying the ***.cfg*** file. The following are the syntax for backup and restore options.

- **`mrfbackuprestore_v1.sh [--backup <full|config>] -c <config file> [backup path]`**
- **`mrfbackuprestore_v1.sh [--restore <full|config>] -c <config file> <restore path>`**

Table 2 lists the CLI options for the backup and restore script.

Backup Operation

For backup operation on the Containerized Decomposed Media Server, see *Backup Configuration on page 376*.

Restore Operation

For restore operation on the Containerized Decomposed Media Server, see *Restore Configuration on page 378*.

Logs

The **`mrfbackuprestore_v1.sh`** script displays the status of the backup and restore operation on the console.

Speech Adapter

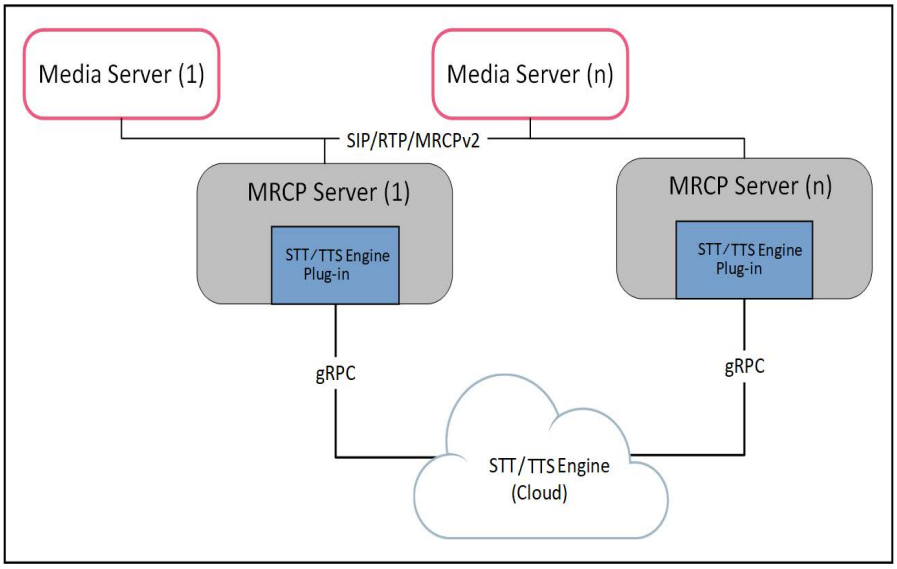
This chapter explains how Radisys Media Server inter-works with Speech Adapter.

About Speech Adapter

Speech Adapter is a new product of Media Server. The Speech Adapter is a cross-platform implementation of the MRCP protocol. The implementation encapsulates SIP, Session Description Protocol (SDP), MRCPv2, and RTP/RTCP stacks and has been integrated with a number of industry-leading speech engines.

Speech Adapter is the interfacing module between the Media Server and third-party speech engines (Google Cloud or Microsoft Azure), which performs Speech-to-Text (STT) and Text-to-Speech (TTS) conversion.

Figure 1. Media Server–Speech Adapter Networking



Speech Adapter supports the following:

- Integration with the third-party speech engine
- English and Hindi language speech recognition
- English and Hindi language text-to-speech announcements

Speech Adapter

I

Features

Speech Adapter interfaces with third-party cloud speech engines (Google Cloud and Microsoft Azure) to perform Speech-to-Text (STT) and Text-to-Speech (TTS) conversion.

Speech-to-Text

STT is also known as Automatic Speech Recognition (ASR).

Speech Recognition converts human speech to text using third-party STT services such as Google STT or Microsoft Azure. Speech Adapter interfaces with third-party STT engines to perform STT conversion. Speech Adapter supports the speech recognition in multiple languages based on the input received from the Media Server. The Speech Adapter controls the **no-input-timeout**, **recognition-timeout**, and **speech-complete-timeout** MRCP timers. For information on MRCP timers, see *Configure MRCP on page 193*.

The Speech Adapter supports the language translation service. Media Server translates the human speech to the language supported by the Speech Adapter using Google Cloud or Microsoft Azure translation and STT services.

Text-to-Speech

Variable text is synthesized into a voice clip with the help of an external TTS engine, and the synthesized clip is played to the user. Speech Adapter interfaces with third-party TTS engines such as Google Cloud or Microsoft Azure to perform TTS conversion.

Speech Adapter supports TTS announcement for English and other languages. The information that cannot be pre-recorded and is caller specific, such as account balance, card expiry date, location-specific details, and so on, is played to the user through the TTS functionality.

The gender of the voice, language, and accent in which the announcement is played can be configured in the Speech Adapter.

Inter-working with Speech Adapter

Licensing Information

You must have a license on the Radisys Media Server to enable STT and TTS sessions. The license must be configured in the **ExternalSpeechSessionsPort** in the Media Server license file.

Speech Adapter Configuration on Media Server

Configure Speech Adapter (MRCP server) for STT and TTS sessions. See *Configure MRCP on page 193*.

You can also configure Speech Adapter through the SNMP. To configure the Speech Adapter through the SNMP, refer to the *Radisys Media Server SNMP Interface Reference*.

Session Refresh

Session timers are implemented between the Speech Adapter and Media Server. The **SIP Session Timer** from the *Configure SIP* Web GUI must be enabled in Media Server. The recommended configuration for the **Minimum Session Expiration Time** and **Session Expiration Time** is two minutes. If configured for less than two minutes, the Speech Adapter sends a reject message with SIP error 422. Speech Adapter sends an update request to refresh the session towards the Media Server at half of the negotiated session refresh time.

Contact Radisys TAC for information on Speech Adapter product and user documentation.

Privacy Documentation

This appendix explains the following categories of personal data collected and processed by the Radisys Containerized Decomposed Media Server.

- *Network Identifiers*
- *User Identifiers*
- *Subscriber Identifiers*
- *Voice File*
- *Media File*

Network Identifiers

Examples of personal data elements collected by the network identifiers category are MAC addresses, serial numbers, and IP addresses of the network elements. The customer employees are the data subjects of this personal data category. Data elements are collected from the interfaces of network elements through the SIP signaling and Media call flows between different network elements. These data elements are stored in the log files and are used only for debugging. Authenticated customer employees can only access these log files and user logins are protected by a role-based access policy. Customer administration with valid credentials has access to network identifiers. The log files are rotated based on a fixed rotation policy, and the retention depends on the volume of the log. After the log rotation, the old files are deleted. When the log files are transferred for debugging, the personal data in the files are pseudonymized.

User Identifiers

Examples of personal data elements collected by the user identifiers category are username, password, database dump, and TCP packet capture. The customer employees are the data subjects of this personal data category. Data elements are collected from the Containerized Decomposed Media Server management interface. Personal data elements of this category are stored in the log files and database. This data is required for the functioning of the product. For example, authenticating a user to the system and debugging. Authenticated customer employees can only access the data elements of this category. The user logins are protected by a role-based access policy. Password is stored after one-way hashing with a strong hashing algorithm. Customer administration with valid credentials has access to User Identifiers. The log files are rotated based on a fixed rotation policy, and the retention depends on the volume of the log. After the log rotation, the old files are deleted. The data in the database is deleted when the data is no longer required, or the user removes the data. When the log files are transferred for debugging, the personal data in the files are pseudonymized. TCP dump and Database dump are pseudonymized.

Subscriber Identifiers

The subscriber identifiers collect personal data elements such as SIP username, SIP contacts, and DTMF digits. The end-user/subscribers are the data subjects of this personal data category. The SIP username and SIP contact are only the next-hop details available with the Radisys Containerized Decomposed Media Server. Data mapping of the next-hop to the end-user from the next-hop element (SBC) is required to map the SIP username to a possible end-user. DTMF digits can potentially contain end-user information. DTMF digits are not stored or processed at this product, but the data is processed in memory and forwarded to other network elements. These data elements can be captured in the system TCP packet or core file. SIP username and SIP contacts are written in the log files. This data is required for the different business use cases of the product, such as capturing the DTMF digits. Core files and packet capture are used only for debugging. Authenticated customer employees can only access subscriber identifier data. The user logins are protected by a role-based access policy. The log files are rotated based on a fixed rotation policy, and the retention depends on the volume of the log. After the log rotation, the old files are deleted. When the log files are transferred for debugging, the personal data in the files are pseudonymized. TCP dump and core files are pseudonymized.

Voice File

The voice file collects personal data elements such as voice mail recording and transient voice mail recording. The end-user/subscribers are the data subjects of this personal data category. Voice files are stored in the file system or on a customer-provided remote HTTPS server. Personal data elements from this category provide voice mail facility business use cases and are collected from media call flow between this product with another network element. These files are encrypted. Authenticated customer employees can only access the data elements of this category. The user logins are protected by a role-based access policy and file system security. To store the voice file locally, the operator provisions enough disc space. When Session Border Controller (SBC) deletes these files, the voice files are permanently deleted from the system. These files are not transferred.

Media File

The media file collects personal data elements such as the conference call media recording file. The end-user/subscribers are the data subjects of this personal data category. Media files are stored in the file system or on a customer-provided remote HTTPS server. Personal data elements from this category provide conference call business use cases and are collected from media call flow between this product with another network element. These files are encrypted. Authenticated customer employees can only access the data elements of this category. The user logins are protected by a role-based access policy and file system security. To store the media file locally, the operator provisions enough disc space. When SBC deletes these files, the media files are permanently deleted from the system. These files are not transferred.