Administering Avaya Session Border Controller

Release 10.2.1
Issue 1
December 2024

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

© 2014-2024, Avaya LLC
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users

are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction 21
Purpose 21
Chapter 2: Overview 22
Avaya SBC security devices 22
Graphical User Interface 22
Command Line Interface 23
Logging in to the EMS web interface 23
Password policies 23
Console and SSH passwords complexity 24
EMS GUI password complexity 24
Resetting the GUI password 25
Grub password complexity 25
Password hashing mechanisms 25
Chapter 3: Administrative user accounts 26
Administrative user accounts and authentication modes 26
Managing user accounts 27
Creating an administrative user account 27
Editing an administrative user account 30
Deleting an administrative user account 30
Configuring password rules and lockout options 31
Configuring LDAP server authentication 32
LDAP server authentication field descriptions 32
Configuring X.509 certificate authentication 34
X.509 certificate authentication field descriptions 35
Enabling EASG 36
Managing a RADIUS server 36
Adding a RADIUS server 36
Editing a RADIUS server 38
Deleting a RADIUS server 38
Configuring RADIUS server authentication 39
AAA field descriptions 42
Chapter 4: Device configuration 48
Prerequisites 48
Adding an Avaya SBC device 48
Device Management field descriptions 49
Using pooled licensing 52
Commissioning an Avaya SBC device 53
Installation Wizard field descriptions 54
Edit device field descriptions 55

Configuring logon banner messages 57
Configuring port bonding 58
Changing the management IP from the EMS web interface 60
High Availability failovers 60
Configuring High Availability 62
HA Node Status States 62
Upgrade of the EMS software 63
Obtaining a license file from Avaya PLDS 63
Viewing the EMS server time zone 64
Setting the EMS server time zone 64
High-Availability pair geographically dispersed 65
Interface connections for an Avaya SBC HA pair 66
Deploying a geographically dispersed Avaya SBC HA configuration 67
Configuring RTCP Monitoring Relay 68
RTCP Monitoring Relay field descriptions 68
Application relay configuration for RTCP monitoring 69
Configuring application relay for RTCP monitoring in core Avaya SBC 69
Configuring application relay for RTCP monitoring in DMZ Avaya SBC 70
Configuring application relay for RTCP monitoring in remote Avaya SBC 70
Configuring application relay for RTCP monitoring in core, remote, and DMZ Avaya SBC field descriptions 71
RTCP monitoring generation support 72
Round Trip Time 73
Configuring RTCP monitoring generation support 73
Adding a new blacklist rule 74
Firewall field descriptions 75
Restarting the IPCS services 76
Chapter 5: Domain policy, routing, and message flow administration 77
Governing Unified Communications with Domain Policies 77
Unified Communications Policies 77
Example: Call server with Avaya SBC securing SIP trunk 78
Example: Call server with Avaya SBC securing SIP phones 80
Rules and policies configuration 81
Architecture 81
Rule and policy associations 83
Rules and policies checklist 85
SIP message processing 86
SIP registration processing 86
Subscriber flow matching 86
Inbound policy invocation registration processing 87
Route resolution 87
Server flow matching 88
Outbound policy invocation call processing 88

Transmit to network registration processing 88
SIP call processing on Avaya SBC 88
SIP servers identification 89
Inbound call processing 91
Server flow matching for calls originated from the server 91
Subscriber flow matching for call originated from remote worker 92
Policy invocation and route resolution 92
Inbound policy invocation 92
Route resolution for call towards remote worker 93
Route resolution for a call towards a server 93
Outbound call processing 94
Server flow matching for a call to a server 94
Outbound policy invocation for registration processing 95
Transmit to network for call processing 95
Application rule processing for endpoint policy group configuration 95
Maximum concurrent sessions per endpoint counter 95
Maximum concurrent sessions counter 96
Rules for call flows 96
In/Out direction flags 96
SIP call flow example 97
Call flow example for call processing 97
Call flow example for server flow matching in calls originated from a server 98
Call flow example for inbound policy invocation 98
Call flow example for route resolution 98
Call flow example for server flow matching in a call towards a server 98
Call flow example for outbound policy invocation 99
Call flow example for transmit to network 99
Call flow example from PSTN trunk to a Call Center Elite user 99
Application rules 103
Creating a new Application Rule 103
Editing an Application Rule 104
Cloning an Application Rule 105
Renaming an Application Rule 105
Deleting an Application Rule 106
Border rules 106
Creating a new border rule 106
Editing an existing border rule 107
Cloning a border rule 108
Renaming an existing border rule 108
Deleting an existing border rule 109
Media rules 109
SDP capability negotiation 109
RTCP multiplexing 110

Creating a media rule ... 110
Media rules field descriptions ... 111
Editing a media rule ... 118
Editing codec prioritization parameters ... 119
Cloning a media rule ... 119
Renaming a media rule ... 119
Deleting a media rule ... 120
Security rules ... 120
Creating a new security rule ... 121
Editing an existing security rule ... 123
Cloning an existing security rule ... 123
Renaming an existing security rule ... 123
Deleting an existing security rule ... 124
Signaling rules ... 124
Creating a new signaling rule ... 125
Editing an existing signaling rule ... 132
Cloning an existing signaling rule ... 139
Renaming an existing signaling rule ... 139
Deleting an existing signaling rule ... 139
Charging rules ... 140
Creating a new charging rule ... 140
Editing an existing charging rule ... 141
Cloning an existing charging rule ... 142
Renaming a charging rule ... 142
Deleting a charging rule ... 143
Endpoint policy groups ... 143
Creating a new endpoint policy group ... 144
Viewing an existing policy group summary ... 145
Editing an endpoint policy set ... 146
Edit an existing End Point Policy Group ... 146
Deleting an existing end point policy group ... 147
Session policies ... 148
Creating a new session policy ... 149
Session Policy field descriptions ... 149
Editing an existing session policy ... 150
Cloning an existing session policy ... 151
Renaming an existing session policy ... 151
Deleting an existing session policy ... 152
Media unanchoring ... 152
Unanchoring media for existing session policies ... 153
Media unanchoring scenarios ... 153
About administering end-point flows and session flows ... 163
Endpoint flow ... 164

Session flow 174
Single Sign-On and Identity Engine 176
Configuring Single Sign-On and an Identity Engine server 176
Reverse Proxy Profile field descriptions 177
Uniform Resource Identifier groups 177
Creating a new URI group 178
Editing a URI group 180
Deleting a SIP URI from an existing URI group 180
Renaming a URI group 181
Deleting a URI group 181
Configuring URN map based routing for NG911 calls 182
Configuring Route header based routing for NG911 calls 184
Add URI Group field descriptions 185
Routing profile field descriptions 186
Configuring access to IP Office features over MTCTI messaging 189
Chapter 6: System Configuration 191
Basic system configuration overview 191
Basic configuration checklist 192
Enabling interfaces 193
Backup and restore 193
About backing up and restoring your system 193
Backup frequency recommendations 194
Designating a snapshot server 194
Creating system snapshots 196
Configuring automatic snapshots 196
About restoring a system snapshot 199
Creating a configurable portable snapshot 203
Restoring a configurable portable snapshot 204
Deleting a system snapshot 205
About VMware snapshots 205
Management of deployed Avaya SBC security devices 209
Shutting down an Avaya SBC security device 209
Restarting an Avaya SBC application 210
Rebooting an Avaya SBC security device 210
Swapping a separate Avaya SBC server deployed under EMS 211
Swapping Avaya SBC devices in an HA pair deployment 211
Swapping an EMS server in a single server deployment 212
Swapping a primary EMS server in an HA pair deployment 213
Swapping a secondary EMS server in an HA pair deployment 213
Viewing device configuration 214
Editing device configuration 214
Deleting a device configuration 215
Upgrading system management 215

Enabling High Availability 216
Managing Avaya SBC logging level 217
Debugging field descriptions 217
Advanced Options configuration 220
Advanced Options field descriptions 220
Security feature control 225
Managing SIP options 225
Allowing reuse of the same IP 226
Managing port options 227
Monitoring RTCP 228
Configuring HA Heartbeat Interval and Max Retries 228
Media Forking overview (Standard Platform only) 229
Adding a Media Forking profile (Standard Platform only) 230
Adding Media Forking Profile to Session Policy (Standard Platform only) 231
MAC-based LDAP authentication 232
LDAP Server Profile 232
Creating a new LDAP server 232
Editing an existing LDAP server 233
Renaming an LDAP server 234
Cloning an existing LDAP server 234
Deleting an LDAP server 235
Administering SNMP access 235
Accessing SNMP settings 235
Uploading a cadf file to System Manager 235
Adding an SNMP user account 236
Editing an SNMP user account 238
Deleting an SNMP user account 239
Adding an SNMP management server 239
Creating an SNMP trap profile 239
Enabling and disabling traps by severity 253
Time of Day (ToD) rules 254
Creating a new Time of Day rule 254
Cloning an existing Time of Day rule 256
Editing an existing Time of Day rule 256
Renaming an existing Time of Day rule 256
Deleting an existing Time of Day rule 257
Routing profiles 257
LDAP based call routing 258
Load balancing 258
Adding a routing profile 259
Routing rule management 263
Cloning an existing routing profile 264
Renaming an existing routing profile 265

Deleting an existing routing profile 265
Syslog parameter management 266
Selecting log levels 266
Syslog management field descriptions 267
User agents (Advanced Services only) 270
Adding a new user agent (Advanced Services only) 270
Editing an existing user agent (Advanced Services only) 271
Viewing authorized user agents (Advanced Services only) 271
Deleting an existing user agent (Advanced Services only) 272
Managing device-specific settings 272
Adding a new signaling interface 272
Signaling interface field descriptions 273
Editing an existing signaling interface 273
Viewing an existing signaling interface 274
Deleting an existing signaling interface 274
Adding a new media interface 274
Editing an existing media interface 275
Viewing an existing media interface 276
Deleting media interface 276
AAA field descriptions 276
Automatic blacklisting of network source IP 283
Overview 283
Creating IP/URI blocklist profile 283
Blocking a subnet 284
Unblocking IP/URI address 285
Blocking an IP/URI permanently 285
Propagating information to other Avaya SBCs 285
Tenant configuration 286
Creating the tenant configuration profile 286
Editing the tenant configuration profile 287
Renaming the tenant configuration profile 287
Deleting the tenant configuration profile 288
Chapter 7: Security configuration 289
Security configuration overview 289
System wide single endpoint DoS configurations 289
Domain DoS configurations 289
SIP server DoS configuration 289
DoS Security features 290
Viewing DoS/DDoS settings 290
Editing DoS/DDoS settings 293
Domain DoS profiles 294
Adding a new Domain DoS profile 294
Viewing a Domain DoS profile 296

Cloning an existing Domain DoS profile ... 296
Renaming an existing Domain DoS profile ... 297
Editing an existing Domain DoS profile ... 297
Deleting a Domain DoS profile ... 297
Setting learned DoS parameters ... 298
DoS Learning field descriptions ... 298
Protocol scrubber ... 299
Scrubber package file path ... 299
Viewing scrubber rules ... 300
Installing a scrubber rules package ... 300
Enabling or disabling an installed scrubber rules package ... 300
Deleting a Scrubber Rules package ... 301
Configuring scrubber actions ... 301
Topology Hiding ... 302
Creating a Topology Hiding profile ... 302
Renaming a Topology Hiding profile ... 304
Cloning a Topology Hiding profile ... 304
Deleting a Topology Hiding profile ... 305
Adding a new Topology Hiding header ... 305
Editing a Topology Hiding Header ... 306
Deleting a Topology Hiding header ... 306
Headers affected by Topology Hiding ... 307
Configuring Mediasec ... 312
GDPR ... 312
Enabling or disabling GDPR ... 314
Configuring a Remote log server ... 314
Decrypting the encrypted files ... 316
Chapter 8: Server and network interface configuration ... 317
About configuring the server and network interfaces ... 317
About SIP server configuration profile management ... 317
Viewing a SIP Server profile ... 317
Adding a new SIP server profile ... 318
Editing a SIP Server profile ... 318
Server configuration profile field descriptions ... 319
Cloning an existing SIP Server profile ... 328
Renaming an existing SIP Server profile ... 328
Deleting an existing SIP Server profile ... 328
DoS Whitelist ... 329
Editing and recalculating the DoS Protection parameters ... 329
Configuring DNS SRV for trunk registration ... 330
Server interworking ... 331
Viewing existing Server Interworking profiles ... 331
Adding a server interworking profile ... 331

Editing the Server Interworking profile parameters 332
Interworking profile field descriptions 332
Cloning a Interworking profile 342
Renaming an existing Interworking profile 342
Deleting an Interworking profile 343
Adding a URI Manipulation rule 343
Editing a URI Manipulation rule 343
Deleting an existing URI Manipulation rule 344
Adding a Header Manipulation rule 344
Editing a Header Manipulation rule 344
Deleting a Header Manipulation rule 345
Networks and interfaces management 345
Adding a new network interface 345
Virtual LAN 347
Passthrough 347
Changing the administrative state of an interface 348
Deleting an existing interface 348
Viewing an existing interface or network 348
Adding a new network 349
Editing network management parameters 349
Chapter 9: TLS management 351
About TLS parameter management 351
Considerations for working with TLS 351
Converting a certificate to PEM format 351
Checklist for establishing end-to-end TLS communications 352
Certificate management 355
Installing third-party certificates 356
Creating a CSR 356
Settings for externally generated CSRs 357
Extracting a certificate and key from a PFX or PKCS#12 keystore 357
About certificates 358
Installing certificates 358
Uploading a certificate file 359
TLS certificates field descriptions 361
Viewing certificate details 363
Deleting certificates 363
About CA certificates 364
Installing a CA certificate 364
CA certificate field descriptions 365
Viewing the CA certificate details 365
Deleting a CA certificate 365
About CRLs 366
Installing CRLs 366

CRL field descriptions ... 366
Viewing CRL details ... 367
Deleting a CRL ... 367
About TLS profile management ... 367
About TLS server profile management ... 368
About TLS client profile management ... 372
Extended hostname validation ... 376
About configuring SNI groups ... 376
Creating a new SNI group ... 377
Renaming an SNI group ... 377
Cloning an existing SNI group ... 377
Deleting an SNI group ... 378
Chapter 10: System monitoring ... 379
About system monitoring ... 379
Dashboard ... 379
Dashboard content descriptions ... 380
Alarms ... 380
Viewing current system alarms ... 380
Clearing system alarms ... 381
System alarms list ... 382
Clearing a “Data Replication is broken” alarm ... 390
Clearing a “Data replication pg_xlog usage more than 1 GB” alarm ... 391
GUI and console alarm list ... 393
Incidents ... 395
Viewing system incidents ... 404
System status ... 407
Viewing SIP statistics ... 408
Viewing periodic statistics ... 412
User registration ... 414
Server status ... 416
Viewing performance statistics ... 417
Viewing IP/URI Blocklist ... 418
Enabling or disabling Telemetry reports ... 418
Viewing Telemetry reports ... 419
Log files ... 422
Viewing system logs ... 422
Viewing audit logs ... 424
Collecting and downloading log files ... 425
Debugging logs ... 427
Troubleshooting ... 432
Viewing system information ... 433
Running diagnostics tests ... 433
Diagnostics field descriptions ... 434

Users ... 435
Viewing administrative users ... 435
Active Users field descriptions ... 436
License usage ... 436
Command line monitoring tools ... 437
traceSBC ... 437
Trace ... 443
tcpdump ... 444
showflow ... 445
sbceinfo ... 447
clipcs ... 447
swversion ... 448
Hardware specifications report file ... 449
Command History file ... 450
Instance commands ... 450
Traps ... 450
SNMP MIBs ... 451
Downloading the Avaya SBC MIB ... 451
Avaya SBC OID Descriptions ... 451
Chapter 11: CLI commands ... 459
About the Command Line Interface ... 459
Accessing Avaya SBC ... 459
Accessing Avaya SBC or EMS device using VGA connection ... 459
Accessing Avaya SBC or EMS device through SSH ... 459
Configuring Avaya SBC for HA deployment using CLI ... 460
Configuring Avaya SBC for single server deployment using CLI ... 461
Reconfiguration command options ... 461
Enabling or disabling network interfaces using CLI ... 465
Editing SIP server profile parameters using CLI ... 465
Editing network management parameters using CLI ... 466
Creating and restoring configurable snapshot using CLI ... 466
Deleting the secondary EMS ... 467
Changing management IP, gateway and network mask details for a single server deployment ... 467
Changing the management IP for an HA deployment ... 467
Changing management IP, gateway IP, and network mask details on primary EMS ... 467
Changing management IP, gateway IP, and network mask details on secondary EMS ... 469
Changing management IP, gateway IP, and network mask details on Avaya SBC ... 470
Changing hostname ... 470
Changing network passphrase ... 470
Regenerating self-signed certificates ... 471
Regenerating the rest credentials ... 471
Changing DNS IP and FQDN ... 471
Regenerating the rest credentials ... 472

Resetting SNMP configuration 473
Restarting spiritAgent 473
Chapter 12: Template Wizard 474
Managing DAT files 475
Prerequisites 475
Installing a DAT file 475
Editing a DAT file 476
Deleting a DAT file 476
Using Template Wizard 476
Template Wizard field descriptions 477
Verifying the configuration 481
Chapter 13: Configuring Remote Worker 483
Remote worker overview 483
Limitations and interactions when administering the Remote Worker solution 484
Session Manager configuration for Avaya SBC 485
Whitelisting Avaya SBC internal IP address 486
Adding the internal IP of Avaya SBC in System Manager 486
Disabling PPM rate limiting 487
Remote worker configuration checklist 487
Cloning the Avaya-ru profile 488
Creating an Avaya call server profile 489
Creating an external signaling interface for a phone network 490
Creating an internal signaling interface for an Avaya call server 491
Add Signaling Interface field descriptions 492
Creating an external media interface for a phone network 493
Creating an internal media interface for an Avaya call server 493
Add Media Interface field descriptions 494
Creating custom PPM mapping profiles 494
Custom PPM mapping profile field descriptions 497
Creating a reverse proxy policy 498
Reverse Proxy Policy field descriptions 498
Creating a reverse proxy relay service for PPM traffic 500
Creating a reverse proxy relay service for file or firmware download 501
Creating reverse proxy service for multi-tenant or IP Office powered deployments 502
Relay Services field descriptions 504
Creating standard PPM mapping profiles 509
Standard PPM mapping profile field descriptions 511
Creating a media rule 512
Creating application rules 513
Creating an endpoint policy group 513
Creating a routing profile towards Avaya Aura® call server 514
Creating a server flow 515
Creating a subscriber flow 516

Configuring application relay for IM 518
Checklist for configuring Presence server 519
Monitoring RTCP for a single Session Manager deployment 519
Application relay settings for RTCP monitoring using single Session Manager 520
Configuring call support for unregistered endpoints 520
Checklist for back-to-back configuration with a single Session Manager 522
Checklist for back-to-back-to-back configuration with a single Session Manager 523
Monitoring RTCP for back-to-back-to-back deployment 524
Application relay settings for monitoring RTCP using back-to-back-to-back deployment 525
Chapter 14: Configuration of server flows for SIP trunking 527
About SIP trunking 527
SIP trunk configuration checklist 528
Creating Interworking Profiles 529
Creating Server Profile for Call Server 530
Creating Server Profile for Trunk-side server 531
Creating a Routing Profile for a Call Server 532
Creating Routing Profile for Trunk Server 533
Creating a Topology Hiding profile 535
Creating external signaling interface toward Trunk-side server 536
Creating Internal Signaling Interface toward Call Server 537
Creating External Media Interface toward Trunk Server 538
Creating Internal Media Interface toward call server 538
Creating call server flow 539
Creating a trunk server flow 540
Configuring Avaya SBC for SIP Trunk 541
Configuring Avaya SBC for other trunks 542
Chapter 15: Branch Survivability 543
Checklist for configuring Branch Survivability 544
Creating a TLS server profile 545
Adding a new signaling interface 545
Creating a Branch Session Manager server profile 546
Creating a routing profile 547
Creating a server flow for Branch Session Manager 547
Creating a server flow for Core Session Manager 548
Chapter 16: Multiple Session Manager 550
Multiple Session Manager support for Avaya SBC in Remote Worker deployment 550
Multiple Session Manager configuration checklist 551
Configuring the Avaya SBC IP addresses corresponding to the primary and secondary Session Managers 553
Creating a server interworking profile 553
Configuring application relay settings for multiple Session Manager 554
Multiple Session Manager support with back-to-back Avaya SBCs 554
Back-to-back configuration checklist 555

Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBC systems 556
Back-to-back-to-back configuration checklist 557
Geographic-redundant deployment 559
Geographic-redundant deployment in the non-HA mode 559
Geographic-redundant deployment in the HA mode 560
Checklist for configuring Geographic-redundant deployment 561
Creating an endpoint policy 563
Configuring Avaya SBC for web collaboration 564
Configuring Presence Server 565
Chapter 17: Signaling manipulation 566
About signaling manipulation 566
SigMa scripting language 566
SigMa primer 566
SigMa Scripting examples 574
SigMa Scripting Tutorial 577
Signaling Manipulation Scripts field descriptions 583
Sigma Design Overview 584
Specifying a SigMa script in a server configuration 584
Chapter 18: Remote access 586
Chapter 19: Zero Down Time support 587
Zero Down Time support for AEC deployments 587
Chapter 20: Video devices interoperability 589
Binary Floor Control Protocol 589
Configuring Binary Floor Control Protocol 589
SRTP overview 590
Considerations for SRTP after failover 590
Forward Error Correction 590
Far End Camera Control 591
Configuring Far End Camera Control 591
Chapter 21: WebRTC-enabled call processing 592
WebRTC-enabled call handling 592
WebRTC considerations 592
Turntop 593
Running the turntop command 593
Configuring the TURN/STUN profile for WebRTC calls in Avaya SBC 594
Add TURN STUN Profile field descriptions 595
Configuring the TURN relay service for WebRTC calls in Avaya SBC 596
Add TURN Relay field descriptions 597
Chapter 22: Configuring SIPREC integration 598
About configuring Avaya SBC for recording media sessions 598
Checklist for configuring Avaya SBC for SIPREC 599
Configuring a recording server 600

Configuring one or more recording profiles and assigning the recording profile to a routing profile ... 602
Enabling UCID for the signaling rules used on the Session Manager endpoint policy group ... 603
Creating a media rule for the Recording Server ... 604
Creating a new session policy for the Recording Server ... 604
Adding a custom wave file for the recording tone ... 605
Adding a session flow for the Recording Server ... 606
Chapter 23: Secure CES proxy ... 608
Secure Client Enablement Services proxy configuration ... 608
Client Enablement Services CA certificate ... 608
Extracting the Client Enablement Services CA certificate ... 608
Creating a client TLS profile ... 609
Configuring CES proxy ... 610
Chapter 24: Call preservation ... 612
About the Avaya SBC configuration for Call Preservation ... 612
Checklist for configuring Avaya SBC for Call preservation ... 613
Creating FGDN groups ... 613
FGDN Group field descriptions ... 614
Enabling FGDN for a Session Manager in the FGDN group ... 614
Creating a routing rule for Call preservation ... 615
Adding the routing rule to the trunk server flow ... 615
Changing transaction expiry time in Server Interworking ... 616
Chapter 25: SIP resiliency ... 617
Avaya Aura® SIP Resiliency ... 617
Enabling SIP Resiliency ... 617
Chapter 26: Transcoding ... 619
About configuring Avaya SBC for transcoding and transrating ... 619
Checklist for configuring Avaya SBC for transcoding ... 620
Enabling transcoding and transrating ... 620
Configuring codec prioritization ... 621
Configuring endpoint policy group ... 622
Configuring a server flow for transcoding ... 622
Chapter 27: CDR measurement and media statistics ... 623
CDR adjunct ... 624
Creating a CDR adjunct ... 624
Radius profile ... 625
Creating a Radius profile ... 625
Editing the Radius profile ... 626
Renaming the Radius profile ... 627
Deleting the Radius profile ... 627
Enabling CDR in an application ... 627
Enabling periodic statistics ... 628
Chapter 28: Media tunneling ... 630

Media tunneling checklist ... 630
Enabling media tunneling ... 631
Disabling media tunneling ... 631
Adding a media interface ... 631
Creating a TLS server profile ... 632
Chapter 29: Configuring Avaya SBC to work with an external Avaya Aura Media Server ... 633
About configuring Avaya SBC and an external Avaya Aura® Media Server ... 633
Checklist for configuring an external media server ... 633
Enabling Avaya Aura® Media Server offloading ... 634
Configuring a media server ... 635
Creating a session policy for a media server ... 635
Adding a session flow for a media server ... 636
Chapter 30: Edge Gateway support ... 637
Edge Gateway ... 637
Checklist for configuring Avaya SBC for Edge gateway ... 639
Configuring the Edge Gateway SNMP trap destination ... 639
H248 Profile field descriptions ... 640
Creating a new H248 server ... 640
Add H248 server field descriptions ... 640
Adding a new media interface ... 641
Add Media Interface field descriptions ... 641
Configuring H248 relay ... 642
Configuring application relay for Edge Gateway ... 643
Back to back H248 Proxy ... 643
Configuring back to back H248 Proxy ... 644
Chapter 31: Resources ... 645
Documentation ... 645
Finding documents on the Avaya Support website ... 647
Accessing the port matrix document ... 647
Avaya Documentation Center navigation ... 648
Training ... 649
Viewing Avaya Mentor videos ... 650
Support ... 650
Appendix A: Solution for simultaneous downloads of config and firmware files ... 651
Simultaneous downloads of config/firmware files ... 651
GROUP identifier in endpoint administration ... 651
File server configuration example ... 652
Phone configuration ... 653
Configuring Avaya SBC ... 653
Appendix B: EMS web interface ... 655
EMS web interface ... 655
EMS screen elements ... 655

Appendix C: RFC support 670
RFC support 670
Appendix D: CDR file field description 672
CDR file field descriptions 672
Glossary 679

Chapter 1: Introduction

Purpose

This document contains information about administering and configuring Avaya Session Border Controller (Avaya SBC).

This document provides information about how to use the Unified Communications Policies features, also referred as Domain Policies, of Avaya SBC. With the Domain Policies feature, you can configure, apply, and manage security rule sets, which are based upon the source and destination endpoint and session call flows entering or exiting the enterprise. The document also provides information to monitor SIP-based UC network security by using the Element Management System (EMS) web interface and various incident and historical reports.

This document is intended for people who administer Avaya SBC.

Chapter 2: Overview

Avaya Session Border Controller (Avaya SBC) is a solution for network security in Unified Communications. You can administer Avaya SBC using the Element Management System (EMS) web interface.

Avaya SBC supports the following redundancy options:

- Standalone
- Geo-redundancy
- High Availability
- Geo-redundancy and High Availability

Avaya SBC security devices

Avaya SBC security devices can be monitored and controlled remotely through Graphical User Interface (GUI) or locally through Command Line Interface (CLI). GUI access is provided through Ethernet management interface ports located on each Avaya SBC equipment chassis. Administrators can have up to 10 simultaneous logins to the EMS web interface with Ethernet management interface ports. CLI access is provided through the console or VGA port based on the parameters selected during installation or upgrade. The ports are located on the Avaya SBC equipment chassis. With console ports, you can establish direct physical connections to the devices using any commonly available terminal device for provisioning, management, troubleshooting, maintenance, and repair. You can access the GUI and CLI interfaces anytime when an Avaya SBC security device is operational. Additionally, the CLI access is provided remotely through an SSH connection to the EMS or SBC server using port 222.

Graphical User Interface

Avaya SBC security devices support GUI through EMS. EMS can be accessed from any remote physical location by using one of the following web browsers:

- Mozilla Firefox 60.0/ 60.0 ESR or later
- Microsoft Internet Explorer 11.0 or later
- Microsoft Edge 20.0 or later
- Google Chrome 59.0 and later

- Apple Safari (4) 9.0 or later

Administrators and maintenance personnel can view concise, real-time, graphical representations of the security activities and operational condition of the network. With EMS, administrators can gain access to all the screens and windows that are necessary to configure and maintain each security aspect of a particular Avaya SBC device.

Command Line Interface

Command Line Interface (CLI) is a management interface that provides local access to a particular Avaya SBC security device for performing administrative and operational tasks. The tasks are executed by using various commands entered through a terminal emulator, such as SSH, or other commonly available serial applications like PuTTY. Ensure that you update to the latest version of PuTTY. CLI is available whenever an Avaya SBC equipment chassis is running. Security is provided through a combination of account login and user access privileges.

Note:

Use Command Line Interface under the direction of authorized Avaya support personnel.

Logging in to the EMS web interface

Procedure

1. Open a compatible web browser.
2. Type the URL `https://IP_Address/sbc`, where IP_Address is the management IP address of the EMS server.
3. Press `Enter`.
4. On the Session Border Controller for Enterprise screen, in the **Username** field, type the username.
5. In the **Password** field, type the password.

   Note:

   After logging in with the default password, you must change the password.
6. Click **Log In**.

   Avaya SBC displays the Dashboard screen.

Password policies

The `root` and `ipcs` passwords are set during product installation. The EMS GUI has a separate password.

The default user IDs and passwords are the following:

Username	Password
`root`	`@V@Y@_123`
`ipcs`	`Avaya_123`
`ucsec` (GUI only)	`ucsec`

Note:

After the factory reset, the golden password for the root user ID is `Avaya_123`.

Security alert:

You must change the default passwords for the CLI root and ipcs user IDs after the first boot during the installation procedure. When prompted, you must enter and confirm the new password. Password restrictions are enforced on the root, ucsec, and ipcs user IDs. The new password must meet the following criteria:

- Contains at least eight characters.
- Contains one uppercase letter, one lowercase letter, and one number.
- Contains one special character from the following: a hyphen (-), an underscore (_), the at sign (@), an asterisk (*), or the exclamation mark (!). Do not use the pound sign (#), the dollar sign ($), or an ampersand (&).

Console and SSH passwords complexity

The Console and SSH passwords must adhere to the following requirements:

- Contain at least eight characters.
- Contain at least two uppercase characters, not including the first character of the password.
- Contain at least one lowercase character.
- Contain at least one special character.
- Contain at least two digits, not including the last character of the password.

The Console and SSH passwords do not have a limit on the maximum length and are hashed by the MD5 hash algorithm.

Note:

Password Authentication Module (PAM) enforces password security, and hashes are stored in: `/etc/shadow`

EMS GUI password complexity

The EMS GUI password must fulfill the following norms:

- Have at least eight characters.
- Contain mixed uppercase and lowercase characters.
- Contain at least one special character.

- Contain at least one number.

The EMS GUI password does not have a limit on the maximum length and is hashed by the MD5 hash algorithm.

Change Password field descriptions

Name	Description
Current Password	The password currently used for logging in.
New Password	The new password that replaces the old password.
Repeat password	The new password repeated for confirmation.

Resetting the GUI password

Procedure

1. Log in to the CLI interface as a root user.
2. To reset the password, run the following command: `gui-user --edit <username> --password <password>`
3. **(Optional)** If the account is expired, run the following command to restore the user status: `gui-user --edit <username> --status ok`
4. **(Optional)** To get additional information on how to use the gui-user command, run the following command: `gui-user --help`

Grub password complexity

The Grub password must adhere to the following requirements:

- Contain at least eight characters.
- Contain uppercase and lowercase characters.
- Contain at least special character except %, &, and $.
- Contain at least two digits.

You can change the Grub password with the **`sbceconfigurator.py change-grub-password`** command.

Password hashing mechanisms

Release	GUI	API / Peon (User only)	Platform
8.x	SHA-256	PBKDF2/SHA-512	SHA-512
10.1.x	SHA-256	PBKDF2/SHA-512	SHA-512
10.2.x	Argon2	PBKDF2/SHA-512	SHA-512

Chapter 3: Administrative user accounts

Administrative user accounts and authentication modes

You must create administrative user accounts for each individual who requires access to Avaya SBC. Use the procedures in this section to assign users, roles, authentication methods, permissions, password policies, and other access-related parameters.

Roles

You can assign the following standard roles to administrative user accounts:

- System Administrator: Has full read/write permissions for Avaya SBC security features, including the ability to add, edit, and delete other administrative accounts.
- System Engineer: Has the same privileges as System Administrator, except they cannot add or modify user accounts.
- Service Administrator: Has the same privileges as System Administrator, but cannot add new accounts. Service Administrator can only view TLS and firewall settings.
- Security Administrator: Can manage system users, TLS, and firewall settings.
- FIPS 140-2 Crypto Officer: Can only view and manage TLS settings.
- Auditor: Has read-only access to view incident and statistical logs.
- Backup Administrator: Can create and restore system snapshots.
- External Users Administrator: Can only manage external users. External users are authenticated using LDAP or a remote RADIUS server.

EASG-Specific roles

For the Avaya Enhanced Access Security Gateway (EASG) feature, the following special roles can be assigned:

- Avaya Services Administrator: A default role for EASG administrators. Privileges are similar to those of System Administrator accounts.
- Avaya Services Maintenance and Support: A default role for EASG support users. Privileges are similar to those of Auditor accounts.

Authentication modes

You can use the following modes to authenticate administrative users:

- Local: Authenticates users through the local administrative control of Avaya SBC.
- RADIUS: Authenticates users through a Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS server must be configured in Avaya SBC before this

authentication method is assigned. For more information, see Adding a RADIUS server on page 36.

- LDAP: Authenticates users through the customer's Active Directory system. LDAP users must also exist in the Active Directory, and the directory must be linked to Avaya SBC.
- X.509: A standard that requires all server-based products to support X.509-formatted user certificates for multi-factor authentication (MFA) of administrative users.
- EASG: Enhanced Access Security Gateway (EASG) provides secure, customer-controlled access for Avaya services personnel. EASG users exist only when the customer grants Avaya access to the system.

Managing user accounts

Creating an administrative user account

Before you begin

- Before creating a user who will use LDAP authentication, configure the LDAP server.

  For more information, see Configuring LDAP server authentication on page 32.
- Before creating a user who will use X.509 certificate authentication, do the following:
  1. Configure the X.509 certificate authentication.

     For more information, see Configuring X.509 certificate authentication on page 34.
  2. Upload CA trust anchors to EMS.

     For example, `/usr/local/ipcs/etc/cert/gui/pki-auth.pem`.
  3. (Optional) Upload CA intermediaries to EMS.

     For example, `/usr/local/ipcs/etc/cert/gui/pki-auth-intermediates.pem`.
  4. (Optional) Upload certificate revocation lists (CRLs) to EMS.

     For example, `/usr/local/ipcs/etc/cert/gui/pki-auth.crl`.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **Users**.
4. On the **Users** tab, click **Add User**.
5. Configure the user.

   For more information about the fields, see Administrative user account field descriptions on page 28.

6. Click **Finish**.

   In the Users tab, the EMS server displays the new administrative account.

Administrative user account field descriptions

Name	Description
User Name	The system-assigned name for the account owner.
Real Name	The actual name of the individual for whom the account is being created.
Contact Information	The contact details of the account owner, such as email address and phone number.
Type	The authentication method for the user. Options include the following: • **Local**: Authenticates the user through the local administrative control of Avaya SBC. • **LDAP**: Authenticates the user through the Active Directory system of the customer. LDAP users must also exist in the Active Directory, and the directory must be linked to Avaya SBC. This option is available only if **LDAP** is enabled on the **Administration Parameters** tab. When you select **LDAP**, the **Password**, **Confirm Password**, and **Force Password Change on Next Login** fields are disabled. • **RADIUS**: Authenticates the user through a Remote Authentication Dial-In User Service (RADIUS) server. This option is available only if a RADIUS server is configured and **RADIUS** is enabled on the **Administration Parameters** tab. When you select **RADIUS**, the **Password**, **Confirm Password**, and **Force Password Change on Next Login** fields are disabled. • **ASG**: A display-only option that identifies a user authenticated through EASG. You cannot change this option.
Password	The password for the user. This field is disabled for LDAP, RADIUS, and EASG accounts.
Confirm Password	The confirmation password for the user. This field is disabled for LDAP, RADIUS, and EASG accounts.
Force Password Change on Next Login	The option to require the user to create a new password at their next login. This field is disabled for LDAP, RADIUS, and EASG accounts.
Allow X.509 Authentication	The option to enable X.509 authentication for the user account. This field is available only if **X.509** is enabled on the **Administration Parameters** tab.

Table continues…

Name	Description
Authentication Mode	The X.509 authentication mode. Options include the following: • **Inherit from AAA Settings**: Authenticates the user based on the global authentication mode settings. For more information, see X.509 certificate authentication field descriptions on page 35. • **Accept X.509 Certificate or Password**: Authenticates the user if a valid certificate or a valid password is provided. • **Require X.509 Certificate**: Authenticates the user only if a valid certificate is provided. Any password the user enters is ignored. • **Require X.509 Certificate and Password**: Authenticates the user only if a valid certificate and a valid password are provided.
Accepted Common Names	Common names that are accepted when authenticating an X.509 certificate. The list of names must be separated by a new-line character.
Role	The level of administrative access to the account. Options include the following: • **System Administrator** (default): Has full read/write permissions for Avaya SBC security features, including the ability to add, edit, and delete other administrative accounts. • **System Engineer**: Has the same privileges as System Administrator, except they cannot add or modify user accounts. • **Service Administrator**: Has the same privileges as System Administrator, but cannot add new accounts. Service Administrator can only view TLS and firewall settings. • **Security Administrator**: Can manage system users, TLS, and firewall settings. • **FIPS 140–2 Crypto Officer**: Can only view and manage TLS settings. • **Auditor**: Has read-only access to view incident and statistical logs. • **Backup Administrator**: Can create and restore system snapshots. • **External Users Administrator**: Can only manage external users. External users are authenticated using LDAP or a remote RADIUS server.

Table continues…

Name	Description
Status	The current status of the user account. Options include the following: • **Normal** • **Disabled** • **Locked** • **Expired** You cannot change the status of the user to **Locked**. The EMS server is set after multiple unsuccessful login attempts. **Note:** Disabling a user account or changing its role disconnects all clients connected to that user account.

Editing an administrative user account

Procedure

1. Log in to the EMS web interface using administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **Users**.
4. On the **Users** tab, select the user and click **Edit**.
5. On the Edit User window, make the necessary changes.

   For more information, see Administrative user account field descriptions on page 28.
6. Click **Finish**.

Deleting an administrative user account

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **System Administration** > **Users**.
4. On the **Users** tab, click **Delete** corresponding to the administrative account that you want to delete.

   The EMS server displays a confirmation window.
5. Click **OK**.

Configuring password rules and lockout options

About this task

Use this procedure to configure password rules and lockout options for the following user accounts:

- Administrator
- Manager
- Supervisor

The options you administer here will apply to all users.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **Users**.
4. On the **Settings** tab, administer the options described in Password and lockout field descriptions on page 31.
5. Click **Save**.

   The EMS server displays a notification in the content area indicating that the new configuration is saved.

Password and lockout field descriptions

Name	Description
Local Account Password Expiration	A check box indicating whether the password assigned to this user account will expire after the number of days indicated in the corresponding field. If selected, the assigned password expires after the indicated number of days. If cleared, you can use the password assigned to this user account indefinitely.
Local Account Password Expiration Notification	A check box indicating whether a notification to the user is displayed at the time of log in. The notification is about the expiry of the password within a specific number of days. If selected, a notification is displayed each time the user logs on to the EMS. If cleared, a notification is not displayed.
Reject Previously Used Passwords	The number of previously used passwords that cannot be used.

Table continues…

Name	Description
Failed Attempts Before Lockout	A check box indicating whether the user account is locked out after the number of login attempts indicated in the corresponding field.
Failed Attempt Window	A check box indicating whether the failed attempt counter must be reset after the least amount of time between login attempts specified in the corresponding field. If cleared, any subsequent failed login attempts increase the failed attempt counter.
Lockout Duration	A check box indicating whether an account remains locked for the number of seconds specified in the corresponding field. After the lockout duration passes, the attempt of the next user to log in to a locked account resets the account state to normal.

Configuring LDAP server authentication

About this task

Note:

SSL/TLS Cipher Suites cannot be configured.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **LDAP** tab.
5. Administer the LDAP server authentication with the options described in LDAP server authentication field descriptions on page 32.
6. Click **Save**.

   The system saves the LDAP authentication configuration.

LDAP server authentication field descriptions

Name	Description
Enabled	Controls whether LDAP authentication is enabled.
Primary Server Address	The IP address and optional port of the primary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.

Table continues…

Name	Description
Secondary Server Address	(Optional) The IP address and optional port of the secondary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.
Secure Mode	Select one of the following options: • **None**: No encryption (not recommended) • **SSL/TLS**: Secure connection established via TLS handshake (highly recommended) • **STARTTLS**: Secure connection established by unsecure connection and upgrading to secure connection (for legacy support, not recommended)
CA Certificate PEM File	The path to the Privacy Enhanced Mail (PEM) file on the EMS server that contains trust anchors for the certificate when connecting with SSL or TLS. You must create this file and put it on the EMS server. If a path is not specified, use the default path of: `/usr/local/ipcs/etc/cert/gui/ldap-auth.pem`. If a path is specified and the PEM file does exist, it is used to build a trust manager that is in turn used to verify the LDAP server certificate upon connection. If at least one certificate matches a CA certificate in the trust manager, the verification succeeds. Otherwise, the verification fails and the connection attempt fails. If a path is specified but the PEM file does not exist, all certificates are trusted. That is, no certificate verification is done on the LDAP server and all certificates are accepted.
Bind DN	The distinguished name (DN) used when initially authenticating to the LDAP server to do a user lookup. This user name must have appropriate permissions to search and read users that need to authenticate.
Bind Password	The password to send with the Bind DN when initially authenticating to the LDAP server.
Base DN	The base DN to use when searching for users.
User Domain	(Optional) An optional domain to use in LDAP searches.
User Search Filter	A filter used to search for an LDAP user. Only the first entry that matches is retrieved, so this filter should be as specific as possible. The {username} and {domain} can be used as placeholders for the actual values when authentication takes place. If no domain is specified, the filter defaults to `(sAMAccountName={username})`. If a domain is specified, the filter defaults to `(userPrincipalName={username}@{domain})`.
Timeout	The timeout, in seconds, before a connection attempt to the primary LDAP server is marked as failed and the next connection attempt is made (if a secondary LDAP server exists).

Table continues…

Name	Description
Use LDAP as Fall-through Authenticator	Select this option to enable a back end authentication server to handle authentication requests for users that are not defined in the EMS user list. This is done by fetching a specified LDAP attribute when running the User Search Filter on the LDAP server to find a user matching the provided credentials as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or any authorization attempts for the user will fail and the user's login requests will be rejected. If the attribute is not present on the user, any authorization attempts for the user fail and the user's login requests are rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both LDAP authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.
Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”. This attribute is not defined in most LDAP schemas and must be defined to function correctly. Alternatively, any other LDAP attribute can be used as long as it is a string value. For an example of how to define a custom attribute in Microsoft Active Directory, see: https://social.technet.microsoft.com/wiki/contents/articles/20319.how-to-create-a-custom-attribute-in-active-directory.aspx

Configuring X.509 certificate authentication

About this task

Note:

X.509 certificate authentication has the following limitations:

- Certificate verification will fail unless the root CA and all intermediate CAs are added as trust anchors and/or intermediates on the Avaya SBC system regardless of whether the client sends the full trust chain.

- Online Certificate Status Protocol (OCSP) checking is currently not supported.
- Certificate Revocation List (CRL) Distribution Point checking is not supported.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **X.509** tab.
5. Administer the X.509 certificate authentication with the options described in X.509 certificate authentication field descriptions on page 35.
6. Click **Save**.

   The system saves the X.509 certificate authentication configuration.

X.509 certificate authentication field descriptions

Name	Description
Enabled	Controls whether X.509 certificate authentication is enabled. X.509 certificate authentication cannot be enabled unless the CA Trust Anchors Privacy Enhanced Mail (PEM) file exists on the file system.
CA Trust Anchors PEM File	This is a PEM file that should contain all CA trust anchors used to verify X.509 certificates. Multiple entries should be concatenated together.
CA Intermediaries PEM File	This is a PEM file that should contain all intermediate CAs used to construct trust chains used to validate certificates. These certificates are not implicitly trusted and are only used in reconstructing the trust chain. Multiple entries should be concatenated together.
CRL File	This is a PEM file that should contain all certificate revocation lists used to revoke X.509 certificates. Multiple entries should be concatenated together.
Authentication Mode	The method used to authenticate X.509 certificate users. Select one of the following options: • **Accept X.509 Certificate or Password**: The user will be authenticated if either a valid certificate or a valid password is provided. • **Require X.509 Certificate**: The user will be authenticated only if a valid certificate is provided. Any password entered by the user is ignored. • **Require X.509 Certificate and Password**: The user will be authenticated only if both a valid certificate and valid password is provided.

Enabling EASG

The Enhanced Access Security Gateway (EASG) system is a key element in protecting passwords and preventing unauthorized use of maintenance and administration login. EASG provides a secure method for Avaya support personnel to access Avaya SBC remotely. Access is under the control of the customer. EASG is a 128–bit AES encrypted challenge-response mechanism for authentication. With this mechanism, Avaya SBC can maintain secure access for services, administration, and maintenance. On Avaya Enterprise Communications System (ECS) products, Avaya services personnel use the EASG challenge and corresponding response for a single access attempt only. After each login, EASG uses a new challenge and response .

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. On the **EASG** tab, click **Enable** if EASG is not already enabled.

Managing a RADIUS server

Adding a RADIUS server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **RADIUS Servers** tab.
5. Click **Add**.

   The system displays the Add Server screen.
6. Administer the server with the options described in RADIUS server field descriptions on page 37.
7. Click **Finish**.

   The system displays the new RADIUS server in the content area.
8. Restart the IPCS services as described in Restarting the IPCS services on page 76.

RADIUS server field descriptions

Name	Description
Server Name	A descriptive name to identify the RADIUS server.
Primary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Secondary Address (ip:port)	The IP address and port number of the server designated as the secondary RADIUS server.
Retry Timeout (seconds)	The maximum time in seconds taken for a successful authentication to be completed. If authentication is not completed within this time, SBC ends the connection automatically and generates an incident .
Max Retry	The maximum number of times that a user can attempt to authenticate before SBC ends the connection .
Ignore Session Expire	The check box that indicates whether the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Select this check box for Avaya SBC to maintain the current session upon receipt of the SESSION EXPIRE message. Clear the check box for Avaya SBC to end the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method that the Avaya SBC security device uses to select a RADIUS server to choose to authenticate a user. The options are: • **Active Standby** • **Round Robin**
Authentication Protocol	The authentication protocol to be used for RADIUS authentication. The options are: • **None** • **EAP_TTLS/EAP_ PAP** • **EAP_PEAP/EAP_GTC**
Server Secret	The shared secret maintained between the Avaya SBC security device and the active RADIUS server with which communications between the two is encrypted.
Confirm Server Secret	Respecifies the shared secret maintained between the Avaya SBC security device and the active RADIUS server .

Table continues…

Name	Description
Accounting Server	The check box to indicate whether this RADIUS server must also to be designated as an Accounting Server and receive CDRs. Select this check box to indicate that RADIUS server is also an Accounting Server and can receive CDRs. Clear the check box to indicate that RADIUS server is not an Accounting Server and does not receive CDRs.

Editing a RADIUS server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **RADIUS Servers** tab.
5. Click **Edit** for the RADIUS server you want to edit.

   The system displays the Edit Server pop-up window.
6. Edit the server with the options described in RADIUS server field descriptions on page 37.
7. Click **Finish**.

   The system updates and saves the RADIUS server configuration.
8. Restart the IPCS services as described in Restarting the IPCS services on page 76.

Deleting a RADIUS server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **RADIUS Servers** tab.
5. Click **Delete** on the RADIUS server that you want to delete.

   The EMS server displays a confirmation pop-up window.
6. Click **OK** to confirm.

   The system deletes the selected RADIUS server.
7. Restart the IPCS services as described in Restarting the IPCS services on page 76.

Configuring RADIUS server authentication

Before you begin

Do the following to verify whether a RADIUS server already exists.

1. Log on to the EMS web interface with administrator credentials.
2. From the **Device** drop-down list, select **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **RADIUS Servers** tab.
5. If a RADIUS server is not listed, create a RADIUS server using the procedure found in Adding a RADIUS server on page 36.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS**.
3. Navigate to **System Administration** > **AAA**.
4. Select the **RADIUS** tab.
5. Administer the RADIUS server authentication with the options described in RADIUS server authentication field descriptions on page 39.
6. Click **Save**.

   The system saves the RADIUS authentication configuration.

RADIUS server authentication field descriptions

Name	Description
Enabled	A check box indicating whether the RADIUS user accounts must be authenticated using Authentication, Authorization, and Accounting (AAA). If selected, RADIUS user accounts are authenticated by the server selected from the **Radius Server** option. If cleared, RADIUS user accounts are not authenticated.
RADIUS Server	Select the RADIUS server being used for AAA.
RADIUS Authentication Protocol	A drop-down menu containing all supported RADIUS authentication methods. This menu is used instead of the authentication protocol of the configured RADIUS profile. The currently supported methods are: • **Password Authentication Protocol (PAP)**: The password is transmitted in plain text to the RADIUS server. • **RFC 5090/Digest**: The password uses a client and server one time to generate an MD5 authentication token for use with an RFC 5090–compliant RADIUS server. • **Challenge-Handshake Authentication Protocol (CHAP)**: The password is salted with a rolling ID, hashed, and transmitted to the RADIUS server.

Table continues…

Name	Description
RADIUS Realm	The realm to use when generating the Digest authentication token. Use the same value in this field as the value configured on the RADIUS server.
Use RADIUS as Fall-through Authenticator	Select this option to enable a back end authentication server to handle any authentication requests for users that are not defined in the EMS user list. This is done by sending an Access-Request packet to the RADIUS server, which looks for a specific attribute in the Access-Accept response as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or the authorization fails and the user login request is rejected. If the attribute is not present in the request, the authorization fails and the user login request is rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both RADIUS authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.

Table continues…

Name	Description

Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”.
	
	If you are using attributes that are defined in the standard RADIUS dictionary, you can use the standard dictionary and a custom dictionary is not required.
	
	However, if you are using the default attribute name “Avaya-SBCE-Role-Name”, or are using a vendor-specific attribute as the role attribute name, you must create a custom dictionary definition. A custom dictionary is required to handle the attribute the Avaya SBC requires for authorization. A sample dictionary is provided below, which can be modified with any values if necessary. If a different RADIUS attribute is desired, then any attribute can be used including both default values and custom values.
	
	Note:
	
	There might be scenarios when a custom dictionary is required to define a new attribute that Avaya SBC administration can recognize, or to handle conflicts if a RADIUS server is already using an existing Avaya dictionary. In this scenario, Avaya SBC administration will read from a file located at `/usr/local/ipcs/etc/gui-radius-dictionary`, if it exists. It is important to note that defining this file will prevent Avaya SBC administration from reading the default dictionary and instead use the contents of the file as the new dictionary.
	
	`############################################################`
	`# WARNING: This dictionary file is intended to be a sample and`
	`# is intended to illustrate how to define attributes for use with`
	`# the Avaya SBCE SSO fall-through authentication functionality.`
	`# The identifiers in this file have not been officially allocated`
	`# and may need modification to interop with other vendor specific`
	`# attributes from Avaya or other vendors.`
	`#####################################################################`
	`VENDOR Avaya-SBCE 6889`
	`BEGIN-VENDOR Avaya-SBCE`
	
	`ATTRIBUTE Avaya-SBCE-Role-Name 1 string`
	
	`END-VENDOR Avaya-SBCE`

AAA field descriptions

RADIUS Server Authentication

Name	Description
Enabled	A check box indicating whether the RADIUS user accounts must be authenticated using Authentication, Authorization, and Accounting (AAA). If selected, RADIUS user accounts are authenticated by the server selected from the **Radius Server** option. If cleared, RADIUS user accounts are not authenticated.
RADIUS Server	Select the RADIUS server being used for AAA.
RADIUS Authentication Protocol	A drop-down menu containing all supported RADIUS authentication methods. This menu is used instead of the authentication protocol of the configured RADIUS profile. The currently supported methods are: • **Password Authentication Protocol (PAP)**: The password is transmitted in plain text to the RADIUS server. • **RFC 5090/Digest**: The password uses a client and server one time to generate an MD5 authentication token for use with an RFC 5090–compliant RADIUS server. • **Challenge-Handshake Authentication Protocol (CHAP)**: The password is salted with a rolling ID, hashed, and transmitted to the RADIUS server.
RADIUS Realm	The realm to use when generating the Digest authentication token. Use the same value in this field as the value configured on the RADIUS server.
Use RADIUS as Fall-through Authenticator	Select this option to enable a back end authentication server to handle any authentication requests for users that are not defined in the EMS user list. This is done by sending an Access-Request packet to the RADIUS server, which looks for a specific attribute in the Access-Accept response as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or the authorization fails and the user login request is rejected. If the attribute is not present in the request, the authorization fails and the user login request is rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both RADIUS authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.

Table continues…

Name	Description

Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”.
	
	If you are using attributes that are defined in the standard RADIUS dictionary, you can use the standard dictionary and a custom dictionary is not required.
	
	However, if you are using the default attribute name “Avaya-SBCE-Role-Name”, or are using a vendor-specific attribute as the role attribute name, you must create a custom dictionary definition. A custom dictionary is required to handle the attribute the Avaya SBC requires for authorization. A sample dictionary is provided below, which can be modified with any values if necessary. If a different RADIUS attribute is desired, then any attribute can be used including both default values and custom values.
	
	Note:
	
	There might be scenarios when a custom dictionary is required to define a new attribute that Avaya SBC administration can recognize, or to handle conflicts if a RADIUS server is already using an existing Avaya dictionary. In this scenario, Avaya SBC administration will read from a file located at `/usr/local/ipcs/etc/gui-radius-dictionary`, if it exists. It is important to note that defining this file will prevent Avaya SBC administration from reading the default dictionary and instead use the contents of the file as the new dictionary.
	
	`############################################################`
	`# WARNING: This dictionary file is intended to be a sample and`
	`# is intended to illustrate how to define attributes for use with`
	`# the Avaya SBCE SSO fall-through authentication functionality.`
	`# The identifiers in this file have not been officially allocated`
	`# and may need modification to interop with other vendor specific`
	`# attributes from Avaya or other vendors.`
	`############################################################`
	`VENDOR Avaya-SBCE 6889`
	`BEGIN-VENDOR Avaya-SBCE`
	
	`ATTRIBUTE Avaya-SBCE-Role-Name 1 string`
	
	`END-VENDOR Avaya-SBCE`

LDAP Server Authentication

Name	Description
Enabled	Controls whether LDAP authentication is enabled.
Primary Server Address	The IP address and optional port of the primary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.
Secondary Server Address	(Optional) The IP address and optional port of the secondary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.

Table continues…

Name	Description
Secure Mode	Select one of the following options: • **None**: No encryption (not recommended) • **SSL/TLS**: Secure connection established via TLS handshake (highly recommended) • **STARTTLS**: Secure connection established by unsecure connection and upgrading to secure connection (for legacy support, not recommended)
CA Certificate PEM File	The path to the Privacy Enhanced Mail (PEM) file on the EMS server that contains trust anchors for the certificate when connecting with SSL or TLS. You must create this file and put it on the EMS server. If a path is not specified, use the default path of: `/usr/local/ipcs/etc/cert/gui/ldap-auth.pem`. If a path is specified and the PEM file does exist, it is used to build a trust manager that is in turn used to verify the LDAP server certificate upon connection. If at least one certificate matches a CA certificate in the trust manager, the verification succeeds. Otherwise, the verification fails and the connection attempt fails. If a path is specified but the PEM file does not exist, all certificates are trusted. That is, no certificate verification is done on the LDAP server and all certificates are accepted.
Bind DN	The distinguished name (DN) used when initially authenticating to the LDAP server to do a user lookup. This user name must have appropriate permissions to search and read users that need to authenticate.
Bind Password	The password to send with the Bind DN when initially authenticating to the LDAP server.
Base DN	The base DN to use when searching for users.
User Domain	(Optional) An optional domain to use in LDAP searches.
User Search Filter	A filter used to search for an LDAP user. Only the first entry that matches is retrieved, so this filter should be as specific as possible. The {username} and {domain} can be used as placeholders for the actual values when authentication takes place. If no domain is specified, the filter defaults to `(sAMAccountName={username})`. If a domain is specified, the filter defaults to `(userPrincipalName={username}@{domain})`.
Timeout	The timeout, in seconds, before a connection attempt to the primary LDAP server is marked as failed and the next connection attempt is made (if a secondary LDAP server exists).

Table continues…

Name	Description
Use LDAP as Fall-through Authenticator	Select this option to enable a back end authentication server to handle authentication requests for users that are not defined in the EMS user list. This is done by fetching a specified LDAP attribute when running the User Search Filter on the LDAP server to find a user matching the provided credentials as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or any authorization attempts for the user will fail and the user's login requests will be rejected. If the attribute is not present on the user, any authorization attempts for the user fail and the user's login requests are rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both LDAP authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.
Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”. This attribute is not defined in most LDAP schemas and must be defined to function correctly. Alternatively, any other LDAP attribute can be used as long as it is a string value. For an example of how to define a custom attribute in Microsoft Active Directory, see: https://social.technet.microsoft.com/wiki/contents/articles/20319.how-to-create-a-custom-attribute-in-active-directory.aspx

X.509 Server Authentication

Name	Description
Enabled	Controls whether X.509 certificate authentication is enabled. X.509 certificate authentication cannot be enabled unless the CA Trust Anchors Privacy Enhanced Mail (PEM) file exists on the file system.
CA Trust Anchors PEM File	This is a PEM file that should contain all CA trust anchors used to verify X.509 certificates. Multiple entries should be concatenated together.

Table continues…

Name	Description
CA Intermediaries PEM File	This is a PEM file that should contain all intermediate CAs used to construct trust chains used to validate certificates. These certificates are not implicitly trusted and are only used in reconstructing the trust chain. Multiple entries should be concatenated together.
CRL File	This is a PEM file that should contain all certificate revocation lists used to revoke X.509 certificates. Multiple entries should be concatenated together.
Authentication Mode	The method used to authenticate X.509 certificate users. Select one of the following options: • **Accept X.509 Certificate or Password**: The user will be authenticated if either a valid certificate or a valid password is provided. • **Require X.509 Certificate**: The user will be authenticated only if a valid certificate is provided. Any password entered by the user is ignored. • **Require X.509 Certificate and Password**: The user will be authenticated only if both a valid certificate and valid password is provided.

RADIUS Server

Name	Description
Server Name	A descriptive name to identify the RADIUS server.
Primary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Secondary Address (ip:port)	The IP address and port number of the server designated as the secondary RADIUS server.
Retry Timeout (seconds)	The maximum time in seconds taken for a successful authentication to be completed. If authentication is not completed within this time, SBC ends the connection automatically and generates an incident .
Max Retry	The maximum number of times that a user can attempt to authenticate before SBC ends the connection .

Table continues…

Name	Description
Ignore Session Expire	The check box that indicates whether the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Select this check box for Avaya SBC to maintain the current session upon receipt of the SESSION EXPIRE message. Clear the check box for Avaya SBC to end the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method that the Avaya SBC security device uses to select a RADIUS server to choose to authenticate a user. The options are: • **Active Standby** • **Round Robin**
Authentication Protocol	The authentication protocol to be used for RADIUS authentication. The options are: • **None** • **EAP_TTLS/EAP_ PAP** • **EAP_PEAP/EAP_GTC**
Server Secret	The shared secret maintained between the Avaya SBC security device and the active RADIUS server with which communications between the two is encrypted.
Confirm Server Secret	Respecifies the shared secret maintained between the Avaya SBC security device and the active RADIUS server .
Accounting Server	The check box to indicate whether this RADIUS server must also to be designated as an Accounting Server and receive CDRs. Select this check box to indicate that RADIUS server is also an Accounting Server and can receive CDRs. Clear the check box to indicate that RADIUS server is not an Accounting Server and does not receive CDRs.

Chapter 4: Device configuration

Prerequisites

To ensure successful device configuration, you must first ensure that Avaya SBC is installed and functional. For more information, see one of the following documents that match your deployment type:

- *Deploying Avaya Session Border Controller on a Hardware Platform*
- *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*
- *Deploying Avaya Session Border Controller on an Avaya Aura® Appliance Virtualization Platform*
- *Deploying Avaya Session Border Controller on an Amazon Web Services Platform*

Adding an Avaya SBC device

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS**.
3. Navigate to **Device Management**.
4. On the Device Management page, click **Add**.
5. On the Add Device page, enter the **Node Name** and the **Management IP** address of the Avaya SBC devices.

   Note:

   Ensure that the host names of the devices are unique.
6. **(Optional)** If the device you add must support high availability, select the **High Availability** check box and enter details in the following fields:
   - **Node name for both Primary and Secondary nodes**
   - **Management IP for both Primary and Secondary**
7. **(Optional)** Administer any other desired options as described in Device Management field descriptions on page 49.

8. Click **Finish**.

   On the Device Management page, the EMS server displays a device list with the status of the newly added device as **Registered**.

9. Restart the IPCS services as described in Restarting the IPCS services on page 76.

Related links

Device Management field descriptions on page 49
Using pooled licensing on page 52

Device Management field descriptions

Devices tab

Name	Description
Device Name	The name of the EMS or Avaya SBC device.
Management IP	The management IP address of the device.
Version	The version of Avaya SBC.
Status	The current status of the device. The options are: • **Registered**: For newly added devices. • **Commissioned**: For devices that were previously installed and commissioned.

Updates tab

Name	Description
Current Version	The current version of the device.
Upgrade from local file	An option to select a local upgrade package.
Upgrade from uploaded file	An option to browse and select an upgrade package along with the signature file.

Licensing tab

When Dynamic Licensing Mode is deployed, **Fetch count**, **Low Watermark** and **High Watermark** fields must be configured properly for features to work.

Name	Description
Use Local WebLM Server	An option to use a local WebLM server. Virtualized EMSes cannot run on a local WebLM server.

Table continues…

Name	Description
External WebLM Server URL	The URL of the WebLM server in one of the following formats: • For a System Manager WebLM server: `https://<SMGR_server_IP> :52233/WebLM/LicenseServer` • For a standalone WebLM server: `https://<WEBLM_server_IP> :52233/WebLM/LicenseServer`
Fetch Count	The value that Avaya SBC uses to determine the number of licenses to: • Request when usage increases. (Refer to the description of **Low Watermark**) • Release when usage decreases. (Refer to the description of **High Watermark**) This value cannot be **0**.
Low Watermark	If the percentage of usage licenses is less than or equal to **Low Watermark**, Avaya SBC requests number of licenses equal to the value of **Fetch Count**. Usage licenses = available licenses/reserved licenses For example, Avaya SBC has 10 licenses reserved, 8 licenses in use, 20% **Low Watermark**, and **Fetch Count** as 5. Available licenses = Reserved licenses – Licenses in use That is, Available licenses = 10-8= 2 Percentage of Usage licenses = (available licenses/reserved licenses) * 100 That is, Percentage of Usage licenses = (2/10)*100 = 20% Now, this percentage is less than or equal to **Lower watermark**, that is, 20%. Therefore, Avaya SBC requests 5 (**Fetch count**) more licenses. However, when requesting for more licenses, Avaya SBC ensures that reserved licenses is not more than configured **MAX** license allocation.

Table continues…

Name	Description
High Watermark	If the percentage of usage licenses is greater than or equal to **High Watermark**, Avaya SBC releases the number of licenses equal to the value of **Fetch Count**. Usage licenses = available licenses/reserved licenses For example, Avaya SBC has 10 licenses reserved, 2 licenses in use, 80% **High Watermark**, and **Fetch Count** as 5. Available licenses = Reserved licenses – Licenses in use That is, Available licenses = 10-2= 8 Percentage of Usage licenses = (available licenses/reserved licenses) * 100 That is, Percentage of Usage licenses = (8/10) * 100 = 80% Now, this percentage is greater than or equal to **High Watermark**, that is, 80%. Therefore, Avaya SBC releases 5 (**Fetch count**) licenses. However, when releasing licenses, Avaya SBC also ensures that the number of reserved licenses is not less than the configured **MIN** license allocation.

Button	Description
Save	Saves the external WebLM server URL.
Refresh Existing License	Refreshes the existing license.
Verify Existing Certificate	Verifies the existing WebLM license to confirm if it is trusted. If the WebLM license is trusted, a pop window will display the certificate details otherwise you can select the option to trust the WebLM certificate manually.

Key Bundles tab

Name	Description
Bundle File	The key bundle file.

Licensing Compliance tab

Licensing compliance provides statistical information for each licensing feature on:

- Maximum licenses used
- Maximum licenses acquired
- Maximum license over usage (over flow from maximum licenses configured for a feature)

Name	Description
Search Criteria	Select the **From** and **To** dates for which you want to view the license compliance data.

Table continues…

Name	Description
Select License	Select the license for which you want to view the compliance data: • **VIDEO** • **TRANSCODING** • **CES** • **PREMIUM** • **AMR** • **STANDARD** • **ADVANCED**
Export Data	Export the data in an Excel sheet.

Using pooled licensing

About this task

Avaya SBC supports pooled licensing. As opposed to static license allocation, Avaya SBC dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBC devices can use a pool of licenses dynamically across the devices as required.

Before you begin

Install a license in WebLM for the pooled licensing feature.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS**.
3. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
4. Navigate to **Device Management**.
5. Click the **Licensing** tab.
6. Provide appropriate values in the following fields:
   - **Fetch Count**
   - **Low Watermark**
   - **High Watermark**

   The EMS server uses, fetches, and releases licenses depending on the demand.
7. **(Optional)** Administer any other desired **Licensing** tab options as described in Device Management field descriptions on page 49.
8. Click **Save**.

9. Restart the IPCS services as described in Restarting the IPCS services on page 76.

Commissioning an Avaya SBC device

About this task

Use this procedure to install and commission the Avaya SBC security device on an existing enterprise VoIP network.

You can identify the Avaya SBC security devices that are physically installed onto the network and available for commissioning by the **Status** column. The newly added devices show the **Registered** status. De-commissioned devices show the **Install** option available. Devices that have previously been installed and commissioned show the **Commissioned** option. Each commissioned device has only the **View** option available.

Before you begin

Install a license file.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.
3. On the Device Management page, click **Add**.
4. In the Add Device window, enter the host name and the management IP address of the Avaya SBC devices.

   Note:

   Ensure that the host names of the devices are unique.
5. Click **Finish**.

   On the Device Management page, the system displays a device list with the status of the newly added device as **Registered**.
6. On the same Device Management page, click **Install**.
7. In the Installation Wizard window, administer the options described in Installation Wizard field descriptions on page 54.
8. Click **Finish**.

   On the Device Management page, the EMS server displays a device list with the status of the newly added device as **Registered**.
9. On the **Devices** tab, click **Install** corresponding to the device that you want to commission.

   The EMS server displays the Installation Wizard.
10. Add an interface for the SBC.

11. Provide an appliance name for the SBC instance being commissioned and complete the deployment settings, such as high availability.
12. Click **Finish**.

Result

The EMS server displays the `Installation is now complete.` message, followed by a list of links to **Server Configuration**, **Media Interface**, **Signaling Interface**, and **End Point Flows**. To set up the device, you can proceed to any configuration area by using those links or access the configuration areas through the task pane.

Related links

Installation Wizard field descriptions on page 54
Edit device field descriptions on page 55

Installation Wizard field descriptions

Installation Wizard provides an interface for configuring an Avaya SBC security device.

Name	Description
Device Configuration	
Appliance Name	A descriptive name assigned to the Avaya SBC security device being provisioned. This name is subsequently used as the device host name.
High Availability	A check box indicating that the Avaya SBC security device being provisioned will be part of a High-Availability (HA) pair. If you select the **High Availability** check box, the system displays a **failover to** field containing a list of HA partners. You can click the required HA partner. **Note:** For information about HA configuration, see *High Availability configurations*.
DNS Configuration	
Primary	The IP address of the primary DNS server.
Secondary	The IP address of the secondary DNS server.
License Allocation **Note:** Licenses must be allocated for features to work.	
Standard Sessions	The number of standard licenses allocated.
Advanced Sessions	The number of advanced licenses allocated.
Scopia Video Sessions	The number of Avaya Meetings Server video licenses allocated.
CES Sessions	The number of Client Enablement Services (CES) proxy licenses allocated.

Table continues…

Name	Description
AMR Sessions	The number of Adaptive Multi Rate (AMR) licenses allocated. In PLDS, AMR licenses are referred as NG911 licenses. Avaya SBC uses an AMR license when a call requires AMR-WB codec.
Transcoding Sessions	The number of transcoding sessions licenses allocated.
CLID	A five-digit number indicating the centralized licensing ID.
Encryption	The encryption field. The default value is **Yes**.
Name	The name of the device.
Default Gateway	The default gateway address.
Subnet Mask	The subnet mask of the Avaya SBC device.
Interface	The physical interface of the Avaya SBC security device, which will be used to provide an interface to the internal/Enterprise and to provide an interface to the external, public network (A1, A2, B1, and B2). **Note:** Ensure that the data interfaces and maintenance interfaces are configured on different subnets. This configuration avoids routing problems when configuring the data interfaces A1/A2 and B1/B2 in Installation Wizard and the maintenance interfaces M1 and M2 during the initial provisioning process in the Management Interface Setup screen. For information about the initial provisioning process, see *Deploying Avaya Session Border Controller*.
Network Configuration	
IP	The IP address of the Avaya SBC device that is being configured.
Public IP	The IP address used by the Avaya SBC security device for network address translation of SIP messages. The device uses the IP address to access the external network. If you have not configured the near-end NAT, the Public IP address can be the same as the IP address.
Gateway Override	The IP address of the device that the Avaya SBC security device uses to send local network traffic to other networks.
DNS Client	The radio button next to the interface (normally A1) that is reachable by the DNS servers that were defined previously in the **Primary** and **Secondary** fields of the **DNS Configuration** section.

Related links

Commissioning an Avaya SBC device on page 53

Edit device field descriptions

Edit Device provides an interface for editing an Avaya SBC or EMS security device.

Name	Description
General Settings	
Appliance Name	A descriptive name assigned to the Avaya SBC security device being provisioned. This name is subsequently used as the device host name.
Device Settings	
Device Pair	The number of HA pairs in Avaya SBC device.
DNS Settings	
Primary	The IP address of the primary DNS server.
Secondary	The IP address of the secondary DNS server.
DNS Client IP	The Avaya SBC IP address that is reachable by the DNS servers that were defined previously in the **Primary** and **Secondary** fields of the **DNS Configuration** section.
High Availability (HA) Network Settings	
IP	The management IP address of the primary and secondary Avaya SBC device.
Netmask	The subnet mask of the Avaya SBC device.
Gateway	The default gateway address.
IPv4 Network Settings	
Management IP	Management IP address of the Avaya SBC device.
Network Prefix and Subnet Mask	The subnet mask of the Avaya SBC device.
Gateway	The default gateway address.
Dynamic License Settings **Note:** Licenses must be allocated for features to work. LicenseUsageExceeed alarm is raised when minimum number of licenses is more than 60% of maximum number of licenses.	
Standard Sessions	The maximum and minimum number of standard licenses allocated.
Advanced Sessions	The maximum and minimum number of advanced licenses allocated.
Premium Sessions	The maximum and minimum number of premium licenses allocated.
Scopia Video Sessions	The maximum and minimum number of Avaya Meetings Server video licenses allocated.
CES Sessions	The maximum and minimum number of Client Enablement Services (CES) proxy licenses allocated.
Transcoding Sessions	The maximum and minimum number of transcoding licenses allocated.

Table continues…

Name	Description
AMR Sessions	The maximum and minimum number of AMR licenses allocated. In PLDS, AMR licenses are referred as NG911 licenses. Avaya SBC uses an AMR license when a call requires AMR-WB codec.
CLID	A five-digit number indicating the centralized licensing ID.
Encryption	The encryption field. The default value is **Yes**.

Related links

[Commissioning an Avaya SBC device](#) on page 53

Configuring logon banner messages

About this task

When users log on to the EMS GUI or command line (CLI) user interfaces, users see a standard banner message. These standard messages are located in the following banner files:

- `/usr/local/ipcs/etc/notice.sbc`
- `/usr/local/ipcs/etc/dod.notice.sbc`
- `/usr/local/ipcs/etc/gui-login-notice`

Important:

Do not edit the original banner files. You must make copies of the original banner files and edit the copies.

You can create copies of these banner files and customize the files with your own greeting or security warnings. You can have different messages on each of the servers in your deployment, customizing the message for different servers. For example, you can put the name of the server in the logon banner message to clarify to which server users are logged on.

Note:

The `/usr/local/ipcs/etc/dod.notice.sbc` banner file is only used with government defense JITC deployments.

Procedure

1. Log in to the CLI with administrator credentials.
2. If needed, use the following command to log on as root:

   `su root`

3. Move to the banner message directory:

   `cd /usr/local/ipcs/etc`

4. Enter one of the following commands to copy the standard banner file to a new file used to customize the message:
   - **cp notice.sbc notice.sbc.custom**
   - **cp dod.notice.sbc dod.notice.sbc.custom**
   - **cp gui-login-notice gui-login-notice.custom**
5. Enter one of the following commands to open the banner files in the vi editor:
   - **vi notice.sbc.custom**
   - **vi dod.notice.sbc.custom**
   - **vi gui-login-notice.custom**
6. Edit the file to display the logon welcome information, including any special security, copyright, legal, or usage warnings.
7. Save and close the file.
8. Enter the following command to activate the new custom banner:

   /usr/local/ipcs/icu3/scripts/setBannersPolicy.sh

Configuring port bonding

About this task

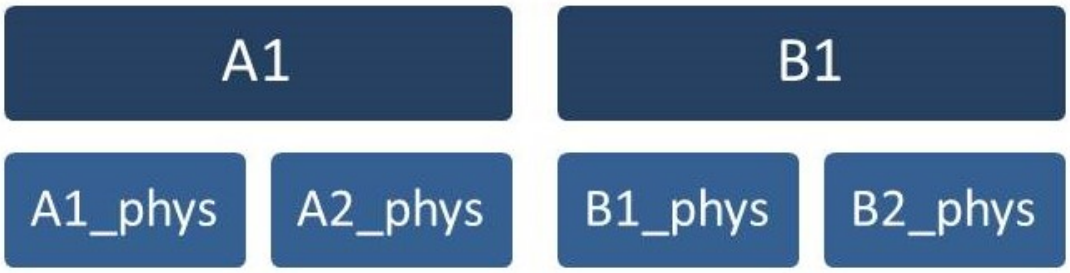
Port bonding is the aggregation of multiple physical network ports (“servant” interfaces) that form a new logical interface (“master” interface). The most common example of port bonding is putting two physical interfaces together to form an active/standby interface. If the active physical port loses carrier, the logical interface fails over to the standby without assistance from higher-level software.

For Avaya SBC Release 8.1.0 and later, only interfaces A1/A2 and B1/B2 can be paired to form a bonded interface. If one pair is bonded, the other pair must also be bonded. The resulting bonds are A1 for the A1/A2 pair and B1 for the B1/B2 pair. Thus, bonding for the A1/A2 and B1/B2 interfaces are either on or off. You cannot have bonding on one pair and no bonding on the other pair.

Consider the following conditions when configuring port bonding:

- After enabling or disabling port bonding, you must reboot the server. Do this reboot during a maintenance period or during low or no traffic periods.
- HA logic does not consider “master/servant” status when making failover decisions. Physical link failure might be good criteria to consider when making a failover decision, but HA logic is not aware of the link status when port bonding is enabled.
- Bonded interfaces are named A1 and B1. The “servant” interfaces are renamed by appending “_phys” to the original name, for example, “A1_phys”.

  The following diagram shows how the ports are renamed after port bonding is enabled:



- Port bonding configurations are not backed up. This means that if you are upgrading to a new release and port bonding was configured on the old system, you must reconfigure port bonding.
- Enabling and disabling port bonding must be done on each server in an SBC pair. If you fail to configure matching port bonding across server pairs, the interfaces will not operate properly.
- If interfaces A2 and B2 are already configured as active interfaces, those interfaces will not work when bonding is enabled. Existing configurations on A1 and B1 will continue to work, but existing configurations on A2 and B2 will cease to work because they are now servant interfaces for the new A1 and B1 bonds. Any configuration that uses A2 and B2 must be deleted before you enable bonding, and possibly reconfigured to A1 or B1, if required.
- The NIC port drivers using port bonding must support Media Independent Interface (MII). Ports that do not support MII cannot use port bonding. Port bonding is also not supported on servers that use the TILEncore-Gx36 network interface card.

Before you begin

Before you enable or disable port bonding, you should first determine the current status of port bonding. To do this, open the following file:

`/usr/local/ipcs/etc/sysinfo`

Search for the setting “BONDING”. The setting will either show Yes or No. If the BONDING setting is not found, it means that port bonding is disabled.

Procedure

1. Log on to Linux as root.
2. Run the following command:

   `sbceconfigurator.py change-port-bonding`
3. Reboot the server.
4. Repeat this procedure on the other SBC server if part of an HA pair.
5. Open the following file on each server and confirm that bonding is either enabled or disabled on both servers:

   `/usr/local/ipcs/etc/sysinfo`

Changing the management IP from the EMS web interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.
3. Find the device whose IP address you want to change, and click **Edit**.
4. In the **Management IP** field, type the new management IP, and click **Finish**.
5. **(Optional)** Find the Avaya SBC device on the Device Management page, and click **Restart Application**.
6. **(Optional)** If you change the management IP address of the EMS, restart each Avaya SBC connected to the EMS.

High Availability failovers

High Availability (HA) support for both media and signaling ensures that Avaya SBC security functionality is provided continuously, regardless of hardware or software failures. High availability requires minimum two Avaya SBC devices and one standalone EMS server.

Any Avaya SBC in the pair can be the primary Avaya SBC. The primary and secondary Avaya SBCs exchange HA control messages and heartbeat messages. When the primary Avaya SBC fails, the secondary Avaya SBC takes over and begins serving traffic.

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBC fails over, the secondary Avaya SBC broadcasts a GARP message to announce that the secondary Avaya SBC is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBC IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication. For example, to handle GARP, branch gateways, Medpro, Crossfire, and some PBXs/IVRs must be deployed in a different network from Avaya SBC, with a router or L3 switch. If you do not put the Avaya SBC interfaces on a different subnet, after failover, active calls will have a one-way audio. Devices that do not support GARP continue sending calls to the original primary Avaya SBC.

All IP addresses configured in the Network Configuration screen are shared between both HA devices in HA deployment mode. The HA devices are also configured with private, default IPs which are used to replicate signaling and media data between each other. The configured interfaces will be inoperative on the stand-by (secondary) device until it becomes active (primary). When the devices switch, the new active device sends a GARP message to update the adjacent ARP tables so that they start receiving traffic.

Failover scenarios

Keep alive or heartbeat failure: The secondary Avaya SBC sends a keep alive request or heartbeat every 500 ms, and the primary Avaya SBC responds with a keep alive response. If the primary Avaya SBC does not respond to two consecutive keep alive requests, the secondary Avaya SBC takes over as the primary Avaya SBC.

Peer node unavailable: If a peer node is unavailable, the currently active or running Avaya SBC becomes the primary Avaya SBC. The active Avaya SBC attempts connecting with the peer every 15 seconds.

Link failures: The HA module has a list of physical ports and the status of the ports. The HA module gets the configured ports from the physical ports configured in the server and the subscriber flows. During a link failure, the primary Avaya SBC compares its active links with the number of active links for the peer Avaya SBC. When the primary Avaya SBC detects that the secondary Avaya SBC has more active links, the secondary Avaya SBC takes over as the new primary Avaya SBC. Failovers are not initiated for M1 and M2 link failures.

Note:

Avaya SBC compares the number of active links with the peer to determine whether a failover is necessary. For example, when one link from the primary Avaya SBC is down, but the secondary Avaya SBC also has the same number of links active, failover is not required.

Avaya SBC provides duplicate HA connection by using HA pair management addresses. With HA replication, if any M2 to M2 or M1 to M1 connections are down, the HA connection continues uninterrupted.

Avaya SBC supports an EMS HA active/active configuration. If the EMS hardware fails, the EMS server can switch to the other EMS in the HA pair without manual intervention.

Split brain: When both SBCs in HA pair loose the communication between them, then declare themselves as primary. This condition is called split brain. In split brain condition, Avaya SBC handles the calls on the network state:

- fully functional no disruption to an going call
- partial outage, some users/calls are affected
- complete outage

In split brain state, Avaya SBC does not preserve active calls.

For example, SBC1 is a primary SBC and SBC2 is a secondary SBC. When you disconnect all the interfaces of SBC1:

- SBC assumes that network is down.
- SBC2 losses connectivity with SBC1 and SBC2 assumes role of primary SBC and failovers all active calls.
- SBC1 continues to stay in the primary state with all interfaces down.
- When interfaces are connected back, SBC1 and SBC2 establishes HA connection with split brain condition.
- You must restart SBC1 and SBC2 to recover from split brain condition. When you restart SBC, you cannot place a new call and SBC drops all active calls. After the restart, SBC comes to Primary Secondary states and start serving new calls.

Configuring High Availability

About this task

Use this procedure to configure Standard High Availability (HA). The devices can be co-located or geographically dispersed.

High-Availability support for both media and signaling ensures that Avaya SBC security functionality is provided continuously, regardless of any hardware or software failures. High availability requires a minimum of two Avaya SBC devices and one standalone EMS server.

Before you begin

* Get a license file with the feature FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1. * Ensure that the **Values** field for the Session Border Controller High Availability per Configuration feature is set to On.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS**.
3. Navigate to **Device Management**.
4. In the **Node Name** field, type the name of the device.
5. In the **Management IP** field, type the management IP address.
6. Select the **High Availability** check box.
7. In the **Node Name for second Node** field, type the name of the device to which the Avaya SBC must fail over.
8. In the **Management IP for second Node** field, type the management IP of the failover device.
9. Click **Finish**.

Related links

Adding an Avaya SBC device on page 48

HA Node Status States

When creating a new Security Rule, refer to this table for information on the Domain DoS selections.

Status	Description
Primary	Avaya SBC is active and handling call traffic.
Secondary	Avaya SBC is inactive and in stand-by mode.

Table continues…

Status	Description
Down	The Primary SBC detects that Avaya SBC is offline. This status indicates that the application is not running, the network interfaces are disabled, or the device is not running at all.
Initializing	Avaya SBC is going through the initialization procedure.
HAElection	Avaya SBC is determining whether to go into active or standby mode.
Synchronizing	Avaya SBC is replicating data from the other SBC.
Unconfigured	Avaya SBC is configured as an HA device but not yet received the configuration from EMS.
Unknown	EMS does not recognize the HA status Avaya SBC is reporting.

Upgrade of the EMS software

You can upgrade the Element Management System (EMS) or GUI interface from the task pane when required by using the **Device Management** option . For more information , see *Upgrading Avaya Session Border Controller*.

Obtaining a license file from Avaya PLDS

About this task

Use the Avaya Product Licensing and Delivery System (PLDS) website to get a license file for Avaya SBC. You can gain access to the PLDS website through the Avaya Support portal.

Before you begin

Get the following:

- Organization name. You can get this name from the sales order.
- Device hostname. If you do not want to use the default name, you can use the hostname assigned to you when you first install the device.

Procedure

1. Start a secure shell (SSH) connection with the standalone device, that is, the combined SBC or EMS, or with the separate EMS device as applicable.
2. At the dollar sign ($) prompt, type `sudo su`.

   The CLI displays the pound sign (#) prompt.
3. **(Optional)** To view the MAC addresses of all Ethernet interfaces, type `ifconfig –a`.

Use the **ifconfig –a** command to get the MAC address to install the license file on a local WebLM server, except on VM. To install the license file on an external WebLM server, use the MAC address of the external WebLM server as the license host in PLDS.

For standalone devices (combined SBC/EMS), the CLI displays two MAC addresses.

Note:

The management interface (M1) is used for licensing. The MAC address required for obtaining the license file on PLDS is the MAC address of EMS. The corresponding Ethernet name for the required MAC address can be determined as follows:

- Standalone SBC (Portwell & Dell): In the listing, look for the MAC address associated with the Ethernet interface: **Eth5**
- For HA, EMS (Dell or AMAX): In the listing, look for the MAC address associated with the Ethernet interface: **Eth0**

4. Log in to PLDS and type the requested information.

   The XML-formatted license file is sent to you as an email attachment.

5. Configure WebLM Server.

   For more information about configuring WebLM, see Configuring WebLM server IP address on EMS in *Deploying Avaya Session Border Controller on a Hardware Platform*.

Viewing the EMS server time zone

Procedure

1. Start a secure shell (SSH) connection to the Stand-By server.
2. On the log in screen, type `sudo su` after the dollar sign ($) prompt.
3. At the pound sign (#) prompt, type `sbceconfigurator.py view-timezone`.

   The system displays current time zone on screen.

Setting the EMS server time zone

Procedure

1. Start a secure shell (SSH) connection to the Stand-By server.
2. On the initial login screen, type `sudo su` after the dollar sign ($) prompt.
3. At the new pound sign (#) prompt, type `sbceconfigurator.py change-timezone`.

   This is an interactive command. After you enter the command, system prompts you to answer few questions. Based on your answers the system sets the time zone.

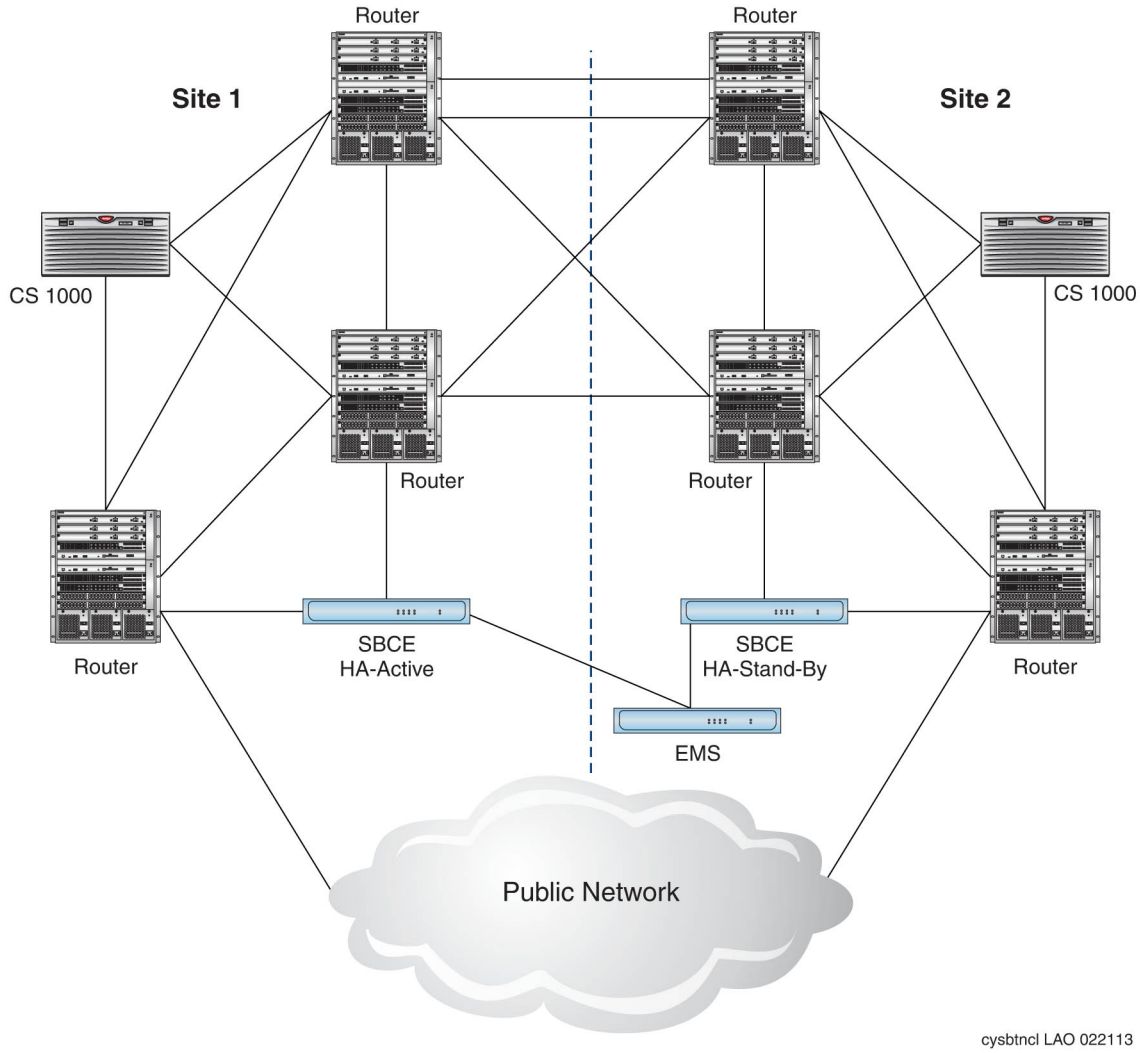
High-Availability pair geographically dispersed

The following sections contain the information necessary to deploy two Avaya SBC security devices in a High-Availability (HA) configuration where they are not geographically co-located.

One Avaya SBC security device is deployed as the HA Primary at Site 1 and another as the HA Secondary at Site 2. Both are controlled by Avaya EMS, which synchronizes the database in to the lower node Avaya SBC to maintain real-time network information. If the HA Primary Avaya SBC fails, the HA Secondary Avaya SBC immediately takes up its monitoring and mitigation activities while the EMS raises the appropriate alarm indications.

The following figure illustrates that you can use most Avaya SBC device models in the HA implementation , except the Portwell Cad Avaya SBC .

Example



Interface connections for an Avaya SBC HA pair

The following interface connections are required before deploying an Avaya SBC HA pair.

Interface	Description
EMS	
M1 interface or management IP	EMS uses this IP to: • Communicate with the Avaya SBC devices. • Send the database to the Avaya SBC devices. • Check the status of the Avaya SBC devices. • Communicate with the NTP and DNS. **Note:** M1 interface does not support IPv6 address.
Avaya SBC	
M1 interface or management IP	Avaya SBC devices use this IP to: • Communicate with EMS and access the server box through SSH port 22 for maintenance. • Communicate with NTP, most likely on the same subnet as EMS M1. **Note:** If the Avaya SBC M1 IP is not on the same subnet as EMS M1 IP, the Avaya SBC IP must be routable to the EMS M1 IP. **Note:** M1 interface IP does not support IPv6 address.
A1 internal interface towards PBX	This IP cannot be on the same subnet as the PBX or media board IPs or the M1 IP.
B1 external interface towards trunk or remote users	This IP cannot be on the same subnet as the M1 IP.
M2 connection	This interface is a layer 2 connection between the two Avaya SBC devices. This interface does not require an IP.

In an HA pair deployment, primary and secondary Avaya SBC instances use a Keep alive mechanism to check call processing module availability for the other Avaya SBC. This mechanism is controlled by two parameters:

- **Keep alive interval**: The duration between two Keep Alive requests.
- **Max retries**: The number of Keep Alive requests sent before declaring that other Avaya SBC instance's call processing module is unavailable.

Secondary Avaya SBC sends a Keep Alive request packet after **Keep alive interval** is expired. If a response is not received after the **Max Retries** value, secondary Avaya SBC takes over as primary Avaya SBC.

For example, if **Keep alive interval** is set to **1500** and **Max Retries** is set to **3** and secondary Avaya SBC has not received a Keep Alive response for (3 x 1500 milliseconds), secondary Avaya SBC takes over as primary Avaya SBC.

You can change this value on the EMS web interface from **Network & Flows** > **Advanced Options** > **HA pairs**. For more information, see the “HA Pairs” section in Advanced Options field descriptions on page 220.

If frequent failovers are seen in delay prone deployed platforms such as VMWare, these numbers can be adjusted to increase the detection time to prevent frequent failovers.

Important:

The A1 and B1 IP addresses are shared between the two Avaya SBC devices. These IPs must be capable of routing and being handled at both sites. The IPs are swapped between the Avaya SBC devices using a gratuitous ARP (GARP) request that is handled by a switch or router. The GARP request indicates the MAC of the new Primary Avaya SBC interface that will now handle the IPs that were being handled by the new Secondary Avaya SBC.

All interfaces on the switches and routers to which the Avaya SBC devices and EMS are plugged in must be set as auto/auto.

Deploying a geographically dispersed Avaya SBC HA configuration

Procedure

1. Install each Avaya SBC security device.
2. Install Avaya EMS security device.
3. Log in to the EMS web interface with administrator credentials.
4. In the navigation pane, click **Device Management**.
5. On the Device Management page, click **Add**.

   The EMS server displays the Add Device page.
6. Provide appropriate values in the following fields:
   a. **Node Name**
   b. **Management IP**
   c. **High Availability**
   d. **Node Name for second Node**
   e. **Management IP for second Node**

Note:

When you select the High Availability (HA) check box, the system with HA mode replicates and preserves complete signaling state for all active calls and registration information of endpoints on the standby box. In the event that the active box fails, the standby box can maintain the state of the active call so that all the features for that active call are available. The EMS server with HA mode maintains state information for calls on UDP transport only. In an event when a particular call leg uses TCP transport, EMS server with HA mode will be unavailable for that call. Avaya SBC then falls back to Media HA where only audio information is replicated.

7. Click **Finish**.

Configuring RTCP Monitoring Relay

About this task

The RTP Control Protocol (RTCP) Monitoring Relay feature (formerly known as RTCP Monitoring) in Avaya SBC updates RTCP packets with appropriate End Point IP and Hop Information.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**.
4. On the **RTCP Monitoring** tab, select the **RTCP Monitoring Relay** check box to enable the RTCP feature.
5. Click **Save**.

RTCP Monitoring Relay field descriptions

Name	Description
RTCP Monitoring Relay	Specifies whether RTCP monitoring relay is enabled or not.
Node Type	Configures the node type based on the role of the Avaya SBC device. The options are: • **Core** • **DMZ** • **Remote**
Relay IP	Specifies the RTCP service listen IP address and network name for that device. If there are multiple RTCP relays configured on the device, select the IP address that belongs to the private network.
Port	Specifies the port. By default, the port is 5005.

Application relay configuration for RTCP monitoring

You must configure two relay services to send the RTCP MON traffic to the prognosis server.

- Relay 1: For RTCP MON traffic coming from DMZ Avaya SBC and Core Phones. RTCP MON traffic is received on Core SBC-1 public IP-A and is sent out to the prognosis server using Core SBC-1 private IP-A.
- Relay 2: For traffic coming from Media Gateway. RTCP MON traffic is received on core SBC-1 private IP-A and is sent out to the prognosis server using Core SBC-1 private IP-B.

46xx settings file configuration for RTCP monitoring

You must add the following parameters in the `46XX settings` file for Remote SBC and Core SBC phone groups:

- SET RTCPCONT 1
- SET RTCPMON 192.168.11.105 {SBC Relay IP towards Phone}
- SET RTCPMONPORT “5005"
- SET RTCPMONPERIOD 5

Communication Manager/Media Gateway configuration for RTCP monitoring

You must provision the RTCP Monitor IP address with the Core Avaya SBC internal signaling IP address on the System Parameter ip-options page.

- **RTCP Monitor Server IP**: Core Avaya SBC Internal Signaling IP
- **Server Port**: 5005

In back-to-back Avaya SBC deployment, calls go through the remote Avaya SBC, DMZ Avaya SBC, and Core Avaya SBC.

Therefore, you must configure application relay RTCP monitoring in:

- Core Avaya SBC
- Remote Avaya SBC
- Remote user deployment

  A regular remote user deployment can have one Avaya SBC with or without high availability. The steps for configuring application relay for RTCP monitoring in remote Avaya SBC deployment are the same as the configuration steps for Core Avaya SBC.

Configuring application relay for RTCP monitoring in core Avaya SBC

About this task

You can use the same steps for configuring application relay for RTCP monitoring in remote user deployment and in core Avaya SBC

Before you begin

Navigate to **Network & Flows** > **Advanced Options** > **RTCP Monitoring** to enable **RTCP Monitoring Relay**. and do the following:

- In the **Node Type** field, select **Core**.
- In the **Relay IP field.** field, click the network name and **Core SBC Relay IP address / Core SBC Private IP-A**.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **Relay**.
4. On the Application Relay page, click **Add**.
5. Enter the required information in the appropriate fields and click **Finish**.

Configuring application relay for RTCP monitoring in DMZ Avaya SBC

About this task

You can use the same steps for configuring application relay for RTCP monitoring in remote user deployment and in core Avaya SBC

Before you begin

Navigate to **Network & Flows** > **Advanced Options** > **RTCP Monitoring** to enable **RTCP Monitoring Relay**. and do the following:

- In the **Node Type** field, click **DMZ**.
- In the **Relay IP field.** field, click the network name and **Core SBC Relay IP address / Core SBC Private IP-A** .

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **Relay Services**.
4. On the Application Relay page, click **Add**.
5. Enter the required information in the appropriate fields and click **Finish**.

Configuring application relay for RTCP monitoring in remote Avaya SBC

About this task

The application relay configuration is mandatory to monitor RTCP data from Avaya 96X1 / 96X0 phones.

Before you begin

Navigate to **Network & Flows** > **Advanced Options** > **RTCP Monitoring** to enable **RTCP Monitoring Relay**. and do the following:

- In the **Node Type** field, select **Remote**
- In the **Relay IP field.** field, click the network name and **DMZ SBC Relay IP address / DMZ SBC Private IP-A**

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **Relay Services**.
4. On the Application Relay page, click **Add**.
5. Enter the required information in the appropriate fields and click **Finish**.

Configuring application relay for RTCP monitoring in core, remote, and DMZ Avaya SBC field descriptions

Name	Description
Name	The descriptive name of the application relay.
Service Type	The service type for the application relay. Select **RTCP** for configuring application relay for RTCP monitoring in core, DMZ and, remote Avaya SBC.
Remote IP/FQDN	• Prognosis server IP address for configuring application relay for RTCP monitoring in core and DMZ Avaya SBC. • Remote SBC Relay IP address for configuring application relay for RTCP monitoring in remote Avaya SBC.
Remote Port	The port number of the server IP. Remote port for configuring application relay for RTCP monitoring in core, DMZ and, remote Avaya SBC is 5005.
Remote Transport	The transport protocol for contacting the server IP. Select **UDP** for RTCP monitoring in core, DMZ and, remote Avaya SBC is 5005.
Listen IP	The network name and the IP address to which an endpoint sends packets or the interface facing the endpoint. This IP must be different from the IP used for SIP signaling and media.

Table continues…

Name	Description
Listen Port	The port number to which endpoints send packets or the port number of the interface facing the end point. Listen port for RTCP monitoring in core, DMZ and, remote Avaya SBC is 5005.
Connect IP	The IP address for communicating with the prognosis server. • Type the remote Avaya SBC internal signaling IP for configuring application relay for RTCP monitoring in remote.Avaya SBC. • Click the network name, and select the interface that prognosis can reach for configuring application relay for RTCP monitoring in core and DMZ.Avaya SBC.
Listen Transport	The transport protocol used for communication between the endpoint and interface at Avaya SBC. Select **UDP** for RTCP monitoring in core, DMZ and, remote Avaya SBC is 5005.
Whitelist Flows	The check box to enable white list flows.
Use Relay Actors	The check box to enable relay actors. Use control and click simultaneously to select or clear multiple items. The options are: • **End-To-End-Rewrite**, **Hop-by-Hop Traceroute**, and **Bridging**. for configuring application relay for RTCP monitoring in remote and core Avaya SBC. • **Hop-by-Hop Traceroute** for configuring application relay for RTCP monitoring in DMZ Avaya SBC.

RTCP monitoring generation support

Avaya SBC receives RTCP streams from a SIP trunk that does not have any Avaya specific control information. Avaya SBC converts RTCP streams into Avaya specific format and sends it to the quality monitoring server.

Important:

RTCP monitoring generation is applicable only for SIP trunks.

Avaya SBC calculates Round Trip Time based on the RTCP streams coming from a SIP trunk or from a enterprise network.

Avaya SBC generates the RTCP monitoring report and sends it to the RTCP monitoring server. RTCP monitoring server can be configured from the web interface. At the quality monitoring server, you can calculate Mean Opinion Score (MOS) from Round Trip Time.

Avaya SBC itself generates RTCP streams and calculates Round Trip Time to calculate the quality metrics. Avaya SBC also calculates the lost packets based on the media statistics components.

RTCP monitoring report contains UCID in the Priv Type in SDES message to have unique identifier at call level.

Related links

Round Trip Time on page 73

Configuring RTCP monitoring generation support on page 73

Round Trip Time

Round Trip Time or Round Trip Delay Time is the time it takes for a network request to go from a starting point to a destination and return back . The time is indicated in milliseconds. You can calculate Round Trip Time by using the following formula:

Round Trip Time = (T2–T1) — Delay Since Last Sender Report (DLSR), where

T2–T1 is the time between two RTP packets

DLSR is the time between receiving a sender report and sending a sender or receiver report to the receiver end. DLSR is a component of the Round Trip Delay Time that is not provided by the network.

Configuring RTCP monitoring generation support

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**.
4. On the **RTCP Monitoring** tab, select the **RTCP Monitoring Report Generation** check box to enable the feature.
5. Enter the required information in the appropriate fields and click **Save**.

RTCP Monitoring Report Generation field descriptions

Name	Description
RTCP Monitoring Report Generation	Specifies whether RTCP monitoring report generation is enabled.

Table continues…

Name	Description
SBC Interface IP	Specifies the source IP address of Avaya SBC for communication between Avaya SBC and the monitoring tool. **Note:** The IP address must be the IPv4 address.
SBC Interface Port	Specifies the source port number of Avaya SBC for communication between Avaya SBC and the monitoring tool.
Monitoring server IP/FQDN and Port	Specifies the destination IP address and port number of the remote monitoring tool. **Note:** The IP address must be the IPv4 address.
Monitoring Frequency based on RTCP Report	Specifies the number of RTCP packets received from a SIP trunk after which Avaya SBC generates the RTCP monitoring report.
Monitoring interval in absence of RTCP Report	Specifies the interval (in seconds) between two consecutive RTCP monitoring reports.

Adding a new blacklist rule

About this task

You can add a blacklist rule to prevent Avaya SBC from accepting data from specific IP addresses. Apart from the IPs listed in black list, all other IPs are allowed. You can set up whitelist rules for specific IP addresses to avoid any checks for IPs in that list. In the firewall settings, you can change the number of connections initiated per second for a particular service and prevent DoS attacks. Avaya SBC whitelist does not block traffic from other IPs except blacklisted IPs.

Note:

The customer is responsible for the security checks associated with whitelisted IPs.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click **SBC**.
3. Navigate to **DMZ Services** > **Firewall**.
4. On the **Blacklist** tab, click **Add**.
5. Enter the required information in the appropriate fields and click **Finish**.

Result

The EMS server creates a blacklist rule based on the specified IP addresses and ports. According to the blacklist rules, Avaya SBC blocks data received from the source IP address and data sent to the destination IP address.

Related links

Firewall field descriptions on page 75

Firewall field descriptions

Blacklist tab

Name	Description
Name	The name of the blacklist rule.
Interface/VLAN	The interface or VLAN for which the rule is applicable.
Source Address	The IP address from which data must be blocked.
Source Port/Sequence	The port number from which data must be blocked. If you do not specify a value for this field, the EMS server uses a default wildcard (*) character and accepts any value.
Protocol	The transport protocol used. This field is mandatory when you enter a source or destination port. If you do not specify a value for this field, the EMS server uses a default wildcard (*) character and accepts any value.
Destination Address	The IP address to which sending data must be blocked. If you do not specify a value for this field, the EMS server uses a default wildcard (*) character and accepts any value.
Destination Port/Sequence	The port number to which sending data must be blocked. If you do not specify a value for this field, the EMS server uses a default wildcard (*) character and accepts any value.

Whitelist tab

Name	Description
Name	The name of the whitelist rule.
Interface/VLAN	The interface or VLAN for which the rule is applicable.
Source Address	The IP address from which data must be allowed.
Source Port/Sequence	The port number from which data must be allowed.
Protocol	The transport protocol used. This field is mandatory when you enter a source or destination port.
Destination Address	The IP address to which sending data must be allowed.
Destination Port/Sequence	The port number to which sending data must be allowed.

Services tab

Name	Description
Service Name	The name of the service.
Status	The current status of the ping service. The options are: • **Blocked** • **Allowed**

Source Rate Limiting

Name	Description
Service Name	The name of the service. The options are: • **HTTP** • **HTTPS** • **XMPP** • **SIP** • **SCEP** • **LDAP** • **DNS** • **CES**
Drop Threshold	The maximum connections that are allowed per second for the service. All connections received after the threshold is exceeded are dropped.

Related links

Adding a new blacklist rule on page 74

Restarting the IPCS services

About this task

When updating the Data access objects (DAOs) of the OAMP server on a standalone Avaya SBC installation, you must restart the IPCS services. The DAOs that require a restart include the Radius server, license manager, and SNMP profile configurations.

Procedure

1. Log in to the EMS CLI interface as an administrator.
2. Run the following command: `/etc/init.d/ipcs-init restart`

   Avaya SBC restarts the IPCS services.

Chapter 5: Domain policy, routing, and message flow administration

Governing Unified Communications with Domain Policies

You can create, manage, and assign Domain Policies, also referred to as Unified Communications Policies. With the policies, you can control the call flows entering or leaving the enterprise based upon a wide range of conditions and parameters.

Unified Communications Policies

With Unified Communication Policies, enterprise UC administrators can govern Unified Communications through the enforcement of business rules. Rules can be based on user identity, domain affiliation, network identity, time of day, and time of week.

UC Policies have two high-level concepts, flows and Domain Policies. When Avaya SBC receives a packet , the content of the packet, such as IP addresses and URIs, determines the flow that the packet matches. After the flow is determined, the flow points to a policy that contains several rules concerning processing, privileges, authentication, and routing. After Avaya SBC applies routing and determines the destination endpoint , it applies the policies for this destination endpoint . The context is applied to future packets in the same flow.

Flows

The packet field values that are configured in flows are matched to categorize a packet so that the appropriate policy can be applied. The flows match starting with the highest order, lowest numeric value. The most particular flows are used at the top, while those lower in the order can be more general.

Endpoint Flows

Endpoint Flows are used to determine signaling endpoints to apply the appropriate endpoint policy.

The types of endpoint flows are:

- Subscriber Flows: Identify SIP phones and users.
- Server Flows: Identify SIP servers

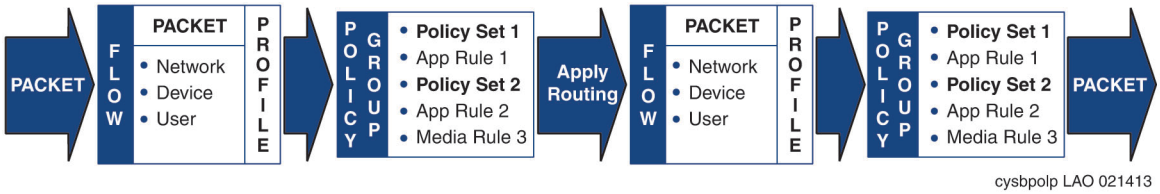
Domain Policies

- End Point Policy Groups: An ordered list of policy sets. The policy set with the highest order, lowest numeric value, is applied if Time of Day (ToD) matches what?. Smaller time windows are used at the top with larger time windows further down the order.

- Policy Set: A set of application, border, media, security, signaling, vcharging, and ToD rules.
- Rules: The processing method, privileges, and authentication method of packets.
- Session Policies: The set of policies for the media sessions. For example, which codec is to be applied to the media session between the source and destination.

The following is an example of matching flows and policies for securing a SIP Trunk and SIP Phones with Avaya SBC:

Example



Example: Call server with Avaya SBC securing SIP trunk

To be created by user

- End Point Policy Groups
  - Call Server Policy Group
  - Trunk Server Policy Group
- Endpoint Flows
  - between Call Server and Avaya SBC Flow.
  - between Trunk Server and Avaya SBC Flow.
- Session Policies
  - Trunk Server/Call Server SIP Phone Session Policy
- Session Flows
  - Trunk Server to Call Server SIP Phone Flow (bidirectional)

End Point Policy

Call coming from Call Server

1. Avaya SBC receives the packet.
2. Avaya SBC determines Flow.
3. Call Server to Avaya SBC Flow points to Call Server Policy Group. Avaya SBC applies the policy and routes the packet to the determined destination.
4. Trunk Server to Avaya SBC REVERSE Flow points to Trunk Server Policy Group. Avaya SBC applies the policy.
5. Packet is sent to Trunk Server.

Call coming from Trunk Server

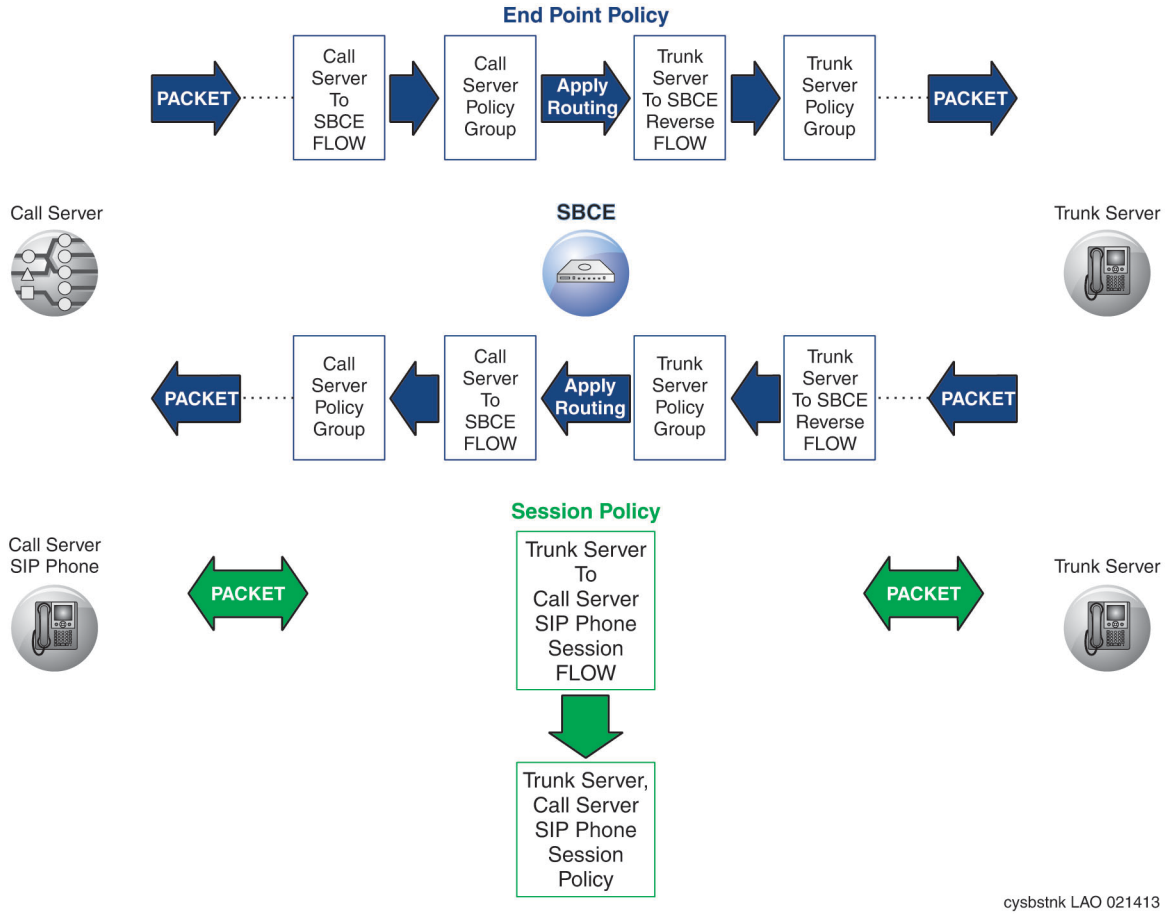
1. Avaya SBC receives the packet.

2. Avaya SBC determines Flow.
3. Trunk Server to Avaya SBC Flow Points to Trunk Server Policy Group. Avaya SBC applies the policy and routes the packet to the determined destination.
4. Call Server to Avaya SBC REVERSE Flow points to Call Server Policy Group. Avaya SBC applies the policy.
5. Packet is sent to Call Server.

Session Policy

1. Avaya SBC receives the packet.
2. Avaya SBC determines Flow.
3. Trunk Server to Call Server SIP Phone Session Flow points to Trunk Server/Call Server SIP Phone Session Policy. Avaya SBC applies the policy.
4. Packet is sent.

Example



Example: Call server with Avaya SBC securing SIP phones

To be created by user

- End Point Policy Groups
  - Call Server Policy Group
  - SIP Phone Policy Group
- Endpoint Flows
  - between Call Server and Avaya SBC Flow.
  - between SIP Phone and Avaya SBC Flow.
- Session Policies
  - SIP Phone Session or Call Server SIP Phone Policy
- Session Flows
  - SIP Phone to Call Server SIP Phone Flow (bidirectional)

End Point Policy

Call coming from Call Server

1. Avaya SBC receives the packet.
2. Avaya SBC determines Flow.
3. Call Server to Avaya SBC Flow points to Call Server Policy Group. Avaya SBC applies the policy and routes the packet to the determined destination.
4. SIP Phone to Avaya SBC REVERSE Flow points to SIP Phone Policy Group. Avaya SBC applies the policy.
5. Packet is sent to the SIP phone.

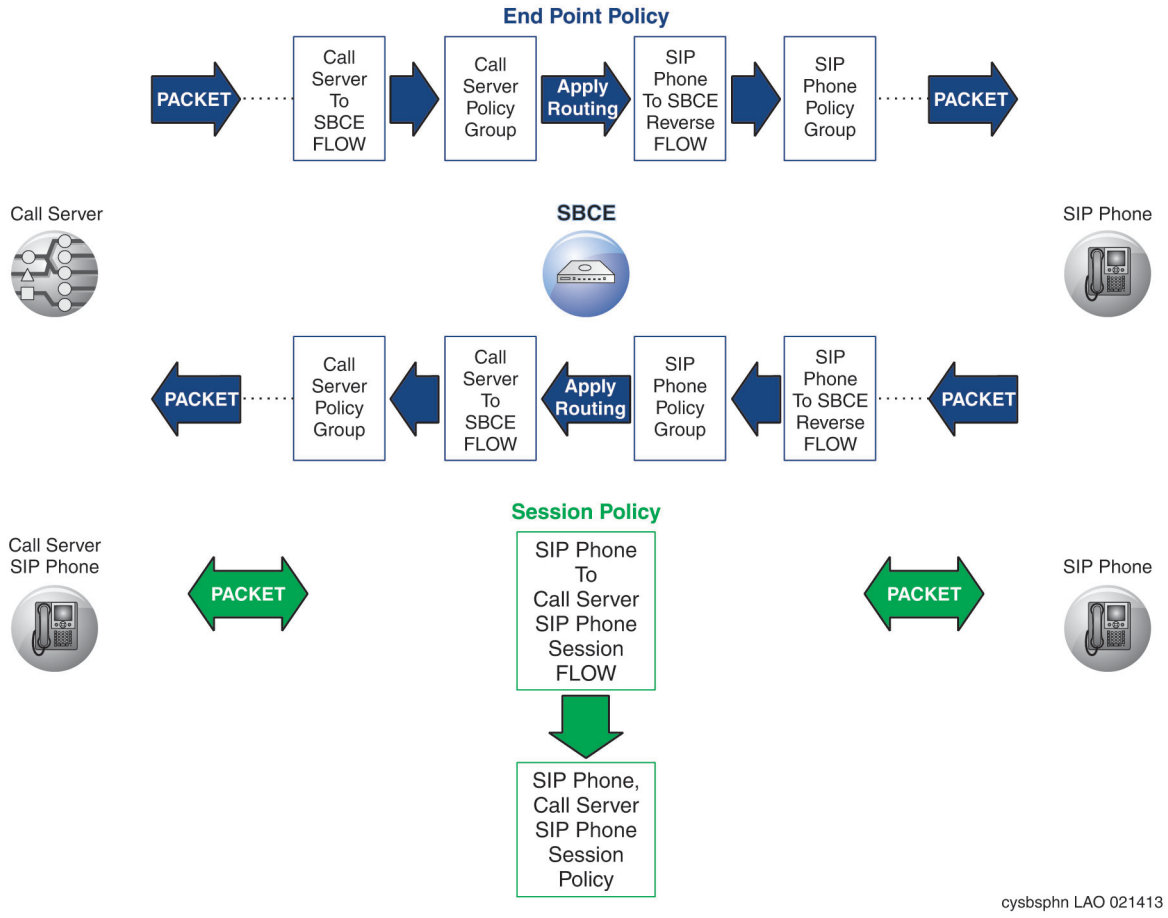
Call coming from SIP Phone

1. Avaya SBC receives the packet.
2. Avaya SBC determines Flow.
3. SIP Phone to Avaya SBC Flow Points to SIP Phone Policy Group. Avaya SBC applies the policy and routes the packet to the determined destination.
4. Call Server to Avaya SBC REVERSE Flow points to Call Server Policy Group. Avaya SBC applies the policy.
5. Call Server receives the packet.

Session Policy

1. Avaya SBC receives the packet.
2. Avaya SBC determines Flow.
3. SIP Phone to Call Server SIP Phone Session Flow points to SIP Phone or Call Server SIP Phone Session Policy. Avaya SBC applies the policy.
4. Packet is sent.

Example



Rules and policies configuration

While configuring rules and policies, do the following:

- Group rules in policy sets.
- Group endpoint policy groups in policy sets.
- Assign endpoint policy groups to endpoint flows.
- Assign session policies to session flows, subscriber flows, and server flows because session policies control codec negotiation, media forking, and media anchoring .

Architecture

The Avaya SBC architecture uses a standard platform and a micro platform. The standard platform example is a single Avaya SBC device deployed in the core with the call server complex and controlled by a separate EMS device. In the following figure, the ports for Dell R210ii are

shown as an example for standard platform servers. The micro platform example is a single SBC device deployed in the enterprise DMZ and controlled by a separate EMS device.

Note:

You can deploy the standard platform device and the Portwell platform device in either architecture.

Example

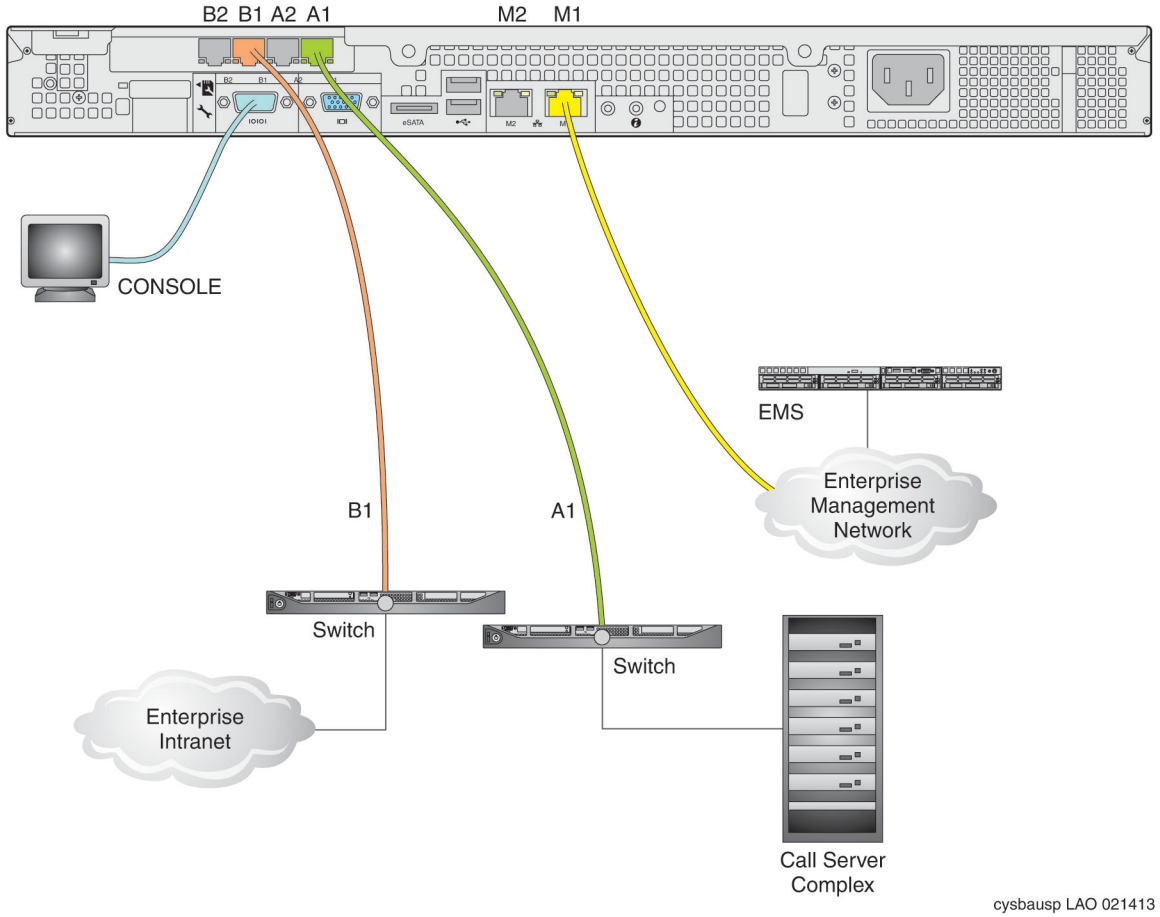


Figure 1: Avaya SBC architecture using a standard platform

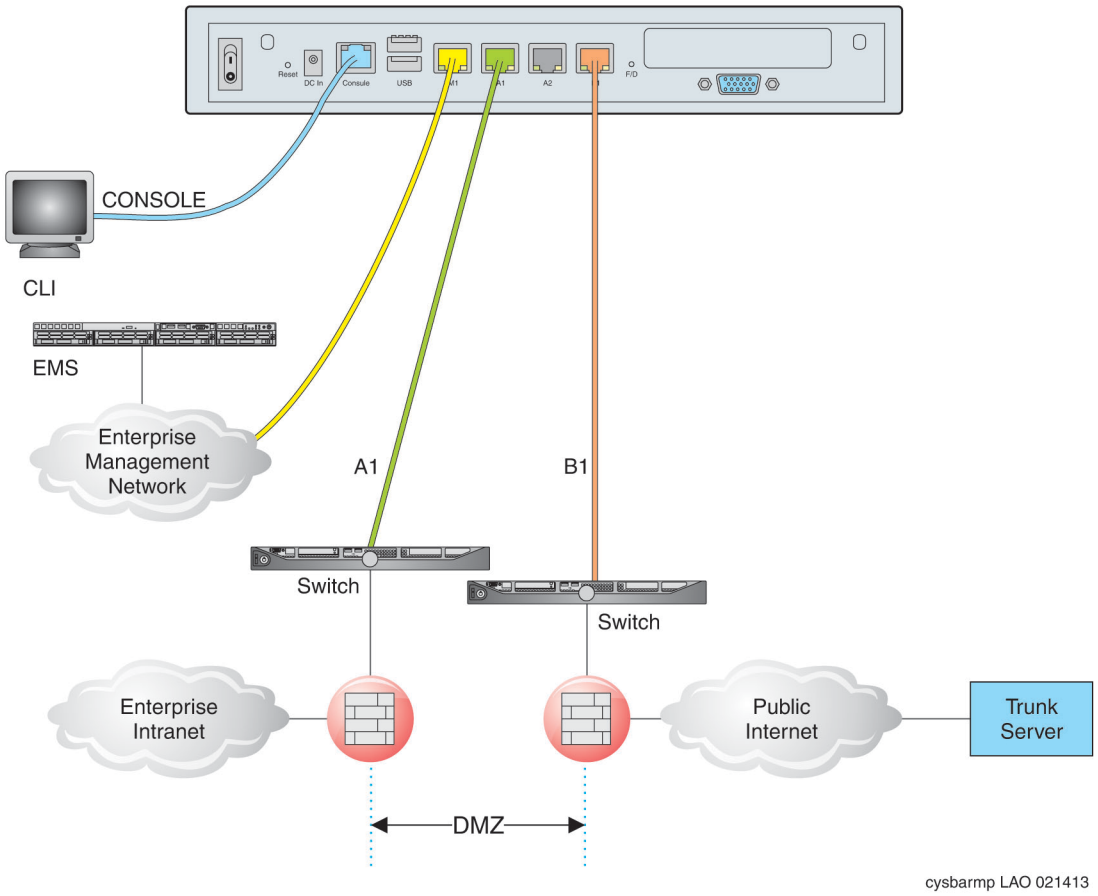


Figure 2: Avaya SBC architecture using a micro platform

Rule and policy associations

The following is the list of rules and policies, for example, application, border, and media rules with domain policies:

Example

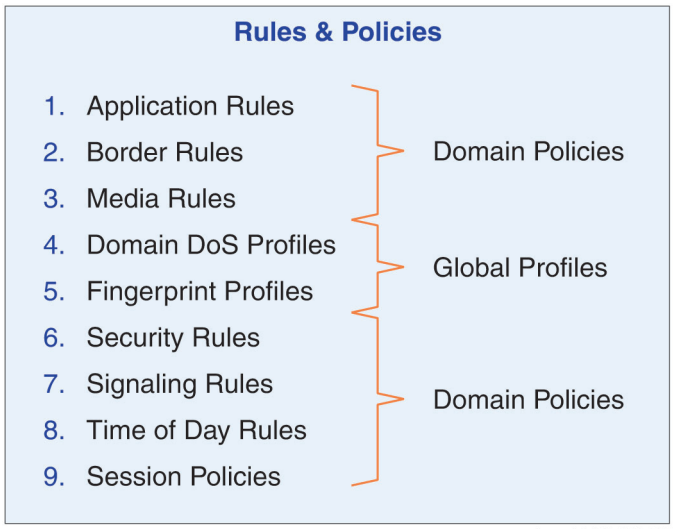


Figure 3: List of rules with the policies

The following are the types of signaling and media flows with the policies, policy groups, and sets, and the interaction with the elements and applications controlled:

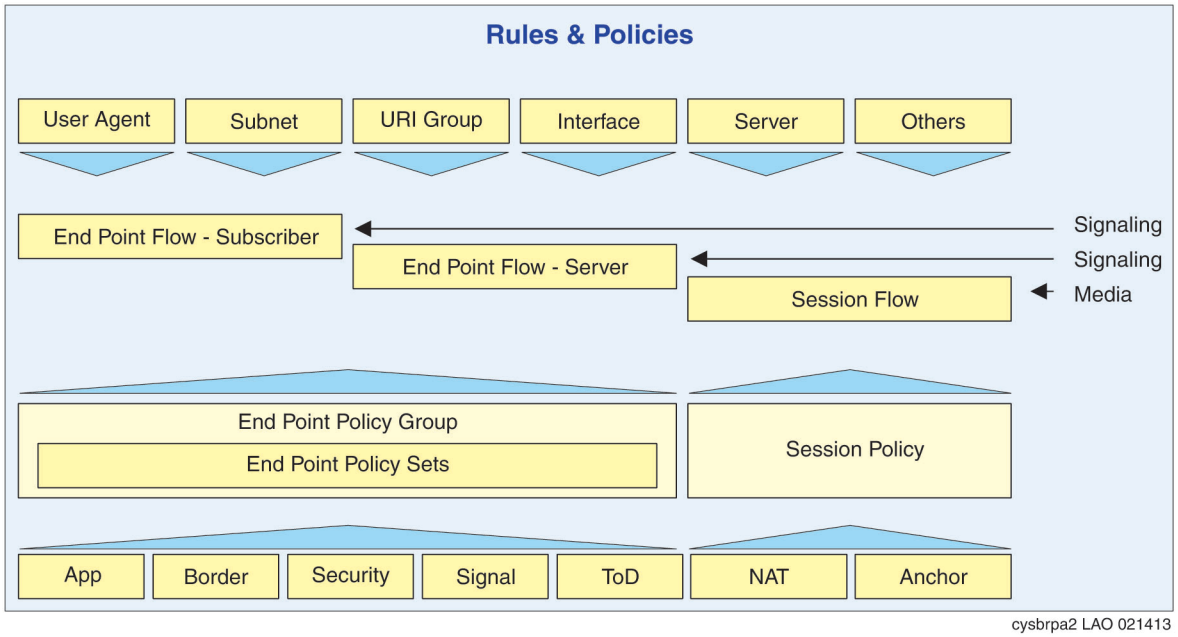


Figure 4: Types of signaling and media flows with the policies and policy groups and sets

The following are the session and subscriber flows with the policies:

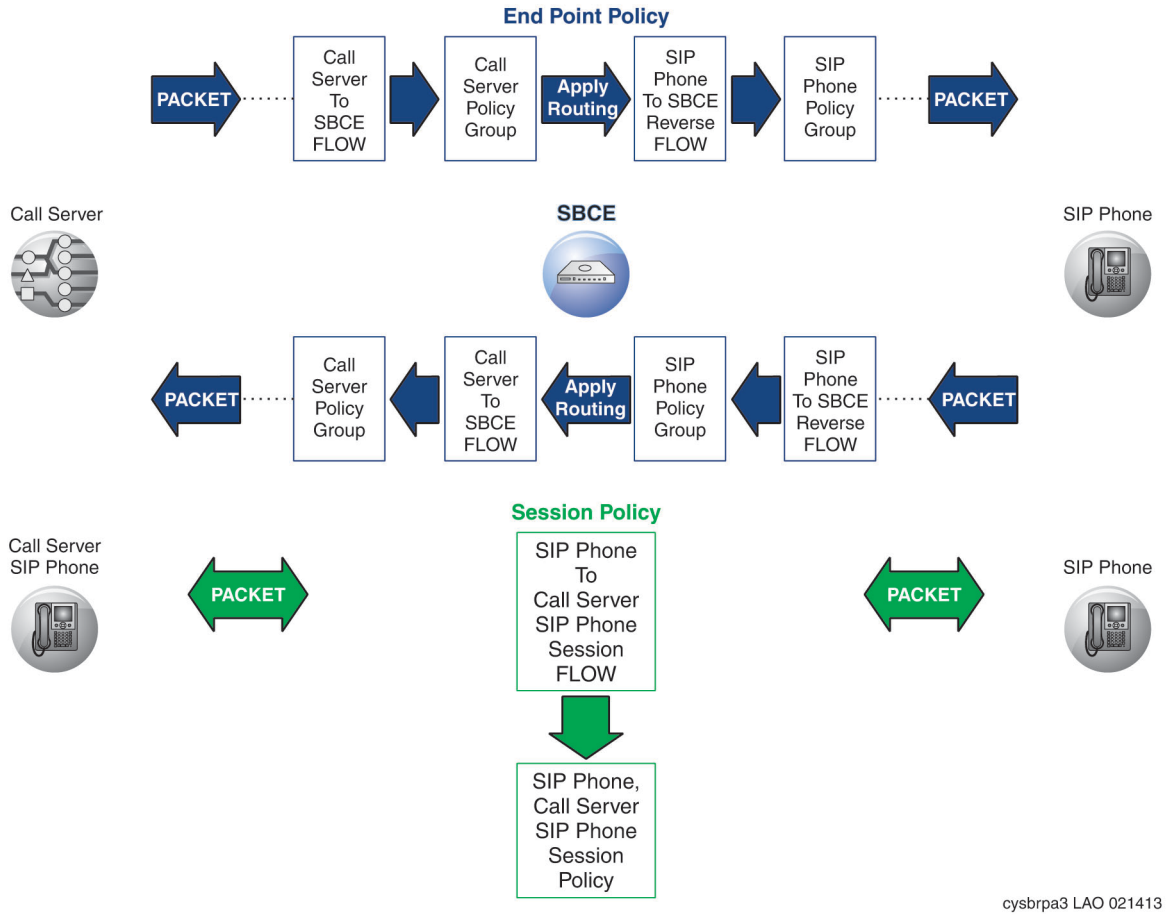


Figure 5: Session and subscriber flows with the policies

Rules and policies checklist

No.	Task	Reference	Notes
1	Configure application rules.	Creating a new application rule on page 103	
2	Configure border rules.	Creating a new border rule on page 106	
3	Define media rules.	Creating a new media rule on page 110	
4	Define domain DoS rules.	Adding a New Domain DoS Profile on page 294	
5	Create security rules.	Creating a new security rule on page 121	
6	Define signaling rules.	Creating a new signaling rule on page 125	Block Option Request Headers with 403 Forbidden.

Table continues…

No.	Task	Reference	Notes
7	Create charging rules	Creating a new charging rule on page 140	
8	Set time-of-day rules.	Creating a new ToD rule on page 254	
9	Create a policy group.	Creating a new policy group on page 144	

SIP message processing

SIP messaging involves the following processes:

- SIP registration processing
- SIP call processing on Avaya SBC
- Border rules
- Media rules
- Security rules
- Signaling rules
- Charging rules
- Endpoint policy groups
- Session policies

SIP registration processing

The SIP routing system routes the SIP REGISTER requests from a remote worker to the call server, which receives them on a TCP or TLS socket.

The SIP routing system tries to find a matching subscriber flow for a new registration. If SIP does not find a subscriber flow match , it rejects the new registration with a `SIP 403 Forbidden` error response.

Subscriber flow matching

The routing system determines a Subscriber Flow match by using additional matching criteria. It uses the following fields of server flow configuration for the match:

- **URI Group**
- **SIP Signaling Interface**
- **Via Host**
- **Contact Host**
- **User Agent**

- **Source Subnet**

To complete the matching, SIP routing system follows a sequence:

1. Uses the `SIP To` header URI of the incoming request for comparison with the provisioned URI Group to decide a match.
2. Upon finding a match, it validates whether the destination IP address of the request matches the provisioned IP Address field of the Signaling Interface configuration.
3. Compares the rest of the fields of the SIP request to match the provisioned values of Subscriber Flow. For example, **Via Host**, **Contact Host**, and Source Subnet.

If any one field does not match, the SIP routing system skips to the next Subscriber Flow, looking for a match from the set of Subscriber Flows.

SIP routing system proceeds with Inbound Policy Invocation only when it finds a Subscriber Flow match.

Inbound policy invocation registration processing

The SIP routing system uses the **Endpoint Policy Group** field within the subscriber flow to determine the policy group provisioned for that endpoint. All the endpoint policy group configurations that are applicable to the SIP REGISTER method are applied on the incoming SIP request before proceeding with the Route Resolution phase.

Route resolution

The SIP routing system uses the **Routing Profile** field from the matched subscriber or server flow to take routing decisions. The SIP routing system uses the **Next Hop** servers specified on the Routing Profile page to determine the communication addresses and transport of the SIP entity for which the incoming SIP call is retargeted.

For DNS NAPTR/SRV procedures followed by Avaya SBC to resolve the **Next Hop Address** fields, see Locating SIP Servers.

After the SIP server is located, the SIP routing system compares the IP address of the located SIP server. The SIP routing system compares the IP address with the IP addresses or Resolved IP Addresses for the FQDNs associated with the provisioned SIP Server Configurations, looking for a match.

If a match is found, the SIP routing system determines the server flow associated with the matched server configuration. The SIP routing system continues with server flow matching.

If no matching server configuration is found, the SIP routing system rejects the registration as there is no valid server configuration.

Related links

Unanchoring media for existing session policies

SIP servers identification on page 89

Server flow matching

The routing system determines a server flow match by using additional matching criteria. It uses the following fields of server flow configuration for the match:.

- **URI Group**
- **SIP Received Interface**

To complete the matching, SIP routing system follows a sequence:

1. Uses the `SIP To` header URI of the incoming request for comparison with the provisioned **URI Group** to decide a match.
2. Upon finding a match, the SIP routing system then validates if the destination IP address of the incoming SIP request matches the provisioned IP Address field of the Received Interface configuration.

If either of the **URI Group** or **Received Interface** fields does not match, the SIP routing system skips to the next Server Flow. The SIP routing system looks for a match from the set of Server Flows associated with Server Configuration.

If no matching Server Flow is found, the SIP routing system rejects the registration as there is no outbound server flow configured.

Outbound policy invocation call processing

If Server or Subscriber Flow is matched, the SIP routing system uses the **Endpoint Policy Group** field to determine the Policy Group provisioned for the target endpoint. All the endpoint policy group configurations are applied on the outgoing SIP request.

Phone or Server Interworking profiles, if configured, are applied on the outgoing SIP message to control the SIP Signaling/Media aspects of the call.

Transmit to network registration processing

The SIP routing system finally routes the SIP registrations to Call Server. The SIP responses are routed by the SIP routing system by using the same Subscriber/Server Flows that were matched during request processing.

Note:

After the remote worker registers successfully to Call Server through the Avaya SBC, subsequent registrations reuse the same Subscriber/Server Flows that were matched during initial SIP registration. Subsequent registrations reuse the same Subscriber/Server Flows until the remote worker deregisters from Call Server.

SIP call processing on Avaya SBC

The SIP routing system processes all Inbound and Outbound calls from an endpoint to Avaya SBC. An endpoint can be a SIP remote worker, Call Server, or Trunk Server. The call processing is in two stages: Inbound and Outbound.

SIP servers identification

The system follows the procedures of RFC 3263 for NAPTR/SRV to correctly identify the SIP communication address, IP Address and Port and Preferred Transport, of the SIP server.

If DNS NAPTR/SRV support is enabled in the routing profile, the outbound transport selection is based on the DNS NAPTR procedures.

- NAPTR/SRV procedures are employed only for SIP dialog creating requests.
- NAPTR procedures are used for determining the transport.
- SRV procedures are used for determining the port and facilitating load balancing.

The SIP routing system uses the following logic to locate a SIP server:

1. If **Next Hop Server** field contains an FQDN, proceed to Step 2, or else proceed below as IP Address is specified.

   The system selects the outbound transport based on the SIP Request-URI scheme selected for the call. By default the scheme is SIP, so the system selects the outbound transport as UDP.

   The system enforces end-to-end SIP scheme in the Request-URI for the following call scenarios.

   a. If SIP scheme is received in the Request-URI message of the incoming request and SBC is not responsible for the Request-URI.
   b. If a call is originating from or terminating to a remote worker that is registered with SIP scheme.

   For both scenarios, the system selects the outbound transport as TLS.

   The system checks if port information is specified as part of the **Next Hop Server** field. If a port is not specified, the system uses a default port based on the transport selected as shown in the following table. If a port is specified, the system uses the configured port.

Transport	Default Port
TLS	5061
TCP/UDP	5060

   The DNS procedures are now complete and a SIP server is located
2. The system performs the DNS NAPTR process to determine the SIP server transport.

   If transport is not specified, NAPTR is enabled because the configuration is mutually exclusive. The system looks up a DNS NAPTR record for the FQDN to determine the preferred transport to the SIP server.

   a. If no NAPTR records are found, the system proceeds with the best effort SRV lookup, assuming that an SRV record exists for the prefixed FQDN. The prefix for the SRV query is based on the SIP Request-URI scheme selected for the call. If SIP scheme is used, UDP SRV record lookup is performed with the `_sip._udp` prefix. If SIPS scheme is used, the TCP SRV record lookup is performed with the `sips._tcp`.
   b. If NAPTR records are found, the system proceeds with the SRV lookup based on the NAPTR lookup result order and preference flags. The SRV record prefix selected is based on the current NAPTR transport selected.

Table 1: Transport protocol and SRV record prefixes

Transport	SRV record prefixes
TLS	`_sips._tcp`
TCP	`_sip._tcp`
UDP	`_sip._udp`

The system selects the outbound transport and proceeds to Step 3.

If transport is specified, the system selects the outbound transport and then proceeds to Step 3.

3. The system performs the DNS SRV processing to locate the SIP server port.

   If SRV is enabled, the system continues as follows:

   If a port is not specified or DNS NAPTR is pending, the system proceeds with DNS SRV lookup for the resulting FQDN from NAPTR response. The system can also perform a DNS SRV lookup for the configured FQDN using the SRV prefixes.

   a. If SRV lookup fails, the system selects the port based on the outbound transport as shown in Table 1 and proceeds to Step 4 assuming that there would be a DNS A record for the FQDN.

   b. If SRV lookup is successful, the system proceeds with a DNS A record lookup on the FQDN returned as part of the SRV result. The system then continues to Step 4.

   If SRV is disabled in the routing profile, the system selects the port based on the transport selected as listed in Table 1. The system continues with Step 4.

4. The system performs DNS A lookup on the resulting FQDN from the SRV response or the configured FQDN if NAPTR/SRV is not performed.

   If DNS A lookup fails and NAPTR/SRV records exist that are yet to be processed, the system returns to NAPTR/SRV processing in Steps 2 and 3 until a DNS A lookup succeeds.

   If the DNS A record lookups are complete, the system returns a DNS error to the SIP routing system. The SIP routing system takes down the call by rejecting the incoming SIP request with a SIP error response because the SIP server could not be located.

   If DNS A record lookup succeeds, DNS procedures are complete and a SIP server is located. The system uses the selected transport, IP Address, and the port for finding a valid server configuration.

   After the SIP server is located, the SIP routing system compares the IP address of the located SIP server with the following IP addresses:

   - IP addresses for the FQDNs associated with the provisioned SIP server configurations.
   - Resolved IP addresses for the FQDNs associated with the provisioned SIP server configurations.

   If a match is found, the SIP routing system determines the server flow associated with the matched server configuration. The system continues with outbound call processing.

Inbound call processing

For inbound calls, the SIP call can be received on a UDP/TCP/TLS socket.

To determine the identity of the SIP entity from which the call originated, the SIP routing system compares the source IP address of the SIP request. The SIP routing system compares the source IP address with the IP addresses or Resolved IP addresses for the FQDNs associated with the provisioned SIP Server Configurations, looking for a match.

If the SIP call matches with a provisioned Server Configuration, the routing system iterates over the provisioned Server Flows associated with the server configuration, looking for a match. See the *Server flow matching* section.

If the SIP call is not associated with any server configuration, the call is rejected unless it matches a provisioned subscriber flow. See the *Subscriber Flow Matching* section.

Related links

Server flow matching for calls originated from the server on page 91
Subscriber flow matching for call originated from remote worker on page 92
Policy invocation and route resolution on page 92
Inbound policy invocation on page 92
Route resolution for call towards remote worker on page 93
Route resolution for a call towards a server on page 93

Server flow matching for calls originated from the server

The routing system uses the URI Group and SIP Signaling Interface fields of the Server Flow configuration as an additional matching criterion to determine a Server Flow match.

The SIP routing system uses the SIP From header URI of the incoming request for comparison with the provisioned URI Group to decide a match. If URI Group is matched, the SIP routing system then validates if the destination IP address of the incoming SIP request matches the provisioned IP Address field of Signaling Interface configuration to decide a match. If either of the URI Group or Signaling Interface fields does not match, the SIP routing system skips to the next Server Flow, looking for a match from the set of Server Flows associated with the Server Configuration.

If a matching Server Flow is found, the SIP routing system performs Policy Invocation and Route Resolution using the matched Server Flow.

- You can configure multiple Server Flows for a single Server Configuration.
- The URI Group field can be configured with the wild card entry (*) that matches any incoming SIP request.
- The Signaling Interface configuration contains the Avaya SBC SIP communication IP Address and Port for each configured transport to receive SIP signaling traffic from the network. The SIP routing system can select a different SIP connect port from Port Ranges for communication with external SIP entities based on configuration.
- The **Received Interface** field must not be confused with the Signaling interface and is not used as part of inbound call processing.

If there is no matching Server Flow, the call is refused and the incoming SIP request is dropped. The SIP routing system stops the call processing for the incoming SIP request after an appropriate SIP error response (403 Forbidden) is sent to the SIP entity for rejecting the call.

Related links

Inbound call processing on page 91
Policy invocation and route resolution on page 92
Server flow matching for a call to a server on page 94

Subscriber flow matching for call originated from remote worker

The SIP routing system consults the internal SIP registration In-memory database to determine whether the SIP call originated from a remote worker.

If SIP registration database lookup is successful, the SIP routing system uses the Subscriber Flow previously matched during the SIP registration process for taking routing decisions. The SIP routing system performs Policy Invocation and Route Resolution using the Subscriber Flow found.

If SIP registration database lookup fails, the SIP routing system refuses the call by generating a SIP error response as the request did not match either a Server or Subscriber Flow. An Incidence/ Syslog is raised for administrative reasons.

Related links

Inbound call processing on page 91
Policy invocation and route resolution on page 92

Policy invocation and route resolution

This section provides an overview of the policy invocation and route resolution process. This section covers the following topics:

- Inbound policy invocation
- Route resolution for calls to a remote worker
- Route resolution for calls to a server

Related links

Inbound call processing on page 91

Inbound policy invocation

If a server or subscriber flow is matched, the SIP routing system uses the Endpoint Policy Group field to determine the Policy Group provisioned for that endpoint. All the endpoint policy group configurations are applied on the incoming SIP request before proceeding with the Route Resolution phase.

Application Rule Processing for Endpoint Policy Group configuration is drafted in a separate section for listing out the recommended values based on the SBC deployment.

Related links

Inbound call processing on page 91

Route resolution for call towards remote worker

If the incoming SIP request does not contain subscriber identification parameter, the routing system proceeds with the normal route resolution.

If an incoming SIP request has a subscriber identification parameter in the SIP request URI header, the call is for a SIP remote worker. The SIP routing system consults the internal SIP Registration in-memory database for determining the communication address of the SIP remote worker.

The subscriber identification parameter (subid_ipcs) is a unique number generated by Avaya SBC for each remote worker during the SIP registration process.

The following is a sample SIP Request line containing the subscriber identification parameter:

```
INVITE sip:5900021@10.1.222.20:5060;transport=tcp;avaya-sc-
enabled;subid_ipcs=2803584614SIP/2.0(SIP Request Truncated)
```

If the SIP registration database lookup is successful, the SIP routing system uses the registration information for routing the call to the SIP remote worker.

The SIP routing system uses the following information available within the registration information to route the SIP call to the remote worker:

- Remote worker Signaling IP Address / Port (including NAT info)
- Remote Signaling Transport (UDP/TCP/TLS)
- Subscriber Flow that matched during the SIP Registration process
- TCP/TLS connection information if connection-oriented transport is used by the remote worker.

The SIP routing system reuses the same TCP/TLS connection and Subscriber Flow for routing any SIP messages to the remote worker.

If the SIP registration database lookup fails, the call is rejected with a SIP 403 Forbidden error response and a Syslog/Incidence is raised. This event occurs when the SIP remote worker is no longer registered through the Avaya SBC.

Related links

Inbound call processing on page 91

Route resolution for a call towards a server

The SIP routing system uses the **Routing Profile** field from the matched subscriber/server flow to take routing decisions. The SIP routing system uses the **Next Hop** servers specified on the Routing Profile page to determine the communication addresses and transport of the SIP entity for which the incoming SIP call is retargeted.

The **Next Hop Address** fields on the Routing Profile page can be configured with an IP Address / IP Address: Port / Domain / Domain: Port. The SIP routing system routes the call to the appropriate server based on the selected load balancing algorithm.

- **Heartbeat failure**: If the server fails to respond to a heartbeat message, subsequent routing takes places towards the next **Next Hop** server.

- **SIP Timer expiration**: SIP RFC 3261 Timer. By default, this functionality is available for all the request messages. If you want to overwrite RFC 3261 timer, use the **server interworking profile** timer configuration.
- **Server Error Message**: If the server sends a 5xx message, Avaya SBC considers the server as currently unavailable.

The **Next Hop Address** fields must resolve to a valid Server Configuration for the SIP routing system to correctly route the SIP calls.

Routing profile can be provisioned with support for DNS NAPTR/SRV procedures as per RFC 3263. DNS support for A-queries is enabled by default and not configurable. The system internally employs an LRU-based DNS cache for facilitating faster lookups.

After the route entry is resolved, the system proceeds with locating SIP servers.

Related links

Inbound call processing on page 91

Outbound call processing

This section provides an overview of outbound call processing covering the following topics:

- Server flow matching (call toward a server)
- Outbound policy invocation
- Transmit to network

Server flow matching for a call to a server

The routing system uses the **URI Group** and **SIP Received Interface** fields of the Server Flow configuration as additional matching criteria to determine a server flow match.

The SIP routing system uses the SIP To header URI of the incoming request for comparison with the provisioned URI Group to decide a match. If URI Group matches, the SIP routing system validates whether the destination IP address of the incoming SIP request matches the provisioned **IP Address** field of the Received Interface configuration . If either of the **URI Group** or **Received Interface** fields do not match the SIP routing, the routing system skips to the next server flow. It scans the set of server flows associated with the server configuration for a match.

Note:

The URI group can be a wild card entry (*) that can match any SIP request.

The **Received Interface** field contains the IP Address of the Interface on which Avaya SBC received the SIP request from the network.

If a matching server flow is found, the system continues with outbound call processing.

If no matching server flow is found, the SIP routing system rejects the call becausean outbound server flow is not configured.

Outbound policy invocation for registration processing

The SIP routing system uses the **Endpoint Policy Group** field within the subscriber flow to determine the policy group provisioned for that endpoint. All endpoint policy group configurations that are applicable to the SIP REGISTER method are applied on the incoming SIP request before proceeding with the Route Resolution phase.

Transmit to network for call processing

The SIP routing system finally routes the call to the target endpoint by using the connection information determined during the routing phase.

Note:

The SIP routing system retries the call to an alternate target destination where the endpoint can be reached when it receives:

- SIP 408 response from the transaction layer.
- SIP 5xx error response from the network.

The alternate target destination can be an IP address from the **Next Hop Server 2** field of the routing profile/pending DNS NAPTR/SRV/A record entries. These entries are yet to be tried if RFC 3263 procedures are used.

The SIP routing system routes all messages including the SIP responses and the in-dialog requests and responses . For routing, the SIP routing system uses the same subscriber and server flows that were matched during the initial INVITE call processing.

Application rule processing for endpoint policy group configuration

The Application Policy Enforcer applies the application rules. Application rules regulate the number of audio, video, and text sessions that are allowed for each endpoint, remote worker, trunk server, or call server. Each application rule contains the following counters for every media type and the incoming and outgoing direction flags for the media type:

- Maximum concurrent sessions per endpoint counter
- Maximum concurrent sessions counter

Important:

Application rule enforcement does not apply if the call is detected as an emergency call using the emergency URI configuration. All emergency calls are allowed even if the configured maximum number of concurrent sessions is reached.

Maximum concurrent sessions per endpoint counter

This counter indicates the maximum number of available concurrent sessions that an endpoint can use for audio, video, and IM. This counter is available for every endpoint. Application Policy Enforcer rejects the call when this counter limit is reached.

Maximum concurrent sessions counter

This counter indicates the maximum number of available sessions for users of this policy group. Any subscriber or server flow using the same policy group is considered as a concurrent session of that policy group. This counter is available for every endpoint policy group. Each application rule is tied to an endpoint policy group. Application Policy Enforcer rejects the call when this counter limit is reached.

Rules for call flows

To increase the call capacity, ensure that:

- The inbound server flow and outbound server flow use separate or unique endpoint policy groups.
- Each endpoint policy group uses a separate application rule.

In/Out direction flags

The In/Out direction flags are available for each media type and refer to the direction of the media stream that the Application Rule processes if checked or enabled.

For an Inbound Call with SDP to the Avaya SBC, Application Policy Enforcer checks if the Inward direction flag is enabled for all the media streams received in the SDP. For an Outbound Call with SDP from the Avaya SBC, Application Policy Enforcer checks if the Outbound direction flag is enabled for all the media streams received in the SDP. If at least one of the required In or Out flags is disabled, the Application Policy Enforcer rejects the call with a SIP error response. An Incidence/Syslog is raised with the appropriate cause for administrative reasons.

The Avaya SBC does not release a call immediately after receiving a SIP BYE from the network. The software internally holds the call state for 32 seconds before releasing the call completely. This hold time is required for internal Avaya SBC call resource management and SIP Protocol procedures.

So the counters Maximum concurrent sessions per endpoint / policy must be configured by accounting for the call hold time and the additional 32 seconds of hold time.

Max Concurrent Sessions Per endpoint = (Number of Calls per second) * (Call Hold Time in seconds + 32)

For example, if an endpoint makes 2 calls every 1 second with a call duration of 60 seconds, the maximum concurrent sessions for each endpoint can be 2*(60 + 32)=184.

1. The system runs the Application Policy Enforcer twice during Inbound / Outbound Policy Invocation while processing a call.

   If the same endpoint policy group is run twice, the counters Maximum concurrent sessions per endpoint / policy are increased twice. This process might cause a Policy violation if not provisioned correctly.

   So use separate Endpoint Policy Groups for Subscriber and Server Flows.

Note:

Also note that in case of a call from a Remote User to Remote User, four Policy Invocations are performed as there are two separate SIP Dialogs involved in a call. This process is the general case where the Call Server acts as a B2B UA.

SIP call flow example

This SIP call flow example is a SIP trunking scenario where a test call is made from a PSTN trunk user (705030) to a Call Centre Elite user (604020) through Avaya SBC.

Trunk User —> ostn-cm —> pstn-asm —> SBC —> cce-asm —> cce-cm —> CCE user

The following table contains the IP addresses of the external SIP entities involved in this call flow.

For information about provisioning the Avaya SBC for routing the calls from PSTN trunk to the CCE server, see Provisioning for PSTN trunk Aura Session Manager on page 99.

The provisioning information in those tables provides a sample reference for examining the call flow example and might be incomplete.

SIP entities and IP addresses

SIP Entity	IP Addresses
Trunk User (705030)	10.129.1.35
PSTN Communication Manager	10.129.10.35
PSTN Aura Session Manager	10.129.3.82
Call Centre Elite Aura Session Manager	10.32.15.8
Call Centre Elite Communication Manager	10.32.11.1
Call Centre Elite User (604020)	10.32.4.5

Call flow example for call processing

This section explains the call processing portion of the call flow example.

An audio call is made from Trunk User (705030) to CCE User (604020) using the transport as TCP.

Avaya SBC receives a SIP INVITE request with SDP offer on a new TCP connection. The TCP connection details are as follows:

- Source IP Address: Port – 10.129.3.82:1056
- Destination IP Address: Port – 10.129.2.1:5060

The SIP routing system proceeds to Server Flow Matching as part of Inbound Call Processing.

Call flow example for server flow matching in calls originated from a server

This section explains the server flow matching portion of the call flow example.

The SIP Routing system finds a matching Server Configuration PSTNASM for the Source IP Address 10.129.3.82. The system proceeds to find a Server Flow associated with PSTNASM Server Configuration.

The system finds a matching Server Flow PSTN-Trunk for the inbound call. The system proceeds with Inbound Policy Invocation and Route Resolution phase.

Call flow example for inbound policy invocation

This section explains the inbound policy invocation portion of the call flow example.

The system uses the Server Flow PSTN-Trunk to determine the Endpoint Policy Group configuration PSTN-default-low. The routing system applies all the endpoint policy group configurations on the incoming SIP INVITE request before proceeding with Route Resolution.

Application Rules for the endpoint policy group PSTN-default-low are enforced by the Application Policy Enforcer on the incoming SIP INVITE request. The counters Maximum sessions per endpoint/policy are increased by one for the profile PSTN-default-low. The counters are decreased after the call is released.

If this is the first call received by Avaya SBC from the PSTN trunk, the value of the counters will be 1.

Call flow example for route resolution

This section explains the route resolution portion of the call flow example.

The SIP routing system uses the Routing Profile field within the Server Flow PSTN-Trunk to take routing decisions. The routing profile resolved is To-CCE-ASM. The system uses the **Next Hop Address** fields within the To-CCE-ASM profile to locate the SIP server and the outbound transport is selected to TLS as provisioned.

As the **Next Hop Address** fields are configured with an IP Address, the system tries to find a matching Server Configuration for that IP address. The system finds a matching Server Configuration CCEASM to route the call towards CCE-ASM server.

As the call is being routed towards a server, the routing system tries to find a matching server flow as part of the outbound call processing.

Call flow example for server flow matching in a call towards a server

This section explains the server flow matching portion of the call flow example.

The system finds a server flow match to CCE-ASM. The system determines the outbound Policy Group using the Endpoint Policy Group configuration of CCE-ASM server flow. The system proceeds with Outbound Policy Invocation.

Call flow example for outbound policy invocation

This section explains the outbound policy invocation portion of the call flow example.

The routing system applies all the endpoint policy group configurations of CCE-default-low on the outgoing SIP INVITE request before sending the request on the network.

Application Rules for the endpoint policy group CCE-default-low are enforced by the Application Policy Enforcer on the outgoing SIP INVITE request.

The counters Maximum sessions per endpoint/policy are increased by one for the profile CCE-default-low. If this is the first outbound call sent by the Avaya SBC towards CCE ASM the value of the counters would be 1.

If the same endpoint policy group is used in the Server Flow STN-Trunk and CCE-ASM, the same counters are increased twice during Inbound/Outbound Policy Invocation.

The counters are maintained for each Endpoint Policy Group, so use separate endpoint policy groups for each server.

After the Endpoint Policy Group configurations are applied, the system routes the call to CCE ASM server.

Call flow example for transmit to network

This section explains the transmit to network portion of the call flow example.

The SIP routing system creates a new TLS connection if none exists towards the CCE ASM server (10.32.15.8:5061) using the Source IP Address: Port from the Signaling Interface CCE-Sig-Interface configured in CCE-ASM Server Flow.

Finally the call is routed to CCE ASM server. All the responses are routed on the same connection using the same Server Flows that are matched during the INVITE request process.

All media ports are released when the SIP call is disconnected using the BYE method. The counters Maximum concurrent sessions per endpoint/policy for each Endpoint Policy Group PSTN-default-low, CCE-default-low are decreased as the call is released.

Call flow example from PSTN trunk to a Call Center Elite user

Example 1

This SIP call flow example is a SIP trunking scenario where a test call is made from a PSTN trunk user (705030) to a Call Centre Elite user (604020) through Avaya SBC.

Trunk User —> ostn-cm —> pstn-asm —> SBC —> cce-asm —> cce-cm —> CCE user

The following table contains the parameter field names and values for the various interfaces, profiles, and policy groups used in this call scenario.

Note:

The provisioning information in this table is a sample reference for examining call flows and might be incomplete.

Table 2: Signaling Interface – PSTN-Sig-Interface

Field	Value
Name	PSTN-Sig-Interface
Signaling IP	10.129.2.1
TCP Port	5060
UDP Port	5060
TLS Port	5061
TLS Profile	Avaya-SBC-Server

Table 3: Media Interface – PSTN-Med-Interface

Field	Value
Name	PSTN-Med-Interface
Media IP	10.129.2.1
Port Range	56000 – 60000

Table 4: Routing Profile – To-PSTN-ASM

Field	Value
URI Group	*
Next Hop Server 1	10.129.3.82
Transport	TCP

Table 5: Server Configuration – PSTNASM

Field	Value
General	
Server Type	Call Server
IP Addresses / FQDNs	10.129.3.82
Supported Transports	TCP, TLS
TCP Port	5060
TLS Port	5061
Advanced	
Enable Grooming	Enabled
Interworking Profile	avaya-ru (default profile)
TLS Client Profile	Avaya-SBC-Client

Table 6: Server Flow – PSTN-Trunk

Field	Value
Flow Name	PSTN-Trunk
Server Configuration	PSTNASM
Received Interface	CCE-Sig-Interface
Signaling Interface	PSTN-Sig-Interface
Media Interface	PSTN-Med-Interface
Endpoint Policy Group	PSTN-default-low
Topology Hiding Profile	default (Default profile)
Routing Profile	To-CCE-ASM

Table 7: Endpoint Policy Group – PSTN-default-low

Field	Value
Application	default
Border	default
Media	default-low-med
Security	default-low
Signaling	default-low
Time of Day	default-low

Example 2

Table 8: Signaling Interface – CCE-Sig-Interface

Field	Value
Name	CCE-Sig-Interface
Signaling IP	10.32.3.1
TCP Port	5060
UDP Port	5060
TLS Port	5061
TLS Profile	Avaya-SBC-Server

Table 9: Media Interface – CCE-Med-Interface

Field	Value
Name	CCE-Med-Interface
Media IP	10.32.3.1
Port Range	56000 – 60000

Table 10: Routing Profile – To-CCE-ASM

Field	Value
URI Group	*
Next Hop Server 1	10.32.15.8
Transport	TLS

Table 11: Server Configuration – CCEASM

Field	Value
General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.15.8
Supported Transports	TCP, TLS
TCP Port	5060
TLS Port	5061
Advanced	
Enable Grooming	Enabled
Interworking Profile	avaya-ru (Default profile)
TLS Client Profile	Avaya-SBC-Client

Table 12: Server Flow – CCE-ASM

Field	Value
Flow Name	CCE-ASM
Server Configuration	CCEASM
Received Interface	CCE-Sig-Interface
Signaling Interface	CCE-Sig-Interface
Media Interface	CCE-Med-Interface
Endpoint Policy Group	CCE-default-low
Topology Hiding Profile	default (Default profile)
Routing Profile	To-PSTN-ASM

Table 13: Endpoint Policy Group – CCE-default-low

Field	Value
Application	default
Border	default
Media	default-low-med
Security	default-low

Table continues…

Field	Value
Signaling	default-low
Time of Day	default-low

Application rules

Application rules define the type of SBC-based Unified Communications (UC) applications Avaya SBC protects. You can also determine the maximum number of concurrent voice and video sessions that your network can process before resource exhaustion. Application rules are part of the Endpoint Policy Group configuration. You can select a customized application rule or the default application rule from a list during the configuration while creating an Endpoint Policy Group. The **Application Rules** function is available in the **Domain Policies** menu.

Creating a new Application Rule

About this task

Caution:

Avaya provides a default application rule set named default. Do not edit this rule because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing application rule sets, and the content pane displays the parameters for the selected application rule.
4. In the application pane, click **Add**.
5. Enter the required values in the appropriate fields, and click **Finish**.

Result

The application pane displays the newly created application rule, and the content pane displays the parameters when you select the new application rule.

Application Rule screen field descriptions

Name	Description
Application Type	The type of SIP application for which this application rule is being configured. The options are: *Audio * Video .

Table continues…

Name	Description
In	Check box indicating that this application rule applies to the audio and video traffic entering the enterprise network.
Out	Check box indicating that this application rule applies to the audio and video traffic originating from within the enterprise network.
Maximum Concurrent Sessions	The maximum number of concurrent application sessions that can be active for the selected application type. Additional application requests are blocked when this threshold is exceeded.
Maximum Sessions Per Endpoint	The maximum number of application sessions that can be active for an endpoint. Additional application requests are blocked when this threshold is exceeded.
Summarize Calls	Check box to specify whether the Call detail records are summarized. Avaya SBC uses the summarized CDR data to generate telemetry reports that contain the usage (for example, overall call count) and performance data (for example, percentage of transfer reliability success calls). These reports are generated for a particular tenant configuration in MS Teams deployment. For more information, see Viewing Telemetry reports on page 419.
CDR Support	CDR option type applicable for the application rule. • **Off**: Call detail records are not provided. • **Radius**: Call detail records are sent to the Radius server. • **CDR Adjunct**: Call detail records are sent to the CDR Adjunct configured in the **Monitoring & Logging** > **CDR Adjunct** section. To store Call detail records locally, select **CDR Adjunct**, but do not configure the CDR Adjunct in the **Monitoring & Logging** > **CDR Adjunct** section.
Radius Profile	The Radius profile that must be used for this application rule.
Media Statistics Support	Check box to specify whether media statistics are made available in the CDR file. If you select the **Media Statistics Support** check box, the CDR file contains data about media statistics.
Call Duration	The options for call duration are: Setup: Stores data in the CDR file from the time Avaya SBC sends an INVITE for connecting the call. Connect: Stores data in the CDR file from the time Avaya SBC receives a 200 OK message for connecting the call.
RTCP Keep-Alive	The RTCP Keep-Alive feature.

Editing an Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing application rule sets, and the content pane displays the parameters comprising the selected application rule set.
4. In the application pane, click the name of the application rule that you want to edit.
5. In the content pane, click **Edit**.

   The EMS server displays the Editing Rule window.
6. Make the appropriate edits, and click **Finish**.

Result

The application pane displays the newly edited application rule.

Cloning an Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing application rule sets, and the content pane displays the parameters comprising the selected application rule set.
4. In the application pane, click the name of the application rule that you want to clone.
5. In the upper-right corner of the content pane, click **Clone**.

   The EMS server displays the Clone Rule window.
6. In the **Clone Name** field, type a name for the new application rule, and click **Finish**.

Result

The application pane shows the newly cloned application rule.

Renaming an Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing application rule sets, and the Content pane displays the parameters of the selected application rule set.
4. In the application pane, select the name of the application rule that you want to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Rule window.

6. In the Rename Rule window, type a new name for the application rule, and click **Finish**.

Result

The application pane displays the renamed application rule.

Deleting an Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing application rule sets, and the content pane displays the parameters comprising the selected application rule set.
4. In the application pane, select the name of the application rule that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to confirm.

Result

The application pane no longer displays the deleted application rule.

Border rules

To control NAT traversal settings, you must define border rules. By defining the NAT Traversal feature, you can enable traversal of call flows through the DMZ. You can also set firewall ports to accommodate traffic from the permitted applications.

Creating a new border rule

About this task

Use the following procedure to create a new border rule.

Caution:

Avaya provides a default border rule set named **default**. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Border Rules**.

The application pane displays the existing border rule sets, and the content pane displays the parameters for the selected border rule set.

4. In the applications pane, click **Add**.

   The EMS server displays the Border Rule window.

5. In the **Rule Name** field, type a name for the new border rule, and click **Next**.

   The EMS server displays the second Border Rule window.

6. Enter the required values in the appropriate fields, and click **Finish**.

Result

The application pane displays the newly created border rule, and the content pane displays the parameters when you select the new border rule.

Border Rule screen field descriptions

Name	Description
Enable Natting	Indicates whether the Network Address Translation (NAT) feature is supported on signaling messages. SIP signaling message contact headers and SDP connection headers are overwritten with the configured Avaya SBC published IP or domains. **Note:** Select this check box for all Avaya Aura® deployments.
Use SIP Published IP	Indicates whether IP addresses are used instead of the respective SIP Published Domain.
SIP Published Domain	The domain name of the enterprise call server and SIP phones. This field is active only if the **Use SIP Published IP** check box is cleared.
Use SDP Published IP	Indicates whether the Media IP addresses of the enterprise call server and SIP phones as defined in **Network & Flows** > **Media Interface** are used instead of the respective SDP Published Domain. If you select this field, the **SDP Published Domain** field becomes inactive and the published Media IP address is used. If you clear this field, the **SDP Published Domain** field remains active and the published Media IP address is not used. The SDP Published Domain is used.
SDP Published Domain	Indicates the domain name of the enterprise call server and SIP phones. This field is active if the **Use SDP Published IP** check box is cleared.

Editing an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Border Rules**.

The application pane displays the existing border rules, and the content pane displays the parameters for the selected border rule.

4. In the application pane, click the name of the border rule that you want to edit.
5. In the content pane, click **Edit**.

   The EMS server displays the Editing Rule window.
6. After making the required edits, click **Finish**.

Result

The EMS server displays the Border Rules screen. The application pane displays the newly edited border rule.

Cloning a border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Border Rules**.

   The application pane displays the existing Border Rule sets, and the content pane displays the parameters for the selected border rule.
4. In the application pane, click the name of the border rule that you want to clone.
5. In the upper-right corner of the page, click **Clone**.

   The EMS server displays the Clone Rule window.
6. In the **Clone Name** field, type a name for the new border rule, and click **Finish**.

Result

The EMS server displays the border rules page. The application pane shows the newly cloned border rule.

Renaming an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Border Rules**.

   The application pane displays the existing border rules, and the content pane displays the parameters for the selected border rule.
4. In the application Pane, select the name of the Border Rule that you want to rename.
5. In the upper-right section of the screen, click **Rename**.

   The EMS server displays the Rename Rule window.

6. In the Rename Rule window, type the new name of the border rule and click **Finish**.

Result

The EMS server displays the border rules screen. The application pane displays the renamed border rule.

Deleting an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Border Rules**.

   The application pane displays the existing border rules, and the content pane displays the parameters comprising the selected border rule.
4. In the application pane, click the border rule to delete.
5. In the upper-right corner of the page, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the border rule.

   The application pane no longer displays the deleted border rule.

Media rules

You can use media rules to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together, these media-related parameters define a strict profile that is associated with other SIP-specific policies. You can also define how Avaya SBC must handle media packets that adhere to the set parameters.

When deploying Avaya SBC with Teams, you must configure Avaya SBC media inter-working rules towards the PSTN and the Teams SIP proxy. Media inter-working is administered to support SRTP cryptography, SRTCP, and the codec priority list. Default lifetime rules are used.

SDP capability negotiation

Avaya SBC only provide an SDP CAPNEG offer if you select two preferred formats (#1 and #2) or three preferred formats (#1, #2, and #3). Set at least two preferred formats for RTP and SRTP.

Irrespective of the **Capability Negotiation** check box configuration, Avaya SBC always processes an incoming SDP CAPNEG offer.

For example, you can configure Avaya SBC as follows: Format #1 [AES_CM_128_HMAC_SHA1_80]; Format #2 [AES_CM_128_HMAC_SHA1_32]; Format #3 RTP with SDP capability negotiation for SRTP selected to provide SDP CAPNEG offer.

RTCP multiplexing

Real-time Transport Control Protocol Multiplexing (RTCP-Mux) is a process where RTP and RTCP share the same socket and connection instead of using two separate connections. In this mechanism, RTP and RTCP share the same channel for the incoming stream towards the Avaya SBC. In turn, the Avaya SBC demultiplexes the RTCP messages and sends them to the odd port of Avaya Aura® or any other PBX. RTCP multiplexing reduces the number of ports that must be managed and reduces the resources required to get a session to work through a firewall or a NAT device.

The feature integrates with MS Teams networks as the current drivers.

Note:

Avaya SBC is administered with RTCP Mux support in Media rules and is only applicable in MS Team networks. This configuration is disabled by default.

Creating a media rule

About this task

Caution:

Avaya provides several default media rules. Do not edit these default rules because an improper default configuration might cause calls to fail. Create a new media rule or clone and edit an existing media rule.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Media Rules**.

   The application pane displays the existing media rule sets, and the content pane displays the parameters of the selected media rule set.
4. In the applications pane, click **Add**.

   The EMS server displays the Media Rule window.
5. Type a name for the new media rule in the **Rule Name** field, and click **Next**.

   The EMS server displays the second Media Rule window.
6. Administer the media rule options as described in Media rules field descriptions on page 111.
7. Click **Finish**.

   The application pane displays the newly created media rule, and the content pane displays the parameters when you select the new media rule.

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 153

Media rules field descriptions on page 111

Media rules field descriptions

Encryption tab

Name	Description
Audio or Video Encryption	
Preferred Format #1	The most preferred encryption method for media traffic. Available selections are: • RTP • SRTP_AES_CM_128_HMAC_SHA1_32 • SRTP_AES_CM_128_HMAC_SHA1_80 • SRTP_AES_192_CM_HMAC_SHA1_32 • SRTP_AES_192_CM_HMAC_SHA1_80 • SRTP_AES_256_CM_HMAC_SHA1_32 • SRTP_AES_256_CM_HMAC_SHA1_80 **Note:** If you select one of the SRTP options, you can encrypt RTCP signaling. The system keeps the RTCP check box active for selection.
Preferred Format #2	The second most preferred encryption method for media traffic. Available selections are the same as those in **Preferred Format #1**.
Preferred Format #3	The third most preferred encryption method for media traffic. Available selections are the same as those shown in **Preferred Format #1**.
Encrypted RTCP	Indicates whether RTCP uses encryption. **Note:** This check box is active for selection if at least one of the three preferred encryption formats include SRTP.
MKI	MKI is the Master Key Identifier. Specifies the master key of the SRTP session and is stored in the SRTP context. You can derive other session keys from this master key after the lifetime expires.
Lifetime	Specifies the time interval after which session keys are generated. These keys are not passed in signaling. Session keys are based on MKI. Currently, Avaya SBC does not support the interworking of different lifetime values. You can leave this field blank to match any value.
Interworking	Indicates whether media from encrypted endpoints can flow to unencrypted endpoints and vice versa. Select this check box for media rules in both the endpoint flows. Enable this setting unless you want to enforce end-to-end encryption.

Table continues…

Name	Description
Symmetric Context Reset	There are two types of SRTP context reset: Symmetric and Asymmetric. For Symmetric, both the Tx and Rx context are set while sending the new offer. For Asymmetric, only Tx is set while sending the new Offer. Avaya media servers support Asymmetric SRTP context reset. However, some Avaya endpoints such as H.323, 96xx, and Avaya Workplace Client do not support Asymmetric SRTP context reset. By default, this option is enabled.
Key Change in New Offer	Use this option to control whether a new cryptography key is generated when a new OFFER message is received. A new OFFER message is defined by a change in any of the following scenarios: • Media direction, such as hold/unhold or video mute/unmute • SDP version change • Delayed offer By default, this option is disabled.
Miscellaneous	
Capability Negotiation	Enables SIP and SDP signaling compliant to the RFC-5939 specification. Select this check box only if the Remote Worker supports SDP Capability Negotiation.

Codec Prioritization tab

Name	Description
Audio Codec	
Codec Prioritization	Force audio codecs to be matched according to the priority defined by the Preferred Codec Priority 1 through Preferred Codec Priority 5 fields.
Allow Preferred Codecs Only	Matches only the codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed are not matched.
Transcode	Specifies that the media matched by this media rule must transcode traffic when possible. When you select this option, the system displays [Transcodable] next to the codecs that can be transcoded.
Transrating	Specifies that the media matched by this media rule must use transrating to reduce the bit rate of the media.

Table continues…

Name	Description
Preferred Codecs	Names of audio codecs that you want matched in a particular order. These are optional fields to be completed only if Codec Prioritization is selected. The **Available** column lists all the available codecs. You can select a single codec, or hold down the `Ctrl` key and click to select multiple codecs simultaneously. Click **>** to move the codecs to the **Selected** column. Click **^** or **v** to change the order of the codecs in the **Selected** column. The **P-Time** column lists the available packetization times. When you select a codec and a p-time, and click **>** to move the codecs to the **Selected** column, the **Selected** column displays the codecs with the p-time next to the codec name. This means the system applies transrating at the selected p-time for the preferred codecs.
Video Codec	
Codec Prioritization	Forces audio codecs to be matched according to the priority defined by the Preferred Codec Priority 1 through Preferred Codec Priority 5 fields.
Allow Preferred Codecs Only	Matches only the codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed are not matched.
Transcode When Needed	This field is unavailable for video codecs. Avaya SBC does not support transcoding for video codecs.
Transrating	This field is unavailable for Video Codecs. Avaya SBC does not support transrating for video codecs.
Preferred Codecs	Names of video codecs that you want specifically matched in a particular order. These are optional fields you must administer only if Codec Prioritization is selected. The **Available** column lists all the available codecs. You can select a single codec, or hold down the `Ctrl` key and click to select multiple codecs simultaneously. Click **>** to move the codecs to the **Selected** column. Click **^** or **v** to change the order of the codecs in the **Selected** column. The **P-Time** column lists the available packetization times. When you select a codec and a p-time, and click **>** to move the codecs to the **Selected** column, the **Selected** column displays the codecs with the p-time next to the codec name. This means the system applies transrating at the selected p-time for the preferred codecs.

Advanced tab

Name	Description
Silencing Enabled	Indicates whether Avaya SBC detects media packets from both legs of a call within the set time. If no media packets are detected, Avaya SBC sends an incident report to the Syslog, and the call is disconnected. By default, this option is enabled.

Table continues…

Name	Description
Timeout	Indicates the period (in seconds) within which the media silencing feature processes media packets from both legs of a call. If no media packets are detected in this period, Avaya SBC sends an incident report to the Syslog or the call is terminated. By default, this option is set to 60 seconds.
BFCP Enabled	Indicates whether Binary Floor Control Protocol (BFCP) is used in a people and content telepresence scenario to control the content channel. Content information is passed as a video stream and is controlled by the BFCP channel. It enables the moderator to release floor control to participants and vice versa to give control of the content channel to various participants. The system works on sending a token on the BFCP control signaling. The moderator allows or denies the access to the token. Avaya SBC can support one BFCP channel for multiple video content channels.
FECC Enabled	Indicates whether Far End Camera Control (FECC) is enabled. It provides mixed encryption support for audio, main video, and FECC. In the media path, using an RTP payload type sends control signaling to control the far end camera. The FECC channel facilitates setting up the signaling for the media path, and control signals are sent on this path using the RTP payload type of a particular codec type (H.224).

RTT Enabled	Real Time Text (RTT) defines a payload type in the SDP offer answer for carrying a text conversation in real time sessions in RTP packets. The text conversation is used along with voice, video and other multimedia conversations. RTT is used with the NG911 feature of Avaya SBC to facilitate sending real time text messages to an emergency PSAP. It can also be used if any other application that requires RTT.
	
	When the **RTT Enabled** option is enabled, Avaya SBC relays RTT (media type = text) in SDP. Avaya SBC invokes NAT for the addresses on SDP and at Media Plane while relaying the RTT in SDP. Avaya SBC does not filter or modify the parameters in SDP in case of RTT.
	
	An SDP with RTT enabled looks similar to the following example:
	
	`m=text 11000 RTP/AVP 100 98`
	`a=rtpmap:98 t140/1000`
	`a=rtpmap:100 red/1000`
	`a=fmtp:100 98/98/98`
	
	When the **RTT Enabled** option is disabled, Avaya SBC responds with Port 0. The default setting for **RTT Enabled** is disabled.

ANAT Enabled	Specifies whether Alternate Network Address Types (ANAT) semantics are enabled for SDP to permit alternate network addresses for media streams. ANAT semantics are useful in environments with IPv4 and IPv6 hosts.
Local Preference	Specifies the order of preference for the Alternate Network Address Types IPv4 and Dual Stack IPv6.
Use Remote Preference	Specifies that the remote party must be given ANAT preference to answer the 200 OK response offer, irrespective of the ANAT preference configured on Avaya SBC.

Table continues…

Name	Description
TTL Override Enabled	When enabled, a TTL value between 1 and 255 can be configured. Avaya SBC overrides TTL value in all outgoing media packets. When configured, it changes TTL field in IPV4 packets and HopLimit field in IPV6 packets. The default value is disabled. This field setting will not have any effect on following Avaya SBC media handling features: • Media tunneling • Turn Controller
Media Line Compliance Enabled	Use this field to maintain compliance between the media lines especially for transfer. For example, if the transferee supports audio and video lines and the transfer target supports only audio and if this field is enabled, Avaya SBC maintains audio lines towards the transfer target and audio and video lines towards the transferee. As per RFC 3264 compliance media lines should match in offer and answer. In case of there are devices on either side of Avaya SBC where media lines are different, Avaya SBC interworking maintains parity of media lines on both sides of Avaya SBC.
ICE Gateway Support	Enables support for Interactive Connectivity Establishment (ICE) used when connecting with Microsoft Teams. When enabled, you can administer the **Local Media Optimization** options.

Table continues…

Name	Description
Local Media Optimization options	Use these options to set the site name, site domain, and the action taken when enabling the Local Media Optimization and Media Bypass features. **Note:** These options are visible only when you enable the **ICE Gateway Support** option. As an example, you have salespeople who work at the main sales office, one of your many branch offices, and visit customers who might be at any location. Avaya SBC and Teams can be administered to handle calls efficiently for the salespeople no matter where they are located, using the call processing facilities that are local to them. For example: • When sales people are in the main sales office, calls placed or received are administered to use the main, or core, Avaya SBC system configured for the main sales office. • When the salespeople are working at the branch sales office, calls placed or received are administered to use the branch Avaya SBC system configured for the branch sales office. • When the salespeople are on the road visiting customers, calls placed or received using their mobile devices are administered to use the PSTN. When administering the Local Media Optimization options, follow this general scenario: • On the local Avaya SBC, administer a local site name, the domain name for that site, and set the action to Local User. • On the proxy Avaya SBC that is visible to the Microsoft Phone system, administer the proxy site name, the domain name for that proxy site, and set the action to Media Bypass. **Note:** If you leave the site name and domain name blank, you effectively disable Local Media Optimization.
Site Name	Use this option to set the site name used within the X-MS message header. **Important:** When administering Local Media Optimization, the Teams client location names must match the Avaya SBC core site name or branch site name.
Site Domain	Use this option to set the domain name used within the X-MS message header.
Action	Select one of the following actions as required: • **Media Bypass** – Use this option to enable Local Media Optimization on the proxy Avaya SBC that is visible to the Microsoft Phone system. • **Local User** – Use this option when you want to enable Local Media Optimization on the downstream Avaya SBC in a local branch office.

Table continues…

Name	Description
Audio Port Change on New Offer Enabled	Specifies whether Avaya SBC generates new ports when a new OFFER message is received. By default, this option is disabled, meaning Avaya SBC will not generate new ports.
Video Port Change on New Offer Enabled	Specifies whether Avaya SBC generates new ports when a new OFFER message is received. By default, this option is disabled, meaning Avaya SBC will not generate new ports.
RTCP-MUX Enabled	Enables RTCP-Mux (Real-time Transport Control Protocol Multiplexing). Enabling RTCP-Mux works only when Ice Gateway Support is enabled.

QoS tab

Name	Description
Enabled	Indicates whether Media QoS marking is enabled.
ToS	Indicates whether Type-of-Service (ToS) is enabled. The **Audio Precedence**, **Audio ToS**, **Video Precedence**, and **Video ToS** fields are activated if the ToS option is selected. The following options are available for the **Audio Precedence** and **Video Precedence** fields: • Network Control • Internetwork control • CRITIC/ECP • Flash Override • Flash • Immediate • Priority • Routine The following options are available for the **ToS** field: • Minimize Delay • Maximize Throughput • Maximize Reliability • Minimize Monetary Cost • Normal Service • Other...

Table continues…

Name	Description
DSCP	Indicates the significant values for Differentiated Services (DiffServ). These values, referred to as the Differentiated Services Point Code (DSCP), provide guaranteed service to critical network traffic. The following options are available for the **Audio** and **Video** fields: • EF • AF11 • AF12 • AF13 • AF21 • AF22 • AF23 • AF31 • AF32 • AF33 • AF41 • AF42 • AF43 • Other...

Editing a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Media Rules**.

   The application pane displays the existing media rules sets, and the content pane displays the parameters comprising the selected media rule set.
4. In the application pane, click the name of the media rule that you want to edit.
5. In the lower center section of the content pane, click **Edit**.

   The EMS server displays the Editing Rule window.
6. Administer the media rule options as described in Media rules field descriptions on page 111.
7. Click **Finish**.

   The EMS server displays the Media Rules screen. The application pane displays the newly edited media rule.

Editing codec prioritization parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Media Rules**.
4. In the Application pane, select the media rule whose codec prioritization parameters you want to edit.
5. Click the **Codec Prioritization** tab.
6. In the lower center section of the page, click **Edit**.

   The system displays the codec prioritization window.
7. Administer the codec options as described in Media rules field descriptions on page 111.
8. Click **Finish**.

   The EMS server displays the Media Rules screen. The application pane displays the newly edited media rule.

Cloning a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Media Rules**.

   The application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected media rule set.
4. In the application pane, select the name of the media rule to clone.
5. In the upper-right corner of the screen, click **Clone**.

   The EMS server displays the Clone Rule window.
6. In the **Clone Name** field, type a name for the new media rule.
7. Click **Finish**.

   The EMS server displays the Media Rules screen. The application pane shows the newly cloned media rule.

Renaming a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. Navigate to **Domain Policies** > **Media Rules**.

   The application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected media rule set.
4. In the application pane, select the name of the media rule to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Rule window.
6. In the Rename Rule window, type a new name for the media rule.
7. Click **Finish**.

   The EMS server displays the media rules screen. The application pane displays the renamed media rule.

Deleting a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Media Rules**.

   The application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected media rule set.
4. In the application pane, select the name of the media rule to delete.
5. In the upper-right section of the screen, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the media rule

   The application pane no longer displays the deleted media rule.

Security rules

With security rules, you can define which enterprise-wide VoIP and Instant Message (IM) security features are applied to a particular call flow. For example, you can configure Authentication, Compliance, Scrubber, and Domain DoS. You can also define the security feature profile so that the feature is applied in a specific manner to a specific situation.

Note:

To be effective, enable the scrubber packages in the Security Rules of Domain Policies.

After the scrubber packages are enabled in the security rules, a list of packages are required for the security rule.

You can administer the following security features by defining the security rules:

- **Authentication**: Authentication of users logging on to devices.
- **Compliance**: Rejection of calls from the devices configured in the Blacklist group.
- **Scrubber**: Detection and drop of malformed messages.
- **Domain Dos**: Detection of DoS attacks within a domain policy.

Creating a new security rule

Before you begin

Before adding a new scrubber package to a security rule here, install the scrubber package on Avaya SBC from the Scrubber feature of Global Parameters. For more information, see and Protocol Scrubber on page 299 and Installing a scrubber rules Package on page 300.

About this task

Use the following procedure to create a new security rule.

Caution:

Avaya provides a default security rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Security Rules**.

   The application pane displays the existing Security Rule sets, and the Content pane displays the parameters of the selected Security Rule set.
4. In the Application pane, click **Add**.

   The EMS server displays the first Security Rule window.
5. In the **Rule Name** field, type a name for the new security rule, and click **Next**.

   The EMS server displays the second Security Rule window.
6. Enter the appropriate values, and click **Finish**.

Result

The application pane displays the newly created security rule, and the Content pane displays the parameters when you select the new security rule.

Security Rules field descriptions

Compliance tab

Name	Description
From URI Blacklist	Used to assign blacklisted callers from where the calls are to be blocked. You can select from the predefined blacklists of callers from whom the subscribers do not want to receive calls. **Note:** A URI blacklist can consist of plain text, a dial plan, or one or more regular expressions.

Scrubber tab

Name	Description
Enable Scrubber	A check box indicating whether the Scrubber feature is enabled. If selected, the Scrubber feature is enabled and the Scrubber Packages field is activated. If cleared, the Scrubber feature is not enabled and the Scrubber Packages field is unavailable.
Scrubber Packages	A collection of existing Scrubber Packages that can be selected for use by the Scrubber feature. Select one or more Scrubber Packages. Use Control+Click to select multiple packages.

Domain DoS tab

Name	Description
Domain DoS	Indicates whether the Domain DoS feature is enabled. If you select the check box, the Domain DoS feature is enabled and the **Domain DoS Profile** field is activated.
Domain DoS Profile	Displays a collection of existing DoS profiles. Use this field to define DoS profiles for the Domain DoS feature.

Authentication tab

Name	Description
Enable MAC-based LDAP Authentication	Indicates whether the MAC-based LDAP Authentication feature is enabled.
LDAP Server Profile	Displays a collection of existing LDAP server profiles. Use this field to define the LDAP server profile for a security rule.
LDAP Base DN (Search)	Displays the configured LDAP Base DN to search the users using the LDAP server.
LDAP MAC Attribute	Displays the non editable string “macAddress”. Avaya SBC queries **LDAP MAC Attribute** in the LDAP search request for the MAC address.

Editing an existing security rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Security Rules**.

   The application pane displays the existing security rule sets, and the content pane displays the parameters of the selected security rule set.
4. In the application pane, click the name of the security rule set that you want to edit.
5. In the lower-center section of the screen, click **Edit**.

   The EMS server displays the Editing Rule window.
6. After making the appropriate edits, click **Finish**.

Result

The EMS server displays the Security Rules screen. The application pane displays the newly edited security rule.

Cloning an existing security rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Security Rules**.

   The application pane displays the existing security rule sets, and the content pane displays the parameters of the selected security rule set.
4. In the application pane, select the name of the security rule that you want to clone.
5. In the upper-right section of the content pane, click **Clone**.

   The EMS server displays the Clone Rule window.
6. In the **Clone Name** field, type a name for the new security rule, and click **Finish**.

Result

The EMS server displays the Security Rules page. The application pane shows the newly cloned security rule.

Renaming an existing security rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the navigation pane, click **Domain Policies** > **Security Rules**.

   The application pane displays the existing security rule sets, and the content pane displays the parameters of the selected security rule set.
4. In the application pane, select the name of the security rule that you want to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Rule window.
6. In the Rename Rule window, type the new name for the Security Rule, and click **Finish**.

Result

The EMS server displays the security rules screen. The application pane displays the renamed security rule.

Deleting an existing security rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Security Rules**.

   The application pane displays the existing security rule sets, and the content pane displays the parameters of the selected security rule set.
4. In the Application pane, select the name of the security rule that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the security rule.

Result

The application pane no longer displays the deleted security rule.

Signaling rules

With Signaling Rules, you can define the action to be taken for each type of SIP-specific signaling request and response message. Actions that can be configured with Signaling Rules include Allow, Block, and Block with Response. When SIP signaling packets are received by the Avaya SBC, the packets are parsed and pattern-matched against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Creating a new signaling rule

About this task

Use the following procedure to create a new Signaling Rule.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing Signaling Rule sets, and the Content pane displays the parameters of the selected Signaling Rule set.
4. In the Application pane, click **Add**.

   The EMS server displays the first signaling rule window.
5. In the **Rule Name** field, type a name for the new signaling rule, and click **Next**.

   The EMS server displays the second signaling rule window.
6. Enter the appropriate values, and click **Finish**.

Result

The application pane displays the newly created signaling rule, and the Content pane displays the parameters when you select the new signaling rule.

Signaling Rules field descriptions

Add Signaling Rule

Name	Description
Rule Name	Name of the signaling rule.
Inbound	
Requests	Drop-box to determine how incoming SIP request messages will be treated by this policy. The following options are available: • **Allow**: Allow all incoming SIP request messages. The corresponding fields to the right are unavailable. • **Block with…**: Block all incoming SIP request messages and return the response indicated in the corresponding fields.

Table continues…

Name	Description
Non-2xx Final Responses	Drop-box to determine how incoming Non-2xx Final SIP response messages will be treated by this policy. The following options are available: • **Allow**: Allow all incoming Non-2xx Final Response messages. The corresponding fields to the right are unavailable. • **Change response to….**: Block all incoming Non-2xx Final Response messages and return the response indicated in the corresponding fields.
Optional Request Headers	Drop-box to determine how optional request headers contained in incoming SIP messages will be treated by this policy. The following options are available: • **Allow**: Allow all incoming SIP messages that contain optional request headers. The corresponding fields to the right are unavailable. • **Remove Header**: Strip optional request headers from all incoming SIP messages and allow the message to proceed. • **Block with...**: Block all incoming SIP messages that contain an optional request header and return the response indicated in the corresponding fields.
Optional Response Headers	Drop-box to determine how optional response headers contained in incoming SIP messages will be treated by this policy. The following options are available: • **Allow**: Allow all incoming SIP messages that contain optional response headers. The corresponding fields to the right are unavailable. • **Remove Header**: Strip optional response headers from all incoming SIP messages and allow the message to proceed. • **Change response to...**: Block all incoming SIP messages that contain an optional response header and return the response indicated in the corresponding fields.
Outbound	
Requests	Drop-box to determine how outbound SIP request messages are treated by this policy. The following options are available: • **Allow**: Allow all outbound SIP request messages. The corresponding fields to the right are inactivated. • **Block with….**: Block all outbound SIP request messages and return the response indicated in the corresponding fields.
Non-2xx Final Responses	Drop-box to determine how outbound Non-2xx Final SIP response messages are treated by this policy. The following options are available: • **Allow**: Allow all outbound Non-2xx Final Response messages. The corresponding fields to the right are unavailable. • **Change response to….**: Block all outbound Non-2xx Final Response messages and return the response indicated in the corresponding fields.

Table continues…

Name	Description
Optional Request Headers	Drop-box to determine how optional request headers contained in outbound SIP messages will be treated by this policy. The following options are available: • **Allow**: Allow all outbound SIP messages that contain optional request headers. The corresponding fields to the right are inactivated. • **Remove Header**: Strip optional request headers from all outbound SIP messages and allow the message to proceed. • **Block with….**: Block all outbound SIP messages that contain an optional request header and return the response indicated in the corresponding fields.
Optional Response Headers	Drop-box to determine how optional response headers contained in outbound SIP messages will be treated by this policy. The following options are available: • **Allow**: Allow all outbound SIP messages that contain optional response headers. The corresponding fields to the right are inactivated. • **Remove Header**: Strip optional response headers from all outbound SIP messages and allow the message to proceed. • **Change response to….**: Block all outbound SIP messages that contain an optional response header and return the response indicated in the corresponding fields.
Content-Type Policy	
Enable Content-Type Checks	Option to enable checks for the content part of the SIP signaling message.
Action	Drop-down menu from which you choose the action to be taken by the Avaya SBC security device when considering the content portion of SIP signaling messages. The following options are available: • **Allow**: Allows the content in each SIP signaling message to pass, with the exception of those items contained in the Exceptions List that are removed. • **Remove**: Removes all content from each SIP signaling message, with the exception of the items contained in the Exceptions List that are allowed to pass.
Exception List	The specific terms to be passed or blocked, according to the action specified in the **Action** field.
Multipart Action	Drop-down menu from which you choose the action to be taken by the Avaya SBC security device when considering the multipart content portion of SIP signaling messages. The following options are available: • **Allow**: Allows the multipart content in each SIP signaling message to pass, with the exception of those items contained in the Exception List that are removed. • **Remove**: Removes all the multipart content from each SIP signaling message, with the exception of the items contained in the Exception List that are allowed to pass.
Exception List	The specific terms to be passed or blocked, according to the action specified in the **Multipart Action** field.
QoS	

Table continues…

Name	Description
Enabled	Indicates whether the Signaling Quality-of-Service (QoS) feature is enabled.
ToS	Indicates whether Type-of-Service (ToS) is enabled. The **Precedence** and **ToS** fields are activated only if the ToS option is selected. The following options are available for the **Precedence** field: • Network Control • Internetwork control • CRITIC/ECP • Flash Override • Flash • Immediate • Priority • Routine The following options are available for the **ToS** field: • Minimize Delay • Maximize Throughput • Maximize Reliability • Minimize Normal Cost • Normal Cost • Other...

Table continues…

Name	Description
DSCP	Indicates the most significant values for Differentiated Services (DiffServ). These values, referred to as the Differentiated Services Point Code (DSCP), are used to provide guaranteed service to critical network traffic. The following options are available for the **Value** field: • EF • AF11 • AF12 • AF13 • AF21 • AF22 • AF23 • AF31 • AF32 • AF33 • AF41 • AF42 • AF43 • Other...
UCID	
Enabled	The status indicates whether UCID is enabled. You must enable this method to have unique identifier at call level.
Node ID	A unique two-byte network node identifier that is assigned to the Avaya SBC device.
Protocol Discriminator	Valid values are 0x00 (User-Specific) and 0x04 (IA5). Communication Manager uses this value for processing the external ASAI UUI field, if any, associated with the call.

Add Request Control

Name	Description
Proprietary Request	A check box indicating whether the Request being defined is a non-standard SIP request. Select the check box to designate a non standard SIP request message or clear the check box to indicate a standard SIP request message.
Method Name	The type of standard SIP request message for which this signaling policy will apply. Select the desired Method Name from the corresponding drop-down box. If you select the **Proprietary Request** field, you can type a method name in the **Method Name**.

Table continues…

Name	Description
In-Dialog Action	The action to be taken for the SIP request message defined in the Method Name field when the session is in-dialog. Available action options are Allow, and Block with.... If you select the Block with... option, the two fields below are activated, and you can provide the type of response to be sent.
Out-of-Dialog Action	The action to be taken for the SIP request message defined in the Request field when the session is out-of-dialog. Available action options are Allow, Block, and Block with Response. If you select the Block with Response option, the two fields below are activated, and you can provide the type of response to be sent.

Add Response Control

Name	Description
Proprietary Response	A checkbox indicating whether the Response being defined is a non standard SIP response. Select the checkbox to designate a non-standard SIP response or clear the check box to indicate a standard SIP response.
Response Code	The specific response message to be sent for the received SIP request. Select the desired response from the drop-down box. If you select the **Proprietary Response** field, you can type a response code in the **Response Code** field.
Method Name	The SIP message that triggers the Response Code selected in the previous field. Select the desired SIP message from the drop-down box.
In-Dialog Action	The action to be taken if the proprietary response is generated in-dialog when the session is established. Available action options are **Allow** and **Change response to…**. If you select the **Change response to…** option, the two fields below are activated, and you can provide the type of response to be sent.

Add Header Control

Name	Description
Proprietary Request Header	A check box indicating whether the header being defined is a nonstandard SIP header. Select the check box to designate a nonstandard SIP header or clear the checkbox to indicate a standard SIP header.
Header Name	The name of the proprietary SIP header. Make your selection from the corresponding drop-down list. If you select the **Proprietary Request Header** check box, you can type a header name in the **Header Name** field.
Method Name	The context or call sequence in which the header is contained.

Table continues…

Name	Description
Header Criteria	The header criteria. The available options are Forbidden, Mandatory, and Optional. The **Action** field specifies the action to be taken if the header is present in the SIP message designated in the **Method Name** field. Depending on the option you select for the Header Criteria, different selections are available for the **Action** field: • If you select the Forbidden option, the system displays the **Presence Action** field with the Remove header and Block with... options. • If you select the Mandatory option, the system displays the **Absence action** field with a Block with... option. • If you select the Optional option, the system displays the **Action** field with an Allow option. If you select Block with..., then the system displays two text boxes to type the response message. The default value in the text boxes are 486 and Busy Here respectively.

Add Response Header Control

Name	Description
Proprietary Response Header	A checkbox indicating whether the header being defined is a nonstandard SIP response header. Select the checkbox to designate a nonstandard SIP response header or clear the checkbox to indicate a standard SIP response header.
Header Name	The standard SIP message header for which the signaling policy will apply. Make your selection from the corresponding drop-down list. If you select the **Proprietary Response Header** field, you can type a header name in the **Header Name** field.
Response Code	The code to be sent as the SIP response. Select the desired code from the drop-down box.
Method Name	SIP signaling message name, such as CANCEL, INVITE, or PUBLISH. Make your selection from the corresponding drop-down list.
Header Criteria	Whether the presence of the header in the response field is Forbidden, Mandatory, or Optional.
Action	The **Action** field specifies the action to be taken if the header is present in the SIP message designated in the **Method Name** field. Depending on the option you select for the Header Criteria, different selections are available for the **Action** field: • If you select the Forbidden option, the system displays the **Presence Action** field with the Remove header and Block with... options. • If you select the Mandatory option, the system displays the **Absence action** field with a Block with... option. • If you select the Optional option, the system displays the **Action** field with the Allow option. If you select Block with..., then the system displays two text boxes to type the response message. The default value in the text boxes are 486 and Busy Here respectively.

Editing an existing signaling rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters of the selected signaling rule set.
4. In the application pane, select the name of the signaling rule set that you want to edit.
5. In the lower-center section of the content pane, click **Edit**.

   The EMS server displays the Editing Rule window.
6. After making the appropriate edits, click **Finish**.

Result

The EMS server displays the Signaling Rules screen. The application pane displays the newly edited signaling rule.

Adding Request Parameters

About this task

Use the following procedure to add In Request and Out Request parameters to a Signaling Rule if not defined. In Requests refer to SIP message requests being directed to enterprise endpoints. Out Requests refer to SIP message requests being directed to endpoints external to the enterprise.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the name of the signaling rule where you want to add In Request or Out Request or both parameters from the Applications pane.

   The EMS server displays the selected Signaling Rule information window.
5. Click the **Requests** tab.
6. Click **Add In Request Control** or **Add Out Request Control**.

The EMS server displays the corresponding Add Request Control pop-up window.

7. Select the appropriate information and click **Finish**.

Result

The EMS server displays the selected signaling rule information again.

Configuring inbound signaling rule to send 200 OK response for OPTIONS request

About this task

You must configure an inbound signaling rule so that Avaya SBC can handle OPTIONS request from Session Manager.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the signaling rule where you want to add In Request parameters.
5. Click the **Requests** tab.
6. Click **Add In Request Control**.
7. In the **Method Name** field, click **OPTIONS**.
8. In the **In Dialog Action** field, click **Allow**.
9. In the **Out of Dialog Action** field, click **Block with...**.
10. In the fields below **Out of Dialog Action**, type `200` and `OK`.
11. Click **Finish**.

Next steps

In the endpoint policy group created for Session Manager, add this signaling group.

Responses Parameters tab

This section provides procedures for adding and editing In Response parameters and Out Response parameters of a Signaling Rule.

Adding Response Parameters

About this task

Use the following procedure to add In Response and Out Response parameters for a Signaling Rule if not defined. In Response refers to SIP message responses being directed to enterprise endpoints. Out Responses refers to SIP message responses being directed to endpoints external to the enterprise.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the name of the Signaling Rule where you want to add In Request or Out Request or both parameters from the Applications pane.

   The EMS server displays the selected Signaling Rule information.
5. Click the **Responses** tab.
6. Click **Add In Response Control** or **Add Out Response Control**.

   The EMS server displays the corresponding Add Response Control pop-up window.
7. Select the appropriate information in the Add Response Control window. and click **Finish**.

Result

The EMS server displays the signaling rule information window for the selected signaling rule.

Editing Response Parameters

About this task

Use the following procedure to edit In Response and Out Response parameters for a Signaling Rule if not defined. In Responses refer to SIP message requests being directed to enterprise endpoints. Out Responses refer to SIP message requests being directed to endpoints external to the enterprise.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the name of the signaling rule where you want to edit In Request or Out Request or both parameters from the Applications pane.

The EMS server displays the selected signaling rule information window.

5. Click the **Responses** tab.
6. Click **Add In Response Control** or **Add Out Response Control**.

   The EMS server displays the corresponding Edit Response Control pop-up window.
7. Edit the required information and click **Finish**.

Result

The EMS server displays the selected signaling rule information window again.

Request Headers Parameters tab

This section provides procedures for adding and editing In Request Header parameters and Out Request Header parameters of a Signaling Rule.

Adding Request Header parameters

About this task

Use the following procedure to add In Request Header Control and Out Request Header Control parameters for a Signaling Rule if not defined. In Request Header Control parameters are applied to the headers of SIP messages directed to enterprise endpoints. Out Request Header Control parameters are applied to the headers of SIP messages directed to endpoints external to the enterprise.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the name of the signaling rule where you want to add In Request Header and Out Request Header or both parameters from the applications pane.

   The EMS server displays the selected Signaling Rule information window.
5. Click the **Request Headers** tab.
6. Click **Add In Header Control** or **Add Out Header Control**.

   The EMS server displays the corresponding Add Header Control pop-up window.
7. Select the appropriate information and click **Finish**

Result

The EMS server displays the selected Signaling Rule information window again.

Editing Request Header parameters

About this task

Use the following procedure to edit existing Request Header parameters.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Select the name of the signaling rule where you want to edit In Header Control or Out Header Control or both parameters from the Applications pane.

   The EMS server displays the selected Signaling Rule information window.
5. Click the **Request Headers** tab.
6. Click **Add In Header Control** or **Add Out Header Control**.

   The EMS server displays the corresponding Add Header Control pop-up window.
7. Edit the appropriate information in the Add Header Control pop-up window and click **Finish**.

Result

The EMS server displays the selected Signaling Rule information window.

Response Headers Parameters tab

This section provides procedures for adding and editing In Response Header parameters and Out Response Header parameters of a Signaling Rule.

Adding Response Header parameters

About this task

Use the following procedure to add In Response Header Control and Out Response Header Control parameters for a Signaling Rule if none are already defined. In Response Header Control parameters are applied to the headers of SIP response messages destined for enterprise end-points. Out Response Header Control parameters are applied to the headers of SIP response messages destined for end-points external to the enterprise.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. Click the name of the Signaling Rule where you want to add In Response Header or Out Response Header or both parameters from the Applications pane.

   The EMS server displays the selected Signaling Rule information window.
5. Click the **Response Headers** tab.
6. Click **Add In Header Control** or **Add Out Header Control**.

   The EMS server displays the corresponding Add Header Control pop-up window.
7. Select the appropriate information on the Add Header Control pop-up window and click **Finish**.

Result

The EMS server displays the selected Signaling Rule information window again.

Editing Response Header Parameters

About this task

Use the following procedure to edit existing Response Header parameters.

⚠ Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected signaling rule set.
4. Click the name of the signaling rule where you want to edit In Response Header or Out Response Header or both parameters from the applications pane.

   The EMS server displays the selected Signaling Rule information window.
5. Click the **Response Headers** tab.
6. Click the response header that you want to edit and click **Edit**.

   The EMS server displays the corresponding Edit Response Control pop-up window.

7. Edit the appropriate information in the Edit Response Control pop-up window and click **Finish**.

Result

The EMS server displays the selected Signaling Rule information window.

Editing signaling QoS parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
4. In the Application Pane, select the name of the signaling rule where you want to edit the QoS parameters.
5. Click the **Signaling QoS** tab in the content pane.

   The EMS server displays the Signaling QoS pop-up window.
6. Edit the appropriate fields and click **Finish**.

Result

The EMS server displays the signaling rules screen again.

Enabling the UCID parameter

Avaya SBC generates a UCID if you enable this option. You must activate this feature in a SIP trunking situation, when AACC is involved and the feature must apply to the signaling rule in the internal side of Avaya SBC.

About this task

Use the following procedure to enable the UCID parameter.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected signaling rule set.
4. Click the **UCID** tab.
5. Edit the appropriate fields and click **Finish**.

Result

The EMS server displays the selected Signaling Rule information window again.

Cloning an existing signaling rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. On the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters comprising the selected signaling rule set.
4. In the application pane, select the name of the signaling rule that you want to clone.
5. In the upper-right section of the content pane, click **Clone**.

   The EMS server displays the Clone Rule window.
6. In the **Clone Name** field, type a name for the new signaling rule, and click **Finish**.

Result

The EMS server displays the Signaling Rules page. The application pane shows the newly cloned signaling rule.

Renaming an existing signaling rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing Signaling Rule sets, and the content pane displays the parameters of the selected signaling rule set.
4. In the application pane, select the name of the signaling rule that you want to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Rule window.
6. In the Rename Rule window, type a new name for the signaling rule, and click **Finish**.

Result

The EMS server displays the signaling rules screen. The application pane displays the renamed signaling rule.

Deleting an existing signaling rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.

   The application pane displays the existing signaling rule sets, and the content pane displays the parameters of the selected signaling rule set.
4. In the application pane, select the name of the signaling rule that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the signaling rule.

Result

The application pane no longer displays the deleted signaling rule.

Charging rules

With Charging rules feature, you can define the charging rules for calls from customers to an Avaya Aura® Contact Center agent. For a specific URI, Avaya SBC displays a charging indication to an Avaya Aura® Contact Center agent for a specific business process. The indication is for the point at which the call must be terminated.

Avaya Experience Portal sends the URI patterns in the Refer-To header to Avaya SBC. If the URI pattern of the Refer-To header matches with the URI patterns administered and defined by Avaya SBC, then Avaya SBC inserts a P-Charging-Vector for the charge during the call.

If the call goes back to Avaya Experience Portal for additional inputs for the call, then Avaya SBC removes the P-Charging-Vector for the call. When the call comes back to the Avaya Aura® Contact Center agent from Avaya Experience Portal, then Avaya SBC adds the existing P-Charging-Vector for that session again.

Related links

Creating a new charging rule on page 140
Editing an existing charging rule on page 141
Cloning an existing charging rule on page 142
Renaming a charging rule on page 142
Deleting a charging rule on page 143

Creating a new charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Charging Rules**.

   The application pane displays the existing charging rule sets, and the content pane displays the parameters of the selected charging rule set.

4. In the application pane, click **Add**.

   The EMS server displays the first charging rule window.

5. In the **Rule Name** field, type a name for the new charging rule, and click **Next**.

   The EMS server displays the second Charging Rule window.

6. Enter the appropriate values, and click **Finish**.

Result

The application pane displays the newly created charging rule, and the content pane displays the parameters when you select the new charging rule.

Related links

Charging rules on page 140
Charging Rules field descriptions on page 141

Charging Rules field descriptions

Name	Description
Rule Name	The name of the charging rule.
URI Group	The field from where you select a currently defined SIP URI Group to match with the SIP headers based on the **URI Source** field value.
URI Source	A list to select the header of the SIP message. The options are: • **Refer-to** • **P-Asserted-Id** • **From** • **To**
Media Mode	A list to select the Avaya Aura® Contact Center topology type. The options are: • **Shuffling** • **Direct Media**. • **Media Anchor**

Related links

Creating a new charging rule on page 140

Editing an existing charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Charging Rules**.

The application pane displays the existing charging rule sets, and the content pane displays the parameters of the selected charging rule set.

4. In the application pane, click the name of the charging rule set that you want to edit.
5. In the lower-center section of the content pane, click **Edit**.

   The EMS server displays the Editing Rule window.
6. Edit the required fields, and click **Finish**.

Related links

Charging rules on page 140

Cloning an existing charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Charging Rules**.

   The application pane displays the existing charging rule sets, and the content pane displays the parameters comprising the selected charging rule set.
4. In the application pane, select the name of the charging rule that you want to clone.
5. In the content pane, click **Clone**.
6. In the Clone Rule window, type a name for the new charging rule, and click **Finish**.

Result

The Application pane displays the newly cloned charging rule.

Related links

Charging rules on page 140

Renaming a charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Charging Rules**.

   The application pane displays the existing charging rule sets, and the content pane displays the parameters of the selected charging rule set.
4. In the application pane, select the name of the charging rule that you want to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Rule window.

6. In the Rename Rule window, type a new name for the charging rule, and click **Finish**.

Result

The Application pane displays the renamed charging rule.

Related links

Charging rules on page 140

Deleting a charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Charging Rules**.

   The application pane displays the existing charging rule sets, and the content pane displays the parameters of the selected Charging Rule set.
4. In the Application pane, select the name of the charging rule that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the charging rule.

   The application pane no longer displays the deleted charging rule.

Related links

Charging rules on page 140

Endpoint policy groups

With the Endpoint Policy Group feature, you can create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies or rule sets, such as application, border, media, security, signaling, and ToD. A Policy Group is comprised of one or more Policy Sets. Policy Sets and Policy Groups aggregate and simplify the application of Avaya SBC security features to specific types of SIP signaling messages traversing through the enterprise.

As various types of signaling traffic pass through the enterprise, the Avaya SBC security product exhaustively inspects traffic. The Avaya SBC then compares the traffic with the criteria defined by the active Policy Group, as determined by the constituent ToD policy. The specific Policy Set that the packets are compared to is determined by the order in which the Policy Sets are placed in the parent Policy Group. Packets are usually placed in the Policy Group in the order beginning with most restrictive to least restrictive.

The packets are compared to each Policy Set in the Policy Group prioritized list from top to bottom beginning with the most restrictive down to the least restrictive. After finding a Policy Set match for a packet, Avaya SBC further qualifies the match by:

- the Time-of-Day (ToD) rule for the Policy Set
- the Policy Set or priority number

When Policy Sets have ToD rules that match, the Policy Set number is used for the final selection, and the higher priority number wins. The selected Policy Set is applied to the packet and an action is taken.

When a match is found, one of three possible actions is taken, depending upon the policies defined in the Policy Group:

- ALLOW: allows the packet to proceed to its destination without applying any security features.
- DENY: immediately blocks the packet.
- APPLY: applies the security features defined by the Policy Sets.

Note:

The user can add different Policy Sets with different ToD rules in the same Endpoint Policy Group.

Based on each ToD rule, a different security configuration can be applied to an incoming message.

Creating a new endpoint policy group

About this task

Use the following procedure to create a new policy group.

Caution:

Avaya provides default End point policy group set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The application pane displays the existing End Policy group sets, and the Content pane displays the parameters of the selected End point policy set.

   Note:

   At least one Security Rule set must be defined before a Policy Group can be created. If you do not create a security rule, Avaya SBC displays a prompt to create a rule.
4. In the application pane, click **Add**.

   The EMS server displays the first Group Name window.

5. In the **Group Name** field, type a name for the new policy group, and click **Next**.

   The EMS server displays the second Policy Group window where you must define the policy group parameters.

6. Enter the appropriate values, and click **Finish**.

Result

The Application pane displays the newly created policy group. When you click the policy group, the system displays the details in the Content pane.

End Point Policy Group field descriptions

Name	Description
Group Name	Specifies the name of the policy group.
Application Rule	Specifies the application rule that defines the type of SBC- based Unified Communications (UC) applications which Avaya SBC protects.
Border Rule	Specifies the border rule to control the NAT traversal settings.
Media Rule	Specifies the media rule that is used to match media packets.
Security Rule	Specifies the security rule that determines the Avaya SBC security policies that are applied when this policy group is activated.
Signaling Rule	Specifies the signaling rule that is used to match SIP signaling packets.
Charging Rule	Specifies the charging rule that is used to charge for the calls from customer to Avaya Aura® Contact Center agent. The default value for the **Charging** field is none.
RTCP Monitoring Report Generation	Specifies the method of generating RTCP monitoring report for a specific policy group. The options are : • Off: Does not generate the RTCP monitoring report.for the endpoint policy group. • RTP + RTCP: Generates the RTCP monitoring report based on the received RTCP packets on a SIP trunk. You must selet this method to have unique identifier at call level. • RTP only: In absence of RTCP, generates the RTCP monitoring report based on received RTP packets. For information about global configuration, see Configuring RTCP monitoring generation support on page 73

Viewing an existing policy group summary

About this task

Endpoint policy groups comprise a group of endpoint policy sets, all of which are specifically configured using a number of relevant parameters. These parameters can be viewed for any policy group in a single aggregate list that is displayed in a separate window. Use the following procedure to view a policy group summary.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The EMS server displays the existing End Point Policy Groups.

   Note:

   In the Content Area, clicking anywhere on a specific information line of a policy group displays configuration information for that policy group. The Media Rule page contains the **Media Encryption**, **Codec Prioritization**, and **Advanced** tabs.
4. On the Policy Group page, click **Summary**.

   The EMS server displays the Policy Group Summary page.
5. Use the scroll bar to view the entire report.
6. Click **Print** to print the report.

Editing an endpoint policy set

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The EMS server displays the existing End Point Policy Groups.
4. From the application pane, select the Policy Group with the policy sets you want to edit.

   The EMS server displays the policy sets currently assigned to the selected Policy Group.
5. In the content pane, click **Edit**.

   The EMS server displays the Edit Policy Set window.
6. Edit the required fields, and click **Finish**.

Edit an existing End Point Policy Group

Editing an End Point Policy Group comprises the following tasks:

- adding a Policy Set.
- reordering the precedence with which the constituent Policy Sets are executed within a Policy Group.
- editing an existing Policy Set.
- renaming or deleting an existing Policy Set.

Each of these procedures is described in the following sections.

Changing the order of endpoint policy sets within a policy group

About this task

Use the following procedure to reorder the precedence with which constituent policy sets are executed within a policy group. The policy set priority position is the deciding factor when ToD rules match on the applied policy set to an incoming message.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The application pane displays the existing End Point Policy groups. The content pane displays the endpoint policy sets of the selected End Point Policy Group.
4. In the application pane, select the policy group that requires change in the priority positions of the policy sets.
5. Change the number in the **Order** field to correspond to the order in which you want the policy sets to be executed.
6. Click **Update**.

Result

The content pane displays the reordered policy sets.

Deleting an existing endpoint policy set

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The EMS server displays the existing End Point Policy Groups.
4. In the application pane, select the Policy Group with the policy sets you want to delete.
5. Click the **Delete** option corresponding to the policy sets you want to delete.

   The EMS server displays a delete confirmation pop-up screen.
6. Click **OK** to delete the selected policy set.

Result

The EMS server displays the End Point Policy Groups screen again.

Deleting an existing end point policy group

About this task

Use the following procedure to delete an existing end point policy group.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The EMS server displays the existing End Point Policy Groups.
4. In the application pane, select the policy group that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays a delete confirmation message.
6. Click **OK** to continue with the deletion of the policy group.

Result

The application pane no longer displays the deleted end point policy group.

Session policies

With Session Policies, you can define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. These media-related parameters define a strict profile that is associated with other SIP-specific policies. These parameters determine how the Avaya SBC security product handles media packets matching these criteria.

Avaya SBC uses session policies for:

- Media anchoring
- Media forking
- Converged conferencing (not available in this release)
- SIPREC recording servers and profiles
- Media servers and routing profiles

You must use the session policy to configure these features and then configure the session policy in the session flows. Session flow selection depends on the packet parameters such as From and To URI, and source and destination subnets.

Related links

Creating a new session policy on page 149
Session Policy field descriptions on page 149
Editing an existing session policy on page 150
Cloning an existing session policy on page 151
Renaming an existing session policy on page 151
Deleting an existing session policy on page 152

Creating a new session policy

About this task

Use the following procedure to create a new session policy.

Caution:

Avaya provides a default Signaling Rule set named default. Do not edit this rule set because improper configuration might cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. In the applications pane, click **Add**.

   The EMS server displays the Session Policy window.
5. In the **Policy Name** field, enter a name that describes the purpose of the new policy. Click **Next**.

   The EMS server displays the second Session Policy window.
6. Administer the options as shown in Session Policy field descriptions on page 149 and click **Finish**.

   The application pane displays the session policy and the content pane displays the parameters when you select the session policy.

Session Policy field descriptions

Table 14: Media tab

Name	Description
Media Anchoring	Enables or disables media anchoring. The system enables the **Media Forking Profile**, **Converged Conferencing**, **Recording Server**, and **Media Server** options only when you select the **Media Anchoring** option.
Media Forking Profile	Select an administered media forking profile.
Converged Conferencing	Do not enable this option.
Recording Server	Enables or disables the recording server. The system enables the **Recording Profile** option if you select the **Recording Server** option.

Table continues…

Name	Description
Recording Profile	Select a recording profile that you have administered in Configuring one or more recording profiles and assigning the recording profile to a routing profile on page 602.
Media Server	Enables or disables the media server. The system enables the **Routing Profile** option if you select the **Media Server** option.
Routing Profile	Select a routing profile that you have administered in Routing profiles on page 257.
Optimize Hairpin Calls	Enables or disables optimization of SIPREC sessions on Hairpin calls. By default: • This field is disabled for new session policy. • This field is enabled for an existing session policy after Avaya SBC upgrade or migration.
Call Type for Media Unanchoring	Specifies the call type that is used for media unanchoring. The options are: • Media Tromboning Only: Releases media for hairpin calls only. • All: Releases media for all calls including hairpin and non-hairpin calls. **Important:** The features Media Unanchoring and Delayed SDP Handling cannot both be enabled for a call. For more information about administering these features, see Media unanchoring on page 152 and Server interworking on page 331.

Table 15: URN Profile tab

Name	Description
Enable URN Mapping	Enables or disables URN Mapping. The system enables the **URN Mapping Profile** option only when you select the **Enable URN Mapping** option.
URN Mapping Profile	Select an administered URN mapping profile. The profiles are administered in Configuring URN map based routing for NG911 calls on page 182.

Related links

Session policies on page 148

Editing an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. In the application pane, select the name of the session policy whose media forking parameters you want to edit.

   The content pane displays the session policies parameters for the selected session policy.
5. Click the **Media** tab and in the lower-center section of the content pane, click **Edit**.

   The EMS server displays the Media page.
6. Administer the options as shown in Session Policy field descriptions on page 149 and click **Finish**.

   The application pane displays the session policy and the content pane displays the parameters when you select the session policy.

Cloning an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. In the application pane, select the session policy that you want to clone.
5. In the content pane, click **Clone**.
6. In the Clone Policy window, type a name for the new session policy, and click **Finish**.

   The application pane displays the newly cloned session policy.

Renaming an existing session policy

About this task

Use the following procedure to rename an existing session policy.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.

4. In the application Pane, select the name of the session policy that you want to rename.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename Policy window.
6. In the **New Name** field, type a new name for the session policy, and click **Finish**.

   The application pane displays the renamed session policy.

Deleting an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. In the Application Pane, select the name of the session policy that you want to delete.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the session policy.

   The application pane no longer displays the deleted session policy.

Media unanchoring

To enhance bandwidth usage for endpoints within the same subnetwork and to allow direct media to flow between these endpoints, unanchor media for sessions. Use this feature to enhance bandwidth usage when you connect to a managed MPLS network or a cloud network.

Avaya SBC supports media unanchoring for all non-hairpin calls, including trunk to enterprise, enterprise to trunk, remote to enterprise, and enterprise to remote. Avaya SBC supports media unanchoring for audio, video, and multimedia calls.

Related links

Unanchoring media for existing session policies on page 153
Media unanchoring scenarios on page 153

Unanchoring media for existing session policies

About this task

Important:

The features Media Unanchoring and Delayed SDP Handling cannot both be enabled for a call. For more information about administering these features, see Media unanchoring on page 152 and Server interworking on page 331.

Before you begin

Configure a session policy profile, and then use the profile to create a session flow.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Session Policies**.
4. On the Session Policies page, in the Session Policies section, click an existing session policy and then click the **Media** tab.
5. Clear the **Media Anchoring** field.

   Note:

   - If you clear the media anchoring check box, media forking profile becomes unavailable. If you want to use the media forking feature, Avaya SBC cannot unanchor the media.
   - In a deployment, if a network has a remote Avaya SBC deployed before the core Avaya SBC deployment and a subnet user is behind a NAT device, you can unanchor media for the core Avaya SBC.
6. In the **Call Type for Media Unanchoring** field, click one of the following:
   - **Media Tromboning Only**: To release media for hairpin calls.
   - **All**: To release media for all calls including hairpin and non-hairpin calls.
7. Click **Finish**.

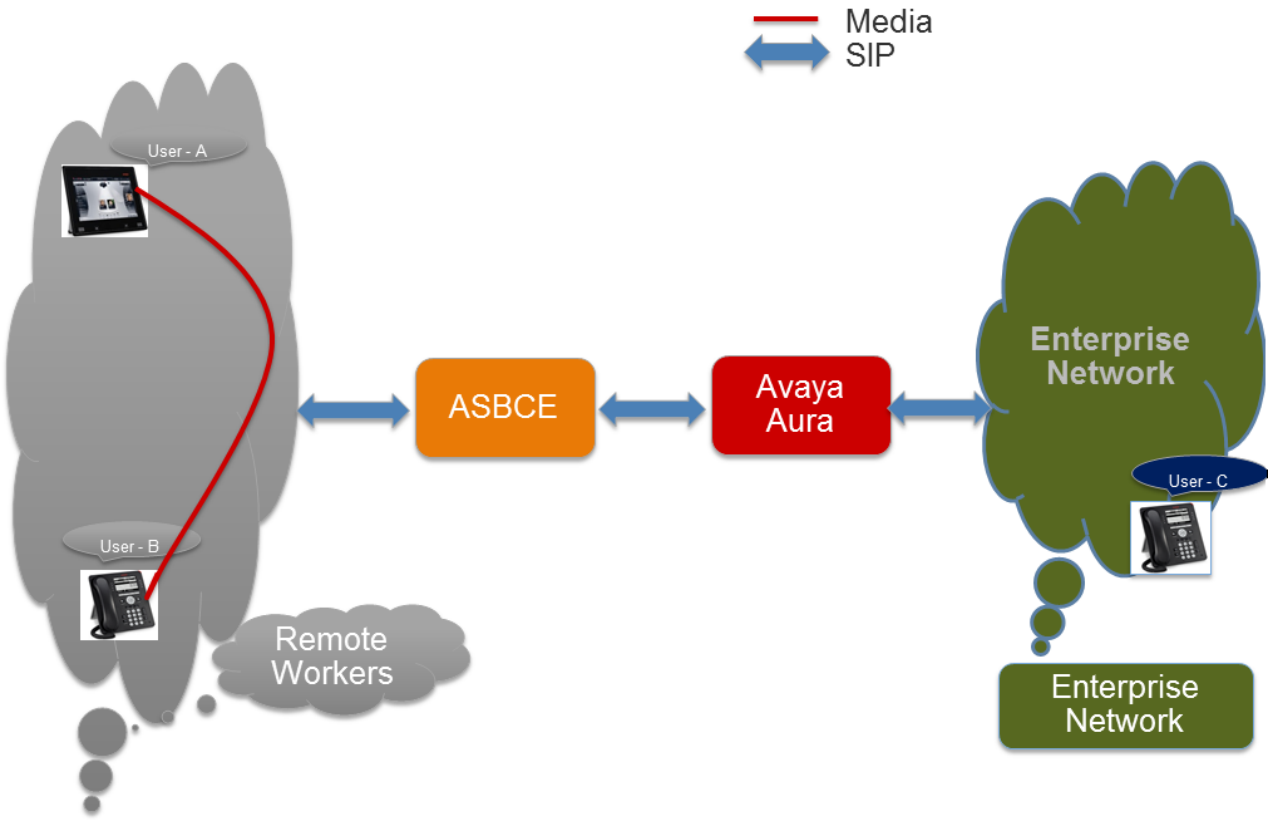
Media unanchoring scenarios

Avaya SBC can release media when:

- Both endpoints or ends of the call pass through the same Avaya SBC
- Both end points can negotiate with the same media format, SRTP or RTP

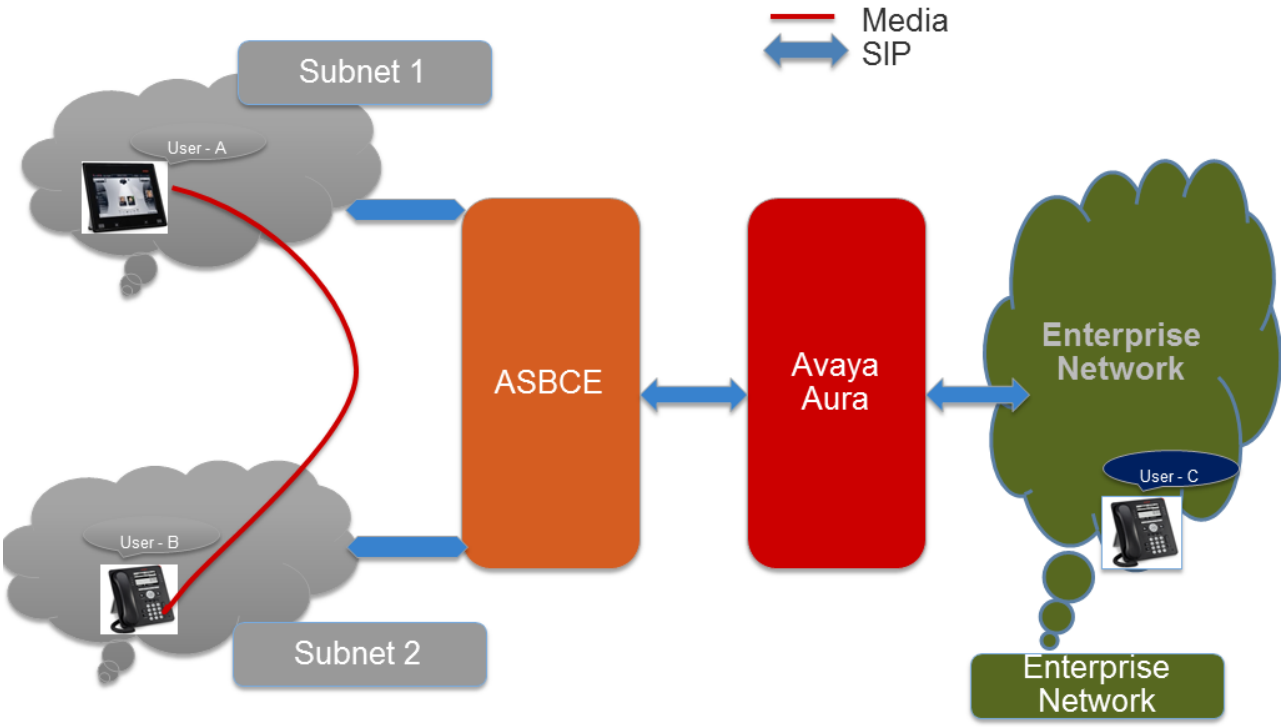
This section covers a few scenarios in which Media unanchoring can be used.

Remote workers in the same subnet



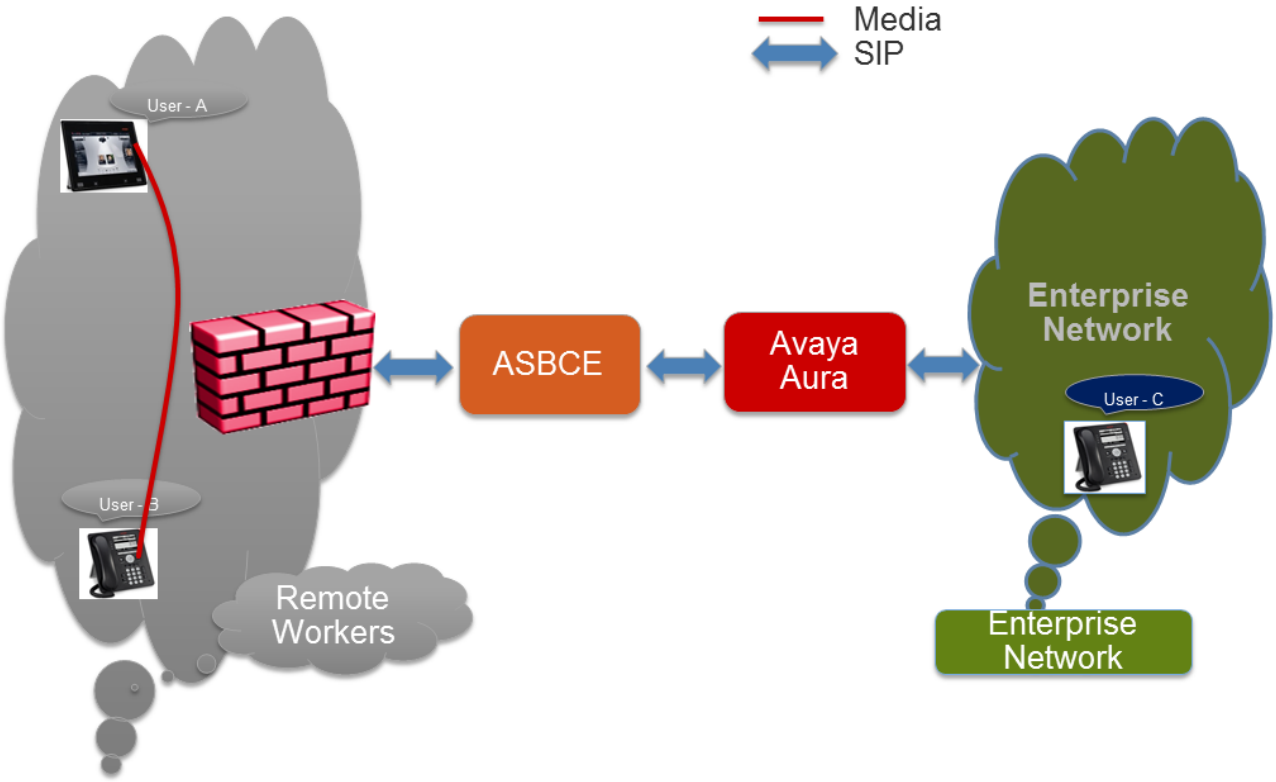
As the endpoints are in the same subnet, the Avaya SBC can be configured to flow the media directly between the endpoints.

Remote workers in two different subnets



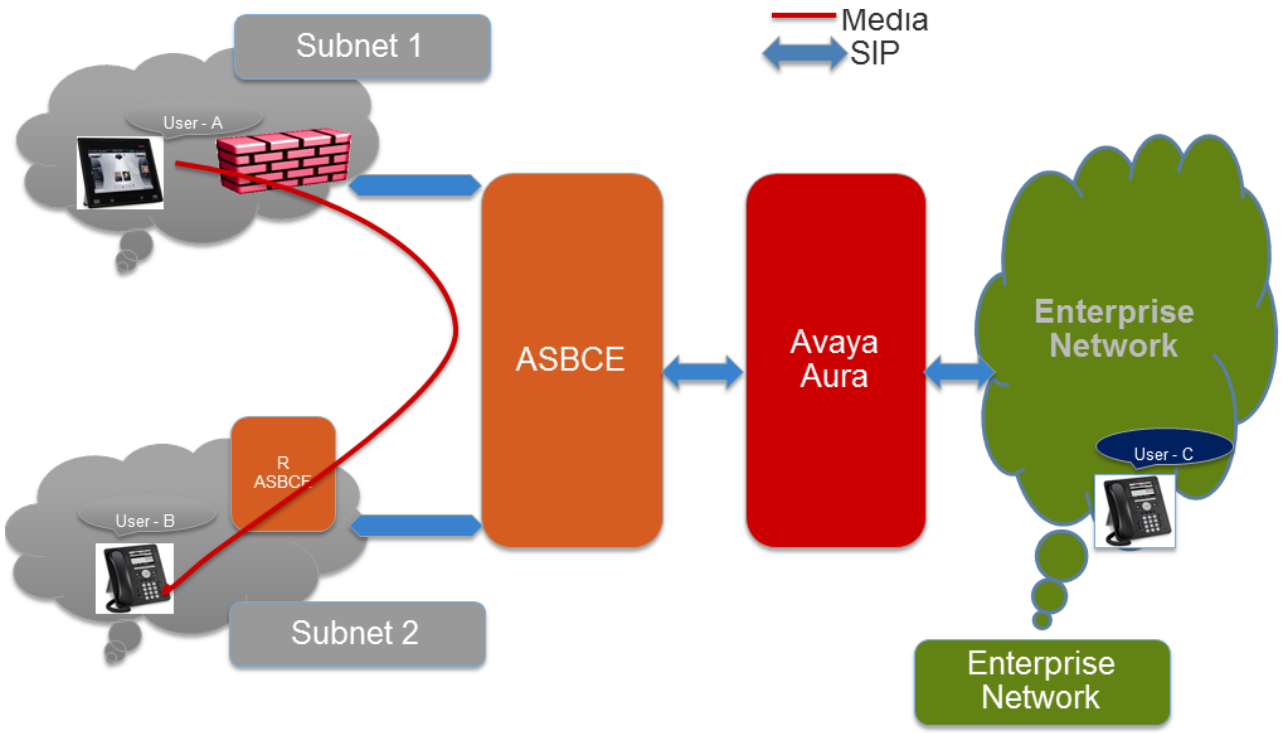
Avaya SBC can be configured to release the media between two different subnets. The subnets must be reachable to flow the media.

Remote workers behind the same NAT



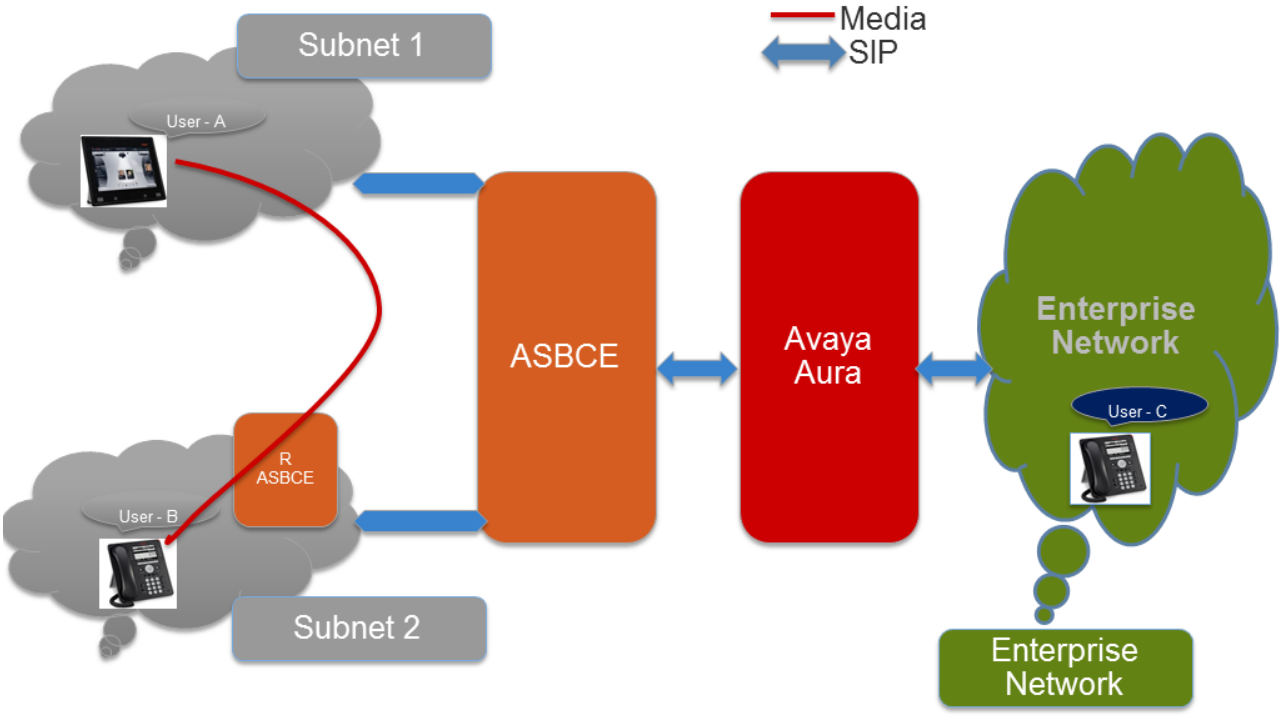
When Avaya SBC detects that both remote workers in the call are behind the same NAT device, Avaya SBC can enable media flow directly between the remote workers.

Remote branch office with Avaya SBC



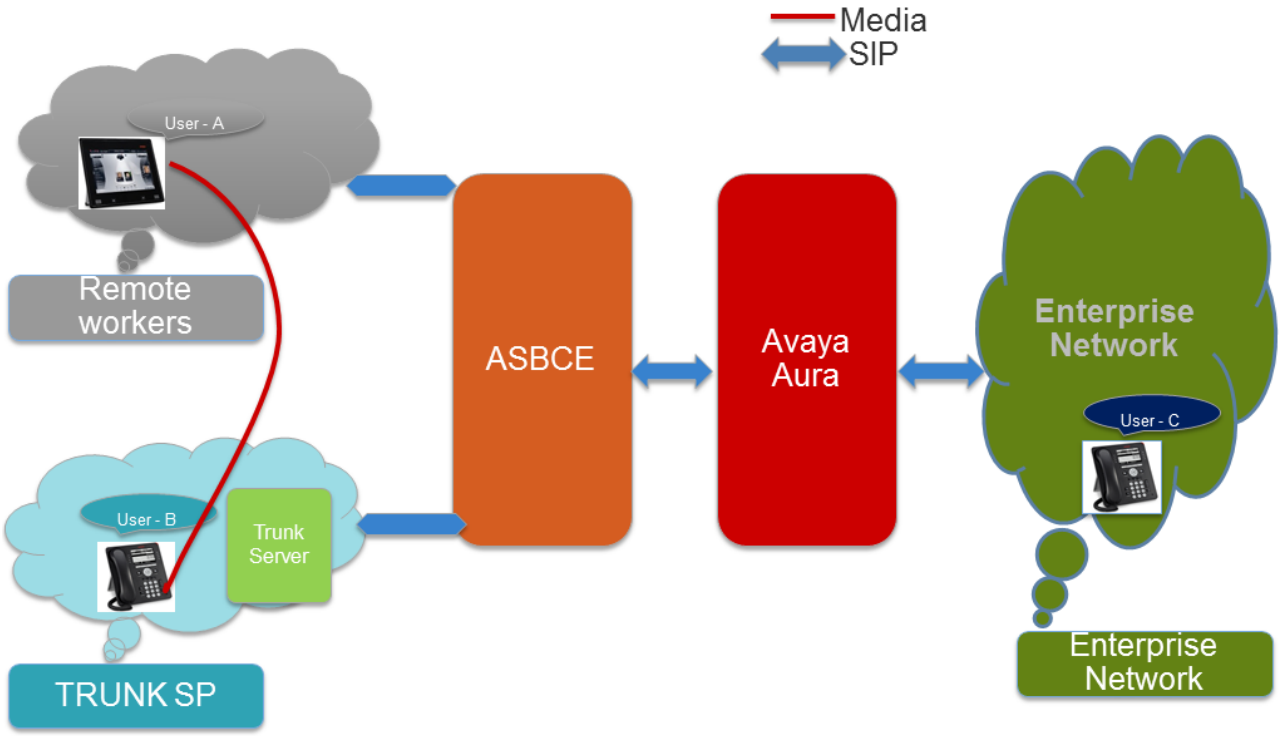
In this scenario, the endpoints belong to two different subnets. However, one of the endpoints is behind a NAT device, and the other subnet has remote Avaya SBC. The Core Avaya SBC can be configured to release the calls between these subnets by using the remote Avaya SBC. To release the media from core Avaya SBC, enable the **has remote sbc** flag during Session Flow configuration.

Remote branch office with Avaya SBC



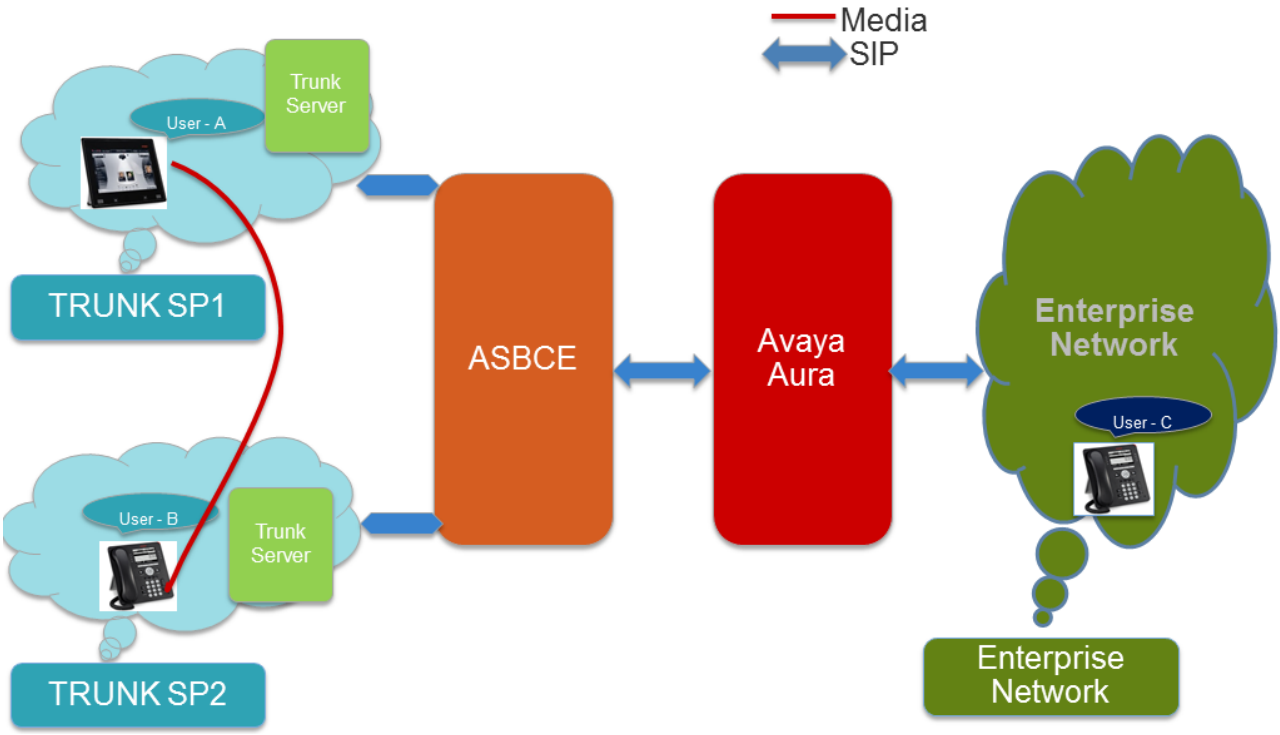
In this scenario, the endpoints belong to two different subnets, and one of the subnets has remote Avaya SBC. The Core Avaya SBC can be configured to release the calls between these subnets.

Calls between remote workers and Trunk users with same Avaya SBC



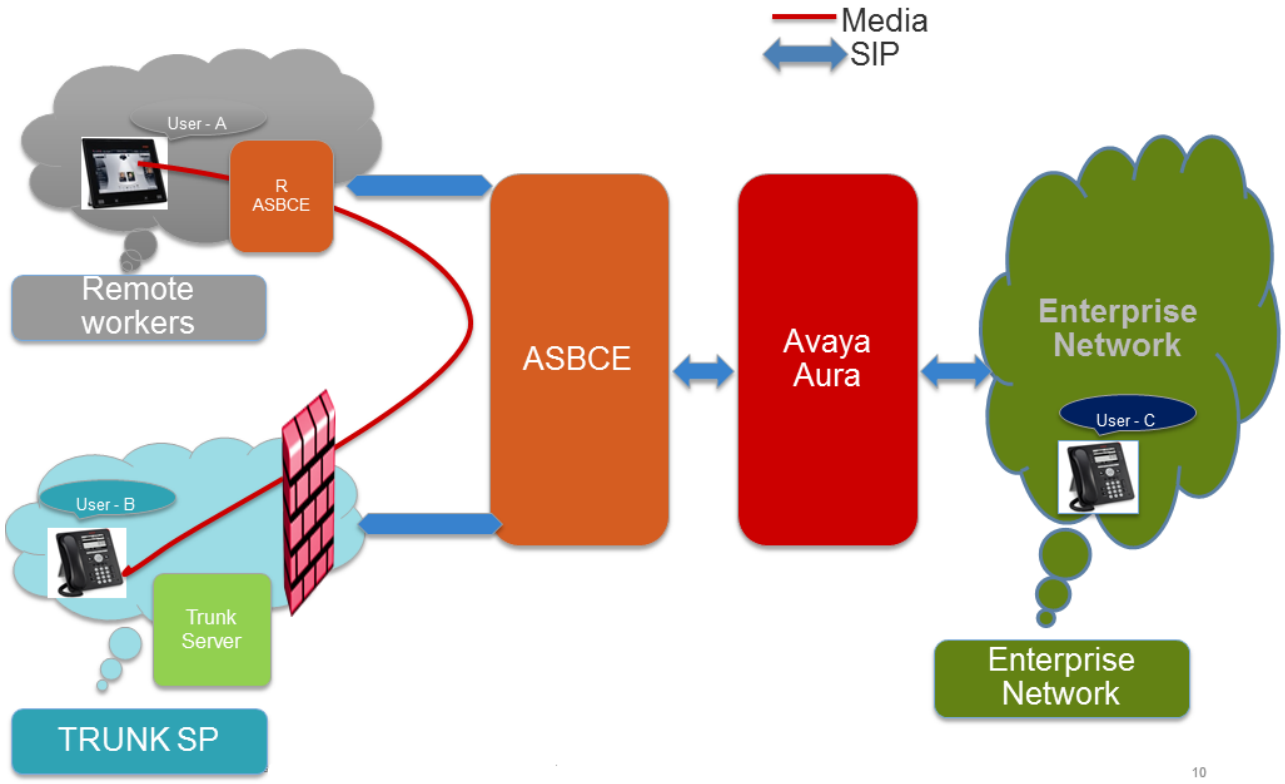
In this scenario, a call is established between remote worker from one subnet to the trunk subnet user. As these endpoints pass through the same Avaya SBC, the Avaya SBC device can be configured to release media between these endpoints. Both subnets must be reachable.

Calls between two trunks with the same Avaya SBC



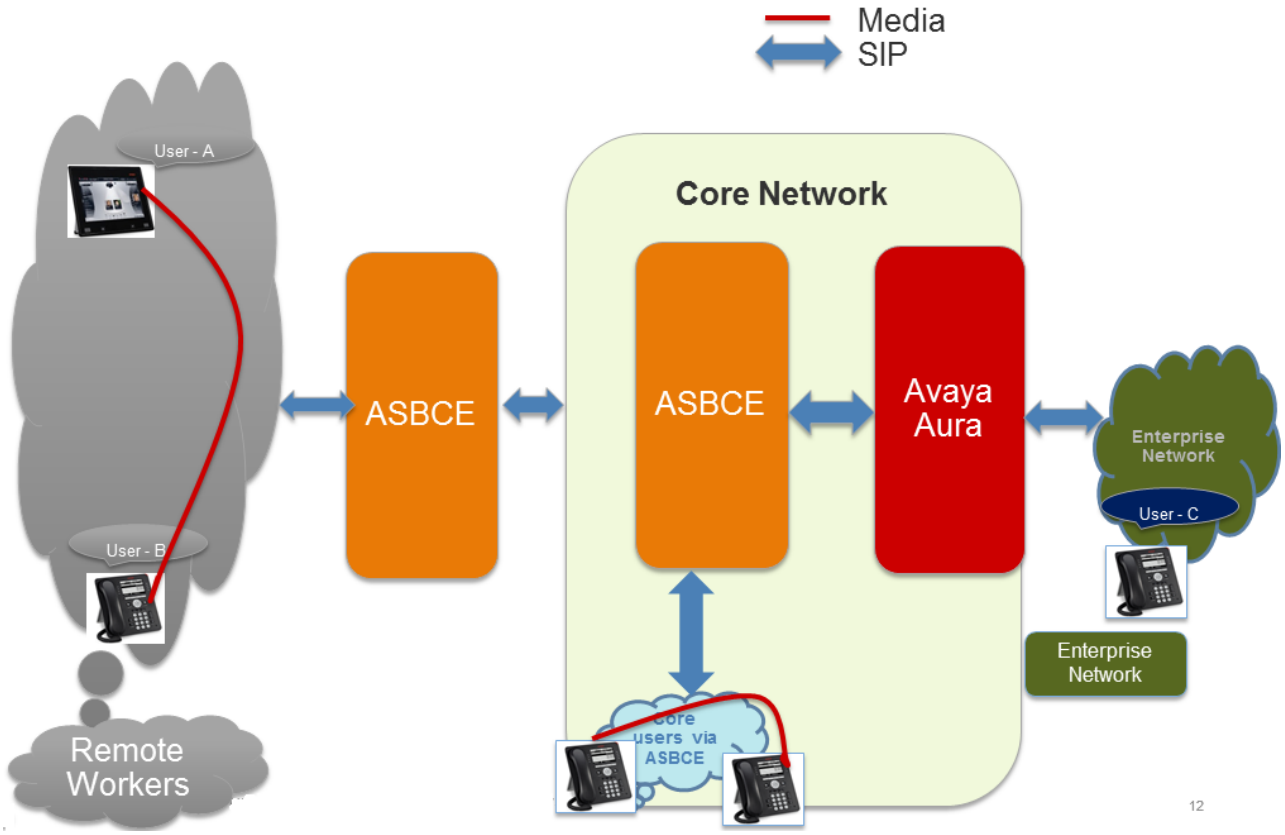
In this scenario, a call is established between two different trunk subnet users. As the endpoints pass through the same Avaya SBC, the Avaya SBC device can be configured to release media between these endpoints. Both subnets must be reachable.

Trunk behind firewall and Remote branch office with Avaya SBC



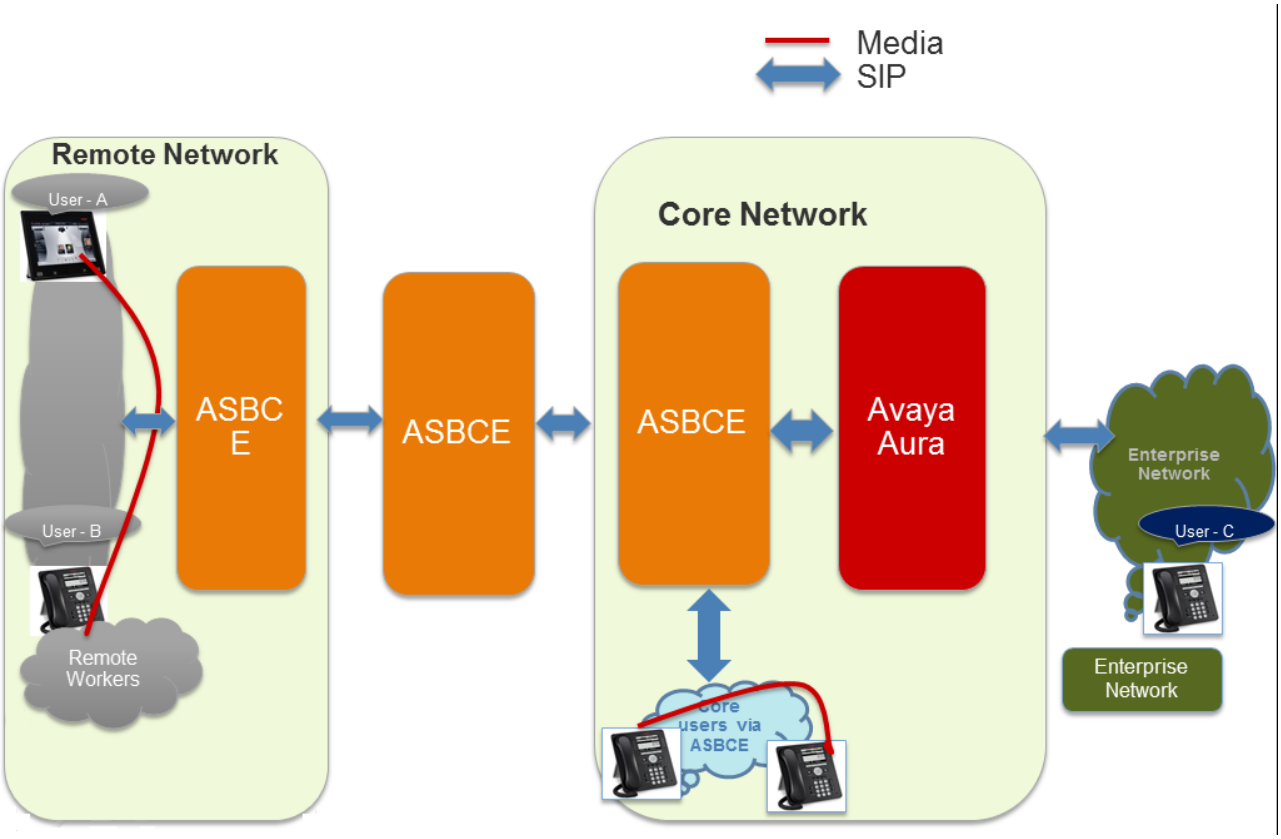
In this scenario, one subnet belongs to the trunk connected to Avaya SBC, and the other subnet has a remote worker connected to Avaya SBC with remote Avaya SBC. The core Avaya SBC can be configured to release calls between these subnets, by using the remote Avaya SBC. To release the media from core Avaya SBC, enable the **has remote sbc** flag during Session Flow configuration.

Back-to-back Avaya SBC deployment



In this scenario, core and DMZ Avaya SBC devices can be configured to release the media between the endpoints. For more information, see the section for back-to-back Avaya SBC deployment.

Back-to-back-to-back Avaya SBC deployment



In this scenario Remote, DMZ, and core Avaya SBC devices can be configured to release the media between the endpoints. For more information, see the section for back-to-back-to-back Avaya SBC deployment.

Related links

Media unanchoring on page 152

About administering end-point flows and session flows

With the End Point Flows and Session Flows features, you can define certain parameters that pertain to the signaling and media portions of a call. The call can originate from within the enterprise or outside the enterprise. The features provide complete and unparalleled flexibility to monitor, identify, and control very specific types of calls based upon the user defined parameters. End Point Flows are combined with Session Flows to completely identify and characterize a call placed through the network. End Point Flows profile SIP signaling parameter, and Session Flows profile SDP media parameters. Any number of End Point and Session Flows can be defined.

Two methods can be used to create a new End Point or Session Flow. The first method uses the Add Flow function of the Flows feature. You manually define a signaling or media flow by configuring all the necessary parameters on a number of sequential display screens or pop-up

windows. The second method is called Cloning. You can copy an existing flow and only change those parameters which would make the endpoint or session flow distinct.

Endpoint flow

Subscriber flow

Creating a subscriber flow

About this task

Subscriber flows refer to the actual endpoint devices, from which SIP messages originate and to which they are destined. Endpoint devices include hard phones, soft phone clients, and wireless handsets.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   In the content area, the EMS server displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBC security devices.
4. Click the **Subscriber Flows** tab.
5. Click **Add**.

   The EMS server displays the Add Flow window.
6. Enter the requested information in the appropriate fields, and click **Finish** to save and exit.

   From the Add Flow screen, you can click **Back** to view the fields on the previous Add Flow screen.

Add Subscriber Flow field descriptions

Name	Description
Criteria	
Flow Name	A field in which you can enter a name for the Subscriber Flow profile.
URI Group	A drop-down list from which you select a currently defined SIP URI Group policy to identify the source of an originating call.
User Agent	A drop-down list containing all valid SIP devices that can legitimately originate a call.
Source Subnet	The subnet address from which calls originate.
Via Host	The domain name or subnet of the SIP proxy servers through which the SIP signaling messages are routed.
Contact Host	The domain name or subnet of the endpoint from where the SIP message originates.

Table continues…

Name	Description
Signaling Interface	The Signaling Interface profile to be used by the SIP proxy servers.
Profile	
Source	A radio button to select the SIP signaling source: Subscriber or Click-to-Call client.
Methods Allowed before REGISTER	A scroll window to select the SIP signaling messages that precede the REGISTER message.
Media Interface	A drop-down menu from which you can select the Media Interface profile to be used for RTP media traffic.
Secondary Media Interface	A drop-down menu from which you select the secondary Media interface to be used for this Server End Point Flow. If a public IP address has not been defined, the IP address will used as the Public IP. This field is available only if the Endpoint Policy Group has a media rule with ANAT enabled. The media interface in the **Secondary Media Interface** field cannot be the same as the **Media Interface** field, and must have a different class of IP. For example, if the public IP of the Media Interface is an IPv4 address, the public IP of the Secondary Media Interface must be an IPv6 address.
End Point Policy Group	A drop-down menu from which you can select the End-Point Policy Group to be used for this Subscriber End-Point Flow.
Routing Profile	A drop-down menu from which you can select the Routing Profile to be used for this End-Point Flow.
Optional Settings	
TLS Client Profile	A drop-down menu from which you can select the TLS Client Profile to be used for this Subscriber End-Point Flow.
Signaling Manipulation Script	A drop-down menu from which you can select the Signaling Manipulation Script to be used for this Subscribe End-Point Flow.
Presence Server Address	The address of the presence server.
IP / URI Blocklist Profile	A drop-down menu from which you can select the blocklist Profile to be used for this Subscriber End-Point Flow.
Trusted Address	The IP address from trusted servers. Request from these IP addresses are always allowed.

Editing an existing subscriber flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

Separate tabs display the parameters comprising subscriber endpoint flows and server endpoint flows.

4. Click the **Subscriber Flows** tab.

   The content area displays existing endpoint flows.

5. Locate the flow that you want to edit, and click **Edit**.

   The EMS server displays the Edit Flow screen.

6. Edit the existing fields.

   The Edit Flow screen for has two pages. You must complete the fields on the first page and click **Next** to edit fields on the second page.

7. Click **Finish**.

Cloning an existing subscriber flow

About this task

You can add endpoint flows by cloning existing subscriber flows and editing the required parameters to create new flow policies.

Note:

An endpoint flow cannot be cloned from one Avaya SBC security device and applied to another Avaya SBC security device. A clone can only be assigned to the same Avaya SBC security device from which the original flow came.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   Separate tabs display the parameters comprising the server end-point flows and subscriber end-point flows.

4. Click the **Subscriber Flows** tab.

   The content area displays the existing Subscriber endpoint flows.

5. Locate the Subscriber endpoint flow that you want to clone, and click **Clone**.

   The EMS server displays the Clone Flow screen.

6. In the **Flow Name** field, type a name for the Subscriber Flow.
7. Edit any other parameters, if necessary, and click **Finish**.

Result

The EMS server displays the End Point Flows screen, showing the newly cloned Subscriber Flow.

Reordering the precedence of subscriber flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Click the **Subscriber Flows** tab.

   The Content Area displays the existing endpoint flows for the selected device.
5. In the **Priority** field, type a number corresponding to the order or precedence in which you want the flow to be executed.
6. Click **Update**.

   The Content Area displays the endpoint flows in the new order of precedence.

Deleting an existing subscriber flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Select the **Subscriber Flows** tab.
5. Locate the flow that you want to delete, and click **Delete**.

   The EMS server displays a delete confirmation window.
6. Select **OK** to continue deleting the flow.

   Alternatively, click **Cancel** to cancel the delete operation without saving.

Server flow

Creating a server flow

About this task

Server flows refer to the IP call servers that connect to SIP trunk services.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   In the content area, the EMS server displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBC security devices.
4. Click the **Server Flows** tab.

5. Click **Add**.

   The EMS server displays the Add Flow window.

6. Enter the requested information in the appropriate fields, and click **Finish**.

   From the Add Flow screen, you can click **Back** to view the fields on the previous Add Flow screen.

Add Server Flow field descriptions

Name	Description
Criteria	
Flow Name	The name assigned to this Subscriber End Point Flow.
SIP Server Profile	A drop-down menu from which you can select the Server Configuration Hiding Profile to be used for this Server End Point Flow.
URI Group	The domain of the call server or domain of the SIP trunk from which a call will originate, depending upon the direction of traffic flow.
Transport	The transport protocol type supported by the SIP server. Available selections are TCP, UDP, and TLS.
Remote Subnet	The subnet of the remote server or phones.
Received Interface	A drop-down menu from which you select the Received Interface to be used for this Server End Point Flow.
Signaling Interface	A drop-down menu from which you select the Signaling Interface to be used for this Server End Point Flow.
Media Interface	A drop-down menu from which you select the Media interface to be used for this Server End Point Flow. Select the internal or external media interface depending upon the direction of the flow of traffic. You cannot change the class of the selected IP's public IP address if the Media Interface is associated with a Server Flow with ANAT enabled.
Secondary Media Interface	A drop-down menu from which you select the secondary Media interface to be used for this Server End Point Flow. If a public IP address has not been defined, the IP address will used as the Public IP. This field is available only if the Endpoint Policy Group has a media rule with ANAT enabled. The media interface in the **Secondary Media Interface** field cannot be the same as the **Media Interface** field, and must have a different class of IP. For example, if the public IP of the Media Interface is an IPv4 address, the public IP of the Secondary Media Interface must be an IPv6 address.
End Point Policy Group	A drop-down menu from which you select the End-Point Policy Group to be used for this Server End-Point Flow.
Routing Profile	A drop-down menu from which you select the Routing Profile to be used for this End-Point Flow.

Table continues…

Name	Description
Topology Hiding Profile	A drop-down menu from which you select the Topology Hiding Profile to be used for this Server End Point Flow.
Signaling Manipulation Script	A drop-down menu from which you select the Signaling Manipulation Script to be used for this Server End Point Flow. Specify a signaling manipulation script in this field when you want to use a signaling manipulation script different from the script used during server configuration. **Note:** If you select different scripts in the server configuration and the server flow, the system uses the signaling manipulation script selected in the server flow. However, if you apply the manipulation as INBOUND and AFTER_NETWORK, the system uses the script selected in the server configuration.
Remote Branch Office	A drop-down menu from which you select the Remote Branch Office to be used for this Server End Point Flow. **Note:** If the server configuration for the end point flow is for a Remote Branch Office, the system sets the **Remote Branch Office** field to **Any**.
Link Monitoring from Peer	When **Link Monitoring from Peer** check box is selected, Avaya SBC sends 200 OK response for a match of the SIP OPTIONS request with a server flow. When **Link Monitoring from Peer** check box is cleared, Avaya SBC relays OPTIONS request to the destination server.
FQDN Support	When **FQDN Support** check box is selected, Avaya SBC adds the FQDN in headers. When **FQDN Support** check box is cleared, Avaya SBC adds the IP address in headers. By default, the **FQDN support** check box is cleared.
FQDN	The FQDN value. The **FQDN** field is available only when the **FQDN support** check box is selected.
Tenant Configuration Profile	A drop-down menu from which you select the tenant configuration profile to be used for this Server End Point Flow. The default value is **None**.
ELIN Gateway	The check box to enable ELIN Gateway. For more information, see Emergency call routing for Direct Routing users on page 170.
Callback Timeout	The timeout value after which the mapping between ELIN and the MS Teams user who dials the 911 emergency number is cleared and callback is not supported. You can enter a value from **10** to **40** minutes. The default value is **20** minutes.

Emergency call routing for Direct Routing users

To deploy Emergency call routing for direct routing users, Avaya SBC can be configured either as an ELIN gateway or not depending on the emergency calling network within a given country or region.

When Avaya SBC is used as an ELIN gateway, it is configured the same way as above with a few additional steps outlined below. When an emergency call arrives with ELIN number, Avaya SBC:

- Emergency routing service provider should be configured as trunk server in Avaya SBC.
- Avaya SBC should be configured to route Emergency URIs to Emergency routing service provider.

When Avaya SBC is used as an ELIN gateway, it is configured the same way as above. When an emergency call arrives with ELIN number, Avaya SBC:

- Parses ELIN phone number.
- Maps the emergency caller's number with the ELIN phone number.
- Stores ELIN number Mappings in an internal table.
- Substitutes the emergency caller's number with the ELIN phone number.
- Routes the call to the service provider configured on Avaya SBC.

Upon a call back to the emergency number, Avaya SBC will do the reverse called number substitution to that of the original emergency caller.

This mapping is kept in the internal table for a period of "Callback Timeout" in minutes and removed after. This helps to route the call back to original emergency caller in case call drops.

Configuring ELIN Gateway

About this task

You must configure ELIN Gateway for each MS Teams customer.

Before you begin

Ensure that you enable the ELIN feature.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   In the content area, the EMS server displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBC security devices.
4. Click the **Server Flows** tab.
5. Select the server flow whose SIP server profile is the MS Teams server and click **Edit**.
6. Select the **ELIN Gateway** check box.

7. In the **Callback Timeout** field, select a value from **10** to **40** minutes.

   The default value is **20** minutes.

   Callback timeout determines how long ELIN to Caller number mapping should be kept after the call is disconnected.

8. Click **Finish**.

Editing an existing server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   Separate tabs display the parameters comprising subscriber endpoint flows and server endpoint flows.

4. Click the **Server Flows** tab.

   The content area displays existing endpoint flows.

5. Locate the flow that you want to edit, and click **Edit**.

   The EMS server displays the Edit Flow screen.

6. Edit the existing fields.
7. Click **Finish**.

Cloning an existing server flow

About this task

You can add endpoint flows by cloning existing server flows and editing the required parameters to create new flow policies.

Note:

An endpoint flow cannot be cloned from one Avaya SBC security device and applied to another Avaya SBC security device. A clone can only be assigned to the same Avaya SBC security device from which the original flow came.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   Separate tabs display the parameters comprising subscriber endpoint flows and Server endpoint flows.

4. Click the **Server Flows** tab.

   The content area displays the existing Server endpoint flows.

5. Locate the Server endpoint flow that you want to clone, and click **Clone**.

   The EMS server displays the Clone Flow screen.
6. In the **Flow Name** field, type a name for the new server flow.
7. Edit any other parameters, if necessary, and select **Finish**.

Result

The End Point Flows screen shows the newly cloned Server Flow.

Reordering the precedence of server flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Click the **Server Flows** tab.

   The Content Area displays the existing endpoint flows for the selected device.
5. In the **Priority** field, type a number corresponding to the order or precedence in which you want the flow to be executed.
6. Click **Update**.

   The Content Area displays the endpoint flows in the new order of precedence.

Deleting an existing server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Select the **Server Flows** tab.
5. Locate the flow that you want to delete, and click **Delete**.

   The EMS server displays a delete confirmation window.
6. Select **OK** to continue deleting the flow.

   Alternatively, click **Cancel** to cancel the delete operation without saving.

Filtering server flows

About this task

Use this procedure to search for the required server flows.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. On the **Device** menu, click the Avaya SBC instance.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Click the **Server Flows** tab.

   The EMS server displays a list of server flows for the selected Avaya SBC instance.
5. Click **Filter**.
6. Click **Add Criteria**.
7. Select one of the following criteria from the drop-down list:
   - **Flow Name**
   - **Server Configuration**
   - **URI Group**
   - **Transport**
   - **Remote Subnet**
   - **Received Interface**
   - **Signaling Interface**
   - **Media Interface**
   - **Secondary Media Interface**
   - **End Point Policy Group**
   - **Routing Profile**
   - **Topology Hiding Profile**
   - **Signaling Manipulation Script**
   - **Remote Office Branch**
   - **Link Monitoring from Peer**
   - **FQDN Support**
   - **FQDN**
   - **Tenant Configuration Profile**

   Some fields provide a text box to enter the required value, while others do not.
8. Select one of the following options and enter the required value in the text box:
   - **Contains**
   - **Starts with**
   - **Ends with**
   - **Exact Match**
9. To add more filter criteria, repeat Steps 6 to 8.

10. To remove a filter criteria, click **Remove**.
11. Click **Filter**.

    The EMS server displays the results based on the ANDing of the criteria.

Session flow

Creating a new session flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Session Flows**.

   The content area displays currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flow screen.
5. Administer the options as described in Session flow field descriptions on page 174 and click **Finish**.

   The Content Area displays the new session flow.

Session flow field descriptions

Name	Description
Criteria	
Flow Name	The name of the session flow.
URI Group # 1	A SIP URI Group policy to identify the source or destination of a call.
URI Group # 2	A SIP URI Group policy to identify the source or destination of a call.
Subnet # 1	A subnet address from which calls originate or terminate.
Subnet # 2	A subnet address from which calls originate or terminate.
SBC IP address	The network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBC. Configure to media IP interface to unanchor the media received at media IP interface.
Session Policy	The Session Policy profile to be used for this session flow.
Has Remote SBC	Select if a remote Avaya SBC system is deployed before core Avaya SBC deployment and any of the subnet users are behind a NAT device. In this deployment core, Avaya SBC unanchors the media.

Editing session flows

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Session Flows**.

   The content area displays a specifically ordered list of session flows for the selected Avaya SBC security device.
4. Locate the Session flow that you want to edit and click **Edit**.

   The EMS server displays the Edit Flow screen.
5. Administer the options as described in Session flow field descriptions on page 174 and click **Finish**.

   The Content Area displays the edited session flow.

Cloning an existing session flow

About this task

You can add session flows to the Avaya SBC security repertoire by cloning existing session flows and editing the desired parameters to create new flow policies.

Note:

A Session Flow cannot be cloned from one Avaya SBC security device and applied to another Avaya SBC security device. A clone can only be assigned to the same Avaya SBC security device from which the original flow came.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The Content Area displays a specifically ordered list of Session Flows for the selected Avaya SBC security device.
4. Locate the session flow that you want to clone, and click **Clone**.

   The EMS server displays the Clone Flow screen.
5. In the **Flow Name** field, type the name of the new file.
6. Edit any other fields that you want to change and click **Finish**.

Result

The Content Area displays the cloned session flow.

Reordering the precedence of session flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

The content area displays the session flows currently defined for that Avaya SBC device.

4. In the **Priority** field, type a number corresponding to the order or precedence in which you want the flow to be executed.
5. Click **Update**.

Result

The Content Area displays the session flows in the new order of precedence.

Deleting an existing session flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The content area displays a specifically ordered list of session flows for the selected Avaya SBC security device.
4. Locate the session flow that you want to delete, and click **Delete**.

   The EMS server displays a confirmation screen is displayed to confirm whether you want to proceed with deletion.
5. Click **OK**.

Result

The EMS server no longer displays the deleted session flow.

Single Sign-On and Identity Engine

Avaya SBC uses split DNS for the Single Sign-On and Identity Engine feature. In a split DNS infrastructure, internal hosts are directed to an internal domain name server for name resolution. Internal hosts resolve the IDE domain to an IDE server address. External hosts are directed to an external domain name server for name resolution. External hosts resolve the IDE domain to an Avaya SBC external address.

Configuring Single Sign-On and an Identity Engine server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **Relay**.

   The EMS server displays the Relay Services page.

4. In the **Reverse Proxy** tab, click **Add**.
5. Administer the options as described in Reverse Proxy Profile field descriptions on page 177.
6. Click **Finish**.

   The content pane displays the newly created reverse proxy profile.

Reverse Proxy Profile field descriptions

Name	Description
Service Name	Enter a name for the reverse proxy profile.
Enabled	Select this check box to enable the profile.
Listen IP	Select the IP address of an external Avaya SBC system.
Listen Port	Enter the port number that remote workers use for SSO service. For HTTPS, the default value is 443. For HTTP, the default value is 80.
Listen Protocol	Select the protocol that remote workers use for the SSO service.
Listen TLS Profile	Select a TLS profile that has been configured. **Listen TLS Profile** field is accessible if you select HTTPS in **Listen Protocol** field.
Listen Domain (optional)	Enter the domain name which remote workers use for SSO service.
Connect IP	Select the IP address that Avaya SBC uses for communicating with the IDE server.
Server Protocol	Select the protocol for the IDE server. **Security alert:** For security reasons, you must use HTTPS.
Server TLS Profile	Select a server profile that has been configured.
Rewrite URL	Select the check box to enable **URL Replace** for the profile.
Load Balancing Algorithm	Select a load balancing algorithm for the reverse proxy profile.
PPM Mapping Profile	Select a PPM mapping profile that has been configured.
Reverse Proxy Policy Profile	Select the number of requests permitted per second.
Whitelisted IPs	Enter the IP addresses for which traffic is allowed.

Uniform Resource Identifier groups

With the Uniform Resource Identifier (URI) group setting, you can create any number of logical URI groups consisting of each SIP subscriber located in the particular domain or group. Various domain policies use the groups to determine if the allow, block, or apply policy actions are taken for a specified call flow.

URI groups can be used to create new subscriber flows and server flows. You can use a new server flow by giving addresses and providing different number patterns in a URI group.

Creating a new URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **URI Groups**.
4. In the application pane, click **Add**.

   The EMS server displays the Add URI window.
5. Enter the appropriate values and click **Finish**.

   The content pane displays the new URI group.

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 153
Add URI Group field descriptions on page 179

Adding an additional URI to an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **URI Groups**.

   The application pane displays the existing URI groups. The content pane displays the URIs that comprise the URI group.
4. In the application pane, click the URI group to which you want to add a URI.

   The **URI Group** tab on the content pane displays a list of SIP URIs assigned to the selected **URI Group**.
5. In the content pane, click **Add**.

   The EMS server displays the Add URI window.
6. Add the required URIs. and click **Finish**.

Result

The content pane displays the new URI added to the group.

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 153
Add URI Group field descriptions on page 179

Add URI Group field descriptions

When creating a new URI group, see the following table for information about the fields in the second Add URI Group screen:

Name	Description
URI	The name of the URI group.
Scheme	The URI scheme. The options are: • **sip/sips:** For Session Initiation Protocol or Secure Session Initiation Protocol. • **tel:** For a telephone.
Type	URI type of the URI group. The options are: • **Plain** Common SIP URI in the format: - *@192.168.15.12 - *@avaya.com You cannot select the **Plain** URI type when the **tel:** scheme is selected. • **Dial Plan** Valid SIP Dial Plan in the format: - 9555XXXX@.* - 011*@.* - 9555NXXX@avaya.com • **Regular Expression** REGEX in the format: - [0-9]{3,5}\.user@domain\.com - (simple|advanced)\-user[A-Z]{3}@.*
URIs	URIs entered by using the format selected in the **URI Type** field.

Related links

Configuring Route header based routing for NG911 calls on page 184

Emergency group

The Emergency URI group is an integral part of the system that is user defined. You create the Emergency group to define special numbers that must not be restricted by any dial-out restrictions imposed by Domain Policies. Avaya SBC administrators must put all applicable emergency numbers for the country for special handling in the group.

Note:

The **SIP Options** tab on the Advanced Options screen defines the management of numbers contained in the Emergency URI group. See Managing SIP options on page 225.

Related links

Unanchoring media for existing session policies

Managing SIP options on page 225

Editing a URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **URI Groups**.

   The application pane displays the existing URI groups. The content pane displays the URIs that comprise the URI group.
4. In the application pane, click the URI group that you want to edit.

   The content pane displays a list of SIP URIs assigned to the selected URI group.
5. In the content pane, click **Edit** for the URI that you want to edit.

   The EMS server displays the Edit URI window.
6. Make the required changes to the URI and click **Finish**.

Result

When you select the edited URI, the content pane displays the new parameters.

Deleting a SIP URI from an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **URI Groups**.

   The application displays the existing USI groups. The content pane displays URIs that comprise the URI group.
4. In the application pane, click the URI group from which you want to delete a SIP URI.

   In the content pane, the **URI Group** tab displays a list of SIP URIs currently assigned to the selected URI group.
5. In the content pane, click the **Delete** option that corresponds to the URI that you want to delete.

   The EMS server displays a delete confirmation screen.

6. Select **OK** to perform the delete operation, or select **Cancel** to stop the delete operation.

Result

The EMS server displays the **URI Groups** screen again. If **OK** was selected, the SIP URI is removed from the list of URIs comprising the selected URI group.

Renaming a URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **URI Groups**.

   The application pane displays the existing URI groups, and the content pane displays the URIs that comprise the URI group.
4. In the application pane, click the URI Group that you want to rename.
5. In the content pane, click **Rename**.

   The EMS server displays the Rename Group window.
6. In the **New Name** field, enter a new name for the existing URI Group and click **Finish**.

Result

The URI Groups page displays the renamed URI Group.

Deleting a URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **URI Groups**.

   The application pane displays the existing URI groups, and the content pane displays the URIs that comprise the URI group.
4. In the application pane, click the URI Group that you want to delete.
5. In the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.

   Note:

   The server displays the message only when the selected URI Group is associated with a security policy or a call flow

   If the selected URI Group is associated with a security policy or a call flow, the EMS server displays an information window instead of the delete confirmation window. The information window displays a message:

```
You can't delete URI_1 because it's used with a flow. To
delete, first remove any associations.
```

For more information about managing URIs and the associated session flows, see Managing end-point and session flows.

6. To delete the selected URI Group, click **OK**.

Result

The application pane does not show the name of the deleted URI group .

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 153

About administering end-point flows and session flows on page 163

Configuring URN map based routing for NG911 calls

About this task

The support required for Next Generation 911 (NG911) is different than Enterprise 911. Avaya SBC supports the mapping of a Uniform Resource Name (URN) to one or more dialed strings that connects users to an emergency Public-Safety Answering Point (PSAP). The mapping must be done on a location-by-location basis. Also, multimedia for voice and video is passed through the SBC server. A third-party vendor splits the multimedia stream in the PSAP. URN mapping is administered on an SBC server at the edge of an NG911 PSAP.

To administer URN mapping, you must create a new unique URN profile and then enable that profile in a new unique session policy.

With Avaya SBC Release 8.1.0, the URN mapping for NG911 calls feature supports the following functions:

- URN mapping support for all NG911 calls coming into an NG911 PSAP using Avaya SBC.
- Hold and unhold for all of the supported calls.
- Secure Real-Time Transport Protocol (SRTP) and Real-Time Transport Protocol (RTP) media interworking.
- Multimedia support for audio and video.
- Support for other calls to the Public Switched Telephone Network (PSTN) using Avaya SBC without going through an NG911 CS and without the support of the URN mapping.

With Avaya SBC Release 8.1.2, the URN mapping for NG911 calls feature is enhanced to support the following functions:

- Subscription (SUBSCRIBE) and notification (NOTIFY) of states and events between Avaya SBC at the NG911 Public-Safety Answering Point (PSAP) and Emergency Services Routing Proxy (ESRP) at the NG911 Core Services (CS) per Bell Canada NG911 specifications.
- Support for adhoc conferencing.

- Support for a call transfer.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **URN Profile**.
4. Click **Add**.

   The system displays the URN Profile window.
5. Enter a name for the URN profile in the **Policy Name** field.
6. Click **Next**.

   The system displays the URN Mapping window.
7. Enter a appropriate value for the **URN Map**.

   The following are some examples of URN map formats:

   urn:nena:service:sos.fire

   urn:nena:service:sos.police

   urn:nena:service:sos.ambulance

   urn:nena:service:responder.police

   urn:nena:service:responder.fire

   urn:nena:service:responder.ambulance

   urn:service:counseling
8. Enter the digits to be dialed in the **Dial Digit** field. These are the actual digits that are dialed when the system software runs the URN Map.
9. **(Optional)** Click **Add** to create additional URN maps within the same URN profile.
10. Click **Finish**.

    The system displays the list of administered URN profiles.
11. Repeat these steps to create additional URN profiles.

    Note:

    Use **Edit** to change existing profiles, use **Rename** to change the profile name, and use **Delete** to delete the profile.
12. Navigate to **Domain Policies** > **Session Policies**.

    The system displays the administered session policies.
13. Click **Add** to create a new unique session policy to associate with the URN mapping profile. For the complete procedures to administer session policies, refer Session policies on page 148.

14. Select the **URN Profile** tab for the emergency session policy.
15. Click **Edit**.

    The system displays the URN Mapping window.
16. Enable the **Enable URN Mapping** option.
17. Select a profile from the **URN Mapping Profile** drop-down list.
18. Click **Finish**.

Next steps

After you create URN mapping policies and session policies, you must review and administer the following options:

- Attach the session policy created for URN mapping with a session flow. For more information, refer About administering end-point flows and session flows on page 163 and Creating a new session flow on page 174.
- For Adhoc Conferencing support, you must enable the **NG911 Support** option as described in About SIP server configuration profile management on page 317.
- Disable the Refer Handling feature for the Server Interworking profile that is used for any NG911 CS trunk server. This is required for Call Transfer and Adhoc Conferencing support.
- Enable the **NATing for 301/302 Redirection** option in the Server Interworking profile that is applied to the PSAP server. The default setting is **Yes**. This is required in Adhoc conferencing.

Configuring Route header based routing for NG911 calls

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The system displays the administered session policies.
4. To disable the URN mapping, clear the **Enable URN Mapping** checkbox.
5. Navigate to **Configuration Profiles** > **URI Groups**.
6. In the application pane, click **Add**.

   The EMS server displays the Add URI window.
7. Enter the appropriate values for **Scheme** and **Type** fields.
8. In the **URIs** field, enter a appropriate value for the URN Map.
9. Click **Finish**.
10. In the navigation pane, click **Configuration Profiles** > **Routing**.

The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.

11. In the application pane, click **Add**.
12. Type a distinctive name for the new routing profile, and click **Next**.
13. Enter the requested information into the appropriate fields.

    To use alternate routing, ensure that you set the **Trans Expire** field on the **Timers** tab from **Configuration Profiles** > **Server Interworking** to an appropriate short duration. Any request sent from the server times out if a response is not received within the time set as the transaction expiration timer. Therefore, alternate routing does not work if the **Trans Expire** field is set to the default value of 32 seconds.
14. Click **Finish**.

    The application pane displays the new routing profile.

Note:

If Avaya SBC uses user part based routing for PSAP, resulting in multiple backend PSAP servers then a SigMa script is required by replacing the domain (for example, psap.com) with Avaya SBC IP address.

Related links

Add URI Group field descriptions on page 179
Routing profile field descriptions on page 186

Add URI Group field descriptions

When creating a new URI group, see the following table for information about the fields in the second Add URI Group screen:

Name	Description
URI	The name of the URI group.
Scheme	The URI scheme. The options are: • **sip/sips:** For Session Initiation Protocol or Secure Session Initiation Protocol. • **tel:** For a telephone.

Table continues…

Name	Description
Type	URI type of the URI group. The options are: • **Plain** Common SIP URI in the format: - *@192.168.15.12 - *@avaya.com You cannot select the **Plain** URI type when the **tel:** scheme is selected. • **Dial Plan** Valid SIP Dial Plan in the format: - 9555XXXX@.* - 011*@.* - 9555NXXX@avaya.com • **Regular Expression** REGEX in the format: - [0-9]{3,5}\.user@domain\.com - (simple|advanced)\-user[A-Z]{3}@.*
URIs	URIs entered by using the format selected in the **URI Type** field.

Related links

Configuring Route header based routing for NG911 calls on page 184

Routing profile field descriptions

Name	Description
Rule Name	Specifies the descriptive name of the routing profile
URI Group	Specifies the URI Group to which the next hop routing profile applies. The options are: • * • Emergency
Time of Day	Specifies the time of day for the trunk server to resolve the routing profile. **Note:** For remote users, do not use the **Time of Day** profile to resolve the routing profile.

Table continues…

Name	Description
Load Balancing	Specifies the type of load balancing option. The options are: • **Priority** • **Round-Robin** • **Weighted Round-Robin** • **DNS/SRV**
NAPTR	Activates or deactivates Naming Authority Pointer. When you select the Load Balancing algorithm as DNS SRV, the EMS server enables the NAPTR check box. If you disable NAPTR, you must specify the transport protocol.
Transport	Assigns the transport type for each next hop address. Select the protocol for transporting outgoing signaling packets. The options are: • **None** • **TCP** • **TLS** • **UDP** In this case, **Common Transport Type** field is unavailable. You can select the transport type according to the next hop address.
LDAP Routing	Enables LDAP based call routing.
LDAP Server Profile	Displays a collection of existing LDAP server profiles. Use this field to define the LDAP server profile for a routing profile and sends the LDAP search requests to the LDAP server. This field is available only when you select the **LDAP Routing** check box.
LDAP Base DN (Search)	Displays the configured LDAP Base DN to search the users using the LDAP server. This field is available only when you select the **LDAP Routing** check box. You must specify only one Base DN to search the user using the LDAP server.
Matched Attribute Priority	Specifies if the matched attributes based on **LDAP Base DN (Search)** will get priority. This field is available only when you select the **LDAP Routing** check box.

Table continues…

Name	Description
Alternate Routing	Enables the alternate routing for using the next routing entry if Avaya SBC fails to route messages using resolved routing entry. This field is available only when you select the **LDAP Routing** check box.
Next Hop Priority	Specifies if the Next Hop Priority option is enabled. If Avaya SBC fails to route the message using resolved routing entry from message, that is using request URI or Route Header then the system will send the message to the alternate routing entry from the routing profile.
Next Hop In-Dialog	Specifies the Next Hop configuration for the In-Dialog message. If you enable the **Next Hop In-Dialog** option, then the In-Dialog request tries to use the same routing entry to route the message. **Note:** Avaya does not recommend **Next Hop In-Dialog** option for remote worker configuration.
Ignore Router Header	Enables Avaya SBC to ignore the Route Header.
ENUM	Enables support for the E.164 Number Mapping (ENUM) protocol.
ENUM Suffix	Specifies the ENUM suffix that is added to change the number to a domain name. This field is available only when you select the ENUM check box.
Server Name Indication (SNI)	Enables support for Branch Survivability to route messages from Branch Session Manager to Session Manager.
Server name	Specifies the server name used to route messages from Branch Session Manager to Session Manager. This field is available only when you select the **Server Name Indication (SNI)** check box.
Add	Adds a next hop address.
Priority / Weight	Specifies the priority and weight assigned for load balancing options.
LDAP Search Attribute	The search attribute present in the LDAP search request. This field is available only when you select the **LDAP Routing** check box.

Table continues…

Name	Description
LDAP Search Regex Pattern	Specifies the regex pattern that is used to get the phone number from the request URI of INVITE message. This field is available only when you select the **LDAP Routing** check box.
LDAP Search Regex Result	Specifies the regex result after getting the phone number from the request URI of INVITE message. This field is available only when you select the **LDAP Routing** check box.
SIP Server Profile	Specifies the server configuration.
Next Hop Address	Specifies the IP address or domain of the Next Hop server. You can add up to 20 next hop addresses.
Transport	Assigns the transport type for each next hop address. Select the protocol for transporting outgoing signaling packets. The options are: • **None** • **TCP** • **TLS** • **UDP** In this case, **Common Transport Type** field is unavailable. You can select the transport type according to the next hop address.

Related links

Configuring Route header based routing for NG911 calls on page 184

Configuring access to IP Office features over MTCTI messaging

About this task

IP Office uses a Multi-Tenancy Computer Telephony Integration (MTCTI) interface to provide support for specific telephony features. For example, Avaya Workplace Client uses MTCTI to provide features such as hunt groups.

Avaya SBC supports the MTCTI interface. It relays MTCTI messages from clients of a specific tenant to an IP Office instance for the tenant through a Reverse Proxy in a Network Address Translation (NAT) environment. Avaya SBC applies NAT on these messages and relays the payload without modification. Distribution of MTCTI messages is done using a host-header in HTTP messages and server name indication (SNI) information in a certificate. That is, Avaya SBC

has different SNI and host header for a specific tenant and uses it to route these messages for that tenant.

Procedure

1. Configure multiple SIP IP Office servers use for multi-tenancy as described in Adding a new SIP server profile on page 318.
2. Configure a reverse proxy relay service using XMPP to the IP Office systems for each tenant as described in Creating reverse proxy service for multi-tenant or IP Office powered deployments on page 502.
3. Configure an SNI group for each IP Office system as described in About configuring SNI groups on page 376 and Creating a new SNI group on page 377.
4. Configure multi-tenant TLS server profiles with an SNI group as described in Creating a TLS server profile on page 368. Note that the server profile must have another certificate to be used along with the certificates already administered in the SNI group.
5. Configure multi-tenant TLS client profiles with an SNI group as described in Creating a TLS client profile on page 372. The TLS client profiles must have certificates for each tenant.
6. Configure a network signaling interface to use the tenant profiles as described in Adding a new signaling interface on page 272.
7. Configure a subscriber flow with URI groups for SIP routing as described in Creating a subscriber flow on page 516 and Creating a new URI group on page 178.

Chapter 6: System Configuration

Basic system configuration overview

With the Avaya SBC EMS web interface, you can configure and manage the following system-related security features of the Avaya SBC security products deployed in an enterprise VoIP network:

- Back up/Restore system information.
- Manage Avaya SBC security devices.
  - Provision installed Avaya SBC security devices.
  - Establish secure shell sessions.
  - Shutdown and reboot individual Avaya SBC devices.
  - Restart Avaya SBC applications.
  - View, edit, and delete Avaya SBC device configurations.
- Manage configuration profile, services, and monitoring information:
  - Authenticate RADIUS settings.
  - Manage SNMP settings.
  - Manage routing profiles.
  - Manage trace settings.
  - Manage syslog settings.
  - Authorize user agents.
- Manage networks and their flows.
  - Manage signaling interface.
  - Manage media interface.
- Configure advanced options.
  - Manage subsystem logs.
  - Manage CDR listing.
  - Manage Feature Control.
  - Configure SIP options.

- Configure signaling port ranges.

This section provides an overview of the overall basic configuration process, including the following:

- Avaya SBC architecture
- Basic configuration quick-start steps checklists
  - Reconfigure Avaya SBC.
  - Enable interfaces.
  - Configure URI groups.
  - Configure routing profiles.
  - Configure interworking.
  - Add servers.
  - Add TLS certificates.
  - Add TLS server profiles.
  - Add domain policy groups.
  - Add signal interfaces.
  - Add media interfaces.
  - Add subscriber flows.
  - Add server flows.
  - Add session flows.

This section only provides a brief basic configuration checklist. For detailed procedures regarding each topic in this overview section, see the appropriate sections in the following chapters:

- Domain policy administration
- System configuration
- Security configuration
- Network configuration

Basic configuration checklist

Task	Description
Enable Interfaces	See Enabling interfaces on page 193.
Configure URI Groups	See Creating a new URI group on page 178.
Configure Routing Profiles	See Creating a new routing profile on page 259.

Table continues…

Task	Description
Interworking Profiles	See Adding a new Server Interworking Profile on page 331.
Add Servers (Call/Trunk)	See Creating an Avaya call server profile (advanced services only) on page 489 and Adding a new SIP Server profile on page 318.
TLS Certificates	See Creating a Certificate Signing Request on page 356 and Installing certificates on page 358.
TLS Profiles	See Creating a new TLS server profile on page 368.
Domain Policy Group	See Creating a new policy group on page 144.
Signaling Interface	See Adding a new signaling interface on page 272.
Media Interface	See Adding a new Media Interface on page 274.
Subscriber Flow	See Creating a new subscriber end-point flow on page 164.
Server Flow	See Creating a new server endpoint flow on page 167.
Session Flow	See Creating a new session flow on page 174 and Creating a new session policy on page 149.

Enabling interfaces

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.
4. Click the **Interfaces** tab and enable the required interfaces.

Backup and restore

About backing up and restoring your system

The backup and restore features provide the ability to create and restore snapshots of the EMS and configured SBC devices. Backup information is stored in a user-defined location, on the local EMS server or a configured remote server. The location must be secure and physically separate from the SBC equipment chassis to ensure later retrieval or restoration.

When you perform a backup on the EMS, the following components are backed up:

- Primary EMS configuration data
- Secondary EMS configuration data, if deployed

- Configuration data for all deployed SBC devices
- Certificates installed in the deployment

When you perform a backup on an SBC device, the following components are backed up:

- Configuration data of that SBC device
- Certificates installed in the deployment

Note:

- You can do a system backup anytime and it does not require a maintenance window. However, try to schedule backups during a no-traffic or low-traffic time of day.
- For EMS, you can take a configuration backup manually and restore it as needed. You can also configure automatic snapshots for EMS.
- For SBC devices, you can only take a backup manually. You can back up and restore the functional SBC devices.
- To download the snapshot, you can use the download link provided in the **Snapshot** tab.

Backup frequency recommendations

Data backups are important to ensure your administrative data is safe and secure and can be restored for a system software or hardware failure. Use the following recommendations to schedule regular backups or take regular snapshots on your systems:

- Take a full system snapshot every 30 days.
- Take snapshots after making critical configuration changes.
- Take a snapshot of your system before doing any deployment configuration changes or software upgrade.

Designating a snapshot server

About this task

Configuration data snapshots contain information such as certificates and keys, which can be misused to gain unauthorized access to Avaya SBC.

You can restore a snapshot to the same Avaya SBC product version on an EMS of the same hardware group. When restoring the snapshot, it is recommended that the EMS server is configured with the same management IP used when the snapshot was created. If the EMS server hardware group or the Avaya SBC product version does not match, the restore operation will fail, and the system settings will revert to the earlier state.

Before you begin

Ensure the following:

- The selected storage directory on the designated remote server is accessible only to authorized users.
- The snapshot server uses SFTP.

- The storage directory does not have read, write, or execute permissions for unauthorized users.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Backup/Restore**.

   The EMS server displays the Backup/Restore page.
4. Click the **Snapshot Servers** tab.

   The EMS server displays the snapshot server profiles in the content area.
5. On the Snapshot Servers page, click **Add**.

   The EMS server displays the Add Snapshot Servers page.
6. Add the requested information in the fields, and click **Finish**.

Next steps

Creating system snapshots on page 196

Related links

Snapshot Server field descriptions on page 195

Snapshot Server field descriptions

Name	Description
Profile Name	A descriptive name for the designated snapshot server.
Server Address (ip:port)	The IP address and port number of the snapshot server to transfer the configuration data or snapshots using secure FTP.
User Name	The user name of the administrative account that is authorized to back up the Avaya SBC configuration data.
Authentication Type	The option to enable the SSH authentication. The options are: • **Password** • **Use ipcs SSH key** If you select **Use ipcs SSH key**, the **Password** and **Confirm Password** fields are unavailable.
Password	The password to authenticate the administrative account.
Confirm Password	The field to enter the password again for confirmation.

Table continues…

Name	Description
Repository Location	The path of the directory on the snapshot server where the configuration backup snapshots are stored.
Host Key	The key that is used to authenticate the login of the host.

Related links

Designating a snapshot server on page 194

Creating system snapshots

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, preform one of the following:
   - Click **EMS** to create a system snapshot for the EMS server.
   - Click **SBC** to create a system snapshot for a specific SBC.
3. Navigate to **Backup/Restore**.
4. Click the **Snapshots** tab.
5. Select the designated snapshot server.
6. Click **Create Snapshot**.

   The system displays the Create Snapshot window.
7. Enter a description for the snapshot, and click **Create**.

   The server creates a snapshot of the EMS security configuration and sends it to all the configured snapshot servers. A banner on the Create Snapshot pop-up window informs you that the snapshot has been successfully created. When the process is complete, the snapshots screen displays the newly created snapshot.

Configuring automatic snapshots

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Backup/Restore**.
4. On the Backup/Restore page, click the **Automatic Snapshot Configuration** tab.

   The EMS server displays the Automatic Snapshot Configuration page. The **Summary** section displays the configuration of a previously saved backup. Otherwise, the default setting of **Never** is displayed.

5. In the **Configuration** section, select one of the following:
   - **Never**
   - **Daily**
   - **Weekly**: The EMS server displays a group of check boxes to choose the day. For example, Su, Mo, Tu, We, Th, Fr, and Sa.
   - **Monthly**: The EMS server displays a group of check boxes to choose the day. For example, Su, Mo, Tu, We, Th, Fr, and Sa. It also displays another row of check boxes for occurrence. For example, 1st, 2nd, 3rd, 4th, and Last.
6. In the **Time** field, select the time.

   The EMS server displays a Select Time window.
7. Click **Save**.

Related links

Backup and restore field descriptions on page 197

Backup and restore field descriptions

Snapshots tab

Name	Description
Date	The date and time at which the EMS server captured the snapshot.
Build	The build number of the snapshot.
Description	The description of the snapshot.

Configurable Snapshot

Name	Description
Hide incompatible snapshots	Hides snapshots that are of a different version.
Upload Snapshot File	Uploads a snapshot file. You can upload a snapshot file that you downloaded earlier. The snapshot file must follow the naming convention `SnapshotName_Date_Time_SBCEVersion.bak`. For example, new_03-20-2019_15-32-25_8.x.x.x-12-13295.bak. Avaya SBC does not accept the snapshot file if the filename does not follow this convention.
Create Configurable Snapshot	Creates a snapshot that you can configure. You can choose the device for which the system must create a snapshot, and then add a name for the snapshot.

Snapshot Servers tab

Name	Description
Profile Name	A descriptive name for the designated snapshot server.
Server Address (ip:host)	The IP address and port number of the snapshot server to transfer the configuration data or snapshots using secure FTP.
User Name	The user name of the administrative account that is authorized to back up the Avaya SBC configuration data.
Authentication Type	The type of authentication. The options are: • **Password** • **Use ipcs SSH key** If you select **Use ipcs SSH key**, the Password and confirm password fields are unavailable.
Password	The password to access the snapshot server.
Confirm Password	The password reentered for confirmation.
Repository Location	The path of the directory on the snapshot server where the configuration backup snapshots are stored.
Host Key	The key that is used to authenticate the login of the host.

Automatic Snapshot Configuration tab

Name	Description
Next Scheduled Backup	Information about the next scheduled backup. **Note:** The summary section of the **Automatic Snapshot Configuration** tab displays information about previously saved backups.
Last Backup	The date on which the last backup was done.
Status	The status of the backup.
Frequency	The frequency of the automatic backup. The options are: • **Never** • **Daily** • **Weekly** • **Monthly**
Time	The time at which the backup starts. The EMS server displays this field only when the **Frequency** field is set to Daily, Monthly, or Weekly.

Table continues…

Name	Description
Day(s)	The days of the week on which the system begins automatic backup. The EMS server displays this field only when the **Frequency** field is set to Monthly or Weekly.
Occurrence	The week of the month on which the system begins automatic backup. The EMS server displays this field only when the **Frequency** field is set to Monthly.

Security Configuration

Name	Description
Encryption type	The encryption type used for the snapshot. The options are: • **Static Key Only**: A static key in the application is used for encryption. This option provides the bare minimum security, therefore, Avaya recommends that you use the Passphrase Only or Static Key + Passphrase options. • **Static Key + Passphrase**: The static key and passphrase provided are used for encryption. • **Passphrase Only**: The passphrase provided is used for encryption.
Encryption Passphrase	The passphrase used for encryption.

Related links

Configuring automatic snapshots on page 196

About restoring a system snapshot

Caution:

Restoring from a snapshot will irreversibly overwrite all existing data. Take note of the following restrictions before restoring from a snapshot:

- Restoration procedures must be completed only during times of relative EMS server inactivity or during scheduled periods of maintenance.
- Avaya SBC detection or mitigation features are unavailable for the entire duration of the restore procedure, making the EMS and Avaya SBC single server deployment vulnerable to intrusions and attacks.
- A snapshot can only be restored to the same version of the same EMS in the same hardware category. Consult the table for more information on hardware categories.
- If the EMS management IP in the snapshot differs from the current management IP, the EMS must be manually restarted to pick up the new management IP.
- During both methods, EMS goes into the offline mode when the files are being transferred and the device is being reconfigured.

- All devices currently registered or commissioned in the snapshot will be disconnected from the EMS. These devices must be reconfigured to resume operation.
- All devices in the snapshot (and the EMS in a single server deployment) will be rebooted after the restore completes.
- All current incidents will be archived to disk and all alarms will be cleared.

You can restore an SBC configuration data snapshot on EMS manually or configure automatic restoration of the snapshots.

You can restore snapshots to an EMS system of the same hardware category, manufacturer, and model of EMS. The following table lists the hardware categories and supported configurations:

Server	NIC Ports	DVD drive	Upgrade supported for	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell™ PowerEdge ™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	6	Yes	10.2.1	Supported	Supported	Supported
Dell™ PowerEdge ™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5	6	Yes	10.2.1	Supported	Supported	Supported
Dell™ PowerEdge ™ R340 Avaya Solutions Platform 110 Appliance server	6	No	10.2.1	Supported	Supported	Supported
Dell 3240	5	No	10.2.1	No	No	Supported
Dell VEP1425N	8 ports available, but only 4 ports are supported	Yes	10.2.1	Not supported	Not Supported	Supported

Table continues…

Server	NIC Ports	DVD drive	Upgrade supported for	Supported device configuration		
				EMS	SBC	EMS+SBC
Dell R660xs Avaya Solutions Platform 110 Appliance server - Profile A2	6	Yes	10.2.1	Supported	Supported	Supported
Dell R660xs Avaya Solutions Platform 110 Appliance server - Profile A3	8 ports available, but only 6 ports are supported	Yes	10.2.1	Supported	Supported	Supported
Dell R360	6	Yes	10.2.1	Supported	Supported	Supported

Related links

Retrieving a snapshot file on page 201
Restoring a snapshot file manually on page 202
Restoring a snapshot file automatically on page 202

Retrieving a snapshot file

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, preform one of the following:
   - Click **EMS** for retrieving snapshot for the EMS server.
   - Click **SBC** for the device specific retrieval of the snapshot.
3. In the navigation pane, click **Backup/Restore**.
4. On the Backup/Restore page, click **Snapshots** tab.
5. In the drop-down box, select snapshot server.
6. Select the check box next to the snapshot to retrieve, and click **Download**.

Result

The EMS server saves the snapshot file in the default download directory.

Next steps

Restore the downloaded configuration data snapshot.

Restoring a snapshot file manually

About this task

The manual restore process is known as the “restore by file” option. After you retrieve the snapshot file from the snapshot server, save the file on the local workstation. You can upload the file to the EMS server where the file is decompressed and used to reconfigure the EMS to a previous state.

Before you begin

Retrieve the snapshot file.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, preform one of the following:
   - Click **EMS** for restoring a snapshot for the EMS server.
   - Click **SBC** for device specific snapshot restoration.
3. In the navigation pane, click **Backup/Restore**.
4. On the Backup/Restore page, click the **Snapshots** tab.
5. Click **Restore by File**.
6. In the Restore Snapshot by File warning window, click **Select File**.
7. In the pop-up window, select a snapshot file, and click **Open**.

   The EMS server enters the selected snapshot file in the **Restore Point File** field of the Restore by File window.
8. Click **Upload**.

   The EMS server displays a warning window for confirmation to proceed with the restoration procedure.
9. Click **OK**.

   The EMS server goes offline and transfers the snapshot file to the EMS server. The file is then decompressed and used to reconfigure the EMS software to a previous configuration.

   After the system successfully restores a snapshot, in an HA configuration both Avaya SBC devices reboot. In a standalone configuration, the EMS and SBC single server reboots. The system takes several minutes to reboot after restoring a backup configuration.

Restoring a snapshot file automatically

Before you begin

Create a system snapshot.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. On the **Device** menu, preform one of the following:
   - Click **EMS** for restoring a snapshot for the complete EMS server.
   - Click **SBC** for device specific snapshot restoration.
3. In the navigation pane, click **Backup/Restore**.
4. Using the drop-down menu in the content area, select the snapshot server that contains the snapshot file that you want to retrieve.

   The EMS server displays all snapshot files on the selected snapshot server in the content area.
5. Select the snapshot file that you want to restore to the EMS or SBC by clicking the corresponding **Restore** option.

   The EMS server displays a warning pop-up window, asking for confirmation to proceed with the automatic restoration procedure.
6. Click **OK**.

   The EMS or SBC goes offline and reconfigures the snapshot file.

   Note:

   After the system successfully restores a snapshot, in an HA configuration both Avaya SBC devices reboot. In a standalone configuration, the EMS and SBC single server reboots. The system takes several minutes to reboot after restoring a backup configuration.

Related links

Retrieving a snapshot file on page 201
Restoring a snapshot file manually on page 202

Creating a configurable portable snapshot

About this task

You can create configurable portable snapshots from an HA system that allow you to separate or combine Avaya SBC instances.

Before you begin

Ensure that the Avaya SBC instance on which the snapshot is being created is in a Commissioned state.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Backup/Restore**.
3. On the Backup/Restore page, click the **Configurable Snapshot** tab.
4. Click **Create Configurable Snapshot**.
5. In the **Device List** field, click a device and click **Create**.

The EMS server creates a portable snapshot in:

`/usr/local/ipcs/snapshots/configurable_snapshot/`

Restoring a configurable portable snapshot

About this task

You can restore configurable portable snapshots from an HA system that allow you to separate or combine Avaya SBC instances.

Before you begin

Ensure that the Avaya SBC instance on which you are restoring the snapshot and the Avaya SBC instance from which the snapshot was taken meet the following requirements:

- The instance has the same number of interfaces.
- The instances are of the same version.

Ensure that the Avaya SBC instance on which the snapshot is being restored is in a Commissioned state.

Important:

The EMS server restore affects services on Avaya SBC because the restore function deletes and restores the database.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Backup/Restore**.
3. On the Backup/Restore page, click the **Configurable Snapshot** tab.
4. In the row corresponding to the snapshot file to be restored, click **Restore**.

   The EMS server displays the Restore Configurable Snapshot page.
5. In the **Device** field, select a device, and click **Finish**.

   The EMS server restores the configuration from the snapshot to the device that you chose. The time taken for restoring the snapshot varies depending on the server type.

   Logs related to the portable snapshot and restore process are stored on the EMS at `/archive/log/icu/DBDumpRestore.log`.

   You can change system-specific data, such as server flow names, manually after the portable snapshot is restored.

Next steps

Synchronize certificates manually.

Deleting a system snapshot

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, preform one of the following:
   - Click **EMS** for deleting the snapshot for the complete EMS server.
   - Click **SBC** for device-specific snapshot deletion.
3. In the navigation pane, click **Backup/Restore**.
4. Select the local server or the designated snapshot server from where you want to delete the file.
5. Select the file and click the corresponding **Delete** option.

   The EMS server displays a warning message asking for confirmation to delete.
6. Click **OK**.

Result

The EMS server deletes the snapshot file.

About VMware snapshots

Snapshots capture the state of the virtual machine when you take the snapshot. To avoid problems, ensure that you take a snapshot when no applications in the virtual machine are communicating with other computers. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file. But when you revert to the snapshot, the file transfer fails.

Warning:

Snapshot operations can adversely affect service. The application that is running on the virtual machine must be stopped or set to out-of-service before you perform a snapshot operation. When the snapshot operation has completed, you can then restart or set the application back into service.

This section contains information about creating, restoring, and deleting snapshots from VMware.

You can also back up and restore system information by using the Backup/Restore option on the EMS web interface. For more information about snapshots for EMS or SBC, see *Administering Avaya Session Border Controller*.

Creating a snapshot for VMware

Before you begin

Warning:

Snapshots can cause performance issues with Avaya SBC. It is recommended to use snapshots for short periods of time.

Warning:

Take a VM snapshot when the application is powered off to avoid .war file corruption on Avaya SBC. If the .war file is corrupted, some GUI pages might not display correctly.

Caution:

Do not perform any activity on the virtual application until the snapshot backup is complete. Snapshot operations can adversely affect service.

Verify with the system administrator that the required privilege **Virtual machine.State.Create snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the following steps accordingly.

Procedure

1. In the **Name** field, enter a name for the snapshot.
2. In the **Description** field, enter a description for the snapshot.
3. Disable **Snapshot the virtual machine's memory**.
4. Enable **Quiesce guest file system (Needs VMware Tools installed)**.
5. Click **OK**.

   The system displays `Completed` when the snapshot backup is complete.

Deleting a snapshot for VMware

Note:

Differences exist between the vSphere Web Client versions. Modify the steps accordingly.

Before you begin

Verify the required privilege **Virtual machine.State.Remove snapshot** is available on the virtual machine.

Procedure

1. To open the **Snapshot Manager** using the vSphere Web Client:
   a. Search for a virtual machine.
   b. Select the virtual machine from the search results list.
   c. Right-click the virtual machine and select **Snapshot** > **Snapshot Manager**.
2. In the **Snapshot Manager**, click a snapshot that you want to delete.
3. Select **Delete from Disk**.
4. When the Snapshot Manager displays a dialog box for confirmation, click **Yes**.
5. Click **Close** to close the Snapshot Manager.

Restoring a snapshot for VMware

Use this procedure to return the memory, settings, and state of the virtual machines to the state when you took the snapshot. The power and data states of the virtual machines return to the state when you took the parent snapshot.

Important:

Do not perform any activity on the virtual application until the snapshot restoration is complete.

Before you begin

Verify with the system administrator that the required privilege **Virtual machine.State.Revert to snapshot** is available on the virtual machine.

Note:

Differences exist between the vSphere Web Client versions. You might need to modify the steps accordingly.

Procedure

1. Click **Inventory** > **Virtual Machine**.
2. Right-click the virtual machine name on which you want to restore the snapshot, and click **Snapshot**.
3. Open **Snapshot Manager**.
4. Select the snapshot version that you want to restore.
5. Click **Go to**.
6. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task.

   Wait until the system displays the `Completed` message

Creating a snapshot for KVM

About this task

Use the following procedure to create a snapshot for the virtual machine(VM). The filename `KVM-SBCE-8.1` is an example of how you could name the filename.

Before you begin

Caution:

Do not perform any activity on KVM until the snapshot backup is complete. Snapshots operations can adversely affect service.

It is recommended that VM is powered off or shut down to take a clean snapshot.

Verify with the system administrator that the required privilege virtual machine.State.Create snapshot is available on the virtual machine.

Procedure

1. Log in to the KVM host with root permissions.

2. At the console, enter the following command:

   virt-manager

   The system displays the Virtual Machine Manager GUI.
3. Type 2 for CLI mode.
4. Take the snapshot by using the **virsh snapshot-create KVM-SBCE-8.1** command.
5. Enter a name to identify the snapshot.
6. View the snapshot, using the **virsh snapshot-list KVM-SBCE-8.1** command.

   The system displays the **Name**, **Creation Time** and the **State** of the snapshot.

Deleting a snapshot for KVM

About this task

Use the following procedure to delete a snapshot for the virtual machine(VM). The filename KVM-SBCE-8.1 is an example of how you could name the filename.

Before you begin

Verify with the system administrator that the required privilege Virtual machine.State.Removal snapshot is available on the virtual machine.

Procedure

1. Log in to the KVM host with root permission.
2. At the console, type virt-manager.

   The system displays the Virtual Machine Manager GUI.
3. Type 2 for CLI mode.
4. List the created snapshots, using the **virsh snapshot-list KVM-SBCE-8.1** command.

   The system displays the list of all the created snapshots.
5. Delete the snapshot, using the following command:

   virsh snapshot-delete KVM-SBCE-8.1 <*Name of the snapshot*>

   The system deletes the specified snapshot.

Restoring a snapshot for KVM

About this task

Use this procedure to return to the memory, settings and state of the virtual machine to the state when you took the snapshot. The power and data states of the virtual machine return to the state when you took the parent snapshot.

Use the following procedure to delete a snapshot for the virtual machine(VM). The filename KVM-SBCE-8.1 is an example of how you could name the filename.

Important:

Do not perform any activity on the virtual application until the snapshot restoration is complete.

Before you begin

Verify with the system administrator that the required privilege Virtual machine.State.Revert to snapshot is available on the virtual machine

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, enter the following command:

   `virt-manager`

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. List the created snapshots, using the **`virsh snapshot-list KVM-SBCE-8.1`** command.

   The system displays the list of all the created snapshots.
5. Restore the snapshot, using the following command:

   `virsh snapshot-revert KVM-SBCE-8.1` *<name of the snapshot>*

   The system restores the specified snapshot.

Management of deployed Avaya SBC security devices

In addition to configuring newly installed Avaya SBC security devices, you can also perform a number of additional functions to effectively manage your network. The additional functions are:

- Shutdown and reboot individual Avaya SBC security devices.
- Restart Avaya SBC applications.
- Swap Avaya SBC devices.
- View, edit, and delete Avaya SBC device configurations.

Shutting down an Avaya SBC security device

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.

4. On the Device Management page, click **Devices** tab.
5. Click **Shutdown** corresponding to the Avaya SBC security device you want to shutdown.

   The EMS server displays a pop-up window to confirm your selection.
6. Click **OK**.

   The EMS server displays a notification pop-up window when the device is successfully shut down.

Restarting an Avaya SBC application

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click **Restart Application** corresponding to the Avaya SBC security device that you want to restart.

   The EMS server displays a confirmation pop-up.
6. Click **OK**.

Result

The EMS server displays a notification pop-up when the device is successfully restarted.

Rebooting an Avaya SBC security device

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click **Reboot** corresponding to the Avaya SBC security device you want to reboot.

   The EMS server displays a pop-up window to confirm your selection.
6. Click **OK**.

   The EMS server displays the notification pop-up window when the reboot of the device is successful.

Swapping a separate Avaya SBC server deployed under EMS

Before you begin

Confirm that you have created and saved the backup file of a functional Avaya SBC device.

Confirm that both Avaya SBC devices have the same software version before you start the swap procedure.

Confirm that all Avaya SBC devices involved in the swap procedures are in the commissioned state after the swap is complete.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. Install a new Avaya SBC with a different IP address. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.
5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
6. When the state of the newly added Avaya SBC device becomes Registered, click **Swap Device**.
7. Select the backup file of old Avaya SBC system (down system).

   Important:

   The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.
8. Click **Finish.**

   The EMS server does not display the old Avaya SBC device in the **Devices** tab.

Swapping Avaya SBC devices in an HA pair deployment

Before you begin

Confirm that one of the Avaya SBC devices in the HA pair is non-functional.

Confirm that both Avaya SBC devices have the same software version before you start the swap procedure.

Confirm that all Avaya SBC devices involved in the swap procedures are in the commissioned state after the swap is complete.

Procedure

1. Log in to the EMS web interface with the administrator credentials.

2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. Install a new Avaya SBC with different IP address.

   For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.
5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
6. When the state of the newly added Avaya SBC device becomes Registered, click **Swap Device**.
7. Select the IP address of the down Avaya SBC system in the HA pair.
8. Click **Finish.**

   The EMS server does not display the old Avaya SBC device in the **Devices** tab.

Swapping an EMS server in a single server deployment

Before you begin

Confirm that you have created and saved the backup file of a functional EMS server.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. When the state of the EMS becomes Commissioned, click **Swap Device**.

   Note:

   The EMS server displays the **Swap Device** option only when there is no SBC device installed on the system.
5. Select the backup file of old EMS device.

   Important:

   The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.
6. Click **Finish** to complete the EMS swap.

Related links

Swapping a primary EMS server in an HA pair deployment on page 213

Swapping a secondary EMS server in an HA pair deployment on page 213
Restarting an Avaya SBC application on page 210

Swapping a primary EMS server in an HA pair deployment

Before you begin

Confirm that the primary EMS server is non functional.

Confirm that both EMS devices have the same software version before you start the swap procedure.

The IP addresses of the old and the new EMS must be different.

Procedure

1. Log in to the newly installed EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. When the state of the newly installed primary EMS becomes commissioned, click **Swap Device**.

   Note:

   The newly installed EMS server displays the **Swap Device** option only when there is no SBC device installed on the system.
5. Provide the IP address for the secondary EMS server.
6. Click **Finish** to complete the EMS swap.

Related links

Swapping an EMS server in a single server deployment on page 212
Swapping a secondary EMS server in an HA pair deployment on page 213
Restarting an Avaya SBC application on page 210

Swapping a secondary EMS server in an HA pair deployment

Before you begin

Confirm that both EMS devices have the same software version before you start the swap procedure.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.

4. On the Device Management page, click **Devices** tab.
5. Click **Uninstall** corresponding to the secondary EMS from the primary EMS web interface.

   The EMS server displays a confirmation pop-up to confirm your selection.
6. Click **OK**.
7. Deploy and configure a new EMS as secondary EMS. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

   Secondary EMS is automatically added until Release 10.1. From Release 10.1.2 onwards, users must add the secondary EMS from primary EMS Device Management on GUI.
8. On the Device Management page, click **Devices** tab.
9. Click **Restart Application** corresponding to all the EMS connected servers.

   The EMS server displays a confirmation pop-up.
10. Click **OK** to confirm.

Result

Secondary EMS will be added in the Devices section.

Related links

Swapping an EMS server in a single server deployment on page 212
Swapping a primary EMS server in an HA pair deployment on page 213
Restarting an Avaya SBC application on page 210

Viewing device configuration

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click the **View** option corresponding to the Avaya SBC security device whose configuration you want to view.

   The EMS server displays a Device Configuration pop-up window.
6. Click the Cancel icon after viewing the configuration information.

Editing device configuration

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.

3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click the Edit option corresponding to the Avaya SBC security device whose configuration you want to edit.

   The EMS server displays the Edit Device pop-up window.
6. Make the necessary edits or click the **Cancel** icon to close the window without saving your changes.
7. Click **Finish**.

Result

The changes are saved to the Avaya SBC configuration file.

Deleting a device configuration

About this task

Caution:

Deleting a device configuration permanently deletes all configuration data for the device. Ensure that you have a snapshot of the configuration data if you need to reinstall the device.

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click the **Devices** tab.
5. Click **Uninstall**, corresponding to the Avaya SBC security device to uninstall.

   The EMS server displays a confirmation pop-up to confirm your selection.
6. Click **OK**.

   The EMS server removes the Avaya SBC device from the list.

Upgrading system management

About this task

This procedure is for the generic upgrade. For detailed procedure, see *Upgrading Avaya Session Border Controller*.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Updates** tab.

   The EMS server displays the System Upgrade screen.
5. Select an upgrade package and click **Upgrade**.

Enabling High Availability

Before you begin

You must obtain a license file with the following feature: FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1. Ensure that the **Values** field for the Session Border Controller High Availability per Configuration feature is set to on.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click **Add**.

   The EMS server displays the Add Device page.
6. Provide appropriate values in the following fields:
   a. **Host Name**
   b. **Management IP**
   c. **High Availability**
   d. **Host Name for second Node**
   e. **Management IP for second Node**

   Note:

   When the High Availability (HA) check box is selected, EMS server with HA mode replicates and preserves complete signaling state for all active calls and registration information of endpoints on the standby box. In the event that the active box fails, the standby box will be able to maintain the state of the active call such that all the features for that active call will be available. The EMS server with HA mode will maintain state information for calls on UDP, TCP, and TLS transport protocols.
7. Click **Finish** to save and exit.

Avaya SBC supports duplicate HA connection by using HA pair management addresses. With HA replication, if any of the M2 to M2 or M1 to M1 connections are down, the other connection continues uninterrupted.

Managing Avaya SBC logging level

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
3. On the Debugging page, click **Subsystem Logs** tab.
4. Select or clear the check boxes corresponding to the type of execution log that you want to enable or disable.
5. Click **Save**.

Result

The EMS server displays a message at the top of the screen: `Configuration update successful`.

Debugging field descriptions

Subsystem Logs

Name	Description
Process Name	Specifies the process for which you want to enable logs. This field displays processes such as: • LogServer • OAMPSERVER • SYSMON • SSYNDI • TURNCONTROLLER Each process contains subsystems. You can select the required subsystems for which you want to enable logs.
Debug	Specifies that debug logs are enabled for a subsystem. If you select the **Debug** check box in the table header, the system selects debug logs for all processes.
Info	Specifies that informational logs are enabled for a subsystem. If you select the **Info** check box in the table header, the system selects informational logs for all processes.

Table continues…

Name	Description
Warning	Specifies that warning logs are enabled for a subsystem. If you select the **Warning** check box in the table header, the system selects warning logs for all processes.

GUI logs

Name	Description
GUI	Controls master log levels for all GUI logs. The options are: • Info • Warn • Error
SOAP	Includes detailed logs generated by a GUI SOAP client. SOAP handles communication with EMS and Avaya SBC Communication Manager servers, for example, restart application, reboot device, and uninstall device. This option is deprecated.
Statistics	Includes the trace logs for Statistics when this field is enabled.
HTTP	Includes the HTTP communication logs for REST API between EMS and SBCs when this field is enabled.
Shell Commands	Include detailed logs when you start any external process.
File Uploads	Includes detailed logs for user file uploads, for example, upgrade packages, scrubber packages, and certificates.
Licensing	Includes detailed logs generated by a GUI WebLM client.
Certificates	Includes the trace logs for TLS certificate installation when this field is enabled.
Backup / Restore	Includes the trace logs for backup and restore when this field is enabled.
Third Party Components	Controls a master log level for third-party logs. This log level covers any logs from third-party libraries that the GUI uses. The options are: • Debug • Info • Warn • Error

Table continues…

Name	Description
SSH	Controls log levels for a third-party SSH library used for backup or restore and remote actions. The options are: • Inherit • Debug • Info • Warn • Error
SNMP	Includes the SNMP logs based on the log level selected.
LDAP	Includes the LDAP logs based on the log level selected.
RADIUS	Includes the RADIUS logs based on the log level selected.
Spring	Includes the Spring framework logs based on the log level selected.
Square Utilities	Includes the Square Utilities logs based on log the level selected.

Third-Party Logs

Name	Description
Nginx	Controls log levels for nginx. The options are: • Info • Notice • Warn • Error • Crit • Alert • Emerg
Ldap	Controls log levels for LDAP. The options are: • Any • Packets • Config • Stats
Transcoding	Controls log levels for transcoding. The options are: • None • All

Table continues…

Name	Description
H248	Controls log levels for H248. The options are: • None • Error • Trace

Advanced Options configuration

With the **Advanced Options** feature, you can:

- Enable or disable Avaya SBC security features.
- Configure SIP signaling message options.
- Designate signaling and media port ranges.
- Configure RTCP monitoring.
- Configure load monitoring.
- Configure HA keepalive timer.

To access these features, navigate to an SBC in your deployment and select **Network & Flows** > **Advanced Options**.

Advanced Options field descriptions

Periodic Statistics tab

Name	Description
Collect Periodic Statistics	Specifies whether collecting periodic statistics must be enabled.
Collection Interval	Specifies the time interval for which the system collects call statistics. The EMS server generates a report with statistics for the specified collection interval. When you enable collection of periodic statistics, the EMS server purges data collected before the collection interval you specify.

Feature Control tab

Name	Description
AMS Offloading	Enables the AMS offloading feature.
Call Walking Protection	Enables the Call Walking Protection feature.
Media Tunneling	Enables the media tunneling feature.

Table continues…

Name	Description
Phone Dos/DDoS Protection	Enables the Phone DoS/DDoS Protection feature.
Single Source DoS Protection	Enables the Single Source DoS Protection feature.
SIP Overload Control	Enables the SIP Overload Control feature.
Stealth DoS/DDoS Protection	Enables the Stealth DoS/DDos Protection feature.
Transcoding	Enables the media transcoding feature.
Transrating	Enables the transrating feature.

SIP Options tab

Name	Description
DNS Caching	Enables DNS Caching.
AS-SIP Mode	To enable the transmission of SIP and SRTP combination towards SIP trunks or call servers in JITC environment or enclave deployment. When **AS-SIP Mode** is enabled Avaya SBC supports SRTP over SIP towards the SIP trunks or call servers. Avaya SBC converts the SIPS to SIP towards the SIP trunks or call servers.
E911 URI Group	Frees the numbers in the Emergency URI group from any dial-out restrictions that might be imposed by Domain Policies. The Emergency URI group is an integral part of the system that is user defined. The Emergency URI group defines special numbers that must not be restricted by any Domain Policies. Avaya SBC administrators must provide all applicable emergency numbers for their country for special handling.
Maximum Concurrent Sessions	Specifies the number of allowed concurrent dial-out sessions. A value of zero provides unlimited sessions.
Allow Emergency Call Preemption	When enabled and the **Maximum Concurrent Sessions** limit is reached for a policy group: • On receiving a non-emergency call, Avaya SBC rejects call and raise an incident. • On receiving an emergency call, Avaya SBC accepts the call and disconnects an active non-emergency call from the same policy group. When disabled and the **Maximum Concurrent Sessions** limit is reached for a policy group: • On receiving a non-emergency call, Avaya SBC rejects call and raise an incident. • On receiving an emergency call, Avaya SBC accepts the call. By default, this field is disabled.

Network Options tab

Name	Description
Allow Non-Unique IPs for Complex Networks	Enables reusing IPs in complex networks.

Port Ranges tab

For SIP deployments, you must create Internal signaling and media interfaces toward Call Server and External signaling and media interfaces toward Trunk Server.

Note:

The fixed ports for TCP, UDP, or TLS defined under **Network & Flows** > **Signaling Interface** must not be assigned a port number that falls within a Signaling Port range. A fixed port for TCP, UDP, or TLS is a shared Listen Port for multiple calls incoming to Avaya SBC from a Trunk Server or Call Server.

Name	Description
Signaling Port Range	Used by Avaya SBC to start connections for outgoing SIP requests from Avaya SBC towards a SIP Server (Call Server or Trunk Server). The direction of these ports is away from Avaya SBC. For the changes to the **Signaling Port Range** field to take effect immediately, ensure that you do one of the following: • Select the **Enable Grooming** check box on the **Services** > **SIP Servers** page and select **Extensions** as **None** on the **Configuration Profiles** > **Server Interworking** page. • Clear the **Enable Grooming** check box on the **Services** > **SIP Servers** page and select **Extensions** as **Avaya** on the **Configuration Profiles** > **Server Interworking** page.
Config Proxy Internal Signaling Port Range	Used by Avaya SBC to start connections from Avaya SBC toward Configuration Servers. For example, configuration servers of the following types: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP. The direction of these ports is away from Avaya SBC.
Listen Port Range	Used in PORTID Mode. See *Managing SIP Server Configurations*. Avaya SBC listens to these ports for requests from a SIP Server, usually a Call Server, during intermittent, phone-related communications. For example, during calls and signaling, where a link does not stay up indefinitely. The direction of these ports is towards Avaya SBC.
HTTP Port Range	Used by Tinyproxy to start connections for Avaya SBC towards the upstream server or http server based on the routing for intermittent communications unrelated to the phone. For example, for web services and media, where a link does not stay up indefinitely. The direction of these ports is away from Avaya SBC.

RTCP Monitoring

Name	Description
RTCP Monitoring Relay	Enables or disables RTCP monitoring.
Node Type	Specifies the type of Avaya SBC configuration for the node. The options are: • **Core** • **DMZ** • **Remote**
Relay IP	Specifies the relay IP address. **Note:** • For CORE Avaya SBC configuration, in the **Relay IP** field, click **Core SBC Internal IP1**. • Core Avaya SBC Internal IP1 address is used to send RTCP traffic received from DMZ SBC and core phones towards monitoring server.
Port	Specifies the port number for RTCP monitoring.
RTCP Monitoring Report Generation	Specifies whether RTCP monitoring report generation is enabled
SBC Interface IP	Specifies the source IP address of Avaya SBC for communication between Avaya SBC and the monitoring tool. **Note:** The IP address must be the IPv4 address.
SBC Interface Port	Specifies the source port number of Avaya SBC for communication between Avaya SBC and the monitoring tool.
Monitoring server IP/FQDN and Port	Specifies the destination IP address and port number of the remote monitoring tool. **Note:** The IP address must be the IPv4 address.
Monitoring Frequency based on RTCP Report	Specifies the number of RTCP packets received from a SIP trunk after which Avaya SBC generates the RTCP monitoring report.
Monitoring interval in absence of RTCP Report	Specifies the interval (in seconds) between two consecutive RTCP monitoring reports.

HA Pairs

Name	Description
Keep Alive Interval	Used by Avaya SBC to keep track of the status of other Avaya SBC in HA pair. The default value is `1500` milliseconds. The time range is `300` to `3000` milliseconds.
Max Retries	The maximum number of attempts for which Avaya SBC must try to reach the HA pair. You can enter a value between `2` and `5`. The default value is `4`.

Load Monitoring tab

Name	Description
Load Balancer Type	Type of load balancer. The available options are: • **INTERNAL**: Load balancer on the A1 side of the network. Iview, the Avaya Meetings Server management entity, does load balancing towards the internal side. All HTTP requests sent for dialing out use the internal load balancer logic to identify the appropriate Avaya SBC. • **EXTERNAL**: Load balancer on the B1 side of the network. All HTTP requests sent for dialing in use the external load balancer, depending on the data sent.
Transport	Transport protocol used by the load balancer. **Note:** If **TCP/TLS Listen Port** in configuring TURN STUN profile is configured as 443, you must use TCP as the **Transport** protocol in load monitoring to avoid port conflict of **Listen IP** port and **Media Relay IP** while configuring TURN Relay.
Listen IP	Load balancer listen IP address. **Note:** Ensure that at least one IP address is configured in **Network Management** for listen IP configuration. The system supports IPv4 and IPv6.
Service Type	Service type supported by load balancer The available options are: • **None** • **TURN** • **Media Tunnel**

Security feature control

With the **Feature Control** tab of the **Advanced Options**, you can enable or disable system wide Avaya SBC security features.

The security features enable or disable settings defined here apply specifically to each Avaya SBC device that is currently selected in the Application Pane. These settings only enable or disable one or more security features for the selected Avaya SBC device.

The actual thresholds for each one of these security features are globally defined for all Avaya SBC devices within the network by selecting: **Configuration Profiles** > **Domain DoS**.

See DoS Security Features on page 290.

Managing security features

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **Feature Control** tab.

   The EMS server displays the Feature Control screen.
5. In the **Enable/Disable** column, do one of the following:
   - Select the check boxes corresponding to the features you want to enable.
   - Clear the check boxes corresponding to the features you want to disable.

   Enabling a feature directs Avaya SBC to detect the indicated anomaly, such as DoS or DDoS, enable media transcoding, or perform the corresponding service.
6. Click **Save**.

Managing SIP options

About this task

With the **SIP Options** tab, you can enable and disable DNS caching.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **SIP Options** tab.

   Make your selections.
5. Click **Save**.

SIP options tab display field descriptions

Name	Description
DNS Caching	To enable or disable DNS Caching.
AS-SIP Mode	To enable the transmission SIP or SRTP combination towards SIP trunks in JITC environment or enclave deployment.
E911 URI Group	To enable the numbers contained in the Emergency URI group to be free from any dial-out restrictions that may be imposed by Domain Policies. The Emergency URI group is an integral part of the system that is user defined. The Emergency URI group defines special numbers that must not be restricted by any Domain Policies. SBC administrators must provide all applicable emergency numbers for their country for special handling.
Maximum Concurrent Sessions	To specify the number of allowed concurrent dial-out sessions. A value of zero provides unlimited sessions.

Allowing reuse of the same IP

About this task

For complex networks, Avaya SBC supports the use of the same IP for more than one data interface. Use the following configuration to assign non-unique addresses to Avaya SBC data interfaces.

Warning:

Do not use the same IP for different Avaya SBC devices in the same network.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **Network Options** tab.
5. Select the **Allow Non-Unique IPs for Complex Networks** check box.

   Avaya SBC supports the use of the same IP for more than one data interface.

Managing port options

About this task

With the Port Ranges tab of the Advanced Options function, you can set the range of ports on which internal signaling traffic will be received and sent. Use the following procedure to manage this feature.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **Port Ranges** tab.

   The EMS server displays the Port Ranges screen.
5. Enter the beginning and ending port numbers for each field.
6. Click **Save**.

Port Ranges field descriptions

Note:

For SIP deployments, you must create the Internal (toward Call Server) and External (toward Trunk Server) signaling interfaces and media interfaces. You must create and define the signaling interfaces and media interfaces by navigating to **Network & Flows** > **Signaling Interface** and **Network & Flows** > **Media Interface**.

Note:

The fixed ports for TCP, UDP, or TLS defined under **Network & Flows** > **Signaling Interface** must not be assigned a port number that falls within a Signaling Port range. A fixed port for TCP, UDP, or TLS is a shared Listen Port for multiple calls incoming to Avaya SBC from a Trunk Server or Call Server.

Name	Description
Signaling Port Range	(Direction = Away from Avaya SBC) This port range is used by Avaya SBC to start connections for outgoing SIP requests from Avaya SBC towards a SIP Server (Call Server or Trunk Server).
Config Proxy Internal Signaling Port Range	(Direction = Away from Avaya SBC) This port range is used by Avaya SBC to start connections from Avaya SBC toward Configuration Servers. For example, configuration servers of the following types: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP.

Table continues…

Name	Description
Listen Port Range	(Direction = Toward Avaya SBC) This port range is used in PORTID Mode, see *Managing SIP Server Configurations*. Avaya SBC listens on these ports for requests from a SIP Server (usually a Call Server) during nonpersistent, phone-related communications, for example, calls and signaling, where a link does not stay up indefinitely.
HTTP Port Range	(Direction = Away from Avaya SBC) This port range is used by Tinyproxy to start connections for Avaya SBC towards the upstream server or any other http server based on the routing for nonpersistent, nonphone-related communications (e.g., web services, media) where a link does not stay up indefinitely.

Monitoring RTCP

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **RTCP Monitoring** tab.

   The EMS server displays the RTCP Monitoring Configuration screen.
5. Enter the appropriate values.
6. Click **Save**.

Configuring HA Heartbeat Interval and Max Retries

Before you begin

You must enable high availability for the device. See the Enabling High Availability section.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, **Network & Flows** > **Advanced Options**.
4. Click the **HA Pairs** tab.

   The EMS server displays the Heartbeat Settings screen.
5. Click **Edit**.

   The system displays the Edit HA Pairs Options page.

6. Type the required values and click **Finish**.

Media Forking overview (Standard Platform only)

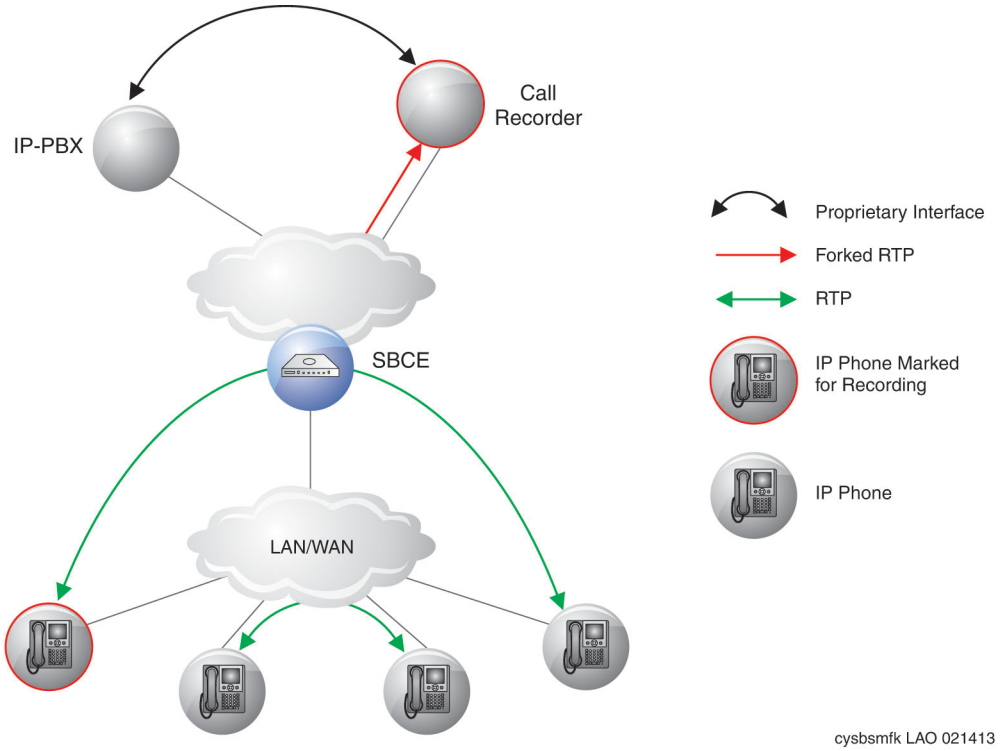
The Media Forking feature allows the Avaya SBC device to fork media packets according to a designated Media Forking Profile. This solution addresses problems faced by call recorders deployed for quality assurance and compliance.

The Media Forking Profile has parameters for sending a duplicate stream of media packets to a call recorder. In general, the call recorder is connected to the IP-PBX through a CTI. This network allows the transfer of call and endpoint information from the IP-PBX to the call recorder through a proprietary interface, for example, JTAPI.

Note:

Without the Avaya SBC device, ports of all phones must be spanned, so that media could be established between phones. Spanning all ports becomes a tedious task. With the Avaya SBC device in the picture, the spanning of all ports is not required, as the Avaya SBC anchors the media and forks the media packets to the call recorder.

A high-level topology illustration of Media Forking is provided below.



Adding a Media Forking profile (Standard Platform only)

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Media Forking**.
4. Click **Add**.

   The EMS server displays the Media Forking Profile window.
5. Make the requested information in the appropriate fields.
6. Click **Finish**.

Result

The EMS server displays the new Media Forking profile in the content area.

Media Forking Profile field descriptions

Note:

For configuring IP-PBX and the recording device, please refer to the individual manuals.

Name	Description
Profile Name	A descriptive name of the media forking profile.
Call Scenario	Indicates the type of call forking: • **Hairpin Calls** • **Non-Hairpin Calls**
Media Type	Indicates the part of the call to mirror. • **Mirror Audio Stream** • **Mirror Video Stream** • **Mirror Other Streams**
Mirror RTCP Stream	Check box to enable mirror RTCP stream.
Quick Record Port	Indicates the port number.
Ethernet Interface	Indicates the interface.
Enable VLAN Tagging	Check box to enable the **Enable VLAN Tagging** feature
VLAN ID	Indicates the VLAN ID. The range is 1 to 4095. **VLAN ID** field is accessible only if you select **Enable VLAN Tagging** check box.

Table continues…

Name	Description
VLAN Protocol	Indicates the VLAN protocol. The options are: • **IEEE 802.1Q** • **Cisco ISL** **VLAN Protocol** field is accessible only if you select **Enable VLAN Tagging** check box.
Destination MAC	Indicates the destination MAC address.
Source MAC	Indicates the source MAC address.

Adding Media Forking Profile to Session Policy (Standard Platform only)

About this task

In SIP deployments, you can add the Media Forking profile on one of the following screens:

- **Configuration Profiles** > **Media Forking**
- **Domain Policies** > **Session Policies**

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Click **Domain Policies** > **Session Policies**.

   The EMS server displays the Session Policies page.
4. Select a Session Policy to add a Media Forking Profile.
5. Click **Edit**.

   The EMS server displays the Media page.
6. Select the **Media Anchoring** check box.

   The EMS server enables the **Media Forking Profile** field.
7. In the **Media Forking Profile** field, select the media forking profile that you want to add to the selected session policy.

Next steps

To add the Session policy to the Session Flow, ensure that the session flow matches with the required call recorders.

MAC-based LDAP authentication

MAC-based LDAP authentication feature uses LDAP to authenticate the MAC address of the endpoints in the SIP REGISTER messages .Avaya SBC supports LDAP version 3.

With this feature, Avaya SBC:

- Queries LDAP server to authenticate endpoints on receiving SIP REGISTER messages from the endpoints.
- Creates a search filter and sends the query to the LDAP server.
- Validates the MAC address received in the LDAP query response in the SIP REGISTER message and authenticates the endpoint.

The communication of Avaya SBC and LDAP server supports:

- IPv4 and IPv6 addresses.
- The management interface.
- The ability to communicate with the primary and alternate LDAP servers. If the primary LDAP server is non-functional, the communication continues with the alternate server.
- Caching of LDAP queries and responses.

LDAP Server Profile

The server profile which is used for MAC-based LDAP authentication and LDAP routing features configuration.

Creating a new LDAP server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **LDAP**.

   The application pane displays the existing LDAP servers and the content pane displays the parameters of the selected LDAP server.
4. In the application pane, click **Add**.

   The EMS server displays the first LDAP server window.
5. Enter the appropriate values, and click **Finish**.

Result

The application pane displays the newly created LDAP server and the content pane displays the parameters when you select the LDAP server.

MAC-based LDAP authentication field descriptions

Name	Description
Profile Name	A descriptive name of the LDAP server profile.
Primary Address	The IP address or FQDN and port number of the server designated as the primary LDAP server.
Secondary Address	The IP address or FQDN and port number of the server designated as the secondary LDAP server.
Secure LDAP	The check box to enable the secure LDAP feature.
TLS Profile	The TLS profile used to secure LDAP. The **TLS Profile** field is visible only if you select the **Secure LDAP** check box.
Bind DN	The credentials to authenticate an LDAP server.
Password	The password for LDAP server authentication.
Confirm Password	The password confirmation for LDAP server authentication.
Base DN	The starting point for users to search a LDAP server.
Timeout	The time interval for which Avaya SBC must wait for a response from the LDAP server.
Caching	The check box to enable caching.
Cache Size	The maximum number of entries that Avaya SBC supports for caching. The **Cache Size** field is visible only if you select the **Caching** check box.
Cache Expiry Time	The time interval after which Avaya SBC deletes the entries in the caching memory. The **Cache Expiry Time** field is visible only if you select the **Caching** check box.

Button	Description
Clear Cache	The button to clear the cache memory. The **Clear Cache** button is visible only if you select the **Caching** check box.

Editing an existing LDAP server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **LDAP**.

The application pane displays the existing LDAP server and the content pane displays the parameters of the selected LDAP server.

4. In the application pane, click the name of the LDAP server.
5. In the lower-center section of the content pane, click **Edit**.

   The EMS server displays the Edit LDAP server window.
6. Edit the required fields, and click **Finish**.

Renaming an LDAP server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **LDAP**.

   The application pane displays the existing LDAP server and the content pane displays the parameters of the selected LDAP server.
4. In the application pane, select the name of the LDAP server.
5. In the upper-right section of the content pane, click **Rename**.

   The EMS server displays the Rename server window.
6. In the **New Name** field, type a new name for the LDAP server, and click **Finish**.

Result

The application pane displays the renamed LDAP server.

Cloning an existing LDAP server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **LDAP**.

   The application pane displays the existing LDAP servers and the content pane displays the parameters comprising the selected LDAP server.
4. In the application pane, select the name of the LDAP server.
5. In the content pane, click **Clone Server**.
6. In the **Clone Name** field, type a name for the new LDAP server, and click **Finish**.

Result

The application pane displays the cloned LDAP server.

Deleting an LDAP server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **LDAP**.

   The application pane displays the existing LDAP servers and the content pane displays the parameters of the selected LDAP server.
4. In the application pane, select the name of the LDAP server.
5. In the upper-right section of the content pane, click **Delete**.

   The EMS server displays the delete confirmation window.
6. Click **OK** to continue with the deletion of the LDAP server.

Result

The application pane no longer displays the deleted LDAP server.

Administering SNMP access

Accessing SNMP settings

About this task

Provisioning SNMP v3 parameters includes granting certain users access to the SNMP information. Use the following procedure to display the SNMP options.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **SNMP**.

   The system displays the SNMP screen. The Content Area contains user-selectable tabs that provide access to global SNMP parameters.

Next steps

Configure SNMP users, servers, and trap settings.

Uploading a cadf file to System Manager

About this task

To see Avaya SBC alarms on System Manager, you must upload the Avaya SBC common alarms definition file (cadf) to System Manager.

Procedure

1. Locate the cadf jar file for Avaya SBC, `ASBCE-CADF-extensions.jar`, at `/opt/spirit/config/cadf`.
2. Log in to System Manager with root permissions.
3. Upload the `ASBCE-CADF-extensions.jar` file to System Manager.
4. Type `cd $MGMT_HOME/plug/install/unix/.`
5. Type one of the following commands:
   - To update existing jar file, type `sh upgrade_plugin_files.sh false Postgres 'jdbc:postgresql://localhost:5432/avmgmt?user=avaya_system_data&password=Avaya_system_data#01' $JBOSS_HOME avmgmt` *path*`/ASBCE-CADF-extensions.jar`, where *path* is the absolute path for the `ASBCE-CADF-extensions.jar` file.
   - To install fresh jar file, type `sh install_plugin_files.sh false Postgres 'jdbc:postgresql://localhost:5432/avmgmt?user=avaya_system_data&password=Avaya_system_data#01' $JBOSS_HOME avmgmt` *path*`/ASBCE-CADF-extensions.jar`, where *path* is the absolute path for the `ASBCE-CADF-extensions.jar` file.

Adding an SNMP user account

About this task

Note:

You can also perform SNMP administration through System Manager. SNMP configuration through EMS overrides configuration from the System Manager. For more information, see the “Managing SNMPv3 user profiles” section in *Administering Avaya Aura® System Manager*.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **SNMP**.
4. Click the **SNMP v3** tab.
5. Click **Add**.

   The system displays the Add User pop-up window.
6. Administer the options as described in SNMP administration field descriptions on page 237.
7. Click **Finish**.

   The content area displays the SNMP account.

SNMP administration field descriptions

SNMP v3 tab

Name	Description
User Name	The name of the user with access to SNMP v3 data
Authentication Scheme	The scheme to authenticate the user before granting access to SNMP data. The options are: • **noAuthNoPriv**: The user is not authenticated and SNMP data is not encrypted. • **authNoPriv**: The user is authenticated, but SNMP data is not encrypted. • **authPriv**: The user is authenticated, and the SNMP data is encrypted.
AuthPassPhrase	The user password for authentication. This field is unavailable if you use the noAuthNoPriv Authentication Scheme.
Confirm AuthPassPhrase	The AuthPassPhrase for confirmation. This field is unavailable if you use the noAuthNoPriv Authentication Scheme.
Authentication Protocol	The type of authentication algorithm to encrypt the user password (AuthPassPhrase). An authentication protocol: ensures data integrity, protects against data modification, provides data origin authentication, and protects against masquerade attacks. The types of authentication protocol currently supported are: • **MD5**: Message Digest Algorithm • **SHA**: Secure Hash Algorithm
PrivPassPhrase	The user password for SNMP: data authentication. This field is unavailable if you use the noAuthNoPriv or AuthNoPriv Authentication Scheme.
Confirm PrivPassPhrase	The PrivPassPhrase for confirmation. This field is unavailable if you use the noAuthNoPriv or AuthNoPriv Authentication Scheme.
Privacy Protocol	The privacy protocol to ensure privacy during communication. The options are: • AES • DES This field is unavailable if you use the noAuthNoPriv or AuthNoPriv Authentication Scheme.

Table continues…

Name	Description
Privilege	The type of privileges available to the user. The options are: • **Read** • **Read/Write**
Trap IP Address	The IP address and port on which SNMP traps will be received. Users can specify up to five destinations with different IP addresses.
Port	The port number for SNMP traps. The default port number is 162.
Trap Profile	The SNMP Trap profile to be used for this trap destination and the user.

Management Servers tab

Name	Description
IP Address	The IP address of the management server. Changes in IP addresses can take up to 15 minutes to take effect.

Trap Severity Settings

Name	Description
Trap Severity	The category of the trap. This column lists the following trap types: • Critical • Minor • Major • Informational
Status	The current status for the trap type. The options are: • **Enabled** • **Disabled**

Editing an SNMP user account

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **SNMP**.
4. Click the **SNMP v3** tab.
5. Click **Edit**.

   The system displays the Edit User pop-up window.
6. Administer the options as described in SNMP administration field descriptions on page 237.

7. Click **Finish**.

   The content area displays the SNMP account.

Deleting an SNMP user account

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **SNMP**.
4. Click the **SNMP v3** tab.
5. Click **Delete** corresponding to the SNMP user account that you want to delete.

   The EMS server displays a confirmation pop-up window
6. Click **OK** to confirm the deletion of the SNMP user.

   The content pane no longer displays the deleted SNMP user account.

Adding an SNMP management server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, select the **SBC** name to administer.
3. Navigate to **Monitoring & Logging** > **SNMP**.
4. Click the **Management Servers** tab.
5. Click **Add**.

   The system displays the Add IP Address screen.
6. In the **IP Address(es)** field, type one or more server IP addresses separated by commas or new lines.
7. Click **Finish**.

   The system displays the administered management server IP addresses.
8. Restart the IPCS services as described in Restarting the IPCS services on page 76.

Creating an SNMP trap profile

About this task

With SNMP trap profiles, you can select the traps that Avaya SBC must send to the Serviceability Agent.

For Avaya SBC, you can create and use new SNMP trap profiles for SNMP v3 users. The EMS server uses the default trap profile for SNMP v3 users.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
4. Click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. Click **Finish**.

   The system displays the new profile with a list of SNMP traps, which are grouped in the Security and Systems categories. All traps are enabled by default.

Related links

Trap descriptions on page 240
Editing an SNMP profile on page 252
Cloning an SNMP trap profile on page 252
Renaming an SNMP trap profile on page 252
Deleting an SNMP trap profile on page 253

Trap descriptions

SNMP trap is a message sent from a network device to an SNMP management system. Trap is triggered when a specific event or condition occurs on the device, such as a link going down, an authentication or a power failure.

The SNMP trap message contains information about the event or condition, such as the device and interface where the event occurred, the time the event occurred and the information related to the event.

Clear traps or alarms are not associated with all the events.

Avaya SBC sends an alarm and a trap during a system event and clears the trap and the alarm when the event is resolved. For some events, clearing the traps and alarms is not required.

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
CPU Usage	ipcsCPUUsage	ipcsCPUUsage ClearAlarm	CPU usage exceeded a set threshold.	System	Critical: CPU utilization is 100% Major: CPU utilization is over 95%	EMS SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Memory Usage	ipcsMemoryUsage	ipcsMemoryUsageClearAlarm	Memory usage exceeded a set threshold.	System	Critical: Memory utilization is 100%	EMS SBC
Disk Usage	ipcsDiskUsage	ipcsDiskUsageClearAlarm	Disk usage exceeded a set threshold.	System	Critical: Disk usage is over 90% Major: Disk usage is over 80% Minor: Disk usage is over 70%	EMS SBC
Network Failure	ipcsNetworkFailure	ipcsNetworkInterfaceClearAlarm	Network failed.	System	Critical	EMS SBC
Process Fail	ipcsProcessFail	ipcsProcessFailClearAlarm	Process in use failed.	System	Critical	EMS SBC
Database Fail	ipcsDatabaseFail	ipcsDatabaseFailClearAlarm	Database failed.	System	Critical	EMS SBC
HA Failure	ipcsHAFailure	-	High Availability failed.	System	Critical : Primary server is down Informational: Secondary server is coming to Primary server	SBC: For HA deployment mode
HA Heart Beat Failure	ipcsHAHeartBeatFailure	-	Heartbeat from secondary HA server failed.	System	Critical	SBC: For HA deployment mode
RSA Failure	ipcsRSAFailure	-	RSA algorithm failed.	System	Critical	EMS SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Incidence Notification	ipcsIncidenceNotification	-	Notification for incidence occurring in Avaya SBC.	System	No severity level is defined for this alarm.	EMS SBC
Certificate Expiry Alert	ipcsCertificateExpiryAlert	ipcsCertificateExpiryAlertClearAlarm	Certificate expiry alert.	System	Critical	EMS SBC
Network Interface M1 Alarm	ipcsNetworkInterfaceM1FaultAlarm	ipcsNetworkInterfaceM1ClearAlarm	Network Interface M1 alarm.	System	Critical	EMS SBC
Network Interface M1 Alarm	ipcsNetworkInterfaceM2FaultAlarm	ipcsNetworkInterfaceM2ClearAlarm	Network Interface M2 alarm.	System	Critical	EMS SBC
Ssyndi alarm	ipcsSsyndiFaultAlarm	ipcsSsyndiClearAlarm	Ssyndi alarm.	System	Critical	SBC
Log server alarm	ipcsLogServerFaultAlarm	ipcsLogServerClearAlarm	Log server alarm.	System	Critical	EMS SBC
OAMP Server alarm	ipcsOAMPServerFaultAlarm	ipcsOAMPServerClearAlarm	OAMP server alarm.	System	Critical	EMS SBC
Turn Controller Alarm	ipcsTurnControllerFaultAlarm	ipcsTurnControllerClearAlarm	Turn controller alarm.	System	Critical	EMS SBC
Kernel Core Alarm	ipcsKernelCoreFaultAlarm	ipcsKernelCoreClearAlarm	Kernel core alarm.	System	Critical	EMS SBC
Slapd alarm	ipcsSlapdFaultAlarm	ipcsSlapdClearAlarm	Slapd alarm.	System	Critical	EMS SBC
Nginx management alarm	ipcsNginxMgmtFaultAlarm	ipcsNginxMgmtClearAlarm	Nginx management alarm.	System	Critical	EMS SBC
Nginx data alarm	ipcsNginxDataFaultAlarm	ipcsNginxDataClearAlarm	Nginx data alarm.	System	Critical	EMS SBC
Firewall alarm	ipcsFirewallFaultAlarm	ipcsFirewallClearAlarm	Firewall alarm.	System	Critical	EMS SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Standard Sessions License Use Exceed	ipcsStdSesLicenseUseExceed	ipcsStdSesLicenseUseExceedClearAlarm	Standard sessions license usage exceeded the set threshold.	System	Critical	EMS SBC
Advanced Sessions License Use Exceed	ipcsAdvSesLicenseUseExceed	ipcsAdvSesLicenseUseExceedClearAlarm	Advanced sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Ces Proxy Sessions License Use Exceed	ipcsCesProxySesLicenseUseExceed	ipcsCesProxySesLicenseUseExceedClearAlarm	CES proxy sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Transcode Sessions License Use Exceed	ipcsTranscodeSesLicenseUseExceed	ipcsTranscodeSesLicenseUseExceedClearAlarm	Transcode sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Video Sessions License Use Exceed	ipcsVideoSesLicenseUseExceed	ipcsVideoSesLicenseUseExceedClearAlarm	Video sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Standard Concurrent Sessions Limit Exceed	ipcsStdConcurrentSesLimitExceed	ipcsStdConcurrentSesLimitExceedClearAlarm	Standard concurrent sessions limit exceeded the set threshold.	System	Critical	SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Advanced Concurrent Sessions Limit Exceed	ipcsadvConcurrentSesLimitExceed	ipcsadvConcurrentSesLimitExceedClearAlarm	Advanced concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
CESP Concurrent Sessions Limit Exceed	ipcsCESPConcurrentSesLimitExceed	ipcsCESPConcurrentSesLimitExceedClearAlarm	CESP concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Transcode Concurrent Sessions Limit Exceed	ipcsTrcdConcurrentSesLimitExceed	ipcsTrcdConcurrentSesLimitExceedClearAlarm	Transcode concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Video Concurrent Sessions Limit Exceed	ipcsVIDConcurrentSesLimitExceed	ipcsVIDConcurrentSesLimitExceedClearAlarm	Video concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Prem Sessions License Use Exceed	ipcsPremSesLicenseUseExceed	ipcsPremSesLicenseUseExceedClearAlarm	Prem sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Prem Concurrent Sessions Limit Exceed	ipcsPremConcurrentSesLimitExceed	ipcsPremConcurrentSesLimitExceedClearAlarm	Prem concurrent sessions limit exceeded the set threshold.	System	Critical	SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Standard Sessions License Acquire Failed	ipcsStdSesLicenseAcquireFailed	ipcsStdSesLicenseAcquireFailedClearAlarm	Standard sessions license acquire failed.	System	Major	SBC
Advanced Sessions License Acquire Failed	ipcsAdvSesLicenseAcquireFailed	ipcsAdvSesLicenseAcquireFailedClearAlarm	Advanced sessions license acquire failed.	System	Major	SBC
CESP Sessions License Acquire Failed	ipcsCESPSesLicenseAcquireFailed	ipcsCESPSesLicenseAcquireFailedClearAlarm	CESP sessions license acquire failed.	System	Major	SBC
Transcode Sessions License Acquire Failed	ipcsTransSesLicenseAcquireFailed	ipcsTransSesLicenseAcquireFailedClearAlarm	Transcode sessions license acquire failed.	System	Major	SBC
Video Sessions License Acquire Failed	ipcsVideoSesLicenseAcquireFailed	ipcsVideoSesLicenseAcquireFailedClearAlarm	Video sessions license acquire failed.	System	Major	SBC
Prem Sessions License Acquire Failed	ipcsPremSesLicenseAcquireFailed	ipcsPremSesLicenseAcquireFailedClearAlarm	Prem sessions license acquire failed.	System	Major	SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
AMR Session License Usage Exceed Alarm	ipcsAMRSesLicenseUseExceed	ipcsAMRSesLicenseUseExceedClearAlarm	AMR Session License Usage Exceed Alarm	System	When (Reserved licenses / Maximum licenses) is more than 60 %, minor alarm is raised When (Reserved licenses / Maximum licenses) is more than 70 %, major alarm is raised When (Reserved licenses / Maximum licenses) is more than 90 %, critical alarm is raised	SBC
AMR Concurrent Session Limit Usage Exceed	ipcsAMRConcurrentSesLimitExceed	ipcsAMRSesLicenseUseExceedClearAlarm	AMR Concurrent Session Limit Usage Exceed	System	If In use licenses are more than maximum licenses, Critical alarm is raised	SBC
AMR Session License Acquire Failed	ipcsAMRSesLicenseAcquireFailed	ipcsAMRSesLicenseAcquireFailedClearAlarm	AMR Session License Acquire Failed	System	Major	SBC
Single Source DoS	ipcsSingleSourceDoS	-	Single Source DoS.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Single Source Call Walk DoS	ipcsSingleSourceCallWalkDoS	-	Single Source Call Walk DoS.	Incidences		SBC
Phone DoS	ipcsPhoneDoS	-	Phone DoS.	Incidences		SBC
Phone Stealth DoS	ipcsPhoneStealthDoS	-	Phone Stealth DoS.	Incidences		SBC
Server DoS	ipcsServerDoS	-	Server DoS.	Incidences		SBC
Phone DDoS	ipcsPhoneDDoS	-	Phone DDoS.	Incidences		SBC
Phone Stealth DDoS	ipcsPhoneStealthDDoS	-	Phone Stealth DDoS.	Incidences		SBC
Domain DoS	ipcsDomainDoS	-	Domain DoS.	Incidences		SBC
Black List Call Blocked	ipcsBlackListCallBlocked	-	Black listed call is blocked.	Incidences		SBC
Turing Test Failed	ipcsTuringTestFailed	-	Turing test failed.	Incidences		SBC
Dropped Scrub Message	ipcsDroppedScrubMsg	-	Dropped Scrub message.	Incidences		SBC
Rejected Scrub Message	ipcsRejectedScrubMsg	-	Rejected Scrub message.	Incidences		SBC
Fingerprint Failed	ipcsFingerprintFailed	-	Fingerprint failed.	Incidences		SBC
ACK Message Out of Dialogue	ipcsACKMsgOutofDialogue	-	ACK Message out of dialogue.	Incidences		SBC
BYE Message Out of Dialogue	ipcsBYEMsgOutofDialogue	-	BYE Message is out of dialogue.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
CANCEL Message Out of Dialogue	ipcsCANCELMsgOutofDialogue	-	CANCEL Message is out of dialogue.	Incidences		SBC
NOTIFY Message Out of Dialogue	ipcsNOTIFYMsgOutofDialogue	-	NOTIFY Message is out of dialogue.	Incidences		SBC
PRACK Message Out of Dialogue	ipcsPRACKMsgOutofDialogue	-	PRACK Message is out of dialogue.	Incidences		SBC
REINVITE Message Out of Dialogue	ipcsREINVITEMsgOutofDialogue	-	REINVITE Message is out of dialogue.	Incidences		SBC
REFER Message Out of Dialogue	ipcsREFERMsgOutofDialogue	-	REFER Message is out of dialogue.	Incidences		SBC
1XX Message Out of Transaction	ipcs1XXMsgOutofTransaction	-	1XX Message out of transaction.	Incidences		SBC
2XX Message Out of Transaction	ipcs2XXMsgOutofTransaction	-	2XX Message out of transaction.	Incidences		SBC
3XX Message Out of Transaction	ipcs3XXMsgOutofTransaction	-	3XX Message out of transaction.	Incidences		SBC
4XX Message Out of Transaction	ipcs4XXMsgOutofTransaction	-	4XX Message out of transaction.	Incidences		SBC
5XX Message Out of Transaction	ipcs5XXMsgOutofTransaction	-	5XX Message out of transaction.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
6XX Message Out of Transaction	ipcs6XXMsgOutofTransaction	-	6XX Message out of transaction.	Incidences		SBC
Auth Realm Mismatch	ipcsAuthRealmMismatch	-	Authorization Realm is mismatched.	Incidences		SBC
Halo Finger Print Failed	ipcsHaloFingerPrintFailed	-	Halo Finger Print has failed.	Incidences		SBC
Call Denied	ipcsCallDenied	-	Call is denied.	Incidences		SBC
Registration Denied	ipcsRegistrationDenied	-	Registration is denied.	Incidences		SBC
Subscription Denied	ipcsSubscriptionDenied	-	Subscription is denied.	Incidences		SBC
Redirection Denied	ipcsRedirectionDenied	-	Redirection is denied.	Incidences		SBC
Message Dropped	ipcsMessageDropped	-	Message dropped.	Incidences		SBC
Routing Failure	ipcsRoutingFailure	-	Routing failed.	Incidences		SBC
Server Heartbeat	ipcsServerHeartbeat	-	Server heartbeat.	Incidences		SBC
Radius Auth Failed	ipcsRadiusAuthFailed	-	Radius authorization failed.	Incidences		SBC
Primary Radius Server Unreachable	ipcsPrimaryRadiusServerUnreachable	-	Primary Radius server is not reachable.	Incidences		SBC
Secondary Radius Server Unreachable	ipcsSecondaryRadiusServerUnreachable	-	Secondary Radius server is not reachable.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
TLS No Client Cert Present	ipcsTlsNoClientCertPresent	-	TLS no client certificate is present.	Incidences		SBC
TLS Client Cert In CRL	ipcsTlsClientCertInCRL	-	TLS client certificate in CRL.	Incidences		SBC
TLS Certificate	ipcsTlsCertificate	-	TLS certificate.	Incidences		SBC
Codec Violation	ipcsCodecViolation	-	Codec is violated.	Incidences		SBC
Packet Size Violation	ipcsPacketSizeViolation	-	Packet size is violated.	Incidences		SBC
SSRC Violation	ipcsSSRCViolation	-	SSRC is violated.	Incidences		SBC
Sequence Number Violation	ipcsSeqNoViolation	-	Sequence number is violated.	Incidences		SBC
Timestamp Violation	ipcsTimestampViolation	-	Timestamp is violated.	Incidences		SBC
Media In Activity From Both Sides	ipcsMediaInActivityFromBothSides	-	Media is in activity from both sides.	Incidences		SBC
Unsupported Media	ipcsUnsupportedMedia	-	Media is not supported.	Incidences		SBC
RTP DoS Attack	ipcsRTPDoSAttack	-	RTP DoS attack.	Incidences		SBC
RTP DDoS Attack	ipcsRTPDDoSAttack	-	RTP DDoS attack.	Incidences		SBC
RTP Injection Attack	ipcsRTPInjectionAttack	-	RTP Injection attack.	Incidences		SBC
Media Port Unavailable	ipcsMediaPortUnavailable	-	Media Port is unavailable.	Incidences		SBC
HA Graceful Failover	ipcsHAGracefulFailover	-	HA Graceful failover.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
HA Ka Fail	ipcsHAKaFail	-	HA Ka failed.	Incidences		SBC
HA Takeover Done	ipcsHATakeoverDone	-	HA Takeover is done.	Incidences		SBC
HA Oct Core Crashed	ipcsHAOctCoreCrashed	-	HA Oct Core crashed.	Incidences		SBC
HA Secondary Down	ipcsHASecondaryDown	-	HA Secondary server is down.	Incidences		SBC
HA Octeon Communication Failed	ipcsHAOcteonCommunicationFailed	-	HA Octeon Communication failed.	Incidences		SBC
SBC License Exceeded	sbcLicenseExceeded	-	SBC license exceeded a set threshold.	Incidences		SBC
SBC Turn Stun Media Relay Creation Failed	sbcTurnStunMediaRelayCreationFailed	-	SBC Turn Stun Media Relay creation failed.	Incidences		SBC
SBC Turn Stun Media Relay Deletion Failed	sbcTurnStunMediaRelayDeletionFailed	-	SBC Turn Stun Media Relay deletion failed.	Incidences		SBC
SBC Turn Stun Server Error	sbcTurnStunServerError	-	SBC Turn Stun Server error.	Incidences		SBC
SBC Ces Proxy 1xM User Login Failed	sbcCesProxy1xMUserLoginFailed	-	SBC Ces Proxy 1xM User Login Failed	Incidences		SBC
Detected Scrub Mssage	ipcsDetectedScrubMsg	-	Detected Scrub Message	Incidences		SBC

Editing an SNMP profile

About this task

You cannot edit the default SNMP trap profile. Use these steps to edit any other SNMP trap profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
4. Select the profile that you want to edit.

   You cannot edit the default SNMP profile.
5. In the content pane, click **Edit**.

   The EMS server displays an Edit Traps By Category window.
6. In the **Update Description** field, type a description of the new profile and click **Finish**.
7. Locate the category of the trap that you want to change, and click **Edit**.
8. Select or clear traps as required, and click **Finish**.

   The system displays the updated SNMP trap profile.

Cloning an SNMP trap profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
4. Click the profile that you want to clone.
5. In the content pane, click **Clone**.
6. In the **Clone Name** field, type a name for the cloned profile.
7. Click **Finish**.

Renaming an SNMP trap profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **SNMP Traps**.

The system displays the SNMP Traps Profiles screen with the existing trap profiles.

4. Click the profile that you want to rename.
5. In the content pane, click **Rename**.
6. In the **New Name** field, type a new name for the profile and click **Finish**.

Deleting an SNMP trap profile

Before you begin

Remove the SNMP trap profile from all SNMP v3 user profiles. You can delete a profile only when none of the SNMP v3 user profiles use the trap profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
4. Click the profile that you want to delete.
5. Click **Delete**.

   The EMS server displays a message to confirm whether you want to continue deleting the profile.
6. Click **OK**.

   The EMS server deletes the SNMP profile.

Enabling and disabling traps by severity

About this task

Avaya SBC supports severity-based enabling and disabling of traps only for traps generated by Avaya SBC. You cannot disable system-generated traps.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Monitoring & Logging** > **SNMP**.
4. Click the **Traps Severity Settings** tab.

   The **Traps Severity Settings** tab contains the following trap severities:

   - Critical
   - Minor
   - Major

- Informational

The tab also contains the status for each trap severity.

5. Click the status displayed against the trap severity that you want to disable.

   The EMS server displays a message to confirm whether you want to disable the trap severity.

   Note:

   When you click the current status displayed next to a trap severity, the status toggles. For example, if the EMS server displays **Enabled** against a trap severity, when you click **Enabled**, the EMS server disables all traps with that severity .

6. Click **OK**.

Time of Day (ToD) rules

With the Time of day (ToD) Rule, you can determine when the domain policy to which the rule is assigned will take effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by determining when a particular domain policy will be in effect. The ToD Rules also determine to whom the domain policy will apply, and for how long the rule will remain in effect.

Creating a new Time of Day rule

About this task

Use the following procedure to create a new Time of Day (ToD) Rule.

Caution:

A default ToD Rule set named default is provided by Avaya. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Time of Day Rules**.

   The application pane displays the existing ToD Rule sets, and the content pane displays the parameters of the ToD Rule set.

4. In the applications pane, click **Add**.

   The EMS server displays the Time of Day Rule window.

5. Enter the required information in the appropriate fields.
6. Click **Finish**.

Result

The EMS server displays the newly added Time-of-Day Rules.

Time of Day field descriptions

Name	Description
Rule Name	Specifies the name of the rule
Date	
Start Date	Specifies the day on which the ToD rule will automatically take effect. Click the Calendar icon to select the desired day.
Now	Indicates that the ToD rule is to take effect immediately.
End Date	Specifies the day on which the ToD rule will automatically end. Click the Calendar icon to select the desired day.
Never End	Indicates that the ToD rule is to remain in effect in perpetuity or until such time as an End Date is distinctly defined.
Time	
Start Time	Specifies the time on the designated day at whichthe ToD rule will take effect. Click the Show Calendar icon to select the desired start time.
All Day	Indicates that the ToD policy is to remain in effect for the entire 24-hour period.
End Time	Specifies the time on the designated day at which the rule will cease being applied. Click the Show Calendar icon to select the desired ending time.
Recurrence	
Daily, Weekly, or Monthly	Indicates when the ToD rule is to automatically be placed into effect.
Daily	Determines the interval for automatic activation: • Every Day – the ToD rule automatically takes effect at the designated time on each weekday with weekends and holidays included. • Every Weekday – the ToD rule automatically takes effect on Monday through Friday. • Every Weekend – the ToD rule automatically takes effect on Saturday and Sunday.
Weekly	Determines which weekly cycle the ToD rule is used for automatic activation. You can select every week, every other week, etc. by selecting the appropriate cycle in the **Weeks** field. Also, you can select which particular day in the designated week the ToD rule starts by selecting the appropriate check box.
Monthly	Designates the specific day of a monthly cycle on which the ToD policy will take effect.

Cloning an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Time of Day Rules**.

   The application pane displays the existing ToD Rule sets, and the content pane displays the parameters of the ToD Rule set.
4. In the application pane, select the name of the ToD Rule that you want to clone.
5. In the upper-right section of the screen, click **Clone**

   The EMS server displays the Clone Rule pop-up window.
6. Enter a name for the new ToD Rule, and select **Finish** to save your changes.

Result

The EMS server displays the ToD Rules screen again, showing the newly cloned ToD Rule.

Editing an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Time of Day Rules**.

   The application pane displays the existing ToD Rule sets, and the content pane displays the parameters of the selected ToD rule set.
4. In the application Pane, select the name of the ToD Rule set that you want to edit.

   The ToD information screen for the selected ToD rule will be displayed in the Content Area.
5. Click **Edit**.

   The EMS server displays the Edit Time of Day Rule screen.
6. Edit the appropriate fields and click **Finish** to save and exit.

Result

The EMS server displays the ToD Rules screen again.

Renaming an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Time of Day Rules**.

The application pane displays the rule sets, and the content pane displays the parameters of the selected ToD Rule set.

4. On the application Pane, select the name of the ToD Rule that you want to rename.
5. Click **Rename** in the upper-right section of the screen.

   The EMS server displays the Rename Rule pop-up window.
6. Enter the new name for the ToD Rule, and click **Finish** to save your changes .

Result

The EMS server displays the ToD Rules screen again, showing the newly-renamed ToD Rule.

Deleting an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Time of Day Rules**.

   The application pane displays the existing ToD Rule sets, and the content pane displays the parameters comprising the selected ToD Rule set.
4. In the application pane, select the name of the ToD rule that you want to delete.
5. In the upper-right section of the screen, click **Delete**.

   The EMS server displays a delete confirmation pop-up window.
6. Click **OK** to confirm the deletion.

Result

The application pane no longer displays the deleted Time of Day rule.

Routing profiles

Routing profiles define a specific set of packet routing criteria that are used with other types of domain policies. Routing profiles identify a particular call flow and ascertain which security features are applied to those packets. Parameters defined by routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Caution:

Avaya provides a default routing profile named Default. Do not edit this profile, as improper configuration might cause subsequent calls to fail.

LDAP based call routing

LDAP based call routing feature routes the SIP INVITE message from a SIP trunk in an enterprise network with multiple SIP call servers.

This feature works in the following sequence:

- Queries the Lightweight Directory Access Protocol (LDAP) server for user data.
- Avaya SBC uses that user data to route incoming calls from a SIP trunk within the enterprise network.
- On receiving SIP INVITE from SIP trunk, Avaya SBC initiates an LDAP query towards LDAP server.
- On receiving the query response from LDAP server, Avaya SBC selects next hop based on the configured routing profiles.

The communication of Avaya SBC and LDAP server supports:

- IPv4 and IPv6 addresses.
- Management interface.
- Ability to communicate with primary and alternate LDAP server. If the primary LDAP server is non-functional, then communication continues with the alternate server.
- Caching of LDAP queries and responses.
- LDAP version 3.

Load balancing

Load balancing is a trunk deployment solution. You can configure trunk or call server entities. When the SIP trunk of one location is not running, the Load balancing feature distributes the SIP traffic to available SIP servers. Distributing the SIP traffic to available SIP servers increases the system throughput and scalability. Avaya SBC supports the following methods to distribute the SIP traffic to the cluster of SIP servers:

- Priority
- Round-Robin
- Weighted Round-Robin
- DNS SRV

Before routing the SIP traffic to the available SIP servers, Avaya SBC monitors the SIP server status and uses the server status information to exclude the unavailable SIP servers. To know the available servers information and to route the SIP traffic to the available SIP servers, Avaya SBC uses the Heartbeat feature configured on the server entity. Avaya SBC uses the time-of-day policy to select the entries that must be routed from the configured routing profile. Routing Profile has two criteria: URI Group and Time of Day.

You can add up to 20 next hop entries in each routing entry to load balance the SIP traffic.

Note:

Ensure that you perform all the steps of trunk server configuration for the primary and subsequent servers listed in the load balancing configuration.

- Priority: The Request message takes first priority from the list of next hop addresses. If a message fails to reach the first next hop address, the message takes the next hop address that has second priority.
- Round-Robin: If you configure 20 next hop addresses, then Avaya SBC sends the request message in the sequence that the IP addresses are configured.
- Weighted Round-Robin: If you assign a weight for each hop address, the messages are sent based on the number of requests that each hop address can handle.
- DNS SRV: If you selected the DNS SRV mechanism option, you cannot enter more than one domain name. You can enable or disable NAPTR. The system uses the DNS priority to route the message.

Alternate routing

If Avaya SBC fails to route messages using resolved routing entry, then Avaya SBC uses the next routing entry from the routing profile.

Adding a routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, click **Add**.
5. Type a distinctive name for the new routing profile, and click **Next**.
6. Enter the requested information into the appropriate fields.

   To use alternate routing, ensure that you set the **Trans Expire** field on the **Timers** tab from **Configuration Profiles** > **Server Interworking** to an appropriate short duration. Any request sent from the server times out if a response is not received within the time set as the transaction expiration timer. Therefore, alternate routing does not work if the **Trans Expire** field is set to the default value of 32 seconds.
7. Click **Finish**.

   The application pane displays the new routing profile.

Routing profile field descriptions

Name	Description
Rule Name	Specifies the descriptive name of the routing profile
URI Group	Specifies the URI Group to which the next hop routing profile applies. The options are: • * • Emergency
Time of Day	Specifies the time of day for the trunk server to resolve the routing profile. **Note:** For remote users, do not use the **Time of Day** profile to resolve the routing profile.
Load Balancing	Specifies the type of load balancing option. The options are: • **Priority** • **Round-Robin** • **Weighted Round-Robin** • **DNS/SRV**
NAPTR	Activates or deactivates Naming Authority Pointer. When you select the Load Balancing algorithm as DNS SRV, the EMS server enables the NAPTR check box. If you disable NAPTR, you must specify the transport protocol.
Transport	Assigns the transport type for each next hop address. Select the protocol for transporting outgoing signaling packets. The options are: • **None** • **TCP** • **TLS** • **UDP** In this case, **Common Transport Type** field is unavailable. You can select the transport type according to the next hop address.
LDAP Routing	Enables LDAP based call routing.

Table continues…

Name	Description
LDAP Server Profile	Displays a collection of existing LDAP server profiles. Use this field to define the LDAP server profile for a routing profile and sends the LDAP search requests to the LDAP server. This field is available only when you select the **LDAP Routing** check box.
LDAP Base DN (Search)	Displays the configured LDAP Base DN to search the users using the LDAP server. This field is available only when you select the **LDAP Routing** check box. You must specify only one Base DN to search the user using the LDAP server.
Matched Attribute Priority	Specifies if the matched attributes based on **LDAP Base DN (Search)** will get priority. This field is available only when you select the **LDAP Routing** check box.
Alternate Routing	Enables the alternate routing for using the next routing entry if Avaya SBC fails to route messages using resolved routing entry. This field is available only when you select the **LDAP Routing** check box.
Next Hop Priority	Specifies if the Next Hop Priority option is enabled. If Avaya SBC fails to route the message using resolved routing entry from message, that is using request URI or Route Header then the system will send the message to the alternate routing entry from the routing profile.
Next Hop In-Dialog	Specifies the Next Hop configuration for the In-Dialog message. If you enable the **Next Hop In-Dialog** option, then the In-Dialog request tries to use the same routing entry to route the message. **Note:** Avaya does not recommend **Next Hop In-Dialog** option for remote worker configuration.
Ignore Router Header	Enables Avaya SBC to ignore the Route Header.
ENUM	Enables support for the E.164 Number Mapping (ENUM) protocol.
ENUM Suffix	Specifies the ENUM suffix that is added to change the number to a domain name. This field is available only when you select the ENUM check box.

Table continues…

Name	Description
Server Name Indication (SNI)	Enables support for Branch Survivability to route messages from Branch Session Manager to Session Manager.
Server name	Specifies the server name used to route messages from Branch Session Manager to Session Manager. This field is available only when you select the **Server Name Indication (SNI)** check box.
Add	Adds a next hop address.
Priority / Weight	Specifies the priority and weight assigned for load balancing options.
LDAP Search Attribute	The search attribute present in the LDAP search request. This field is available only when you select the **LDAP Routing** check box.
LDAP Search Regex Pattern	Specifies the regex pattern that is used to get the phone number from the request URI of INVITE message. This field is available only when you select the **LDAP Routing** check box.
LDAP Search Regex Result	Specifies the regex result after getting the phone number from the request URI of INVITE message. This field is available only when you select the **LDAP Routing** check box.
SIP Server Profile	Specifies the server configuration.
Next Hop Address	Specifies the IP address or domain of the Next Hop server. You can add up to 20 next hop addresses.
Transport	Assigns the transport type for each next hop address. Select the protocol for transporting outgoing signaling packets. The options are: • **None** • **TCP** • **TLS** • **UDP** In this case, **Common Transport Type** field is unavailable. You can select the transport type according to the next hop address.

Related links

[Configuring Route header based routing for NG911 calls](#) on page 184

Routing rule management

Editing a routing profile consists of managing the routing rules that the profile contains. Routing rules within a profile can be added, edited, reordered, and deleted.

Adding a routing rule

About this task

Use the following procedure to add a new routing rule to an existing routing profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, click the routing profile to which you want to add a new routing rule.
5. Click **Add** in the content area.

   The EMS server displays the Add Routing Rule pop-up window.
6. In the Add Routing Rule pop-up window, enter the desired fields and click **Finish**.

Result

The EMS server saves the new routing rule and updates the Add Routing Rule display.

Editing a routing rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, select the routing profile.
5. Click **Edit** corresponding to the routing rule that you want to edit.

   The EMS server displays the Edit Routing Rule pop-up window.
6. Edit the desired fields and click **Finish**.

Result

The EMS server saves the changes and updates the Routing Profile information.

Deleting a routing rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, select the routing profile.
5. Click **Delete** corresponding to the routing rule that you want to delete.

   The EMS server displays the delete confirmation pop-up window.
6. Click **OK**.

Result

The EMS server deletes the routing rule and updates the Routing Profile information.

Reordering routing rule precedence

About this task

Use the following procedure to reorder the precedence of Session Flows.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, select the routing profile whose routing rules you want to reorder.
5. Change the number in the **Order** column to reflect the order or precedence in which you want the routing rules to be executed.
6. Click **Update Priority**.

Result

The EMS server displays the routing rules in the content area to reflect the new order of precedence.

Cloning an existing routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.

3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules that comprise a selected routing profile.
4. In the application pane, select the routing profile you want to clone.
5. In the content pane, click **Clone**.

   The EMS server displays the Clone Profile pop-up window.
6. Provide a name for the cloned routing profile and click **Finish**.

Result

The EMS server clones the existing routing profile.

Renaming an existing routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules that comprise a selected routing profile.
4. In the application pane, select the routing profile that you want to rename.
5. In the content pane, click **Rename Profile**.

   The EMS server displays the Rename Profile pop-up window.
6. Enter a new name for the routing profile and click **Finish**.

Result

The EMS server renames the selected routing profile and updates the Routing Profile screen.

Deleting an existing routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules that comprise a selected routing profile.
4. In the application pane, select the routing profile you want to delete.
5. Click **Delete**.

   The EMS server displays the **Delete Confirmation** pop-up window.

6. To confirm the deletion of the routing profile, click **OK**.

Result

The EMS server deletes the routing profile and updates the Routing profile screen.

Syslog parameter management

Syslog is a standard for forwarding log messages in an IP network. The term syslog is often used for both the actual syslog protocol, as well as the application or library sending syslog messages.

Syslog is a client/server protocol: the syslog sender sends a small (less than 1KB) textual message to the syslog receiver. The receiver is commonly called syslogd syslog daemon or syslog server. Syslog messages can be sent through UDP or TCP or both. The data is sent in cleartext. Although not part of the syslog protocol itself, an SSL wrapper can be used to provide for a layer of encryption through SSL/TLS.

Syslog is typically used for computer system management and security auditing. While syslog has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Selecting log levels

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Monitoring & Logging** > **Syslog Management**.

   The EMS server displays the Syslog Management page.
4. In the **Facility** field, click the desired log collection facility for each class of logs and the types of information to be collected.
5. Click **Save** to save the changes.

Syslog management field descriptions

Log Level tab

Name	Description
Class	Specifies the class of the log. The options are: • Platform - Operating System related log messages like device errors, disk, and other kernel logs. • Trace - Specific to tcpdump messages captured on the system, including traceSBC application traces. • Security - Includes application log-in, logouts, and Operating System users. These logs also includes with specific application detected anomalies/threats. • Protocol - Captures HTTP/SIP and other supported protocols on the system. • Registrations - Specific to SBC application registered messages. • Audit - Recorded events related to configuration changes and audited monitoring events. • SIP Trace - Captures live SIP messages processed by Avaya SBC. You cannot enable **SIP Trace** and **GDPR** configurations simultaneously.
Facility	Specifies the log collection facility for the class of log. The options are: • LOG_LOCAL0 • LOG_LOCAL1 • LOG_LOCAL2 • LOG_LOCAL3 • LOG_LOCAL4 • LOG_LOCAL5 • LOG_LOCAL6 • LOG_LOCAL7 • LOG_DAEMON The EMS server reserves log collection facilities LOG_LOCAL5 and LOG_LOCAL6 for audit logs.
All	Selects all information levels for a log class. If you select the **All** check box in the table header, the EMS server selects all information levels for all log classes.

Table continues…

Name	Description
Info	Selects the Info information level for a log class. If you select the **Info** check box in the table header, the EMS server selects the Info level for all log classes.
Notice	Selects the Notice information level for a log class. If you select the **Notice** check box in the table header, the EMS server selects the Notice information level for all log classes.
Warning	Selects the Warning information level for a log class. If you select the **Warning** check box in the table header, the EMS server selects the Warning information level for all log classes.
Error	Selects the Error information level for a log class. If you select the **Error** check box in the table header, the EMS server selects the Error information level for all log classes.
Critical	Selects the Critical information level for a log class. If you select the **Critical** check box in the table header, the EMS server selects the Critical information level for all log classes.
Alert	Selects the Alert information level for a log class. If you select the **Alert** check box in the table header, the EMS server selects the Alert information level for all log classes.
Emergency	Selects the Emergency information level for a log class. If you select the **Emergency** check box in the table header, the EMS server selects the Emergency information level for all log classes.

Collectors tab

Name	Description
Facility	The log collection facility. The options are: • LOG_LOCAL0 • LOG_LOCAL1 • LOG_LOCAL2 • LOG_LOCAL3 • LOG_LOCAL4 • LOG_LOCAL5 • LOG_LOCAL6 • LOG_LOCAL7 • LOG_DAEMON The EMS server reserves log collection facilities LOG_LOCAL5 and LOG_LOCAL6 for audit logs.
Destination location	The path where the EMS server stores the log file for the log collection facility.

Add Collector Profile

Name	Description
Facility	The log collection facility. The options are: • LOG_LOCAL0 • LOG_LOCAL1 • LOG_LOCAL2 • LOG_LOCAL3 • LOG_LOCAL4 • LOG_LOCAL5 • LOG_LOCAL6 • LOG_LOCAL7 • LOG_DAEMON The EMS server reserves log collection facilities LOG_LOCAL5 and LOG_LOCAL6 for audit logs.

Table continues…

Name	Description
Collector Type	The type of log collector. The options are: • **File** • **Remote Syslog**
Protocol	The protocol used to save the logs. The options are: • **TCP** • **UDP** • **TLS** The **Protocol** field is available only when you select the **Remote Syslog** collector type. **Note:** **TLS** protocol is not applicable only for EMS.
TLS Profile	The TLS client profile to use when connecting to the remote Syslog server
Address	The address used by remote syslog to save the logs. The options are: • **EMS** • **Ip:port** The **Address** field is available only when you select the **Remote Syslog** collector type.

User agents (Advanced Services only)

With the User Agents function of the Global Parameters feature, you can manage the types of Avaya SBC endpoints (user agent) that are authorized to use the network. You can easily add, edit, and delete user agent types from a master global list.

Adding a new user agent (Advanced Services only)

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **User Agents**.

   The EMS server displays the User Agents page.

4. On the User Agents page, click **Add**.

   The EMS server displays the Add User Agents page.

5. Enter the required information in the appropriate fields and click **Finish**.

Example

Avaya one-X Deskphone is an example of a **Name** field entry.

Examples of Regular Expression field entries:

- Aastra.*: Matches any phone ID beginning with Aastra
- RTC/1\.1|RTC/1\.2: Matches either RTC/1.1 or RTC/1.2

Add User Agent field descriptions

Name	Description
Name	The name of the user agent.
Regular Expression	The internal ID of the user agent phone or a regular expression matching multiple phones.

Editing an existing user agent (Advanced Services only)

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **User Agents**.
4. On the User Agents page, click **Edit** corresponding to the user agent type that you want to edit.

   The EMS server displays the Edit User Agent page.

5. Edit the required fields, and click **Finish**.

Result

The EMS server displays the edited user agent.

Viewing authorized user agents (Advanced Services only)

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **User Agents**.

Result

The EMS server displays the User Agents page.

Deleting an existing user agent (Advanced Services only)

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **User Agents**.
4. On the User Agents page, click **Delete** corresponding to the user agent type that you want to delete.

   The EMS server displays a delete confirmation pop-up window.
5. Click **OK** to confirm.

Result

The EMS server deletes the user agent.

Managing device-specific settings

To complete the system configuration, two device-specific features must be defined: the Signaling Interface and the Media Interface.

Adding a new signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS server displays the Signaling Interface screen.
4. In the content pane, click **Add**.

   The EMS server displays the Add Signaling Interface pop-up window.
5. Administer the options as described in Signaling interface field descriptions on page 273.

   Note:

   Port configuration is optional. However, if the user has a data firewall then the user must synchronize the ports configured in the Avaya SBC with the ports in the data firewall. If the user has no data firewall, no action is required.
6. Click **Finish**.

   The EMS server displays the new configuration in the Signaling Interface screen.

Signaling interface field descriptions

Name	Description
Name	The name of the signaling interface.
IP Address	The network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBC used by SIP signaling messages traversing the network. Signaling interface must use the IP address gathered from the load balancer front end.
TCP Port	The port that the Avaya SBC security device processes for TCP packets.
UDP Port	The port that the Avaya SBC security device processes for UDP packets.
TLS Port	The port that the Avaya SBC security device processes for TLS packets.
TLS Profile	The TLS profile for the **TLS Port** specified above.
Enable Shared Control	OneX Client Shared control support on the Avaya SBC security device. This check box must be enabled only on the Internal Side Interface of Avaya SBC, that is, towards call server. You must enable the Avaya SBC TLS port before enabling this check box.
Shared Control Port	The port that the Avaya SBC security device processes for OneX shared control packets.

Note:

Port configuration is the choice of the user. However, if the user has a data firewall then the user must synchronize the ports configured in the Avaya SBC with the ports in the data firewall. If the user has no data firewall, no action is required.

Editing an existing signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS server displays the Signaling Interface screen.
4. In the content pane, click **Edit**.

   The EMS server displays the Edit Signaling Interface pop-up window.
5. Administer the options as described in Signaling interface field descriptions on page 273 and click **Finish**.

   The EMS server displays the edited signaling interface parameters.

Viewing an existing signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS server displays the Signaling Interface page with the configured parameters.

Deleting an existing signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS server displays the Signaling Interface screen.
4. In the content pane, click **Delete** corresponding to the Signaling Interface configuration that you want to delete.

   The EMS server displays the delete confirmation pop-up window.
5. Click **OK** to confirm.

Result

The EMS server deletes the Signaling Interface configuration.

Adding a new media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface screen.
4. In the content pane, click **Add**.

   The EMS server displays the Add Media Interface pop-up window.
5. Enter the requested information in the appropriate fields and click **Finish**.

Result

The EMS server displays the new configuration in the Media Interface display.

Add media interface field descriptions

Name	Description
Name	The name of the media interface.
IP Address	The network name, identified by the associated interface name and VLAN tag, and IP address of the Avaya SBC to which media packets are sent.
Port Range	The range of ports on the Avaya SBC security device allocated to media traffic.
TLS Profile	The TLS profile that the media interface uses for tunneled calls.. **Note:** The **TLS Profile** field is visible only if you click **Media Tunneling** feature in **Network & Flows** > **Advanced Options** > **Feature Control**.
Buffer Size	The maximum size of video frames that Avaya SBC stores on its network buffer. For example, if the **Buffer size** is set to 400 KB, then Avaya SBC can store approximately a 6 second video in a congested network. **Note:** The **Buffer Size** field is visible only if you click **Media Tunneling** feature in **Network & Flows** > **Advanced Options** > **Feature Control**.

Note:

Port configuration is the choice of the user. However, if the user has a data firewall, then the user must synchronize the ports configured in Avaya SBC with the ports in the data firewall.

Editing an existing media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface screen.
4. In the content pane, click **Edit**.

   The EMS server displays the Edit Media Interface pop-up window.
5. Edit the required fields, and click **Finish**.

Result

The EMS server displays the edited media interface parameters.

Viewing an existing media interface

About this task

Use the following procedures to view media interface parameters.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface parameters.

Deleting media interface

Procedure

1. From the **Device** menu, click the **SBC** name to administer.
2. Navigate to **Network & Flows** > **Media Interface**.

   You see the Media Interface list.
3. In the content pane, click **Delete** on the respective media interface.

   You see the delete confirmation pop-up window.
4. Click **OK** to confirm.

Result

The EMS server deletes the media interface.

AAA field descriptions

RADIUS Server Authentication

Name	Description
Enabled	A check box indicating whether the RADIUS user accounts must be authenticated using Authentication, Authorization, and Accounting (AAA). If selected, RADIUS user accounts are authenticated by the server selected from the **Radius Server** option. If cleared, RADIUS user accounts are not authenticated.
RADIUS Server	Select the RADIUS server being used for AAA.

Table continues…

Name	Description
RADIUS Authentication Protocol	A drop-down menu containing all supported RADIUS authentication methods. This menu is used instead of the authentication protocol of the configured RADIUS profile. The currently supported methods are: • **Password Authentication Protocol (PAP)**: The password is transmitted in plain text to the RADIUS server. • **RFC 5090/Digest**: The password uses a client and server one time to generate an MD5 authentication token for use with an RFC 5090–compliant RADIUS server. • **Challenge-Handshake Authentication Protocol (CHAP)**: The password is salted with a rolling ID, hashed, and transmitted to the RADIUS server.
RADIUS Realm	The realm to use when generating the Digest authentication token. Use the same value in this field as the value configured on the RADIUS server.
Use RADIUS as Fall-through Authenticator	Select this option to enable a back end authentication server to handle any authentication requests for users that are not defined in the EMS user list. This is done by sending an Access-Request packet to the RADIUS server, which looks for a specific attribute in the Access-Accept response as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or the authorization fails and the user login request is rejected. If the attribute is not present in the request, the authorization fails and the user login request is rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both RADIUS authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.

Table continues…

Name	Description

Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”.
	
	If you are using attributes that are defined in the standard RADIUS dictionary, you can use the standard dictionary and a custom dictionary is not required.
	
	However, if you are using the default attribute name “Avaya-SBCE-Role-Name”, or are using a vendor-specific attribute as the role attribute name, you must create a custom dictionary definition. A custom dictionary is required to handle the attribute the Avaya SBC requires for authorization. A sample dictionary is provided below, which can be modified with any values if necessary. If a different RADIUS attribute is desired, then any attribute can be used including both default values and custom values.
	
	Note:
	
	There might be scenarios when a custom dictionary is required to define a new attribute that Avaya SBC administration can recognize, or to handle conflicts if a RADIUS server is already using an existing Avaya dictionary. In this scenario, Avaya SBC administration will read from a file located at `/usr/local/ipcs/etc/gui-radius-dictionary`, if it exists. It is important to note that defining this file will prevent Avaya SBC administration from reading the default dictionary and instead use the contents of the file as the new dictionary.
	
	`############################################################`
	`# WARNING: This dictionary file is intended to be a sample and`
	`# is intended to illustrate how to define attributes for use with`
	`# the Avaya SBCE SSO fall-through authentication functionality.`
	`# The identifiers in this file have not been officially allocated`
	`# and may need modification to interop with other vendor specific`
	`# attributes from Avaya or other vendors.`
	`############################################################`
	`VENDOR Avaya-SBCE 6889`
	`BEGIN-VENDOR Avaya-SBCE`
	
	`ATTRIBUTE Avaya-SBCE-Role-Name 1 string`
	
	`END-VENDOR Avaya-SBCE`

LDAP Server Authentication

Name	Description
Enabled	Controls whether LDAP authentication is enabled.
Primary Server Address	The IP address and optional port of the primary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.
Secondary Server Address	(Optional) The IP address and optional port of the secondary LDAP server. If no port is specified, the default port is used. The default ports are 389 for non-secure/STARTTLS and 636 for SSL/TLS.

Table continues…

Name	Description
Secure Mode	Select one of the following options: • **None**: No encryption (not recommended) • **SSL/TLS**: Secure connection established via TLS handshake (highly recommended) • **STARTTLS**: Secure connection established by unsecure connection and upgrading to secure connection (for legacy support, not recommended)
CA Certificate PEM File	The path to the Privacy Enhanced Mail (PEM) file on the EMS server that contains trust anchors for the certificate when connecting with SSL or TLS. You must create this file and put it on the EMS server. If a path is not specified, use the default path of: `/usr/local/ipcs/etc/cert/gui/ldap-auth.pem`. If a path is specified and the PEM file does exist, it is used to build a trust manager that is in turn used to verify the LDAP server certificate upon connection. If at least one certificate matches a CA certificate in the trust manager, the verification succeeds. Otherwise, the verification fails and the connection attempt fails. If a path is specified but the PEM file does not exist, all certificates are trusted. That is, no certificate verification is done on the LDAP server and all certificates are accepted.
Bind DN	The distinguished name (DN) used when initially authenticating to the LDAP server to do a user lookup. This user name must have appropriate permissions to search and read users that need to authenticate.
Bind Password	The password to send with the Bind DN when initially authenticating to the LDAP server.
Base DN	The base DN to use when searching for users.
User Domain	(Optional) An optional domain to use in LDAP searches.
User Search Filter	A filter used to search for an LDAP user. Only the first entry that matches is retrieved, so this filter should be as specific as possible. The {username} and {domain} can be used as placeholders for the actual values when authentication takes place. If no domain is specified, the filter defaults to `(sAMAccountName={username})`. If a domain is specified, the filter defaults to `(userPrincipalName={username}@{domain})`.
Timeout	The timeout, in seconds, before a connection attempt to the primary LDAP server is marked as failed and the next connection attempt is made (if a secondary LDAP server exists).

Table continues…

Name	Description
Use LDAP as Fall-through Authenticator	Select this option to enable a back end authentication server to handle authentication requests for users that are not defined in the EMS user list. This is done by fetching a specified LDAP attribute when running the User Search Filter on the LDAP server to find a user matching the provided credentials as defined in the **Role Name Attribute** option. If the attribute is present, it must match a predefined role in the EMS (that is, System Administrator, Security Administrator, and so on) or any authorization attempts for the user will fail and the user's login requests will be rejected. If the attribute is not present on the user, any authorization attempts for the user fail and the user's login requests are rejected. Disabling fall-through authentication will log out all users logged in using that functionality. A new option has been added to the user's list to forcibly log out any logged in user. This option is only available to users with System Administrator level privileges. **Note:** When using both LDAP authentication and X.509 certificate authentication at the same time, X.509 certificate support will only work if the X.509 **Authentication Mode** option is set to **Require X.509 Certificate and Password**. Any other option will fail in the authorization stage and reject the login request.
Role Name Attribute	Enter a name you want to use as the role name attribute. By default, **Role Name Attribute** is set to “Avaya-SBCE-Role-Name”. This attribute is not defined in most LDAP schemas and must be defined to function correctly. Alternatively, any other LDAP attribute can be used as long as it is a string value. For an example of how to define a custom attribute in Microsoft Active Directory, see: https://social.technet.microsoft.com/wiki/contents/articles/20319.how-to-create-a-custom-attribute-in-active-directory.aspx

X.509 Server Authentication

Name	Description
Enabled	Controls whether X.509 certificate authentication is enabled. X.509 certificate authentication cannot be enabled unless the CA Trust Anchors Privacy Enhanced Mail (PEM) file exists on the file system.
CA Trust Anchors PEM File	This is a PEM file that should contain all CA trust anchors used to verify X.509 certificates. Multiple entries should be concatenated together.

Table continues…

Name	Description
CA Intermediaries PEM File	This is a PEM file that should contain all intermediate CAs used to construct trust chains used to validate certificates. These certificates are not implicitly trusted and are only used in reconstructing the trust chain. Multiple entries should be concatenated together.
CRL File	This is a PEM file that should contain all certificate revocation lists used to revoke X.509 certificates. Multiple entries should be concatenated together.
Authentication Mode	The method used to authenticate X.509 certificate users. Select one of the following options: • **Accept X.509 Certificate or Password**: The user will be authenticated if either a valid certificate or a valid password is provided. • **Require X.509 Certificate**: The user will be authenticated only if a valid certificate is provided. Any password entered by the user is ignored. • **Require X.509 Certificate and Password**: The user will be authenticated only if both a valid certificate and valid password is provided.

RADIUS Server

Name	Description
Server Name	A descriptive name to identify the RADIUS server.
Primary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Secondary Address (ip:port)	The IP address and port number of the server designated as the secondary RADIUS server.
Retry Timeout (seconds)	The maximum time in seconds taken for a successful authentication to be completed. If authentication is not completed within this time, SBC ends the connection automatically and generates an incident .
Max Retry	The maximum number of times that a user can attempt to authenticate before SBC ends the connection .

Table continues…

Name	Description
Ignore Session Expire	The check box that indicates whether the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Select this check box for Avaya SBC to maintain the current session upon receipt of the SESSION EXPIRE message. Clear the check box for Avaya SBC to end the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method that the Avaya SBC security device uses to select a RADIUS server to choose to authenticate a user. The options are: • **Active Standby** • **Round Robin**
Authentication Protocol	The authentication protocol to be used for RADIUS authentication. The options are: • **None** • **EAP_TTLS/EAP_ PAP** • **EAP_PEAP/EAP_GTC**
Server Secret	The shared secret maintained between the Avaya SBC security device and the active RADIUS server with which communications between the two is encrypted.
Confirm Server Secret	Respecifies the shared secret maintained between the Avaya SBC security device and the active RADIUS server .
Accounting Server	The check box to indicate whether this RADIUS server must also to be designated as an Accounting Server and receive CDRs. Select this check box to indicate that RADIUS server is also an Accounting Server and can receive CDRs. Clear the check box to indicate that RADIUS server is not an Accounting Server and does not receive CDRs.

Automatic blacklisting of network source IP

Overview

Automatic blacklisting of network source IP is a safety feature that filters out offending/attack source IP addresses from accessing your networks. The system maintains a list of IP addresses and URIs that do not meet the set policies. The list contains blocked IP/URIs and the IPs subnets that must be blocked.

Blacklisting of an IP/URI is based on the following policies:

- If the number of attempts to log in using an invalid username or password within a configured timer limit exceeds the configured threshold value.

  Note:

  If the IP Threshold timer is not configured, the system blacklists a user based on the number of failed login attempts irrespective of the time value.

- If the attack is from a trusted source and the number of attempts exceeds the configured threshold value. In this case, SBC considers To header URI to validate the invalid username or password.

  Note:

  IP and URI blacklisting features are applicable only to new registrations. It is not applicable after renewing the registration.

  Configure the trusted source in:

  - The **Trusted address** field on the Subscriber Flow Profile page.
  - The **IP / URI Blocklist Trusted Address** field in the Reverse proxy tab on the Relay page.

After the system exceeds the configured threshold values, adds entry to DB with block time, an Incidence/Syslog is raised. It can also propagate the information to other SBCs in a given EMS.

The system maintains the blacklisted source IP/URI with the latest timestamp in IP/URI blocklist section. Use this section to unblock an IP/URI, block an IP subnet, permanently block an IP/URI and to propagate information to other Avaya SBCs in a given EMS (This option would show when an EMS is managing multiple Avaya SBCs or Avaya SBC pairs).

Note:

The threshold value is reset after every successful registration.

Creating IP/URI blocklist profile

About this task

You can use this procedure to create an IP/URI blocklist profile that shows the list of blocked IPs or URIs. The IP/URI blocklist profile maintains the list of IP/URIs that fails to comply with the blocklisting policies.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Device** > **SBC**.

   The EMS server displays the SBC options in the navigation pane.
3. Navigate to **Configuration Profiles** > **IP/URI Blocklist Profile**.

   In the content pane, you see the IP / URI Blocklist Profiles.
4. Click **Add**, to create a new blocklist profile.

   The system displays **IP/URI Blocklist Profile** window.
5. In the **Rule Name** field, enter the profile name.
6. Click **Next**.

   You see a window to set the threshold values for the profile.
7. Enter the threshold value for IP Username in the **IP Username Threshold** field.
8. Enter the threshold value for IP Password in the **IP Password Threshold** field.
9. Enter the threshold value for IP Threshold Timer in the **IP Threshold Timer** field.
10. Enter the threshold value for URI Username in the **URI Username Threshold** field.
11. Enter the threshold value for URI Password in the **URI Password Threshold** field.

    Note:

    The threshold value must be between 3 and 10.
12. Enter the threshold value for URI Threshold Timer in the **URI Threshold Timer** field.
13. Enter the number of minutes in the **Block Timer** field.

    Note:

    Keep the field blank to ensure that the profile never expires.
14. Click **Finish**.

Blocking a subnet

About this task

Blocking a subnet can enhance routing efficiency, network management control, and improve network security. Use this procedure to block a subnet.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.

   You see **IP/URI Blocklist** page with a list of all blocked IPs and URIs.

3. Find the IP to block the subnet.
4. Click **Block Subnet**.

   You see a dialog box.
5. Enter the network prefix of the subnet to block.
6. Click **Ok** to block the subnet.

Unblocking IP/URI address

About this task

Use this procedure to unblock an IP/URI address.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.

   You see the **IP/URI Blocklist** page with a list of all blocked IPs and URIs.
3. Select the IP or URI to unblock.
4. Click **Unblock**.

   The system displays a dialog box.
5. Click **Ok** to unblock.

Blocking an IP/URI permanently

About this task

Use this procedure to permanently block an IP/URI address.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.

   You see the **IP/URI Blocklist** page with a list of blocked IPs and URIs.
3. Select the IP or URI to block permanently.
4. Click **Block Permanently**.

   You see a dialog box.
5. Click **Ok** to block the IP/URI permanently.

Propagating information to other Avaya SBCs

About this task

Use this procedure to propagate information to other Avaya SBCs managed by the EMS.

Note:

You can view the **Propagate To** option only when the EMS manages other Avaya SBCs.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.
3. Click **Propagate To**.

Tenant configuration

For Cloud solutions that deploy MS Teams, you must create a customer tenant configuration profile to generate telemetry reports for the customer.

To enable accurate reporting for customers, Avaya SBC adds the following custom header in the SIP messages to MS Teams:

```
Variable name: X-MS-Partner
Value format: <partner TenantID>/<version>/<customer TenantID>
```

Note:

Currently, you can create only one tenant configuration profile.

After you create a tenant configuration profile, you must add it to the server flow created for MS Teams.

Creating the tenant configuration profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Tenant Configuration**.
4. In the application pane, click **Add**.
5. Enter the values in the fields, and click **Finish**.

   For more information about the fields, see Tenant Configuration field descriptions on page 287.

Result

The application pane displays the newly created tenant configuration profile, and the content pane displays the parameters for the tenant configuration profile.

Next steps

To generate telemetry reports after you create a tenant configuration profile, you must configure the **Tenant Configuration Profile** field of the server flow created for MS Teams. For more information, see Editing an existing server flow on page 171.

Tenant Configuration field descriptions

Name	Description
Partner ID	Specifies the partner tenant ID.
Customer ID	Specifies the customer tenant ID.
Customer Name	Specifies the customer name you have assigned.
Version	Specifies the current version of Avaya SBC.

Editing the tenant configuration profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Tenant Configuration**.
4. Under the Tenant Configuration parameters, click **Edit**.
5. Make the appropriate edits, and click **Finish**.

Result

The application pane displays the newly edited tenant configuration profile.

Renaming the tenant configuration profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Tenant Configuration**.
4. At the top-right corner of the Tenant Configuration parameters, click **Rename**.
5. In the Rename profile screen, in the **New Name** field, enter a new name for the profile.
6. Click **Finish**.

Result

The application pane displays the renamed tenant configuration profile.

Deleting the tenant configuration profile

Before you begin

Ensure to remove any associations to the tenant configuration profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Tenant Configuration**.
4. On the top-right corner of the Tenant Configuration parameters, click **Delete**.
5. Click **OK** to confirm.

Result

The application pane no longer displays the deleted tenant configuration profile.

Chapter 7: Security configuration

Security configuration overview

From the EMS web interface, you can view various security-related features of Avaya SBC security products, such as configuring Denial-of-Service (DoS) policies. The DoS settings relate to:

- SIP endpoints
- Aggregate domains
- DoS activity profiling for each user-definable time period

Note:

Avaya SBC does not officially support the registration of third-party SIP endpoints. When used in combination with Avaya applications such as Avaya Oceana®, Avaya Meetings Server, or Avaya Equinox® Meetings Online, Avaya SBC does not support third-party SIP endpoints unless validated by these Avaya offers or applications.

Related links

Creating a Topology Hiding profile on page 302

System wide single endpoint DoS configurations

System wide single endpoint DoS configurations are available on the DoS / Domain DoS (DDoS) page to configure DoS settings for system wide SIP endpoints.

Domain DoS configurations

Domain DoS configurations are available on the Domain DoS page to create a DoS profile for particular aggregate domains. After a profile is created, the profile is applied to aggregate domains using **Security Rules**.

SIP server DoS configuration

SIP server DoS configurations are available on the Server Configuration page to configure DoS security settings for particular SIP servers. Guidance for DoS thresholds for SIP servers is available on the DoS Learning page. DoS thresholds enable DoS activity profiling for each user-definable time period. These thresholds are applied to DoS configuration for SIP servers.

For more information about DoS configurations, see DoS Security Features on page 290.

DoS Security features

With the DoS Security feature of the EMS web interface, you can view and edit a wide variety of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attack response and control parameters that can be applied either to individual SIP endpoints or the parent domain.

Note:

Avaya SBC uses from header to block the source.

Note:

The threshold settings for each DoS/DDoS attack protection security features defined here apply globally to all Avaya SBC devices in the network. These settings only define the thresholds and not the activation of these security features.

The enabling or disabling of one or more of these DoS/DDoS attack protection security features is done uniquely for each individual Avaya SBC device within the network by selecting: **Network & Flows** > **Advanced Options** > **Feature Control**.

For more information, see the *Security Configuration and Best Practices Guide*.

Viewing DoS/DDoS settings

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **DoS / DDoS**.

   The DoS Settings page displays the **Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Whitelist** tabs.
4. Select the tab containing the DoS/DDoS settings that you want to view.

   The content area displays the selected settings.

Related links

DoS/DDoS attack type descriptions on page 290

DoS/DDoS attack type descriptions

DoS attack type	Description
Single Source DoS	An attack that is directed to one or more enterprise endpoints that originate from a single source. The source is normally spoofed.
Phone DoS/DDoS	An attack that is directed to a single enterprise endpoint.
Stealth DoS/DDoS	A low-volume attack that is directed to an endpoint where the source of the call is constantly changed.
Call Walking	An attack in which serial calls originating from a single source are directed to a sequential group of endpoints. The source is normally spoofed.

Table continues…

DoS attack type	Description
Whitelist	A list of URIs administered in the Whitelist URI group. All URIs in the Whitelist URI group will be whitelisted for the Single Source, Phone, Call Walk, Stealth, and Call Walking DoS/DDoS modules. Anomalies will not be detected and no action is taken for SIP messages that match the Whitelisted URI group configuration.

DoS / DDoS Global Parameters field descriptions

Single Source DoS tab

Name	Description
SIP Method	The SIP method displayed on this page, which is the same as the services on the Domain DoS screen. For example, All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or OPTIONS.
Threshold (over 5 seconds)	The maximum number of sessions that can be started within 5 seconds.
Action	The action to be performed when any threshold is exceeded. The options are: • **Alert Only**: An alert that displays the DoS incident but the call is not blocked. • **Block**: The call is blocked. • **SIP Challenge**: Authentication is initiated. **Note:** You must not select the SIP Challenge action for a DoS profile configuration. Avaya phones do not respond when they are authenticated by Avaya after being challenged by Avaya SBC.

Phone DoS/DDoS tab

Name	Description
SIP Service	The SIP service affected by the DoS attack. The options are: • **TOTAL** • **Registrations** • **Calls** • **Presence Updates** • **Subscriptions** • **Misc**
SIP Method	The SIP method displayed on this page, which is the same as the services on the Domain DoS screen. For example, All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or OPTIONS.

Table continues…

Name	Description
Threshold (over 3 seconds)	The maximum number of sessions that can be started within 3 seconds.
Action	The action to be performed when any threshold is exceeded. The options are: • **Alert Only**: An alert that displays the DoS incident but the call is not blocked. • **Block**: The call is blocked. • **Enforce Limits**: The call is not blocked until the specified limit is reached. • **SIP Challenge**: Authentication is initiated. **Note:** You must not select the SIP Challenge action for a DoS profile configuration. Avaya phones do not respond when they are authenticated by Avaya after being challenged by Avaya SBC.

Stealth DoS/DDoS tab

Name	Description
Timeslot	The time slots in which DoS attacks are monitored. The options are: • **Morning (0600–1159)** • **Afternoon (1200–1759)** • **Evening (1800–2359)** • **Night (0000–0559)**
SIP Service	The SIP service affected by the DoS attack.
SIP Method	The SIP method displayed on this page, which is the same as the services on the Domain DoS screen. For example, All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or OPTIONS.
Average Inter-Call Duration Threshold (in seconds)	The number of seconds between calls.
Consecutive Average Inter-Call Duration Threshold Violations	The number of permissible consecutive violations of the Average Inter-Call Duration threshold.

Table continues…

Name	Description
Action	The action to be performed when any threshold is exceeded. The options are : • **Alert Only**: An alert that displays the DoS incident but the call is not blocked. • **Block**: The call is blocked. • **SIP Challenge**: Authentication is initiated. **Note:** You must not select the SIP Challenge action for a DoS profile configuration. Avaya phones do not respond when they are authenticated by Avaya after being challenged by Avaya SBC.

Call Walking tab

Name	Description
SIP Service	The SIP service affected by the DoS attack.
SIP Method	The SIP method displayed on this page, which is the same as the services on the Domain DoS screen. For example, All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or OPTIONS.
Destinations (per minute)	The number of destinations from which calls are received per minute.
Action	The action performed when any threshold is exceeded. The options are: • **Alert Only**: An alert that displays the DoS incident but the call is not blocked. • **Block**: The call is blocked. • **SIP Challenge**: Authentication is initiated.. **Note:** You must not select the SIP Challenge action for a DoS profile configuration. Avaya phones do not respond when they are authenticated by Avaya after being challenged by Avaya SBC.

Whitelist tab

Name	Description
Whitelist URI Group	The whitelisted URI group.

Editing DoS/DDoS settings

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the navigation pane, click **System Parameters** > **DoS / DDoS**.

   The EMS server displays the DoS Settings screen.
4. Select the tab containing the DoS/DDoS settings that you want to edit.

   The content area displays the selected DoS/DDoS settings.
5. Click the **Edit** icon corresponding to the DoS/DDoS settings that you want to edit.
6. Perform one of the following actions:
   - Edit the fields, and click **Finish**.
   - Click **Cancel**. The EMS server restores the fields to the previous values and closes the window without saving.

Domain DoS profiles

With Domain DoS profiles, you can rate limit a number of SIP-specific services to ensure the availability of VoIP network resources. You can view, add, clone, edit, and delete Domain DoS profiles.

Adding a new Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Domain DoS**.
4. Click **Add**.

   The EMS server displays the Add Domain DoS window.
5. Enter the required information in the appropriate fields and click **Finish**.

Result

The EMS server saves the new Domain DoS profile and displays the Domain DoS screen.

Domain DoS profile field descriptions

Domain DoS screen

Name	Description
Traffic Type	The type of traffic.
Max Concurrent Sessions	Maximum number of concurrent sessions
Number of Remote Users	Number of remote users for the DoS profile

Table continues…

Name	Description
SIP Service	SIP service affected by the DoS attack. The options are: • **TOTAL** • **Registrations** • **Calls** • **Presence Updates** • **Subscriptions** • **Misc**
SIP Method	The SIP Methodfor the DoS profile. The options are: • **ALL** • **REGISTER** • **INVITE** • **SUBSCRIBE** • **PUBLISH** • **OPTIONS**
Initiated Threshold (per 10 seconds)	The maximum number of sessions that can be started within a 10 second period.
Pending Threshold	The maximum number of pending session initiations.
Failed Threshold (per 10 seconds)	Maximum number of failed session initiations.
Action	The action to be performed should any of the above thresholds be exceeded. The options are : • **Alert Only**: An alert that displays the DoS incident but the call is not blocked. • **Enforce Limit**: The call is not blocked until the specified limit is reached. • **Enforce Limit Response**: The call is blocked and the system sends the specified response when the specified limit is reached. • **SIP Challenge:** Initiate Authentication **Note:** The SIP Challenge action should not be selected for a DoS profile configuration because Avayaphones do not respond the second time when they are again authenticated by Avaya after being challenged by Avaya SBC. • **Whitelist**: If the call originator exists in the Whitelist, do not block the call.

Add Domain DoS screen

Name	Description
Profile Name	Name of the DoS profile
Traffic Type	Type of traffic. The options are:Trunk Traffic, Remote Users, Trunk Traffic and Remote Users • **Trunk Traffic** • **Remote Users** • **Trunk Traffic and Remote Users**
Max Concurrent Sessions	Maximum number of concurrent sessions
Number of Remote Users	Number of remote users for the DoS profile

Viewing a Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Domain DoS**.

   The Domain DoS screen displays a list of available Domain DoS profiles in the application pane. The content area displays the rate limited SIP services and the corresponding thresholds.
4. Select the Domain DoS profile you want to view.

   The content area displays the Rate Limit parameters corresponding to the selected Domain DoS profile.

Cloning an existing Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Domain DoS**.
4. In the application pane, click the Domain DoS profile you want to clone.
5. Click **Clone**.

   The EMS server displays the Clone Domain DoS window
6. In the **New Name** field, type a name for the cloned profile and click **Finish**.

Result

The EMS server saves the cloned Domain DoS profile and displays the Domain DoS screen.

Renaming an existing Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Domain DoS**.
4. Click the Domain DoS profile that you want to rename.
5. Click **Rename**.

   The EMS server displays the Rename Domain DoS window.
6. In the **New Name** field, type a new name for the profile and click **Finish**.

Result

The EMS server saves the new name and displays the Domain DoS screen.

Editing an existing Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. IIn the navigation pane, click **Configuration Profiles** > **Domain DoS**.
4. Click the Domain DoS profile that you want to edit.
5. In the **Rate Limit** tab, navigate to the SIP service or method that you want to edit and click **Edit**.
6. In the Edit Domain DoS window, edit the required fields.
7. Perform one of the following actions.
   - To save your changes, click **Finish**.
   - To return the fields to their previous values and close the window without saving, click **Cancel**.

Related links

Domain DoS profile field descriptions on page 294

Deleting a Domain DoS profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Domain DoS**.
4. Click the Domain DoS profile that you want to delete.

5. Click **Delete**.

   The EMS server displays a confirmation window to confirm your selection.

6. Click **OK** to confirm.

Result

The EMS server deleted the selected Domain DoS profile.

Setting learned DoS parameters

About this task

The EMS can learn or gather, save, and report the historical traffic activity towards the server occurring in a particular Avaya SBC device deployed in the network. Use the following procedure to define time-of-week and time-of-day parameters using EMS to save and report historical traffic activity.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Select the Avaya SBC security device whose DoS activity you want to learn.
4. In the navigation pane, click **Monitoring & Logging** > **DoS Learning**.

   The EMS server displays the Learned Information screen with a list of installed Avaya SBC devices.

5. In the **Learned Information** tab, select the time period for which you want to learn the DoS activity.
6. Select **Update**.

Result

The **Learned Information** tab displays the DoS activity detected for the specified time period.

Related links

DoS Learning field descriptions on page 298

DoS Learning field descriptions

Name	Description
SIP Service	The SIP service for which DoS data is displayed.
SIP Method	The SIP method of the SIP service.
Initiated Count (per 10 seconds)	The number of SIP requests initiated for the SIP method in every 10 seconds.

Table continues…

Name	Description
Pending Count	The number of pending requests.
Failed Count (per 10 seconds)	The number of failed SIP requests in every 10 seconds.

In addition to these fields, the **Learned Information** tab has two fields for selecting Weekend or Weekday, and the Time: Morning, Afternoon, Evening, or Night. When you select a day and time in these fields, and click **Update**, the system displays learned information for the selected day and time.

Related links

Setting learned DoS parameters on page 298

Protocol scrubber

Protocol Scrubbing utilizes a statistical mechanism to check incoming SIP signaling messages for protocol-specific events and anomalies.

Protocol scrubbing verifies message attributes against customizable templates obtained from Avaya, such as proper message formatting, message sequence, field length, and content.

- The protocol scrubber templates dictate the security rules and drop the messages that violate them.
- The protocol scrubber either rewrites, truncates, rejects, or drops messages that violate syntax rules. The processing rules imposed by the templates determine how the messages are repaired.

Note:

Avaya prepares the Protocol Scrubbing rule templates. Users can make minimal edits to these templates.

With the Protocol Scrubbing feature for SIP, you can do the following:

- Install a scrubber rules package.
- Enable or disable the scrubber rules defined in the package.
- Delete the package from the EMS server.
- View a list of all installed scrubber rules.

Scrubber package file path

The latest Scrubber packages are present in the following directory in the EMS: `/usr/local/scrubber`.

You must remove the old Scrubber package, and install the new package. See Deleting an Existing Scrubber Rules Package on page 301 and Installing a scrubber rules Package on page 300 respectively.

Viewing scrubber rules

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **Scrubber**.

   The EMS server displays the Scrubber screen.
4. Click the **Rules** tab.

   The EMS server displays all the installed scrubber rules and templates.

Installing a scrubber rules package

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **Scrubber**.
4. Click the **Packages** tab.
5. Click **Install Package**.

   The EMS server displays the Install Scrubber Package window.
6. Click **Browse** and navigate to the directory that contains the scrubber package.
7. Select the scrubber package.
8. Click **Install**.

Related links

Security rules on page 120

Enabling or disabling an installed scrubber rules package

The Security Rules require a list of scrubber rule packages after you enable the scrubber in the Security Rules of Domain Policies.

Before you begin

Ensure that the scrubber rules package is installed.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **Scrubber**.
4. Click the **Packages** tab.

5. From the content area, click the **Toggle** button to enable or disable the scrubber rules package.

Deleting a Scrubber Rules package

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **Scrubber**.
4. Click the **Packages** tab.
5. In the content area, click **Delete** corresponding to the scrubber package that you want to delete.

   The EMS server displays a delete confirmation pop-up window.
6. Click **OK** to confirm.

Result

The EMS server deleted the selected scrubber package.

Configuring scrubber actions

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **System Parameters** > **Scrubber**.
4. On the **Rules** tab, select a package and click **Edit**.
5. In the **Action** field, select one of the following:
   - Allow: No action is taken and continues message processing.
   - Alert: Creates an incident and continues message processing.
   - Block: Drops the message.
   - Reject: Rejects the message with a 400 Bad Request response.

Scrubber field descriptions

Packages tab

Name	Description
Package Name	The name of the scrubber package.
Description	The description of the scrubber package.
Release Date	The date on which the scrubber package was released

Table continues…

Name	Description
Status	The current status of the scrubber package. You can click the **Toggle** link to change the status of the scrubber package.

Rules tab

Name	Description
Package Name	The name of the scrubber package.
Rule Name	The name of the rule in the scrubber package.
Description	The description of the rule.
Method	The method affected by the scrubber rule.
Header	The header affected by the scrubber rule.
Action	The action taken by the scrubber rule.
Status	The current status of the rule.

Topology Hiding

Creating a Topology Hiding profile

About this task

Topology Hiding masks the FQDN or IP address portion of SIP headers. For example, SBC@avaya.com can become SBC@135.122.18.7, or just the opposite. Though changing the headers can mask the internal topology, the headers can be adapted into the format that the recipient requires. All SIP Service Providers require the domain to be expressed as an IP address, but some connections can use an FQDN.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.
4. Click **Add**.

   The EMS server displays the Topology Hiding Profile screen.
5. Administer the options as described in Topology Hiding Profiles field descriptions on page 303.
6. Click **Finish**.

The EMS server saves the data and displays the new profile in the application pane.

Related links

Protocol scrubber on page 299

Topology Hiding Profiles field descriptions

Name	Description
Profile Name	A descriptive name for the new topology hiding profile.
Header	The name of the header that will be changed with topology hiding. The options are: • **Request—Line** • **From** • **To** • **Record-Route** • **Via** • **SDP** • **Refer-To** • **Referred-By**
Criteria	The criteria that are changed with topology hiding. The options are: • **IP/Domain** • **IP** • **Domain** **Note:** Ensure that the values in the **Header** field and the **Criteria** field with topology hiding are same. For example, if you are not sure about the value of the **Header** field, configure the **Criteria** field with topology hiding as **IP/Domain**. If the **Header** is: • **IP** : Configure the **Criteria** field with topology hiding as IP. • **Domain** : Configure the **Criteria** field with topology hiding as Domain.

Table continues…

Name	Description
Replace Action	The data that replaces the header. The options are: • **Auto** • **Next Hop** • **Destination IP** • **Overwrite**
Overwrite Value	The value that overwrites the header. This field is available only when you select **Overwrite Replace Action**.

Renaming a Topology Hiding profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.
4. Click the Topology Hiding Profile that you want to rename.
5. In the content area , click **Rename Profile**.

   The EMS server displays the Rename Profile window.
6. In the **New Name** field, type a new name and click **Finish**.

Result

The application pane displays the new renamed profile.

Cloning a Topology Hiding profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.
4. Click the Topology Hiding Profile that you want to clone.
5. Click **Clone**.

   The EMS server displays the Clone Profile window.
6. In the **Clone Name** field, type a name for the cloned profile and click **Finish**.

Note:

Cloning the default Topology Hiding Profile is the fastest method to create a fully expanded Topology Hiding Profile.

Deleting a Topology Hiding profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.
4. Click the Topology Hiding Profile that you want to delete.
5. Click **Delete**.

   The EMS server displays a message to confirm whether you want to proceed with deleting the profile.
6. Click **OK** to confirm.

Result

The EMS server deleted the selected topology hiding profile.

Adding a new Topology Hiding header

About this task

Use this procedure to add a new Topology Hiding header to an existing Topology Hiding profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.
4. In the application pane, click the Topology Hiding Profile to which you want to add a new Topology Hiding Header.
5. Click **Edit**.

   The EMS server displays the Edit Topology Hiding Profile window.
6. Click **Add Header** button.

   The EMS server adds a new Header description row.

Note:

The number of new Headers that can be added is restricted to the number of parameter names in the **Header** field. For example, if the list contains eight Header parameter names, you can create only eight Headers.

7. In the new **Header** field, use the default value or select another unused Header parameter name for the new Topology Hiding Header.
8. Select values for the **Criteria** and **Replace Action** fields.

   If you select Overwrite as the **Replace Action**, enter an IP address in the **Overwrite Value** field.
9. Click **Finish**.

Result

The Topology Hiding Profile screen now contains the new header.

Editing a Topology Hiding Header

About this task

Use this procedure to edit and delete headers added to a Topology Hiding Header.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.
4. Click the Topology Hiding Profile containing the Topology Hiding header that you want to edit.
5. In the **Topology Hiding** tab, click **Edit**.
6. Select new values, as required, for the **Header**, **Criteria**, and **Release Action** fields.
7. Click **Finish**.

Deleting a Topology Hiding header

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.

4. Click the Topology Hiding Profile that contains the Topology Hiding Header you want to delete.
5. In the **Topology Hiding** tab, click **Edit** .
6. In the Edit Topology Hiding Profile window, locate the Topology Hiding Header that you want to delete, and click **Delete**.
7. Click **Finish** to save the changes.

Headers affected by Topology Hiding

When creating or editing Topology Hiding Profiles, eight types of headers are available for selection:

- **Request-Line**
- **From**
- **To**
- **Record-Route**
- **Via**
- **SDP**
- **Refer-To**
- **Referred-By**

Note:

Some other headers are also affected when you select the **To** or **From** headers.

Topology Hiding Headers on page 308 lists these headers along with the other affected headers under the **Source Headers**, **Destination Headers**, and **SDP Headers** categories.

In the table, where applicable, additional affected headers are noted. In Topology Hiding Settings Examples on page 308, descriptions are provided for all possible combinations of selections in the **Header**, **Criteria**, and **Replace Action** fields.

Avaya SBC ignores the Topology Hiding setting for the Refer-To header if:

- The Refer-To has an embedded Replaces header.
- Avaya SBC has an existing SIP INVITE dialog for the Replaces header.

In this scenario, Avaya SBC uses the contact of the replacing dialog to rewrite the Refer-To URI.

Related links

Topology Hiding headers on page 308
Topology Hiding settings examples on page 308

Topology Hiding headers

Main Header names	Headers affected by Main Header	Header affecting this header
Source Headers		
Record-Route		
Route		
From	• Referred-By • PAsserted Identity	
Referred-By		From
PAsserted Identity		From
Destination Headers		
To	ReferTo	
Request Start Line		
Refer To		To
Diversion		
SDP Headers		
Origin Header		

Topology Hiding settings examples

This section provides examples of all possible combinations of topology hiding settings listed in the **Header** field. Each **Header** type is combined with each combination of the **Criteria** type and **Replace Action** type along with a description of the resulting action or effect.

Topology Hiding examples for Request-Line Header

1. Topology Hiding replaces the **Request-Line** header with the next hop address or domain from the routing profile. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the **Request-Line** header with the next hop address or domain from the routing profile. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **Request-Line** header with the Destination **IP/Domain** from the SIP message. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain

- Replace Action: Destination IP

4. Topology Hiding replaces the **Request-Line** header with the **Overwrite Value**. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain
   - Replace Action: Overwrite

Topology Hiding examples for From header

Note:

The **From** header setting affects the **Referred-By** header and the **P-Asserted-Identity** header. The **To** header setting does not affect **Referred-By** and **P-Asserted-Identity**. When you select the **From** header settings, the **Referred-By** header and **P-Asserted-Identity** header are automatically updated.

1. If the SIP message is from the Subscriber side, then Topology Hiding replaces the **From** Header with the next hop address or domain from the routing profile. If the SIP message is from the Call Server side or Trunk Server side, then Topology Hiding replaces the **From** Header with the Signaling Interface. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the **From** header with the next hop address/domain from the Routing profile. This scenario occurs in the following setting:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **From** header with the Destination IP from the SIP Message. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Destination IP
4. Topology Hiding replaces the **From** header with the Signaling Interface IP/Domain. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Signaling Interface
5. Topology Hiding replaces the **From** header with the Overwrite Value. This scenario occurs in the following settings:
   - Header: From

- Criteria: IP/Domain or IP or Domain
- Replace Action: Overwrite

Topology Hiding examples for To header

Note:

The **To** header setting only affects the **Referred-To** header.

1. If the SIP message endpoint type is Subscriber, then Topology Hiding replaces the **To** header with the Next Hop Address used by the Signaling Interface. If the SIP message endpoint type is Call Server or Trunk Server, then Topology Hiding replaces the **To** header with the Next Hop Address. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the **To** header with the Next Hop Address/Domain from the Routing profile. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **To** header with the Destination IP from the SIP Message. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Destination IP
4. Topology Hiding replaces the **To** header with the Signaling Interface IP/Domain. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Signaling Interface
5. Topology Hiding replace the **To** header with the **Overwrite Value**. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Overwrite

Topology Hiding examples for Record-Route header

Topology Hiding stores the IP/Domain from the outbound message **Record-Route** header and then removes the **Record-Route** header from the outbound message. When the inbound

message is received, Topology Hiding puts the stored IP/Domain in a **Record-Route** header and adds the header to the inbound message. This scenario occurs in the following settings:

- Header: Record-Route
- Criteria: IP/Domain or IP or Domain
- Replace Action: Auto

Topology Hiding examples for Via header

Topology Hiding stores the IP/Domain from the outbound message **Via** header and then removes the **Via** header. When the inbound message is received, Topology Hiding puts the stored IP/Domain in a **Via** header and adds the header to the inbound message. This scenario occurs in the following settings:

- Header: Via
- Criteria: IP/Domain or IP or Domain
- Replace Action: Auto

If Trunk and Call server support Via header format RFC 3261, Avaya SBC must be configured for RFC3261.

If the Service provider or Call server are configured for RFC 2543 Via header support, then Interworking profile must be configured with RFC 2543 support for Via header format. If you configure Via header format that is not inline with the far-end server support, calls will fail.

Topology Hiding examples for SDP header

You can use the following Topology Hiding settings for the **SDP** Header.

1. Topology Hiding replaces the SDP message IP/Domain with the Media Interface IP/Domain. This scenario occurs in the following settings:
   - Header: SDP
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the SDP message IP/Domain with the Overwrite Value. This scenario occurs in the following settings:
   - Header: SDP
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Overwrite

Configuring Mediasec

About this task

MediaSec is a capability to distinguish security mechanisms that apply to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label such security mechanisms.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Enable mediasec handeling.
    a. In the navigation pane, click **SBC**.
    b. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
    c. Select the profile you want to edit.
    d. Click **Edit**.
    e. Select **Mediasec Handeling** checkbox to enable security mechanisms that apply to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label such security mechanisms.
    f. Click **Finish**.
3. Configure SRTP.
    a. In the navigation pane, click **Domain Policies** > **Media Rules**.
    b. Select the media rule you want to edit.
    c. Click **Edit**.
    d. In the **Preferred Formt** field, select SRTP as an ecryption method.
    e. Click **Finish**.
4. Configure signaling transport method.
    a. In the navigation pane, click **EMS**.
    b. In the navigation pane, click **System Administration** > **AAA**.
    c. Select the **LDAP** tab.
    d. Select SSL/TLS as signaling transport method.
    e. Click **Save**.

GDPR

General Data Protection Regulation (GDPR) prevents the loss of personal data by improving data security.

When GDPR is enabled, Avaya SBC uses a 12-character passphrase that you have provided to encrypt the files in the following folders:

Application logs and trace files: The encrypted files can be stored locally or to a remote log server. When configured to store the encrypted files to a remote log server, the encrypted files are pushed to the server based on the duration defined while configuring the log server. Avaya SBC encrypts the files that reach the maximum size of 10 MB or that are older than 6 hours. Application logs:

- SSYNDI logs: /archive/log/ipcs/ss/logfiles/elog/SSYNDI/
- OAMPSERVER logs: /archive/log/ipcs/ss/logfiles/elog/OAMPSERVER/
- SYSMON logs: /archive/log/ipcs/ss/logfiles/elog/SYSMON/
- Turnserver logs: /archive/log/turnserver/
- Nginx logs: /archive/log/nginx/
- Scrubber logs: /archive/log/scrubber/
- /archive/pcapfiles/IPCS2/

Trace files:

- SIP traces: /archive/log/tracesbc/tracesbc_sip/
- PPM traces: /archive/log/tracesbc/tracesbc_ppm/

Packet captures: The encrypted files can be stored locally or to a remote log server. When configured to store the encrypted files to a remote log server, the encrypted files are pushed to the server based on the duration defined while configuring the log server. Avaya SBC encrypts the files every 15 minutes.

- Pcap files: /archive/pcapfiles/IPCS2/

CDR files: CDR files can be stored locally, to a RADIUS server, or to a CDR adjunct server. When stored locally, the files are encrypted as soon as they are created. When stored in the CDR adjunct server, the files are encrypted as soon as they are created and pushed to the server according to the interval defined in the **Update Interval** field. When stored in the RADIUS server, GDPR has not effect. The files are not encrypted and pushed to the server as soon as they are created.

- CDR files: /archive/cdr/

Note:

Avaya SBC compresses the files before encrypting.

Note:

Before enabling GDPR, Avaya SBC might have unencrypted log information that will not comply to GDPR.

You can use the openssl command to decrypt the files.

Tracesbc: You can now run **`tracesbc`** in a GDPR-compliant Avaya SBC. However, encrypted records will not show in the **`tracesbc`** output.

Enabling or disabling GDPR

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **Compliance** > **GDPR**.

   The system displays the **GDPR** tab.
4. Do one of the following:
   - To enable GDPR, select the **Enable GDPR** check box.
   - To disable GDPR, clear the **Enable GDPR** check box.
5. In the **Passphrase** field, enter a 12-character passphrase that Avaya SBC uses for encryption.

   You can use a combination of alphabets, numbers, and special characters in your passphrase.

   After enabling GDPR, you cannot leave this field blank. However, if GDPR is already enabled and a passphrase exists, you can leave this field blank to use the existing passphrase or enter a new passphrase.

   Note:

   After entering a new passphrase, the files that are already encrypted with the older passphrase cannot be decrypted using the new one. You must use the older passphrase to decrypt them.

   Note:

   When you upgrade from an earlier release that had GDPR enabled to Release 10.2 and later, Avaya SBC sets the **Passphrase** field to **default-passphrase** by default.
6. In the **Confirm Passphrase** field, enter the passphrase again for confirmation.
7. **(Optional)** To use a Remote log server to store the encrypted files, do the following:

   By default, the encrypted files are stored locally in Avaya SBC.

   a. Select the **Enable Remote Log Server** check box.

      The system displays the **Remote Log Server Details** tab.

   b. Configure the fields as described in Remote log server field descriptions on page 315.
8. Click **Save**.

Configuring a Remote log server

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **Compliance** > **GDPR**.

   The system displays the **GDPR** tab.
4. Select the **Enable Remote Log Server** check box.

   The system displays the **Remote Log Server Details** tab.

   Note:

   You can select the **Enable Remote Log Server** check box only if the **Enable GDPR** check box is selected.
5. Configure the fields as described in Remote log server field descriptions on page 315.
6. Click **Save**.

Remote log server field descriptions

Name	Description
Protocol	Select either **SFTP** or **HTTPS** as your method for transferring files to the remote server.
TLS Client Profile	When using HTTPS, select the client profile you want to use. These profiles must be administered before creating the connection to the remote server.
Address	Enter the IP address and port or FQDN and port of the remote server.
Username	Enter the user used to log on to the remote server. The user administered must have writer permissions to the path administered in the **Location** option.
Password	Enter the user's password.
Confirm Password	Re-enter the user's password.
Location	Enter the file path on the remote server to where you want the log files uploaded. The user administered must have write permissions to this file path. Depending on the protocol being the used, the files are copied to the remote log server file path in different ways: • SFTP: The IP address or FQDN of the sending Avaya SBC server is appended to the **Location** file path. For example, if the administered file path is `/var/sbce`, the log files are actually copied to the path `/var/sbce/`*`ASBCE_IP_Address`*. • HTTPS: The remote log server's HTTPD configuration path is prepended to the **Location** file path and the IP address or FQDN of the sending Avaya SBC server is appended to the **Location** file path. For example, if the administered file path is `/var/sbce`, the log files are actually copied to the path */`*`HTTPD_Config_Path`*`/var/sbce/`*`ASBCE_IP_Address`*.

Table continues…

Name	Description
Update Interval	Enter how often you want the log files sent to the remote server. You can specify an interval of 15, 30, 60, 120, or 360 minutes.

Decrypting the encrypted files

Before you begin

Ensure that openssl is installed on the server where the encrypted files are stored.

Procedure

1. Log in with the administrator credentials to the server through SSH client where the encrypted files are stored.

   Note:

   If the remote log server is configured, the encrypted files are stored in the configured remote log server. Else, they are stored in Avaya SBC.

2. Decrypt the required file using the following command:

   ```
   openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt
   -in <ENCRYPTED_FILENAME> -out <DECRYPTED_FILENAME> -pass
   pass:<PASS_PHRASE>
   ```

   Where:

   `<ENCRYPTED_FILENAME>` is the encrypted compressed file name with relative path.

   `<DECRYPTED_FILENAME>` is the decrypted compressed file name with relative path.

   `<PASS_PHRASE>` is the passphrase configured for encryption. For more information, see Enabling or disabling GDPR on page 314.

   For example:

   ```
   openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000
   -salt -in tracesbc_sip_1702994829_1702994834_1.gz.enc -out
   tracesbc_sip_1702994829_1702994834_1.gz -pass pass:SIPera_123
   ```

   On successful decryption, a compressed file is generated.

3. Uncompress the file using the following command:

   ```
   gunzip <DECRYPTED_FILENAME>
   ```

   For example:

   ```
   gunzip tracesbc_sip_1702994829_1702994834_1.gz
   ```

   On successful uncompressing, the required file is generated.

Chapter 8: Server and network interface configuration

About configuring the server and network interfaces

You can use the EMS web interface to perform a number of network-specific configuration and management functions, such as:

- Managing SIP server configurations.
- Managing interworking profiles.
- Managing network configurations and custom routes.
- Managing Transport Layer Security (TLS) parameters.

Avaya SBC supports connection reuse policy. With this feature, Avaya SBC supports incoming connections from servers that are not able to accept incoming connections due to policies governing the connections to servers or network environment. SIP server initiates a connection towards Avaya SBC with or without alias parameter in via header and Avaya SBC reuses the incoming connection to send any outgoing SIP requests. You can configure this feature using the **Inbound Connection Reuse Policy** field on the SIP Server Profile page. For more information, see Server configuration profile field descriptions on page 319.

About SIP server configuration profile management

Configurations for SIP call servers (trunk, proxy) can be centrally managed from the Server Configuration SIP feature of the Avaya SBC security device. You can use this feature to define a number of different server profiles for use in a variety of deployments, security profiles, and company policies. You can add new profiles or clone, edit, rename, view, and delete existing server profiles.

When deploying Avaya SBC with Microsoft Teams, you must configure Avaya SBC with the SIP server heartbeat options to track the status of the Microsoft Teams SIP proxy.

Viewing a SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the navigation pane, click **Services** > **SIP Servers**.

   The application pane displays the list of available server profiles.

Adding a new SIP server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
5. In the **Profile Name** field, type a name for the new server profile, and click **Next**.
6. On the Edit SIP Server Profile - General window, administer the options as described in Server configuration profile field descriptions on page 319 and click **Next**.
7. On the Edit SIP Server Profile - Authentication window, administer the options as described in Server configuration profile field descriptions on page 319 and click **Next**.
8. On the Edit SIP Server Profile - Heartbeat window, administer the options as described in Server configuration profile field descriptions on page 319 and click **Next**.
9. On the Edit SIP Server Profile - Registration window, administer the options as described in Server configuration profile field descriptions on page 319 and click **Next**.

   Note:

   The EMS server does not display the Edit SIP Server Profile - Heartbeat window and Edit SIP Server Profile - Registration window for Remote Branch Office servers.
10. On the Edit SIP Server Profile - Ping page, enter the requested information in the appropriate fields and click **Next**.
11. On the Add Server Configuration Profile - Advanced window, administer the options as described in Server configuration profile field descriptions on page 319.
12. Click **Finish** to save the changes.

Editing a SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. In the Server Profiles section, select the server profile that you want to edit.
5. Click the tab you want to edit and click **Edit**.

The EMS server displays the Edit SIP Server Profile window.

6. Edit the required fields based on options described in Server configuration profile field descriptions on page 319 and click **Finish**.

Server configuration profile field descriptions

General options

Note:

The **Registration** tab and **Heartbeat** tab are not available when the **Server type** is administered as **Remote Branch Office**.

Name	Description
Server Type	The type of SIP server for which this profile is being defined. The options are: • **Trunk Server**: To configure a trunk server. • **Call Server**: To configure a call server. • **Media Server**: To configure a media server. • **Remote Branch Office**: To configure a branch office in a remote site that connects to the enterprise through Avaya SBC. • **Recording Server**: To configure a Recording Server to record SIP sessions.
SIP Domain	The SIP domain that validates the host name in a certificate. You must specify a SIP Domain when: • You have enabled extended host name validation. • Custom host name is blank in the client TLS profile associated in the server configuration. To validate the extended host name, Avaya SBC first looks for custom host names configured in the TLS profile. If the custom host name is blank, Avaya SBC then looks for the SIP Domain specified in the server configuration.

Table continues…

Name	Description
DNS Query Type	The DNS query type that Avaya SBC sends to the DNS server. The options are: • **None/A**: Used when IP address or FQDN of A-query is configured in the EMS server. You must configure **IP Address/FQDN**, **Port**, and **Transport** fields to save any changes for the **None/A** type DNS query for the new SIP server profile. • **SRV**: Used when Avaya SBC sends the SRV type query to the DNS server. Use this setting when using the DNS SRV for trunk registration feature. You must configure FQDN in the **IP Address/FQDN** and **Transport** fields to save any changes for the **SRV** type DNS query for the new SIP server profile. • **NAPTR**: Used when Avaya SBC sends the NAPTR type query to the DNS server. You must configure FQDN in the **IP Address/FQDN** field to save any changes for the **NAPTR** type DNS query for the new SIP server profile. **Note:** • Avaya SBC does not support AAAA-query for FQDN. • You can select **DNS Query Type** for **Server Type** as **Trunk Server** only.

Table continues…

Name	Description
Inbound Connection Reuse Policy	The inbound connection reuse policy for the SIP server. The options are: • **None**: With this option, Avaya SBC initiates a connection towards the SIP server and uses that connection for any outgoing requests from Avaya SBC. The default value is **None**. • **Without alias**: With this option, the SIP server initiates a connection towards Avaya SBC. SIP server does not add the alias parameter in the via header and Avaya SBC reuses the incoming connection to send any outgoing SIP requests. • **Alias (RFC 5923)**: With this option, the SIP server initiates a connection towards Avaya SBC. SIP server adds the alias parameter in the via header and Avaya SBC reuses the incoming connection to send any outgoing SIP requests. This field only applies to the following SIP server types: • Call server • Trunk server • Recording server **Note:** Avaya SBC supports a maximum of 256 inbound SIP server connections. This includes incoming connections from the following server types: • Call server (**Inbound connection reuse policy** not set to **None**) • Trunk server (**Inbound connection reuse policy** not set to **None**) • Recording server (**Inbound connection reuse policy** not set to **None**) • Remote Branch office
TLS Client Profile	The TLS Client profile to be used for the SIP server. The **TLS Client Profile** option is activated only when **DNS Query Type** is set to **NAPTR**.
IP Address/FQDN	The IP address or Fully Qualified Domain Name (FQDN) of the SIP server. You can add multiple IP addresses or FQDNs. While configuring a Remote Branch Office server, if the Remote Branch Office is: • Behind a NAT router, enter the IP address or FQDN of the public interface of the router. • Not behind a NAT router, enter the IP address or FQDN of the IPO that is used to connect to the Avaya SBC.

Table continues…

Name	Description
IP Address / FQDN / CIDR Range	The EMS server displays this field when the **Server Type** is **Trunk Server**. The IP address, Fully Qualified Domain Name (FQDN) or CIDR range of the SIP server. You can add multiple IP addresses, FQDNs or CIDR ranges. When you configure CIDR range in the SIP Server by default CIDRs will be configured as whitelist entries. So Avaya SBC enables inbound calls from all IP addresses within the CIDR range. However, the CIDR will not be used for routing outbound calls. For example, in the case of Microsoft Direct Routing, inbound calls to the Avaya SBC can originate from any of the IP addresses within the CIDR blocks 52.112.0.0/14 and 52.120.0.0/14. By configuring these CIDRs along with the Direct Routing Server FQDNs, the Avaya SBC will no longer reject inbound calls from any IP address within the CIDR block. Outbound calls will still route to the resolved FQDN addresses.
Verify TLS Common Name	The EMS server displays this field when the **Server Type** is **Remote Branch Office**. The option for specifying whether the TLS common name must be verified during the TLS handshake.
TLS Common Name	The string used to verify whether the TLS connection from the IPO is valid. If the TLS Common Name configured in the server configuration does not match the TLS Common Name provided by the IPO, Avaya SBC rejects the TLS connection. Use one of the following values for the **TLS Common Name** field: • **FQDN** • **IP Address** • **Name** • **Domain beginning with a wild card (*)** The EMS server displays this field only when the **Server Type** is **Remote Branch Office**.
Port	The port number. The **Port** field is not active when the **Server Type** is **Remote Branch Office**.
Transport	The type of transport protocols for the SIP server. The options are: • **TCP** • **UDP** • **TLS** The **Transport** field is set to **TLS** when the **Server Type** is **Remote Branch Office**.
Whitelist	The call is not blocked if the call originator exists in the Whitelist.

Authentication options

Avaya SBC supports the following secure digest algorithms for authentication challenge responses:

- MD5 (Message digest)
- SHA-256 (Secure Hash)
- SHA-512

Secure digest algorithm is a simple challenge-response mechanism that allows a server (service provider) to challenge a client (Avaya SBC) request and allows a client (Avaya SBC) to provide authentication information in response to that challenge.

SHA-256 and SHA-512 are more secure and strong algorithms than the default algorithm, MD5.

For JITC deployments, Avaya SBC uses the algorithms in the following priority order (high to low):

- SHA-512
- SHA-256

For Non-JITC deployments Avaya SBC uses the algorithms in the following priority order (high to low):

- SHA-512
- SHA-256
- MD5

Name	Description
Enable Authentication	The field to indicate whether the SIP server requires authentication. If selected, authentication is required and the remaining fields are activated. If cleared, authentication is not required and the remaining fields remain inactivate.
User Name	The user name required for authentication.
Realm	The realm from which the legitimate authentication request is made.
Password	The password required for authentication.
Confirm Password	The password entered in the **Password** field.

Heartbeat options

Name	Description
Enable Heartbeat	Indicates whether a synchronization signal (heartbeat) is established between the Avaya SBC security device and the SIP server. Select this check box to indicate that a heartbeat is established and maintained and the remaining fields are activated. Clear the check box to indicate that no heartbeat is maintained and the remaining fields remain inactivated.

Table continues…

Name	Description
Method	Specifies the method by which the heartbeat is maintained. The options are: • **OPTIONS** • **PING**
Retry Timeout on Connection Failure	Specifies the duration for which Avaya SBC pauses after raising the "Server down" incidence, and before sending the next heartbeat signal. The default value is **2** seconds.
Frequency	Specifies the frequency of sending the heartbeat signal.
From URI	Specifies the source of the heartbeat signal.
To URI	Specifies the destination of the heartbeat signal.

Registration options

Name	Description
Register with All Servers	To send a REGISTER message to all servers. • For the **DNS Query Type** as None/A, Avaya SBC sends the REGISTER message to the server configured in the DNS server or the resolved IP address by the DNS server. • For **DNS Query Type** as SRV or NAPTR, Avaya SBC sends the REGISTER message to all servers resolved in the DNS response.
Register with Priority Server	To send a REGISTER message to the highest priority server as received in the DNS query response. Enable this option when using the DNS SRV for trunk registration feature. If the highest priority server is non-functional on DNS TTL expiry, Avaya SBC sends the REGISTER message to the second highest priority server. **Register with Priority Server** field is disabled if **DNS query type** is **NONE/A**.
Refresh Interval	Specifies the time, in seconds, after which Avaya SBC sends a REGISTER message to servers.
From URI	Specifies the source of the REGISTER message.
To URI	Specifies the destination of the REGISTER message.

Ping options

Name	Description
Enable Ping	Select this option to enable ping on the server connections.
Ping Interval	Specifies the amount of time, in seconds, between ping messages sent to the server.
Response Timeout	Specifies the time, in seconds, after which a ping message times out.

Advanced options

Name	Description
Enable DoS Protection	Indicates whether DoS protection is enabled for the SIP server. • When you select the **Enable DoS Protection** check box, the EMS server displays **Next** at the bottom of the page. When you click **Next**, the EMS server displays a second Edit Server Configuration Profile – Advanced page, prompting for the number of users on the Call Server. • When you configure the DoS protection for the SIP server, the EMS server displays two new tabs: **DoS Whitelist** and **DoS Protection** on the Server Configuration page. The EMS server does not display this option for a Recording Server.
Enable Grooming	Indicates whether the same connection is used for the same subscriber or port. You must enable this field while using TCP or TLS. The **Enable Grooming** field is enabled by default. If grooming changes are done on a production system, you must restart the application to clean up the old connections. The **Enable Grooming** field is unavailable when the **Server Type** is Remote Branch Office.
Interworking Profile	Specifies the Interworking profile to be used for the SIP server.
Signaling Manipulation Script	Specifies the signaling manipulation script for the SIP server. Specify a signaling manipulation script in this field in one of the following conditions: • One server flow is associated with the server. • All server flows associated with the server use the same signaling manipulation script. **Note:** If you select different scripts in the server configuration and the server flow, the EMS server uses the signaling manipulation script selected in the server flow. However, if you apply the manipulation as INBOUND and AFTER_NETWORK, the EMS server uses the script selected in the server configuration.
Securable	Specifies whether the server can be secured. Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. Avaya SBC provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBC uses the **Securable** field to determine whether the trunk and call server can use secure protocols, and sets appropriate values for the Av-Secure-Indication header.
Enable FGDN	Enables a Failover Group Domain Name (FGDN) that Avaya SBC uses to route SIP traffic through an alternate Session Manager when a Session Manager is unreachable.

Table continues…

Name	Description
TCP Failover Port	Specifies the TCP port used during failover to the FGDN. This field is available only when you select the **Enable FGDN** check box.
TLS Failover Port	Specifies the TLS port used during failover to the FGDN. This field is available only when you select the **Enable FGDN** check box.
Tolerant	Specifies whether the server processes both IPv4 and IPv6 addresses.
Traffic Type	Specifies the traffic type. The options are: • **Trunk Traffic** • **Remote Users** • **Trunk Traffic and Remote Users** The EMS server displays this field only when you select the **Enable DoS Protection** field.
Max Concurrent Sessions	Specifies the maximum number of concurrent sessions. The default value is 1000. The EMS server displays this field only when you select the **Enable DoS Protection** field.
Number of Remote Users	Specifies the number of remote users. The EMS server displays this field only when you select the **Enable DoS Protection** field. When you select the **Remote Users** or **Trunk Traffic and Remote Users** option, the EMS server enables the **Number of Remote Users** field.
URI Group	Select the URI group you want to use with this profile, if any.
NG911 Support	Select this option to enable NG911 support for NG911 CS trunks. This option is required for adhoc conference support.

DoS Whitelist window

Name	Description
URI/Domain	Specifies the URI or domain that is allowed from an external source. The EMS server displays this tab only when you select the **Enable DoS Protection** check box on the **Advanced** tab.

DoS Protection

Name	Description
Traffic Type	The type of traffic.
Max Concurrent Sessions	The maximum number of concurrent sessions.

Table continues…

Name	Description
SIP Service	The SIP service affected by the DoS attack. The options are: • **TOTAL** • **Registrations** • **Calls** • **Presence Updates** • **Subscriptions** • **Misc**
SIP Method	The SIP Method of the SIP service. The options are: • **All** • **REGISTER** • **INVITE** • **SUBSCRIBE** • **PUBLISH** • **OPTIONS**
Initiated Threshold (per 10 seconds)	The maximum number of sessions that you can start within 10 seconds .
Pending Threshold	The maximum number of pending session initiations.
Failed Threshold (per 10 seconds)	The maximum number of failed session initiations.
Action	The action to be performed after any of the above thresholds are exceeded. The options are : • **Alert Only**: An alert displays the DoS incident, but the call is not blocked. • **Enforce Limit**: The call is not blocked until the specified limit is reached. • **Enforce Limit Response**: The call is blocked, and the EMS server sends the specified response when the specified limit is reached. • **SIP Challenge**: To initiate authentication. **Note:** Do not select the SIP Challenge action for a DoS profile configuration because Avaya phones do not respond the second time when they are again authenticated by Avaya after being challenged by Avaya SBC. • **Whitelist**: The call is not blocked if the call originator exists in the **Whitelist**.

Cloning an existing SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. From the application pane, click the server profile that you want to clone.
5. Click **Clone**.

   The EMS server displays the Add Server Configuration Profile page.
6. In the **Clone Name** field, type a new name for the cloned server profile.
7. Click **Finish**.

Renaming an existing SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. On the application name, click the server profile that you want to rename.
5. Click **Rename**.

   The EMS server displays the Rename Server Configuration Profile page.
6. In the **New Name** field, type a new name for the server profile.
7. Click **Finish**.

Deleting an existing SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. From the application pane, , click the server profile that you want to delete.
5. Click **Delete**.

   The EMS server displays a delete confirmation pop-up window.

6. Click **OK**.

DoS Whitelist

When you configure DoS protection while adding or editing the SIP Server profile on the Edit SIP Server Profile - Advanced tab, the EMS server displays the DoS Whitelist and DoS Protection tabs on the SIP Servers page.

Adding a URI or Domain to DoS Whitelist

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. On the SIP Servers page, click **DoS Whitelist** tab.
5. Click **Add**.

   The EMS server displays the Add Whitelist URI page.
6. In the **URI/Domain** field, type the URI or domain name.
7. Click **Finish**.

Deleting a URI or Domain from DoS Whitelist

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. On the SIP Servers page, click **DoS Whitelist** tab.
5. Click **Delete** corresponding to the URI/Domain that you want to delete.

   The EMS server displays the delete confirmation pop-up window.
6. Click **OK** to confirm.

Editing and recalculating the DoS Protection parameters

About this task

Using the **DoS Protection** tab, you can manage parameters for a specific set of SIP services and methods. When you configure DoS protection while adding or editing the SIP Server profile on the Edit SIP Server Profile - Advanced page, the EMS server displays the DoS Protection tab on the SIP Servers: IPO page.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.
4. On the SIP Servers page, click **DoS Protection** tab.
5. Click **Recalculate Values**.
6. On the Recalculate Values page, reenter the required values.

   You can reenter values for traffic type and the maximum number of concurrent sessions.
7. Click **Finish** to save the settings.
8. Click **Edit** corresponding to the SIP service or method that you want to edit.

   The EMS server displays the Edit Server DoS page.
9. Edit the required fields, and click **Finish**.

Configuring DNS SRV for trunk registration

About this task

Few service providers mandate that an SBC register to the service provider before accepting or invoking calls. An FQDN manages the servers on the service provider side for more reliable call management.

The DNS SRV feature is used to identify the highest priority server resolved to this FQDN so that Avaya SBC can register to that server. For Geo-Redundant deployments, a distributed Avaya SBC HA pair can point to different servers based on priority and how you administer the DNS SRV feature on Avaya SBC. Multi-server Avaya SBC configurations also support the DSN SRV feature, where the FQDN stays the same and the credentials on each server for the Register message vary on each server.

Avaya SBC sends a Register message based on the administered refresh time interval. Based on resiliency designed on the Service Provider side, if the priority of these servers change, Avaya SBC then switches its Register message. If Avaya SBC detects a server failure on the Service Provider side based on a heartbeat mechanism such as OPTIONS, Avaya SBC sends an UnRegister message to the failed server, followed by a Register message to the next highest priority server. Avaya SBC then initiates the call to the registered server. When Avaya SBC switches registration, it rejects new calls. Any calls that were active on the now unregistered Service Provider trunk server remain connected on the Avaya SBC when this failure occurs.

Avaya SBC does not support load balancing during failures and selects one priority server for registration. Avaya SBC can be configured to register with multiple servers so that at time of registration, the system uses different credential that are specific to that service provider.

Procedure

1. Add a new trunk server or edit an existing trunk server as described in Adding a new SIP server profile on page 318 or Editing a SIP Server profile on page 318.

2. In the Add/Edit Server Configuration Profile - General window, set the **DNS Query Type** field to **SRV**.
3. In the Add/Edit Server Configuration Profile - Registration window, enable the **Register with Priority Server** option.
4. Save your changes.

Server interworking

With the Server Interworking in Configuration Profiles, you can set certain parameters to make Avaya SBC function in an enterprise VoIP network using different implementation of the SIP protocol.

Viewing existing Server Interworking profiles

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profile page with the list of available interworking profiles in the application pane. The options for each profile are shown under the various tabs in the application pane.

Adding a server interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles screen, click **Add**.

   The EMS server displays the Interworking Profile window.
5. In the **Profile Name** field, type a name for the new interworking profile, and click **Next**.

   The system displays a series of configuration windows. Administer the profile options as required based on the options described in Interworking profile field descriptions on page 332.

Note:

Options for the **URI Manipulation** and **Header Manipulation** rules cannot be added until after you administer the basic interworking options. After you add a new profile, you can add these rules using the **Add** button located on the two rule tabs.

6. Click **Next** after configuring the options in each window.
7. Click **Finish** to save the settings.

Editing the Server Interworking profile parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Select the profile you want to edit.
5. Click **Edit** on the tab you want to edit.

   The EMS server displays the options for that tab.
6. Administer the profile options as required based on the options described in Interworking profile field descriptions on page 332.
7. Click **Finish**.

Interworking profile field descriptions

General options

Name	Description
Hold Support	Indicates the standard to be used to provide HOLD support. The options are: • **None** • **RFC 2543 - c=0.0.0.0** • **RFC 3264 - a=send only** • **Microsoft Teams** The **Microsoft Teams** option is required for Microsoft Teams deployments to handle the hold/resume feature of Microsoft Teams. It enforces the Microsoft Teams side to send the “a=inactive” message. When this option is set, none of the following messages are sent towards Microsoft Teams: “a=sendonly”, “a=recvonly”, or “c=0.0.0.0”. In addition, when you select the **Microsoft Teams** option, a Feature Flag is set in the Call Detail Record (CDR) by Avaya SBC. The Feature Flag is the 35th field in the CDR and is set to a value of 8. The Feature Flag identifies the call in CDR as a Microsoft Teams call.

Table continues…

Name	Description
180 Handling	Determines how 180 Ringing messages are handled. The options are: • **None** • **SDP** • **No SDP**
181 Handling	Determines how 181 Call Forwarding messages are handled. The options are: • **None** • **SDP** • **No SDP**
182 Handling	Determines how 182 Queued messages are handled. The options are: • **None** • **SDP** • **No SDP**
183 Handling	Determines how 183 Session Progress messages are handled. The options are: • **None** • **SDP** • **No SDP** For Microsoft Teams, the **183 Handling** option must be administered with **No SDP**. This is required so that ringback is heard on trunks.
Refer Handling	Indicates whether Avaya SBC passes or consumes the REFER message. When an endpoint invokes a supplementary service, such as a call transfer, the endpoint generates and sends an in-dialog REFER request to Avaya SBC through the enterprise call server. Avaya SBC applies URI-based routing to the new **INVITE** message triggered towards the transfer target. Refer Handling feature works in either of the following two modes: • **Send Hold** • **Delayed Offer** When configuring a profile to use with Microsoft Teams, enable the **Refer Handling** option.

Table continues…

Name	Description
URI Group	Indicates the URI group that is required for REFER handing. **Note:** Avaya SBC enables the **URI Group** field only when you select the **Refer Handling** checkbox. When configuring Microsoft Teams, it is recommended that the **URI Group** option be set to **None**. However, this option can be enabled if required by the PSTN side and topology.
Send Hold	Indicates whether Avaya SBC sends a HOLD message to a trunk when processing REFER messages for that trunk. Disable this setting for trunks that do not support SIP HOLD. By default, this setting is on. **Note:** Avaya SBC enables the **Send Hold** check box only when you select the **Refer Handling** check box. When configuring Microsoft Teams, it is recommended that the **Send Hold** option be disabled. However, this option can be enabled if required by the PSTN side and topology.
Delayed Offer	Indicates whether Avaya SBC sends an INVITE message to the transferee without SDP. If you select **Delayed Offer**, Avaya SBC gets the complete capabilities of the transferee as an SDP Offer message. Avaya SBC enables the **Delayed Offer** check box only when you select the **Refer Handling** check box. When configuring Microsoft Teams, it is recommended that the **Delayed Offer** option be disabled. However, this option can be enabled if required by the PSTN side and topology.
3xx Handling	Indicates whether the Avaya SBC security device will handle the *3xx Redirection Response* messages.
Diversion Header Support	Indicates whether the Avaya SBC security device supports diversion headers. **Note:** When you select the **3xx Handling** check box, the system enables the **Diversion Header Support** check box.
Delayed SDP Handling	Indicates whether the Avaya SBC security device processes delayed SDP packets. **Important:** The features Media Unanchoring and Delayed SDP Handling cannot both be enabled for a call. For more information about administering those features, see *Administering Avaya Session Border Controller*.

Table continues…

Name	Description
Re-Invite Handling	Indicates whether Reinvite Handling is enabled for Avaya SBC. If a trunk or call server does not want in-dialog **RE-INVITES**, then enable Reinvite Handling. Precondition: **RE-INVITE SDP** must be the same as the previous INVITE transaction SDP. For example, consider a trunk server that has Reinvite Handling enabled. When the first **INVITE** with SDP goes to the trunk server, Avaya SBC stores this message. When the next **INVITE** goes to the trunk server, Avaya SBC tries to match the current **INVITE SDP** with the stored SDP. If both SDPs are same, Avaya SBC stops **INVITE** and responds . However, if a second INVITE comes without any SDP change, while adding extra SDP parameters to Hold or Resume, Avaya SBC handles **RE-INVITE**. **Important:** When **Re-Invite Handling** is enabled, the far end should not change its CODEC, SRTP, and media parameters mid-call. If any of these parameters change, Reinvite Handling will not work
Prack Handling	Indicates whether Provisional Response Acknowledgement (PRACK) handling is enabled. When called party sends provisional requests with 100 rel option in the Require header, called party must receive PRACK message in the response to ensure end to end successful communication. If the trunk or call server does not send 100 rel option in the supported header for the initial INVITE request then by selecting **Prack Handling**, Avaya SBC sends the PRACK for that particular trunk or call server to the called party.
Allow 18X SDP	Indicates whether a PRACK message is permitted in an 18x record route header.
T.38 Support	Indicates whether Avaya SBC security device. supports the T.38 FAX Relay standard.
URI Scheme	Indicates the URI scheme that the Avaya SBC security device will use. The options are: • **SIP** • **TEL** • **ANY**
Via Header Format	Indicates the header format used by the Avaya SBC security device. The options: • **RFC3261** • **RFC2543**

Table continues…

Name	Description
SIPS Required	Use this option to control the SIP/SIPS URI scheme handling for SRTP calls. By default, this option is enabled. When doing an upgrade to Release 8.1.2 or later, this option is automatically enabled after the upgrade. For any configurations that do not use this feature, you must manually disable this option after you do the upgrade. For example, you must disable this option in Server Interworking profiles when the deployment has or uses Microsoft Teams, Skype for Business, or Lync. **Note:** When Assured SIP (AS-SIP) mode is enabled, the **SIPS Required** option is grayed out and is not available.
Mediasec Handling	Use this option to distinguish security mechanisms that apply to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label such security mechanisms.

SIP Timers options

Name	Description
Min-SE	Specifies the minimum value for the SIP min-SE timer. The Min-SE timer is used for a SIP refresh (Re-Invite/Update) session as the minimum session expire time value. The time range is 90 to 86400 seconds.
Init Timer	Specifies the initial request retransmission interval. This interval corresponds to Timer T1 in RFC 3261. This timer is used when sending a request over UDP. The time range is 50 to 1000 milliseconds.
Max Timer	Specifies the maximum retransmission interval for non-INVITE requests. This interval is for non-INVITE requests and corresponds to Timer T2 in RFC 3261. The time range is 200 to 8000 milliseconds.
Trans Expire	Specifies the Transaction Expiration timer. The default value for this field is 32 seconds. Any request that the server sends times out if the server does not receive a response within the time set as the Transaction Expiration time. To use alternate routing, you must set a shorter transaction expiration value than the default value of 32 seconds. The time range is 1 to 64 seconds.
Invite Expire	Specifies the transaction expiration time for an INVITE transaction after what receives a provisional response . The time range is 180 to 300 seconds.
Retry After	Specifies the maximum time after which the server sends the routing request again. The time range is 2 to 32 seconds.

Privacy options

Name	Description
Privacy Enabled	Indicates whether privacy is used between the Avaya SBC security device and the SIP server. **Note:** When you select the **Privacy Enabled** checkbox, the system enables the following fields: **User Name**, **P-Asserted-Identity**, **P-Preferred-Identity**, and **Privacy Header** fields.
User Name	Specifies the user name to be used for privacy authentication.
P-Asserted-Identity	Indicates that Avaya SBC rewrites the FROM header in a trusted SIP message with the P-Asserted-ID. This field is used for maintaining privacy for the FROM header. Trunk servers usually Accept SIP INVITE with P-asserted ID. For some Trunk servers, Avaya SBC inserts this header into the FROM header, insert the header in P-asserted ID and change From as Anonymous user, and send out the request. not clear
P-Preferred-Identity	Indicates that Avaya SBC uses the P-Preferred-ID during private sessions.
Privacy Header	Specifies the Privacy Header to be used during privacy sessions.

Advanced options

Name	Description
Record Routes	Directs the Avaya SBC security device to record route information. The options are: • **None**: Avaya SBC does not add any record route. However, to remove all record routes, enable Topology Hiding (TH) with record route auto. • **Single Side**: Avaya SBC adds only one record route. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed. • **Both Sides**: Avaya SBC adds two record routes. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed and only one record route is retained. When configuring a profile to use with Microsoft Teams, enable the **Both Sides** option. • **Dialog Initiate Only (Both Sides)**: Avaya SBC adds two record routes, but not to the in-dialog message. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed and only one record route is retained. • **Dialog Initiate Only (Single Side)**: Avaya SBC adds one record route, but not to the in-dialog message. If Avaya SBC receives a 200 OK message,

Table continues…

Name	Description
	Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed.
Include Endpoint IP for Context Lookup	Directs the Avaya SBC security device to use endpoint IP while looking for Avaya SBC internal SIP context.
Extensions	Directs the Avaya SBC security device to use functionality specific to different environments. The available options are: • **Avaya** **Important:** You must use the **Avaya** option if you want to use the `traceSBC` command to search for Av-Global-Session-ID (GSID) headers to filter SIP call traces. • **Nortel** • **Lync** **Note:** When configuring a profile to use with Microsoft® Teams, enable the **Lync** option. “Lync” was a prior name for Microsoft® Teams. • **Cisco** • **KDDI**
Diversion Manipulation	Directs the Avaya SBC security device to copy SIP Diversion header from 3xx messages to Sip Request messages while 3xx handling is enabled on Avaya SBC security device.
Diversion Condition	Specifies the diversion condition. **Note:** When you select the **Diversion Manipulation** check box, the system enables the **Diversion Condition** field.
Diversion Header URI	Specifies the Avaya SBC security device to add SIP Diversion header on the SIP Invite message. **Note:** When you select the **Diversion Manipulation** check box, the system enables the **Diversion Header URI** field.
Has Remote SBC	Directs the Avaya SBC security device to use far-end firewall functionality.
Route Response on Via Port	Directs the Avaya SBC security device to use SIP Via header port to route response.
MOBX Re-INVITE Handling	Select this option to enable **MOBX Re-INVITE Handling**. Enable this feature for calls made by Mobile Extension (MOBX) users that are calling through a Mobile Service Provider (MSP) serviced by an Avaya SBC system. The Avaya SBC can terminate these mobile calls to a PSTN

Table continues…

Name	Description
	user through SIP-PRI gateways or to a user connected to an Avaya private network communication server. Use this option to allow Avaya SBC to filter the reinvite messages coming from an Avaya private network communication server to the MSP. The Re-INVITE handling configuration must be enabled on the MSP trunk server interworking profiles.
NATing for 301/302 Redirection	When **NATing for 301/302 Redirection** is enabled for server interworking, Avaya SBC will NAT 301/302 contact addresses going to the server. Select this option for Adhoc conferencing support with the Next Generation 911 feature. When enabled, Avaya SBC will NAT on 301/302 contact address received from the Next Generation Core Services (NGCS) conference factory. This option has no affect operation of 301/302 messages on Remote Worker configurations.
SIP Recording	
Relay INVITE Replace	Select this option to enable **Relay INVITE Replace**.
Include Called Participant	Select this option to set the AOR attribute of the called participant in the SIPREC metadata to To header AOR of the communication session. By default, this option is disabled. **Note:** Configure this field only if the **Server Type** is administered as **Recording Server**.
Conference URI	Enter the conference URI to be updated in the conference media stream participant information. Avaya SBC and the recording vendor use this conference URI to identify the mixed media streams coming from the conference bridge. You can leave this field blank if there is no requirement from the recording vendor. **Note:** Configure this field only if the **Server Type** is administered as **Recording Server**.
DTMF	
DTMF Support	These options define whether and how RFC 2833 DTMF touch-tone signals are converted to SIP messages. When conversion occurs, the DTMF signals and SIP messages are sent in parallel in the call path to support signaling devices that require either DTMF signals (such as an IVR) or SIP messages (such as SIP trunks). You must have interworking profiles for both inbound calls (always set to **None**) and outbound calls (using one of the options defined below). You must define the profiles for the servers.

Table continues…

Name	Description
	Note: DTMF signal conversion to SIP messages will not happen when a registered user is involved in the call. **Important:** Avaya recommends that for deployments where personal data protection based on GDPR requirements are critical, you should not use DTMF interworking. For more information about Avaya SBC support for GDPR, see *Avaya Session Border Controller Overview and Specification*. • **None** – RFC 2833 DTMF touch-tone signals are passed through and are not converted to SIP messages. • **SIP Notify** – RFC 2833 DTMF touch-tone signals are converted to out-of-band SIP Notify messages. Conversely, SIP Notify messages are converted back to RFC 2833 DTMF touch-tone signals. • **RFC 2833 Relay & SIP Notify** – RFC 2833 DTMF touch-tone signals passed through and are also converted to out-of-band SIP Notify messages. Conversely, SIP Notify messages are converted back to RFC 2833 DTMF touch-tone signals. See the information below about how this option is used for MOBX calls. • **SIP INFO** – RFC 2833 DTMF touch-tone signals are converted to out-of-band SIP Info messages. Conversely, SIP Info messages are converted back to RFC 2833 DTMF touch-tone signals. • **RFC 2833 Relay & SIP Info** – RFC 2833 DTMF touch-tone signals passed through and are also converted to out-of-band SIP Info messages. Conversely, SIP Info messages are converted back to RFC 2833 DTMF touch-tone signals. See the information below about how this option is used for MOBX calls. • **Inband** – RFC 2833 DTMF touch-tone signals are converted to in-band DTMF. Conversion in the opposite direction is not supported. Avaya SBC uses the **RFC 2833 Relay & SIP Info** or **RFC 2833 & SIP Notify** options to fork the incoming RFC 2833 DTMF touch-tone signals and SIP Info or SIP Notify messages to carry the DTMF signals in SIP signaling messages. The MOBX URI group configuration is required to configure these DTMF options. MOBX calls use standard mobile user features that invoke RFC 2833 DTMF touch-tone signals, such as digits for an IVR. Avaya SBC must pass the original DTMF touch-tone signals to a media gateway or endpoint in parallel with sending the SIP Notify or SIP Info messages to an Avaya private network communication server. Any server configured on Avaya SBC that supports MOBX users on a Mobile Service Provider (MSP) must also have a URI group configured that identifies the MSP users.

Table continues…

Name	Description
Adaptive Inband Detection	Select this check box to enable Avaya SBC adaptive conversion of RFC 2833 DTMF touch-tone signals to INBAND DTMF based on the SDP Answer received from the service providers. Avaya SBC uses SIP/SDP signaling for this functionality. If the SDP answer has no telephone codec, the conversion happens from RFC 2833 to INBAND. Otherwise, it will be RFC 2833 relay. This field is available only when you set the **DTMF Support** field to **None**.

URI Manipulation options

Note:

Options for the **URI Manipulation** and **Header Manipulation** rules cannot be added until after you administer the basic interworking options. After you add a new profile, you can add these rules using the **Add** button located on the two rule tabs.

Name	Description
User Regex	The Regex rule to be used to match the **User** field in the SIP message.
Domain Regex	The Regex rule to be used to match the **Domain** field in the SIP message.
User Action	The action that the Avaya SBC security device takes on finding a User Regex match . The options are: • **None** • **Add prefix [Value]** • **Remove prefix [Value]** • **Replace with [Value]** • **Replace [Value 1] with [Value 2]**
User Values	The values to be used as specified in the **User Action** field. **Note:** When you select the **Replace [Value 1] with [Value 2]** option, the system enables the second text box.
Domain Action	The action that the Avaya SBC security device takes on finding a Domain Regex match . The options are: • **None** • **Add prefix [Value]** • **Remove prefix [Value]** • **Replace with [Value]** • **Replace [Value 1] with [Value 2]**
Domain Values	The values to be used as specified in the **Domain Action** field. **Note:** When you select the **Replace [Value 1] with [Value 2]** option, the system enables the second text box.

Header Manipulation options

Name	Description
Header	The SIP header field to be manipulated. The options are: • **Contact** • **Diversion** • **From** • **P-Asserted-Identity** • **RequestURI** • **To**
Action	The action to be performed. The options are: • **Add Parameter w/ [Value]** • **Remove Parameter w/ [Value]**
Parameter	The parameter to be used in the action performed in the **Action** field.
Value	The value of the parameter defined in the **Parameter** field.

Cloning a Interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles page, click the interworking profile that you want to clone.
5. Click **Clone**.

   The EMS server displays the Clone Profile page.
6. In the **Clone Name** field, type a name for the cloned interworking profile.
7. Click **Finish**.

Renaming an existing Interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles page, click the interworking profile that you want to rename.
5. Click **Rename**.

The EMS server displays the Rename Profile page.

6. In the **New Name** field, type a name for the interworking profile.
7. Click **Finish**.

Deleting an Interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles page, click the interworking profile that you want to delete.
5. Click **Delete**.

   The EMS Server displays a delete confirmation pop-up window.
6. Click **OK** to confirm.

Adding a URI Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Click **URI Manipulation** tab.
5. Click **Add**.
6. Administer the options as described in Interworking profile field descriptions on page 332.
7. Click **Finish**.

Editing a URI Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Click **URI Manipulation** tab.
5. On the URI Manipulation page, click **Edit** corresponding to the URI manipulation rule that you want to edit.

   The EMS server displays the Edit Regex page.
6. Administer the options as described in Interworking profile field descriptions on page 332.

7. Click **Finish**.

Deleting an existing URI Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profiles page.
4. Click **URI Manipulation** tab.
5. On the URI Manipulation page, click **Delete** corresponding to the URI manipulation rule that you want to delete.

   The EMS server displays a delete confirmation pop-up window.
6. Click **OK** to confirm the deletion.

Adding a Header Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Click **Header Manipulation** tab.
5. Click **Add**.
6. Administer the options as described in Interworking profile field descriptions on page 332.
7. Click **Finish**.

Editing a Header Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Click **Header Manipulation** tab.
5. Click **Edit** corresponding to the header manipulation rule that you want to edit.

   The EMS server displays the Edit Rule page.
6. Administer the options as described in Interworking profile field descriptions on page 332.
7. Click **Finish**.

Deleting a Header Manipulation rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profiles page.
4. Click **Header Manipulation** tab.
5. On the Header Manipulation page, click **Delete** corresponding to the header manipulation rule that you want to delete.

   The EMS server displays a delete confirmation pop-up window.
6. Click **OK** to confirm the deletion.

Networks and interfaces management

With the Network Management feature in **Network & Flows**, you can configure the network and network interface settings affecting the Avaya SBC security devices deployed throughout the enterprise. You can configure many networks, network interfaces, and Virtual LANs (VLANs).

Note:

Source-based routing essentially overrides normal Avaya SBC routing protocols, thus requiring an intimate knowledge of the VoIP network topology to be effective.

When you install an Avaya SBC security device, certain network-specific information is defined, such as device IP addresses, public IP addresses, netmask, and gateway to interface the device to the network. For information about installing a Avaya SBC device, see *Installing an Avaya SBC device*. The network-specific information populates various **Network Management** tabs. To optimize the device performance and network efficiency, you can change the information.

Related links

Passthrough on page 347

Adding a new network interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management page.
4. On the Network Management page, click **Interfaces** tab.

5. Click **Add VLAN**.
6. On the Add VLAN page, enter the required values in the appropriate fields.
7. Click **Finish** to save the changes.

Network Management field descriptions

Interfaces tab

Name	Description
Interface Name	Name of the interface.
VLAN Tag	VLAN tag for the interface.
Status	Status of the interface: enabled or disabled.

Add VLAN

Name	Description
Name	Provide the interface name or VLAN interface name.
Interface	Click an appropriate data interface, such as A1 or A2 or B1 or B2.
Tag	Type an appropriate tag.

Networks tab

Name	Description
Name	Specifies the network name.
Gateway	Specifies the gateway of the network.
Subnet Mask	Specifies the subnet mask of the network.
Interface	Specifies the appropriate data interface, such as A1, A2, B1, or B2
IP Address	Specifies the IP address.

Add Network

Name	Description
Name	Specifies the network name.
Default Gateway	Specifies the default gateway of the network.
Subnet Mask	Specifies the subnet mask of the network.
Interface	Specifies the appropriate data interface, such as A1, A2, B1, or B2
IP Address	Specifies the IP address.
Public IP	Specifies the public IP address.
Gateway	Specifies the gateway.
Passthrough	Option to configure pass-through network IP addresses along with the local IP address.

Virtual LAN

A Virtual Local Area Network (VLAN) is a logical group of network elements, such as workstations, servers, and network devices spanning various physical networks. A VLAN overlays a virtual layer-2 network on top of a physical layer-2 network by inserting a VLAN tag in the layer-2 header of a packet. VLAN-aware network devices, such as switches, can send packets through the VLAN overlay.

Tag a VLAN to distinctly identify the VLAN as part of a logically different layer-2 network.

The first step for VLAN tagging is to create a VLAN interface. The packets leaving and entering Avaya SBC on a VLAN use a physical link connected to a physical interface.

The second step is to configure all networks to which Avaya SBC connects. Each network to which Avaya SBC connects is defined and attached to an interface.

Note:

A VLAN is supported on data and signaling interface.

Tagging a VLAN

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.
4. On the Network Management page, click **Interfaces** tab.
5. Click **Add VLAN**.
6. On the Add VLAN page, do the following:
   a. In the **Name** field, type the VLAN name.
   b. In the **Interface** field, click the required interface.
   c. In the **Tag** field, type a tag number to identify the VLAN.

      You can use tag numbers from 1 through 4094.
   d. Click **Finish** to save the changes.

Passthrough

The Avaya SBC Passthrough option enables you to configure pass-through network IP addresses along with the local IP address. Avaya SBC enables an IP address that is different from the subnet to listen. The pass-through network IP addresses must be routable on the same subnet configured on Avaya SBC.

Use case

A system is configured with the B1 network to handle external traffic. For instance, the network address of B1 is 10.0.4.0, the IP address assigned to the system is 10.0.4.37, and the gateway is set to 10.0.4.1.

Now, the user has decided to configure an IP address that does not belong to the B1 subnet. However, the user ensured that the newly configured IP address is routable on the same subnet and gateway. To provide a specific example based on the previous scenario, the IP address the user configured in their environment is 34.168.112.241.

Related links

Networks and interfaces management on page 345

Changing the administrative state of an interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management page.
4. Click **Interfaces** tab.
5. In the **Status** column, click **Enabled** or **Disabled**.

   The EMS server displays a confirmation pop-up window.
6. Click **OK**.

Deleting an existing interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management page.
4. Click **Interfaces** tab.
5. Click **Delete** corresponding to the interface that you want to delete.

   The EMS server displays the delete confirmation pop-up window.
6. Click **OK** to confirm the deletion.

Viewing an existing interface or network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management page.

4. On the Network Management page, click **Interfaces** tab or **Networks** tab.

Result

The EMS server displays the existing networks and interfaces in the content area.

Adding a new network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.
4. On the Network Management page, click **Networks**.
5. Click **Add**.
6. On the Add Network page, enter the required values in the appropriate fields.
7. Click **Finish** to save the changes.

Editing network management parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS Server displays the Network Management page.
4. Click **Networks** tab or **Interfaces** tab for which you want to edit the parameters.
5. Click **Edit** corresponding to the interface or network that you want to edit.

   The EMS server displays the Edit VLAN or Edit Network page.
6. Edit the required fields, and click **Finish**.

Editing network management parameters using CLI

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. Run the following command to list all the configured network configurations:

   ```
   sbceconfigurator.py network-config-show
   ```
3. Run the following command to export the network configuration to your system:

   ```
   sbceconfigurator.py network-config-export <Network Name>
   ```

Important:

It is recommended not to rename the exported file. Renaming the file will fail the importing of the edited file.

4. Edit the required fields in the exported file.
5. Run the following command to import the updated network configuration back to the EMS server:

```
sbceconfigurator.py network-config-import <NetworkConfig filename>
```

Chapter 9: TLS management

About TLS parameter management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. TLS enables clients to authenticate servers or servers to authenticate clients. Avaya SBC security products utilize TLS primarily to facilitate secure communications with remote users.

Avaya SBC includes several certificates and profiles that you can use to quickly set up secure communications using TLS. These certificates and profiles are listed in the pre-installed Avaya Profiles and Certificates section. Alternatively, Avaya SBC supports the configuration of third-party certificates and TLS settings. For optimum security, use System Manager or third-party certificates. For more information about how to configure third-party certificates, see Certificate management on page 355 and About TLS profile management on page 367.

Considerations for working with TLS

While working with TLS, keep the following in mind:

- Permit enough time for setting up encryption. Strong encryption takes a long time to set up.
- Ensure that the time is properly synchronized between all entities. X.509 certificates are time sensitive. Ensure that all entities interacting with each other match each other's UTC times as closely as possible.
- Ensure that the certificates that you use are valid. One of the most common TLS failures is an expired or not yet valid certificate. Ensure that the selected certificates are valid for the time period for which they are being used.

For information about extracting a certificate and Private Key from a keystore, see Extracting a certificate and key from a PFX or PKCS#12 keystore on page 357.

Converting a certificate to PEM format

About this task

An X.509 certificate might come in many different formats, two of the most prominent being DER, a binary form, and PEM, an ASCII-encoded form. As the Avaya SBC currently only accepts PEM-encoded certificates, any binary DER certificates must be converted to PEM encoding. To convert a binary DER certificate into an ASCII-encoded PEM certificate, you must use a third party

SSL library. The EMS ships with an open source SSL library called OpenSSL, which can be used to encode a DER certificate to PEM format.

Procedure

1. Type `openssl x509 -in input.der -inform DER -out output.crt -outform PEM`.
2. Press `Enter`.

Checklist for establishing end-to-end TLS communications

Prerequisites

To establish end-to-end TLS communication, it is assumed that:

- Avaya SBC must have an existing, working end-to-end TLS remote user setup using the default Avaya certificates and profiles.

  Note:

  If you want to use Avaya default certificates and profiles, skip Steps 1 through 5, and go directly to step 6.

- The remote phones must already have the third-party CA root certificate installed.
- The Session Manager and Communication Manager systems must be configured for TLS and already have the third-party CA root certificate installed.
- The same CA root certificate must have directly signed all relevant certificates.

No.	Task	Description	✔
1	Install the trusted third-party CA root certificate.	This procedure ensures that Avaya SBC can identify and communicate with all external entities.	
2	Generate a certificate signing request.	A CSR must be generated for Avaya SBC for signing by the CA. The signed certificate is used to identify the Avaya SBC. For more information, see Creating a CSR on page 356.	
3	Install the third-party certificate.	After the CA signs the CSR, upload the signed CSR to Avaya SBC. For more information, see Installing certificates on page 358.	

Table continues…

No.	Task	Description	✔
4	Create a TLS server profile.	After installing certificates, create a TLS profile to define the TLS settings for incoming connections. After all of the certificates are installed, a TLS profile must be created to define the TLS settings for incoming connections. For this case, the Avaya SBC will require mutual authentication from all incoming connections and verification that the certificate was signed directly by the CA root certificate. To achieve this, create a TLS server profile with the following settings: • Profile Name: ThirdPartyServer • Certificate: certificate.crt • Peer Verification: Required • Peer Certificate Authorities: root-ca.crt • Peer Certificate Revocation List: None • Verification Depth: 1 • Renegotiation Time: 0 • Renegotiation Byte Count: 0 • Ciphers: All • Options: None Checked • Value: N/A For more information, see Creating a server profile on page 368.	

Table continues…

No.	Task	Description	✔
5	Create a TLS client profile.	Next, create a TLS client profile to define how outgoing TLS connections should be handled. For this case, the Avaya SBC verifies that the remote server identity certificate was signed by the CA root certificate and provides the configured certificate for mutual authentication. To achieve this, create a TLS client profile with the following settings: • Profile Name: ThirdPartyClient • Certificate: certificate.crt • Peer Verification: Required • Peer Certificate Authorities: root-ca.crt • Peer Certificate Revocation List: None • Verification Depth: 1 • Renegotiation Time: 0 • Renegotiation Byte Count: 0 • Ciphers: All • Options: None Checked • Value: N/A For more information, see Creating a client profile on page 372.	
6	Update the signaling interface.	After the TLS profiles are set up, you must associate the profiles to the correct components. The Signaling Interface is the entry point for any incoming signaling traffic from the endpoints or feature servers to the Avaya SBC. **Note:** A TLS server profile cannot be configured unless a TLS port has been configured for a signaling interface. For more information, see Editing an existing signaling interface on page 273.	

Table continues…

No.	Task	Description	✔
7	Update the subscriber flow.	To enable the Avaya SBC in establishing a TLS connection back towards the phone, you must update the subscriber flow to use the TLS client profile. For more information, see Editing an existing subscriber flow on page 165.	
8	Update the server configuration for the call server.	Finally, update the server configuration profiles for the relevant SIP servers. As these define how the Avaya SBC connects to each respective SIP server, they will require a TLS client profile in order to be able to connect via TLS. **Note:** A TLS server profile cannot be configured unless a TLS port has been configured for a server configuration. For more information, see Editing a SIP Server profile on page 318.	

Certificate management

Use the Certificate management page in EMS to manage all certificates used in TLS handshakes.

Note:

You must upload valid PEM-encoded X.509 certificates to the EMS for all certificates, certificate authorities, and certificate revocation lists. You must convert the certificates that are in an incorrect format by using an SSL tool, such as OpenSSL. You can access the OpenSSL tool at: https://www.openssl.org/. For tips and tricks about working with certificates using OpenSSL, see Considerations for working with TLS on page 351.

Certificate Signing Requests (CSRs)

You can use the basic built-in tool in EMS to generate a CSR that is compatible with Avaya SBC. However, is not mandatory to use this tool to generate a CSR.

Note:

- Generate a CSR if the device does not have an ID certificate or if you change any of the device attributes, such as CN or Subject Alt Name.
- Do not generate a CSR to renew a certificate that is about to expire. Use existing CSR from the Certificate management page.

Installing third-party certificates

About this task

Use this procedure to change the TLS certificate presented to the user when logging in to the EMS and SBC management GUI. This task applies to both the management GUI on EMS as well as the management interface on the SBC servers.

Note:

You do not have to encrypt any certificates installed through EMS.

Set up the certificate with the following parameters:

- Either the primary management IP or a DNS name that points to the EMS management IP must be administered.
- Both the Common Name and the Subject Alt Name must have the same name administered.

Before you begin

Ensure that you have an X.509 certificate signed by a trusted CA. This certificate must have the primary management IP of the EMS set as the Common Name or Subject Alt name.

RSA private keys must be equal to or greater than 2048-bit. Avaya SBC supports certificates with 2048-bit or 4096-bit keys.

Procedure

1. Copy the PEM-encoded certificate and associated private key to the EMS server.
2. Navigate to the directory where you saved the copy of the certificate and private key.
3. Login with root credentials and type `install-nginx-certificate` *`path-to-certificate-file path-to-key-file`*.

   Here, *path-to-certificate-file* is the path where the certificate file is uploaded, and *path-to-key-file* is the path where the RSA private key is uploaded.

   If any errors occur, resolve the issues by following the instructions in the error message.

   If the EMS becomes inaccessible, use the **`ipcs-options`** command to regenerate a new self-signed certificate for EMS.

Creating a CSR

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.

   The EMS server displays the Certificates window.

4. Click **Generate CSR**.

   The EMS server displays the TLS Management Generate CSR window.

5. Enter the appropriate information in the TLS Management Generate CSR window and click **Generate CSR**.

   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected.

Related links

TLS certificates field descriptions on page 361

Settings for externally generated CSRs

If you want to generate your own CSR for use with the Avaya SBC, the following settings are recommended:

- Private Key Strength: 2048-bit or greater — Avaya SBC supports certificates with 2048-bit or 4096-bit keys
- Key Usage: keyUsage=keyEncipherment,digitalSignature,non-repudiation
- Extended Key Usage: extendedKeyUsage=serverAuth,clientAuth

Extracting a certificate and key from a PFX or PKCS#12 keystore

About this task

If you have a third-party or non Avaya certificate and key that is in the PKCS#12 format (.p12 or .pfx), use the following procedure to extract the certificate and key.

Note:

PKCS#12 was formerly known as PFX.

Procedure

1. Copy the keystore file to the `/home/ipcs/` directory on Avaya SBC.
2. To extract the certificate from the keystore file, type `openssl pkcs12 -in` *`filename`*`.pfx -out` *`filename`*`.crt -nokeys -clcerts`, where *filename* is the name of the certificate file.
3. To extract the key from the keystore file, type `openssl pkcs12 -in` *`filename`* `-out` *`filename`*`.key -nocerts`

Next steps

After you complete the extraction procedure, install the certificate.

About certificates

An X.509 public key certificate is used to identify the Avaya SBC when performing a TLS handshake for incoming and outgoing connections. The EMS GUI provides several options to manage certificates of this type. In general, the corresponding private key cannot be managed directly from the EMS GUI and can only be uploaded to the EMS when uploading its public counterpart.

Avaya SBC supports certificates with 2048-bit or 4096-bit keys.

Related links

Installing certificates on page 358
Uploading a certificate file on page 359
TLS certificates field descriptions on page 361
Viewing certificate details on page 363
Deleting certificates on page 363

Installing certificates

About this task

Important:

For an HA pair, the certificate and key are uploaded to the primary device and synchronized to the secondary device. However, if you add a new certificate and key on the EMS, you must manually click **Synchronize to HA Peer** to so that the certificate and keys are synchronized onto the secondary device.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificate**.
4. Click **Generate CSR**.
5. Enter appropriate information in the Generate CSR screen, and click **Generate CSR**.

   If you have any other method available, you need not generate CSR using the Avaya SBC EMS web interface.
6. Use the following settings if you want to generate CSR using alternate methods:
   - Certificate: keyUsage = keyEncipherment
   - Private Key: SHA256 with 2048–bit size

   These settings are generated automatically when you generate CSR using the Avaya SBC EMS web interface.
7. If you generate CSR using the Avaya SBC EMS web interface, download the CSR to your computer.

8. Send the CSR to the Certificate Authority (CA) for signing.

   The CA signs the CSR by using the methods that are acceptable at the site.

Next steps

Upload the signed X.509 certificate, the key file, and the trust chain, if necessary, to the EMS through the EMS GUI.

Uploading a certificate file

Before you begin

Obtain the signed certificate from the Certificate Authority (CA). You might also receive a certificate trust chain if the CA did not directly sign the certificate. The certificate trust chain might be provided as a separate file or it might be concatenated directly onto the signed certificate.

If the signed certificate is not in a PEM-encoded format, re-encode the certificate in the PEM format before uploading it to the EMS.

An open-source SSL library with utilities for conversions is available at:

http://www.openssl.org

You can use this utility to convert a file with a DER-encoded format to a PEM format, as shown in the example below:

```
openssl x509 -in input.der -inform DER -out output.pem -outform PEM
```

You can convert a certificate with a .PEM extension to the `.crt` extension by renaming the file and changing the PEM extension to `.crt`.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Click **Install**.
5. In the **Type** field, select **Certificate**.
6. In the **Name** field, type the name of the Certificate file.

   Note:

   You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the name of the Certificate file that you browse for uploading has a different name, that name will be changed with the Certificate name that is uploaded to the EMS.
7. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
8. In the **Key** field, select one of the following options:
   - **Use Existing Key**: Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

Note:

If you are using this option, ensure that the Common Name in the Generate CSR screen matches with the name of the install certificate.

- **Upload Key File**: Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

  In this option, you must upload the private key as described in Step 7.

9. In the **Key File** field, click **Browse** and browse to the location of the key file.
10. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

    This step is required if the CA provided a separate certificate trust chain.

    If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBC. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
11. Click **Upload**.

    The EMS server uploads the signed X.509 certificate and the key file, if necessary, to the SBC. The EMS server automatically synchronizes and installs the certificate and key on multi-server and single server deployments.

Important:

For an HA pair, the certificate and key are uploaded to the primary device and synchronized to the secondary device. However, if you add a new certificate and key on the EMS, you must manually click **Synchronize to HA Peer** to so that the certificate and keys are synchronized onto the secondary device.

Related links

TLS certificates field descriptions on page 361

TLS certificates field descriptions

Certificates tab

Name	Description
Installed Certificates	Some Certificate Authority (CA) signed certificate or self-signed certificate. This certificate is incorporated into a server certificate profile and sent to clients to set up a TLS connection. **Note:** All certificates, certificate authorities, and certificate revocation lists uploaded to the EMS must be valid X.509 certificates in the PEM format. Certificates not in this format might be converted using a proper SSL tool, such as the publicly available OpenSSL tool. You can access this tool from: https://www.openssl.org/
Installed CA Certificates	The unsigned public key certificates from a Certificate Authority (CA), which vouch for the correctness of the data contained in a certificate and verify the signature of the certificate.
Installed Certificate Revocation Lists	The Certificate Revocation Lists (CRLs) that contain the serial numbers of CSRs that have been revoked, or are no longer valid, and should not be relied upon by any system subscriber.
Installed Certificate Signing Requests	The installed certificate signing requests on the system.
Installed Keys	The installed keys for third party certificates.

Install Certificate

Name	Description
Type	The type of certificate that you want to install. The options are: • **Certificate** • **CA Certificate** • **Certificate Revocation List**
Name	The name of the certificate that you want to install. This field is optional, and if not specified, the filename of the uploaded certificate is used as the certificate name. Additionally, specifying a name same as another certificate will overwrite the existing certificate with the one being uploaded.
Overwrite Existing	An option to control whether uploading a certificate with the same name is permitted. If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, when you upload a certificate with the same name overwrites an existing certificate.

Table continues…

Name	Description
Allow Weak Certificate/Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. By default, private keys with a key size less than 2048 bits, signed with a SHA-1 or MD5 based hash, or no key usage extension or extended key usage extension, will be rejected.
Certificate File	The location of the certificate on your system. Depending on your browser, click **Browse** or **Choose file** to browse for the file. If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBC. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
Trust Chain File	The trust chain file used to verify the authenticity of the certificate. Depending on the browser, click **Browse** or **Choose File** to locate the file.
Key	The private key that you want to use. You can opt to use the ilexisting key from the filesystem or select a file containing another key.
Key File	This field is available when you select **Upload Key File** in the **Key** field. Depending on the browser, click **Browse** or **Choose File** to locate the file.
Key Passphrase	This field is available when you select **Upload Key File** in the **Key** field. A key passphrase is used to to protect the key file while installing certificates. You must use the same passphrase in the **Key Passphrase** which you created while creating the third party certificate. For successful encryption of the key, Avaya recommends not to use the dollar sign ($) in **Key Passphrase**.

Generate CSR

Name	Description
Country Name	The name of the country within which the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Locality Name	The locality (city) where the certificate is being created.
Organization Name	The name of the company or organization creating the certificate.
Organizational Unit	The group within the company or organization creating the certificate.
Common Name	The name used to refer to or identify the company or group creating the certificate. It is recommended not to use wildcard (*) character in this field.
Algorithm	The hash algorithms (SHA256) to be used with the RSA signature algorithm.
Key Size (Modulus Length)	The certificate key length (2048 or 3072) in bits.
Key Usage Extension(s)	The purpose for which the public key might be used: Key Encipherment, Non-Repudiation, Digital Signature. The Digital Signature and Key Encipherment options are selected by default.

Table continues…

Name	Description

Subject Alt Name	An optional text field to further identify the certificate.
	You can provide multiple comma-separated entries in this field. You can make a maximum of 10 **Subject Alt Name** entries.
	Avaya SBC supports DNS hostname, IP address and SIP domain name as valid entries for **Subject Alt Name** field. Avaya SBC does not support SIP URI as a valid value for the **Subject Alt Name** field.
	Though wildcard (*) character is supported in this field, it is recommended not to use this character.
	Example of supported format:
	`DNS:.test.com`
	Examples of unsupported formats:
	`DNS:*`
	`DNS:*.com`

Passphrase	The password to encrypt the private key.
Confirm Passphrase	A verification field for the Passphrase.
Contact Name	The name of the point-of-contact within the issuing organization for issues related to the certificate.
Contact E-mail	The contact's e-mail address.

Viewing certificate details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen.
4. Locate the Avaya SBC certificate that you want to view, and click **View**.

   The EMS server displays the View Certificate window.
5. After viewing the certificate information, click the Cancel icon.

Deleting certificates

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen.

4. Locate the Avaya SBC certificate that you want to delete, and click the **Delete**.

   The EMS server displays the delete confirmation window. If the certificate is currently in use by a reverse proxy or TLS profile, the EMS server displays a message to indicate that the certificate is in use. You cannot delete certificates that are currently in use.

5. Click **OK** to confirm.

   The EMS server closes the delete confirmation window and the selected certificate is no longer listed.

About CA certificates

A Certificate Authority (CA) certificate is used to verify that a party is trusted by Avaya SBC. Avaya SBC accepts both CA root certificates and intermediary CA certificates.

Related links

Installing a CA certificate on page 364
CA certificate field descriptions on page 365
Viewing the CA certificate details on page 365
Deleting a CA certificate on page 365

Installing a CA certificate

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Click **Install**.
5. In the **Type** field, select **CA Certificate**.
6. In the **Name** field, type a name for the certificate.
7. Click **Browse** to locate the certificate file.
8. Click **Upload**.

Related links

TLS certificates field descriptions on page 361

CA certificate field descriptions

Name	Description
Type	The type of certificate that you want to install. To install a CA certificate, select **CA Certificate**.
Name	The name of the certificate that you want to install.
Overwrite Existing	An option to control whether uploading a certificate with the same name is permitted. If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, when you upload a certificate with the same name overwrites an existing certificate.
Allow Weak Certificate/Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. By default, private keys with a key size less than 2048 bits, signed with a SHA-1 or MD5 based hash, or no key usage extension or extended key usage extension, will be rejected.
Certificate File	The location of the certificate on your system. Click **Browse** to locate the file.

Viewing the CA certificate details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Locate the Avaya SBC CA certificate that you want to view and click **View**.

   The EMS server displays the View CA Certificate window.
5. After viewing the CA certificate information, click **Concel**.

Deleting a CA certificate

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen in the Content Area.
4. Locate the Avaya SBC CA certificate that you want to delete, and click **Delete**.

   The EMS server displays the delete confirmation window. If the certificate is currently in use by a reverse proxy or TLS profile, the EMS server displays a message to indicate that the certificate is in use. You cannot delete certificates that are currently in use.
5. Click **OK**.

   The EMS server displays the Certificates screen with the deleted CA certificate.

About CRLs

A Certificate Revocation List (CRL) is used to revoke certificates that have been issued by a CA that Avaya SBC trusts. CRL is the only way to revoke an invalid certificate. CRLs list information embedded in certificates, and CA certificates are ignored.

Native CRL file format (Distinguished Encoding Rule - DER) is not supported, and must be converted to PEM format. To convert to PEM format, run the following command: `openssl crl -in SystemManagerCA.crl -inform DER -out SMGRCRL.pem`

Related links

[Installing CRLs](#) on page 366
[CRL field descriptions](#) on page 366
[Viewing CRL details](#) on page 367
[Deleting a CRL](#) on page 367

Installing CRLs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Click **Install**.
5. In the **Type** field, select **Certificate Revocation List**.
6. In the **Name** field, type the name of the certificate.
7. Click **Browse** to locate the certificate file.
8. Click **Upload**.

Note:

When you select **Overwrite existing file** to upload certificate file or CRL using the same name, Avaya SBC receives a trigger about this change. Existing server and client profile in TLS management needs to be edited and saved again so that trigger is sent to Avaya SBC about availability of new cert file. After you edit and save, Avaya SBC gets a trigger for further processing.

CRL field descriptions

Name	Description
Type	The type of certificate that you want to install. In this case, select **Certificate Revocation List**.
Name	The name of the Certification Revocation List (CRL) file to be installed.

Table continues…

Name	Description
Overwrite Existing	An option to control whether uploading a certificate with the same name is permitted. If this field is cleared, uploading a certificate with the same name as another certificate causes failure. If this field is selected, when you upload a certificate with the same name overwrites an existing certificate.
Certificate File	The location on your system of the Certification Revocation List (CRL) file.

Viewing CRL details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Locate the Avaya SBC certificate revocation list that you want to view, and click **View**.
5. After viewing the certificate revocation list information, click **Cancel**.

Deleting a CRL

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Certificates**.
4. Locate the Avaya SBC certificate revocation list that you want to delete and click **Delete**.
5. Click **OK** to delete the selected certificate revocation list.

   The EMS server displays the Certificates screen with the deleted CRL.

About TLS profile management

The basis of the Avaya SBC TLS configuration rests within the TLS profile. A TLS profile is used to control the parameters when performing a TLS handshake with a remote entity. TLS profiles are of two distinct types: server and client.

Related links

[About TLS server profile management](#) on page 368
[About TLS client profile management](#) on page 372

About TLS server profile management

A TLS server profile is used where Avaya SBC processes an incoming connection over TLS from a remote entity. For example, server profile is used while processing a connection from an endpoint.

Use the following procedures to create, edit, and delete TLS server profiles.

Related links

About TLS profile management on page 367
Creating a TLS server profile on page 368
TLS server profile screen field descriptions on page 368
Editing a TLS server profile on page 371
Deleting a TLS server profile on page 372

Creating a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click **Add**.

   The EMS server displays the New Profile window.
5. Administer the options as described in TLS server profile screen field descriptions on page 368.
6. Click **Finish**.

   The EMS server creates, installs and lists the TLS server profile in the application pane.

TLS server profile screen field descriptions

Field	Description
TLS Profile	
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.

Table continues…

Field	Description
SNI Options	Indicates whether the SNI group is required or not. The options are: • **None**: SNI functionality does not have any effect on the client server handshake process. The Avaya SBC server approves the handshake between the client and the server with and without the SNI request. • **Optional**: If there is an SNI request from the client and server_name extension in the client handshake packet matches with the CN or SAN fields of the TLS certificate. The Avaya SBC server approves the handshake between the client and server, otherwise TLS handshake is rejected. If there is no SNI request from the client, the TLS profile associated with the **Signaling Interface** will be used for communication. • **Mandatory**: If there is an SNI request from client and server_name extension in the client handshake packet matches with the CN or SAN fields of the TLS certificate. The Avaya SBC server approves the handshake between the client and server, otherwise handshake is rejected. If there is no SNI request from client, then also the Avaya SBC server rejects the TLS handshake.
SNI Group	Specifies the configured SNI groups. **SNI Group** field is accessible only if **SNI Options** is either Optional or Mandatory.
Certificate Verification	
Peer Verification	One of three check boxes indicating whether peer verification is required: • **Required**: The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** check box is a locked setting and cannot be deselected. • **Optional**: The incoming connection may optionally provide a certificate. If a certificate is provided, but is not contained in the Peer Certificate Authority list, or is contained in a Peer Certificate Revocation List, the connection will be rejected. • **None**: No peer verification will be performed. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.

Table continues…

Field	Description
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Renegotiation Parameters	
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count	The amount of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	
Version	The TLS versions that the client or servers accepts or offers. For Release 10.1.0, the options are: • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** For Release 10.1.2, the options are • **TLS 1.3** • **TLS 1.2** The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the server supports.

Table continues…

Field	Description
Ciphers	The level of security to be used for encrypting data. The options are: • **Default**: The cipher suite recommended by Avaya. • **FIPS**: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • **Custom**: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. **Note:** The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure. For a full list of possible values, see the OpenSSL ciphers documentation at https://www.openssl.org/docs/manmaster/man1/openssl-ciphers.html. To get the list of cipher suites supported by Avaya SBC, run the following command: `openssl ciphers -s -v -<TLS version> '<cipher string>'`, where `<cipher string>` is `DEFAULT:!SHA` for Default ciphers and `FIPS:!ECDH:!ADH:!3DES:!KRB5` for FIPS ciphers. For example, run the following command to get the list of cipher suites supported by Avaya SBC for Default ciphers when using TLS version 1.2: `openssl ciphers -s -v -tls1_2 'DEFAULT:!SHA'`

Note:

The only exception is regarding the Peer Verification parameter setting (see description below). This setting determines if a peer verification operation should be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**, while in a TLS server profile, the Peer Verification parameter may be set to one of three possible values: **Required**, **Optional**, or **None**.

Editing a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Server Profiles**.
4. Click the server profile that you want to edit.
5. From the content area, click **Edit**.

   The EMS server displays the Edit Profile window.

6. Administer the options as described in TLS server profile screen field descriptions on page 368 and click **Finish**.

   To go to the previous field values and close this screen, click **Cancel**.

Deleting a TLS server profile

About this task

Caution:

At least one TLS server profile must be configured for the TLS feature to function properly.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click the server profile that you want to delete.
5. Click **Delete**.

   The EMS server displays a confirmation window to confirm your selection.
6. Click **OK**.

   The EMS server deletes the TLS server profile.

About TLS client profile management

A TLS client profile is used where the Avaya SBC starts an outgoing connection towards a remote entity over TLS, such as a call server.

Use the following procedures to create, edit, and delete TLS client profiles.

Related links

About TLS profile management on page 367
Creating a TLS client profile on page 372
TLS client profile screen field descriptions on page 373
Editing a TLS client profile on page 375
Deleting a TLS client profile on page 375

Creating a TLS client profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Client Profiles**.

4. Click **Add**.

   The EMS server displays the **New Profile** window.

5. Enter the requested information in the appropriate fields.
6. Click **Finish** to save the changes.

   The EMS server installs and displays the new TLS client profile.

TLS client profile screen field descriptions

Name	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
SNI	A check box to enable the SNI feature.
Certificate Verification	
Peer Verification	The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** is selected for this field. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Extended Hostname Verification	Determines whether or not server certificates will be verified only by the DNS entry in the Common Name or Subject Alt Name of the certificate served by the remote server.

Table continues…

Name	Description
Server Hostname	Permits the user to define a custom hostname that will be accepted if served by the remote server. This is primarily intended for use with legacy Avaya products. You must configure **Server Hostname** field for: • Non SIP traffic • Non HTTP traffic • PPM traffic **Server Hostname** field is accessible only if either **Extended Hostname Verification** or **SNI** or both of these check boxes are selected.
Renegotiation Parameters	
Renegotiation Time	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count	The number of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Handshake Options	
Version	The TLS versions that the client or servers accepts or offers. For Release 10.1.0, the options are: • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** For Release 10.1.2, the options are • **TLS 1.3** • **TLS 1.2** The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the client supports.
Ciphers	The level of security to be used for encrypting data. The options are: • **Default**: The cipher suite recommended by Avaya. • **FIPS**: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. • **Custom**: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html. **Note:** The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure.

Note:

The only exception is regarding the Peer Verification parameter setting. This setting determines whether a peer verification operation must be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**. In a TLS server profile, the Peer Verification parameter can be set to one of three possible values: **Required**, **Optional**, or **None**.

Editing a TLS client profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Client Profiles**.
4. Click the client profile that you want to edit.

   The EMS server displays the configuration of the selected client profile in the content area.
5. Click **Edit**.

   The EMS server displays the Edit Profile window.
6. Edit the desired fields and click **Finish**.

   On this screen, you can click **Cancel** to revert to the previous field values and close the window.

Related links

TLS client profile screen field descriptions on page 373

Deleting a TLS client profile

About this task

Caution:

At least one TLS client profile must be configured for the TLS feature to function properly.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **Client Profiles**.
4. In the application pane, click the client profile that you want to delete.
5. Click **Delete**.

   The EMS server displays a confirmation window to confirm your selection.
6. Click **OK**.

   The EMS server deletes the TLS client profile.

Extended hostname validation

With the Extended Hostname Validation feature, the system validates the host name or domain name of the server with the value of the **subject** or **subjectAltName** field in the identity certificate for establishing the SSL connection.

For the Extended Hostname Validation feature, Avaya SBC must support TLS Server Name Indication (SNI).

Note:

Avaya SBC provides server default certificate for backward compatibility for clients that do not support SNI.

About configuring SNI groups

A Server Name Indication (SNI) group is a collection of TLS profiles. The functionality of an SNI group depends on whether the Avaya SBC is acting as a client or as a server during the communication.

Avaya SBC as a server

When client sends a handshake packet to the Avaya SBC server, then depending on the **Server Profiles** option in **TLS Management** > **Server Profiles**, Avaya SBC server checks the SNI string. If the SNI string of the client matches with the Subject Alternative Name (SAN) and Common Name (CN) fields of the server certificate then only the Avaya SBC server accepts handshake packet and allows the communication.

Avaya SBC as a client

For enabling SNI from the Avaya SBC client, enable **Extended Hostname Verification** from **TLS Management** > **Client Profiles** and provide the **Server Hostname**. Avaya SBC client sends an SNI request with the **Server Hostname** as the SNI string to the server. If the **Extended Hostname Verification** field is not enabled, then Avaya SBC sends **SIP Server IP Address** in the handshake request packet. Communication between the client and server depends on the configurations at the server side.

Note:

- If the Avaya SBC client sends a handshake packet with an empty **Server Hostname** and with the SIP server IP address, the TLS client profile cannot be associated with the reverse proxy policy.
- If **Extended Hostname Verification** is not required for the client server handshake, then Avaya recommends you to configure IP Address in **IPAddress/FQDN** field in **Services** > **SIP Servers** for DNS resolution and routing of the PPM traffic.
- If **Extended Hostname Verification** is required for the client server handshake, then Avaya recommends to configure IP Address in **IPAddress/FQDN** field in **Services** > **SIP Servers** and provide the **Server Hostname** for the Extended hostname validation feature to work properly.

- If the TLS certificate in the SNI group matches with the server_name of SNI request from the client, Avaya SBC replaces the certificate in the TLS profile with the certificate of the SNI request received from the client.

Creating a new SNI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **SNI Group**.

   The application pane displays the existing SNI group.
4. Click **Add**.

   Avaya SBC displays the first SNI Group window.
5. In the **Rule Name** field, type a name for the new SNI Group, and click **Next**.

   Avaya SBCdisplays the second SNI Group window.
6. In the **TLS Profiles** field, enter the already configured TLS server profile, and click **Finish**.

Result

The application pane displays the newly created SNI Group.

Renaming an SNI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **SNI Group**.

   The application pane displays the existing SNI group.
4. Click the name of the SNI group that you want to rename.
5. In the upper-right section of the screen, click **Rename**.

   The Avaya SBCdisplays the Rename Profile window.
6. Type a new name for the SNI group in the **New Name** field, and click **Finish**.

Result

The application pane displays the renamed SNI group.

Cloning an existing SNI group

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **SNI Group**.

   The application pane displays the existing SNI group.
4. In the application pane, click the name of the SNI group that you want to clone.
5. In the content pane, click **Clone**.

   Avaya SBC displays the Clone Profile window.
6. In the **Clone Name** field, type a name for the new SNI group and click **Finish**.

Result

The application pane displays the newly cloned SNI group.

Deleting an SNI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **TLS Management** > **SNI Group**.

   The application pane displays the existing SNI group.
4. Click the name of the SNI group that you want to delete.
5. In the upper-right section of the screen, click **Delete**.

   Avaya SBC displays the delete confirmation window.
6. Click **OK**.

Result

The application pane no longer displays the deleted SNI group.

Chapter 10: System monitoring

About system monitoring

There are many tools available to help you monitor the health and status of your Avaya SBC. This section describes the following tools:

- Dashboard – The first screen you see when you log on to the system. It summarizes connectivity, alarms, and incidents, giving you quick access to troubleshoot any problems.
- System alarms – The **Alarms** menu provides access to any open alarms and allows you to resolve and close alarms.
- Incidents – The **Incidents** menu item provides quick access to the list of the most recent incidents so you can troubleshoot problems.
- System status - The **Status** menu gives you access to SIP, user, server, and performance status.
- Logs – The **Logs** menu gives you access to system logs and audit logs.
- Diagnostics – The **Diagnostics** menu item allows you to run a quick diagnostics on links between servers within your deployment and ping specific servers.
- Administrative users – The **Users** menu item gives you a quick listing of which administrative users are logged on to the system.

In addition, there are other tools described in this section to help diagnose and fix problems within your system.

Dashboard

The Dashboard screen displays system information, installed devices, alarms, and incidents. The screen displays additional separate summary windows, such as Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The summary windows contain active, up-to-the-minute alarms, incident, statistical, log, diagnostic, and user information, and review and exchange textual messages with other administrative user accounts.

The Content area of the Dashboard screen contains various summary areas that display top-level, systemwide information, such as:

- Which alarms and incidents are currently active.

- Links to available Quick Links.
- List of installed Avaya SBC security devices.
- Avaya SBC deployment information.
- Area for viewing and exchanging text messages with other administrators.

Dashboard content descriptions

Name	Description
System Time	The current system time.
Version	The system software version.
GUI Version	The system GUI version.
Build Date	The system software build date.
License State	The license state.
Aggregate Licensing Overages	The aggregate license information.
Peak Licensing Overage Count	The peak licensing count.
Last Logged in at	The date and time when the user last logged in.
Failed Login Attempts	The number of failed login attempts.
Installed Devices	A list of all Avaya SBC security devices currently deployed throughout the network.
Incidents (past 24 hours)	A list of current incidents reported by Avaya SBC security devices to the EMS web interface.
Active Alarms (past 24 hours)	A list of current alarms reported by Avaya SBC security devices to the EMS web interface.
Add	A user-editable text message exchange area.
Notes	The text message created by using the **Add** function.

Alarms

Current system alarms are reported to the EMS web interface. The alarms are displayed as a red indicator on the Alarm viewer page and on the dashboard for the respective device.

The notifications provide the information necessary to clear the condition causing the alarm notification.

Viewing current system alarms

About this task

The Alarms screen displays a summary of all currently active system alarms. If no alarms are active, the system displays a blank screen. The Alarms screen is accessed only if the **Alarm Status Indicator** on the toolbar indicates an alarm status, flashed red. Use the following procedure to view current system alarms.

Procedure

1. Log in to the EMS web interface web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. On the toolbar, click **Active Alarms** or click on the specific alarm you want to view from the **Alarms (past 24 hours)** section of the Dashboard screen.

   The EMS server displays the Alarms Viewer screen.
4. Select the Avaya SBC device for which you want to view the alarms.

   The Alarms section displays all the currently active alarms for the selected Avaya SBC security device.

   For the field description of each security reporting component of the Alarms screen, see Alarm Viewer field descriptions.

Alarm Viewer field descriptions

Name	Description
ID	Sequential, numerical identifier of the alarm being reported.
Details	The specific or descriptive name of the active alarm.
State	Current state of the alarm: ON The **State** field for any displayed alarm is always: ON
Time	Date and time when the alarm was generated.
Device	The Avaya SBC device that generated the alarm.

Clearing system alarms

About this task

You can either delete a selected alarm or all alarms. Most of the alarms are cleared automatically when the condition to create these alarms no longer exist. However, there are some alarms that need to be cleared manually.

Procedure

1. Log in to the EMS web interface web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. To clear the selected alarm or all alarms, on the Alarms screen, click **Clear Selected** or **Clear All**.

   The EMS server displays a confirmation pop-up window.
4. Click **OK**.

System alarms list

This section covers the description of system alarms. Some system alarms require manual intervention, while some get cleared automatically. For information about clearing these alarms, see the Clearing event and Manual intervention columns. System alarms are reported on both the primary and secondary servers in High Availability (HA) deployments.

CPU alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
CPU	CPU utilization is over 80%	CPU utilization is between 80%-89%.	No	Alarm	Minor	CPU utilization is between 80%-89%.	CPU utilization goes below 80% or above 89%.	No
CPU	CPU utilization is over 90%	CPU utilization is between 90%-99%.	No	Alarm	Major	CPU utilization is between 90%-99%.	CPU utilization goes below 90% or becomes 100%.	No
CPU	CPU utilization is 100%	CPU utilization is 100%.	Yes	Alarm	Critical	CPU utilization is 100%.	CPU utilization becomes 100%.	No

Memory alarms (including Swap Space)

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Memory	Memory utilization is over 80%	Memory utilization is between 80%-89%.	No	Alarm	Minor	Memory utilization is between 80%-89%.	Memory utilization goes below 80% or above 89%.	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Memory	Memory utilization is over 90%	Memory utilization is between 90%-99%.	Yes	Alarm	Major	Memory utilization is between 90%-99%.	Memory utilization goes below 90% or becomes 100%.	No
Memory	Memory utilization is 100%	Memory utilization is 100%.	Yes	Alarm	Critical	Memory utilization is 100%.	Memory utilization becomes 100%.	No

Disk partition space alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Disk partition <partition_name> utilization is over 80%	Disk partition utilization is between 80%-89%.	No	Alarm	Minor	Disk partition utilization is between 80%-89%.	Disk partition utilization goes below 80% or above 89%.	No
Disk partition space	Disk partition <partition_name> utilization is over 90%	Disk partition utilization is between 90%-99%.	Yes	Alarm	Major	Disk partition utilization is between 90%-99%.	Disk partition utilization goes below 90% or becomes 100%.	No
Disk partition space	Disk partition <partition_name> utilization is 100%	Disk partition utilization is 100%.	Yes	Alarm	Critical	Disk partition utilization is 100%.	Disk partition utilization becomes 100%.	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Database pg_committs usage more than 1GB	If disk usage of '/var/lib/pgsql/9.4-bdr/data/pg_xlog/' gets more than 1 GB, this alarm is raised.	No	Alarm	Critical	pg_committs directory size is more than 1 GB.	Yes	No
Disk partition space	Database replication pg_xlog usage more than 1GB	If disk usage of '/var/lib/pgsql/9.4-bdr/data/pg_committs/' gets more than 1 GB, this alarm is raised.	Yes	Alarm	Critical	Pg_xlog directory size is more than 1 GB.	No	Yes
Disk partition space	Database replication pg_logical snapshots usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/snapshots' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / snapshots directory.	Yes	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Database replication pg_logical mappings usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/mappings' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / mappings directory.	Yes	No
Disk partition space	Database replication pg_logical checkpoints usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/checkpoints' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / checkpoints directory.	Yes	No

Hard disk failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Hard disk failure	Hard disk <disk_id> failure	Hard disk failure	Yes	Alarm	Critical	The hard disk drive has failed and cannot be used.	The alarm is cleared only when the kernel detects no failures when testing the hard disk drive. This will only happen when the hard disk drive is replaced.	Yes. Hard disk drive must be replaced.[1]

Link failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Link failure	Network link failure <interface>	Network link goes down on the given interface.	Yes. No traffic can be sent or received on the failed link.	Alarm	Critical	A link on a particular interface in down and cannot be used.	Network connection is restored and alarm manually cleared by user.	Yes. User needs to manually restore the link.

[1] See Swapping a separate Avaya SBC server deployed under EMS on page 211, Swapping Avaya SBC devices in an HA pair deployment on page 211, Swapping an EMS server in a single server deployment on page 212, Swapping a primary EMS server in an HA pair deployment on page 213, and Swapping a secondary EMS server in an HA pair deployment on page 213.

Process failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Process failure	Application failure	One or more system processes failed to send a heartbeat ping.	Yes. Port By-pass is automatically enabled.	Alarm	Critical	One or more system processes is malfunctioning	Malfunctioning process is restarted either automatically by the system or manually by the Security Administrator and the alarm cleared.	Yes. Required if automatic self-start is not successful.

Database failure alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database failure	Database failure	Connectivity to the database has been lost.	Yes. Port By-pass is automatically enabled after multiple failed restarts.	Alarm	Critical	Either the database is down or connectivity to the database has been lost.	The database failure being cleared either automatically by the system or manually by the Security Administrator.	Yes. Required if automatic self-start is not successful.

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database Failure	Data Replication is broken	Database replication is broken between the HA SBC systems or the active-active EMS systems	No. But if the alarm does not get user attention and if ignored in the long run could lead to disk space issues and could cause the SBC to go down. Also, in case if the SBC displays the alarm 'Database replication pg_xlog usage more than 1 GB then it needs immediate attention.	Alarm	Critical	Database Replication has stopped working between HA SBC's or the active-active EMS and needs attention.	1. If this alarm pops up in the middle of upgrade / rollback, it is safe to ignore the alarm. 2. If this alarm pops up in a working system on 8.1 where both SBC's or EMS's are at the same version, the alarm is cleared after manual intervention is successful.	1. No 2. Yes

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database Failure	Peer SBC is Unreachable	The Peer HA SBC or EMS is down.	No. But in case if the SBC displays the alarm 'Database replication pg_xlog usage more than 1GB' then it needs immediate attention.	Alarm	Critical	If this alarm is seen on HA SBC, it means the peer SBC is not reachable. If this alarm shows up for EMS, it means the peer EMS is down.	Alarm gets cleared automatically once the peer SBC comes back online.	If the peer SBC was kept down intentionally, power on the SBC and make sure it comes back up again. Manual intervention is also needed in case if the SBC has hard disk failure and is never going to come back again.

Component failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Component failure	Component failure	One or more elements (signaling, media, intelligence, or EMS) in a multi-component configuration has failed to send a heartbeat ping.	Yes	Alarm	Critical	One or more SBC server elements (signaling, media, intelligence, or EMS) is malfunctioning.	The malfunctioning elements could be restarted manually and the alarm cleared manually.	Required if self restart in not successful.

Clearing a “Data Replication is broken” alarm

Use this procedure to clear a “Data Replication is broken” alarm on either an SBC HA pair or on an active-active EMS pair.

Caution:

This procedure is service interrupting and will cause down time on the deployment. Try to do this during low or no traffic periods.

Condition

Alarm message text	Data Replication is broken
Alarm level	Critical

Solution

1. On SBC A in an HA pair or the Primary EMS in an active-active EMS pair, do the following:
   a. Do a database backup using the following command:

      `/usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup`

   b. Stop replication using the following command:

      `/usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication`

2. On SBC B in an HA pair or the Secondary EMS in an active-active EMS pair, do the following:
   a. Do a database backup using the following command:

      /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup

   b. Stop replication using the following command:

      /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication

3. Reboot SBC A or the Primary EMS using the following command:

   /sbin/reboot

4. Once SBC A or the Primary EMS is online and processes are up, reboot SBC B or the Secondary EMS using the following command:

   /sbin/reboot

Clearing a “Data replication pg_xlog usage more than 1 GB” alarm

Use this procedure to clear a “Data replication pg_xlog usage more than 1 GB” alarm.

Caution:

This procedure is service interrupting and will cause down time on the deployment. Try to do this during low or no traffic periods.

Condition

Alarm message text	Data replication pg_xlog usage more than 1 GB
Alarm level	Critical

Solution

Scenario 1 — Check the replication status between the SBC systems to see if the “Data Replication is broken” alarm is active.

1. Do one of the following depending on the type of system you are troubleshooting:
   - On an SBC system, run the following commands:

     psql -U postgres -d sbcedb

     sbcedb=# select * from alarms;
   - On an EMS system, run the following commands:

     psql -U postgres -d commondb

     commondb=# select * from alarms;

   If the alarm is seen, then follow the steps in Clearing a Data Replication is broken alarm on page 390 to clear the alarm. This should also fix the “Data replication pg_xlog usage more than 1 GB” issue.

Scenario 2 — The number of pg_xlogs will grow if the peer SBC or EMS system is down for a long time. To prevent the disk space from getting full, you must act immediately when this alarm is seen.

2. Check the database alarms table. If the table has the alarm “Peer SBC is unreachable”, confirm that the peer SBC or EMS system is powered up and in operation. It must be in operation so that database replication can occur.
   - On an SBC system, run the following commands:

     psql -U postgres -d sbcedb

     sbcedb=# select * from alarms;
   - On an EMS system, run the following commands:

     psql -U postgres -d commondb

     commondb=# select * from alarms;

   If the peer SBC or EMS has a true hardware failure, break the replication on the SBC or EMS system that is in operation so that pg_xlogs will no longer grow on that system. To break the replication, downtime is required.
3. On the operational SBC or EMS system, do the following:
   a. Do a database backup using the following command:

      /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup
   b. Stop replication using the following command:

      /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication
   c. Reboot the system using the following command:

      /sbin/reboot

Scenario 3 — Disk space of `/var` becomes 100% full and the SBC or EMS system goes down. This happens when the alarms “Data Replication is broken”, “Data replication pg_xlog usage more than 1 GB”, and “Peer SBC is unreachable” have occurred and were not attended to.

4. Run the following command to check the `/var` partition files to see which files are causing the disk space issue:

   cd /var

   du –sh

   This command lists the file size of each file in the `/` root directory. Confirm whether any pg_xlog files are more than 1 GB verify that the cause of the issue is really due to log size or replication being down.
5. Do a backup of the entire database. In a HA system or active-active EMS system, do a backup of the database on both systems, if possible. In the SBC or EMS that is operational, run the following command:

   /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup
6. For any systems that are down because `/var` is 100% full, you cannot use the standard backup command. You must use the following commands:

Important:

Confirm that the archive directory you select has enough space for the complete database backup.

```
mkdir /archive/tst

tar -zcvf /archive/tst/db-bkp.tar.gz /var/lib/pgsql/9.4-bdr/data/
```

When using Steps 7–9, the down SBC will get all of the SBC configurations from the SBC that is up and running.

7. On the SBC or EMS system that is operational, break the database replication and reboot the system using the following commands:

   ```
   /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication

   /sbin/reboot
   ```

8. Confirm that the operational SBC or EMS system comes back online and starts all processes.
9. On the SBC or EMS system that is down or has database issues, confirm that both application processes and the database are down. Run the following commands to delete the database directory, recreate the database directory, recreate the database, break replication, and reboot the server:

   ```
   rm -rf /var/lib/pgsql/9.4-bdr/data/

   /usr/local/ipcs/db/scripts/db_post_tasks.sh 1

   /usr/local/ipcs/db/scripts/dbmanage.py --dbcreate --dbname sbcedb
   --dbtype sbcedb --no-schema True

   /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication

   /sbin/reboot
   ```

GUI and console alarm list

- New User Added Alarms on page 394
- New Administrator Added Alarms on page 394
- User Privilege Change Alarms on page 394
- User Deleted Alarms on page 395
- Login Failure Alarms on page 395

New user-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New User Added	New User Added: <username>	A new GUI/ System user was added.	No	Alarm	Informational	A new user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

New Administrator-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New Admin-added	Admin User Added: <username>	A new GUI/ System admin user was added.	No	Alarm	Informational	A new admin user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

User privilege change alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Privilege Change	User Privilege Changed: <username>	A user's access privilege was changed (either from admin to normal or from normal to admin).	No	Alarm	Informational	A user's access privilege was changed (either from admin to normal or from normal to admin).	Alarm either cleared by the administrator or it times-out.	No

User deleted alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Deleted	User deleted: <username>	A new GUI/ System admin user was deleted.	No	Alarm	Informational	A user was deleted from the system.	Alarm either cleared by the administrator or it times-out.	No

Login failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Login failure	User login failure: <username>	A user had multiple consecutive login failures.	No	Alarm	Warning	A user had more than a certain number of consecutive login failures.	Alarm either cleared by the administrator or it times-out.	No

Incidents

The following sections describe the incidents that can occur in Avaya SBC.

Denial of Service (DoS) incidents

Incident Name	Component generating the trap	Cause and solution
ipcsSingleSourceDoS	SBC	Avaya SBC detects a single source DoS
ipcsSingleSourceCallWalkDoS	SBC	Avaya SBC detects a call walk DoS
ipcsPhoneDoS	SBC	Avaya SBC detects a phone DoS
ipcsPhoneStealthDoS	SBC	Avaya SBC detects a phone stealth DoS

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsServerDoS	SBC	Avaya SBC detects a server DoS or blocks a server DoS The incident occurs due to any of the following reasons: • Initiated Threshold Crossed - Action Whitelist • Pending Threshold Crossed- Action Whitelist • Failed Threshold Crossed- Action Whitelist • attack from Server side - Initiated Threshold Crossed- Action SIV • attack from Server side - Pending Threshold Crossed- Action SIV • attack from Server side - Failed Threshold Crossed- Action SIV • Initiated Threshold Crossed- Action Limit • Pending Threshold Crossed- Action Limit • Failed Threshold Crossed- Action Limit
ipcsPhoneStealthDDoS	SBC	Avaya SBC detects a phone stealth DDoS
ipcsDomainDoS	SBC	Avaya SBC detects a domain DoS

Blacklist/Whitelist incidents

Incident Name	Component generating the trap	Cause and solution
ipcsBlackipcsListCallBlocked	SBC	Avaya SBC comes across a blacklisted caller

Scrubbing related incidents

Incident Name	Component generating the trap	Cause and solution
ipcsDroppedScrubMsg	SBC	Avaya SBC comes across a SDP parser error or scrubber anomaly
ipcsRejectedScrubMsg	SBC	Avaya SBC comes across a scrubber anomaly
ipcsDetectedScrubMsg	SBC	Avaya SBC comes across a scrubber anomaly

Protocol discrepancy incidents

Incident Name	Component generating the trap	Cause and solution
ipcsACKMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue ACK message
ipcsBYEMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue BYE message
ipcsCANCELMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue CANCEL message
ipcsNOTIFYMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue NOTIFY message
ipcsPRACKMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue PRACK message
ipcsREINVITEMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue REINVITE message
ipcsREFERMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue REFER message
ipcs1XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 1xx class response
ipcs2XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 2xx class response
ipcs3XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 3xx class response
ipcs4XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 4xx class response
ipcs5XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 5xx class response
ipcs6XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 6xx class response
ipcsAuthRealmMismatch	SBC	Avaya SBC comes across a realm mismatch

Policy related incidents

Incident Name	Component generating the trap	Cause and solution
ipcsCallDenied	SBC	Calls to the Avaya SBC are denied due to any of the following reasons: • Video is disabled or disallowed • Audio is disabled or disallowed • Maximum number of video sessions is exceeded • Maximum number of audio sessions is exceeded • Maximum number of audio sessions per endpoint is exceeded • Maximum number of video sessions per endpoint is exceeded • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed out of dialog message • Standard method disallowed out of dialog message • No Routing Rule is matched • Codec is disallowed • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsRegistrationDenied	SBC	Avaya SBC denies registration because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed out of dialog message • Standard method disallowed out of dialog message • No Routing Rule is matched • Method is disallowed
ipcsSubscriptionDenied	SBC	Avaya SBC denies subscription because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed in dialog message • Standard method disallowed in out of dialog message • No Routing Rule is matched • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsRedirectionDenied	SBC	Avaya SBC denies redirection because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed in dialog message • Standard method disallowed in dialog message • Prop method disallowed in out of dialog message • Standard method disallowed in out of dialog message • No Routing Rule is matched • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsMessageDropped	SBC	Avaya SBC drops a message because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Response prop header is disallowed • Response standard header is disallowed • Response prop header is mandatory • Response standard header is mandatory • Response prop header is disallowed • Response standard header is disallowed • Request prop header is mandatory • Request standard header is mandatory • Prop method disallowed in dialog message • Standard method disallowed in dialog message • Method is disallowed • Prop method disallowed in out of dialog message • Standard method disallowed in out of dialog message

Route incidents

Incident Name	Component generating the trap	Cause and solution
ipcsPrimaryRadiusServerUnreachable	EMS	Primary Radius server is unreachable
ipcsSecondaryRadiusServerUnreachable	EMS	Secondary Radius server is unreachable

TLS certificate failure incidents

Incident Name	Component generating the trap	Cause and solution
ipcsTlsCertificate	SBC	Avaya SBC comes across a TLS certificate error because of any of the following causes: • Could not create TLS context - for default client mode • No cipher list is provided • Could not create TLS context for either server or client mode • Could not read Certificate • Could not read private key • Private key does not correspond to the loaded certificate • Unable to load Root Certificate or CA list • Unable to load CRL list • Unable to cipher list provided • No cipher list provided

Media anomaly detection incidents

Incident Name	Component generating the trap	Cause and solution
ipcsPacketSizeViolation	SBC	Avaya SBC comes across a packet size violation
ipcsSSRCViolation	SBC	Avaya SBC comes across a synchronization source
ipcsSeqNoViolation	SBC	Avaya SBC comes across a sequence number violation
ipcsTimestampViolation	SBC	Avaya SBC comes across a timestamp violation
ipcsMediaInActivityFromBothSides	SBC	Avaya SBC comes across a media inactivity from both sides of the call There is call audit that runs on the SBC. If there is no media activity or signaling activity for some specified period, that call will be cleared by the audit. You can track the call ID in the incident and then check that in using traceSBC to see the call flow for the specified call.

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsUnsupportedMedia	SBC	Avaya SBC comes across unsupported media
ipcsRTPDoSAttack	SBC	Avaya SBC comes across an RTP denial of service attack
ipcsMediaPortUnavailable	SBC	No free media ports are available
ipcsRTPInjectionAttack	SBC	Avaya SBC comes across an RTP injection attack

HA link failover incident

Incident Name	Component generating the trap	Cause and solution
ipcsHAGracefulFailover	SBC	The primary server has gone down voluntarily
ipcsHAKaFail	SBC	High Availability keep alive messages fail
ipcsHATakeoverDone	SBC	HA takeover is completed
ipcsHASecondaryDown	SBC	HA secondary server is down and HA will not be available until the secondary server is up

License incidents

Incident Name	Component generating the trap	Cause and solution
sbcLicenseExceeded	SBC	Avaya SBC gets requests after the maximum number of licensed sessions is exceeded

TURN/STUN incidents

Incident Name	Component generating the trap	Cause and solution
sbcTurnStunMediaRelayCreationFailed	SBC	Media relay flow creation failed
sbcTurnStunMediaRelayDeletionFailed	SBC	Media relay flow deletion failed

Table continues…

Incident Name	Component generating the trap	Cause and solution
sbcTurnStunServerError	SBC	Avaya SBC detects a TURN/STUN error because of any of the following reasons: • Invalid User Name is configured • Invalid Realm is configured • Invalid Password is configured • Invalid Realm is configured • Relay Port is unavailable • TCP/TLS Listener has failed • Invalid User Account is configured • Invalid User Name is configured

CES Proxy incidents

Incident Name	Component generating the trap	Cause and solution
sbcCesProxy1xMUserLoginFailed	SBC	Login attempts from an Avaya one-X® Mobile user to the CES proxy fails because of any of the following reasons: • Protocol Type validation failed • CesProxy data is not present • Avaya SBC received an invalid response other than login response • Object Type validation failed • Login request data type validation failed • Login request key id validation failed • API object type validation failed • API data type and key Id validation failed • API data type validation failed • API key id validation failed • Object type validation failed • Avaya one-X® Mobile user login failed

Viewing system incidents

About this task

You can view a complete descriptive list of all system incidents that have occurred since the last viewing period by using the Incident screen. The screen displays the last five incidents at any point of time. With this feature, you can view system-wide incidents according to category, such

as DoS, Policy, and Scrubbing. When the Incident screen is open, the latest incident information is available, and the operator can scroll through the incidents list. The screen can display up to 15 incidents at one time. Use the following procedure to view current system incidents.

Note:

You can only view the incidents. They cannot be edited or deleted.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. On the toolbar, click **Incidents**.

   The EMS server displays the Incidents Viewer page.

   You can view the incidents by clicking the specific incident on the **Incidents (past 24 hours)** section of the Dashboard screen.
4. Using the **Device** and **Category** fields, choose a search filter to find and display the particular incidents that you want to view.

   The Incident screen display changes to reflect the search criteria when a selection is made.
5. To ensure that the EMS server displays all required incidents, periodically click **Refresh** to refresh the display.
6. Click **Clear Filters**.

   The EMS server clears the filtering criteria of the **Device** and **Category** fields and sets the value of the fields to All.
7. Click **Generate Report** and select the start and end date to generate the report.

Incident Viewer field descriptions

Search Criteria

Name	Description
Device	The device for which you want to view incidents.

Table continues…

Name	Description
Category	The category of the incident. The options are: • Authentication • Black White List • DoS • High Availability • Media Anomaly Detection • Policy • Protocol Discrepancy • RSA Authentication • Scrubbing • Spam • TLS Certificate • DNS • Licensing • TURN/STUN • CES Proxy • Accounting • WebUA

Search Results

Name	Description
Type	The type of incident.
ID	A number that identifies the incident.
Date	The date on which the incident occurred.
Time	The time at which the incident occurred.

Table continues…

Name	Description
Category	The category of the incident. The options are: • **All** • **Authentication** • **Black White List** • **CES Proxy** • **DNS** • **DoS** • **High Availability** • **Licensing** • **Media Anomaly Detection** • **Policy** • **Protocol Discrepancy** • **RSA Authentication** • **Scrubbing** • **Spam** • **TLS Certificate** • **TURN/STUN**
Device	The device associated with the incident.
Cause	The cause of the incident.

Button	Description
Clear Filters	Clears filters applied to the search results and displays all incidents.
Refresh	Refreshes the list of incidents.
Generate Report	Opens the Generate Report page.

Generate Report

Name	Description
Start Date	The date from which incidents must be included in the incidents report.
End Date	The date to which incidents must be included in the incidents report.

System status

Using the **Status** menu on the administration user interface. You can view several statistics that give you an indication of how your deployment is operating.

Related links

Viewing SIP statistics on page 408
Viewing periodic statistics on page 412
User registration on page 414
Server status on page 416
Viewing IP/URI Blocklist on page 418
Enabling or disabling Telemetry reports on page 418

Viewing SIP statistics

About this task

The Statistics screen provides a snapshot display of certain cumulative, system-wide generic and SIP-specific operational information.

Note:

You can only view the statistics information. You cannot edit or delete the statistics information. However, you can reset the counters for the SIP statistics.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **SIP Statistics**.

   Important:

   Do not click **SIP Statistics** repeatedly. If you repeatedly click and trigger frequent loading of the Statistics page, the Statistics Viewer page shows a communication error.

   The EMS server displays the Statistics Viewer screen.
3. To view the statistics, click one of the following tabs:
   - **SIP Summary**
   - **CES Summary**
   - **Subscriber Flow**
   - **Server Flow**
   - **Policy**
   - **From URI**
   - **To URI**
   - **Transcoding Summary**
   - **Dynamic License Summary**

   Information for each of these tabs are shown in SIP statistics field descriptions on page 409.

SIP statistics field descriptions

SIP Summary tab

Name	Description
Active Registrations	The total number of active SIP registrations.
Active TCP Registrations	The number of active SIP registrations with TCP transport.
Active UDP Registrations	The number of active SIP registrations with UDP transport.
Active TLS Registrations	The number of active SIP registrations with TLS transport.
Total Active Calls	The total number of active calls. **Total Active Calls** is the sum of SRTP (anchored), SRTP (unanchored), RTP (anchored), and RTP (unanchored) calls.
Total Direct Media Calls	The total number of active calls in which media is unanchored. **Total Direct Media Calls** is the sum of SRTP (unanchored) and RTP (unanchored) calls. This value is a subset of **Total Active Calls**.
Active SRTP Calls	The number of active SRTP calls. **Active SRTP Calls** is the sum of SRTP (anchored) and SRTP (unanchored) calls. This value is a subset of **Total Active Calls**.
Active Direct Media SRTP Calls	The number of active SRTP calls in which media is unanchored. **Active Direct Media SRTP Calls** is the number of SRTP (unanchored) calls. This value is a subset of **Total Active Calls**, **Total Direct Media Calls**, and **Active SRTP Calls**.
Active Subscriptions	The number of active subscriptions.
Active Video calls	The number of active video calls.
Active Transfer sessions	The number of active transfer sessions.
Active Shared Control sessions	The number of shared control sessions.
ipcssipcActiveTurnSession	The number of IPCS SIP active TURN sessions. **Note:** This statistic is only shown on the **Subscriber Flow**, **Server Flow**, and **Policy** tabs.

CES Summary tab

Name	Description
1XM User Logins Failed	The number of failed Avaya one-X® Mobile user logins.
1XM User Logins Succeeded	The number of successful Avaya one-X® Mobile user logins.
Reset	All values are reset.

Subscriber Flow tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Subscriber Flow	Selects the subscriber flow for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Server Flow tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Server Flow	Selects the server flow for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Policy tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the policy group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

From URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
URI Group	Selects the source URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

To URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the destination URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Transcoding Summary

Name	Description
Streaming	Specifies whether live statistics are displayed.
Total Active Transcoding Sessions	The number of active transcoding sessions.
Total Transcoding Sessions	The number of transcoding sessions.
Total Transcoding Sessions Failed	The number of failed transcoding sessions.
Total Transcoding Sessions Modifications	The number of transcoding sessions that resulted in a change in codecs.
Total Transcoding Sessions Modifications Failed	The number of transcoding sessions that resulted in a failure while changing codecs.
Reset	All values are reset.

Dynamic License Summary

Name	Description
Streaming	Specifies whether live statistics are displayed.
Standard Sessions Reserved	The number of standard session licenses that are reserved.
Standard Sessions In-Use	The number of standard session licenses that are currently in use.
Advanced Sessions Reserved	The number of advanced session licenses that are reserved.
Advanced Sessions In-Use	The number of advanced session licenses that are currently in use.
Scopia Video Sessions Reserved	The number of Avaya Meetings Server video session licenses that are reserved.
Scopia Video Sessions In-Use	The number of Avaya Meetings Server video session licenses that are currently in use.
CES Sessions Reserved	The number of Client Enablement Services (CES) session licenses that are reserved.
CES Sessions In-Use	The number of CES session licenses that are currently in use.

Table continues…

Name	Description
AMR Sessions Reserved	The number of AMR session licenses that are reserved.
AMR Sessions In Use	The number of AMR session licenses that are currently in use.
Transcoding Sessions Reserved	The number of transcoding session licenses that are reserved.
Transcoding Sessions In-Use	The number of transcoding session licenses that are currently in use.
Premium Sessions Reserved	The number of premium session licenses that are reserved.
Premium Sessions In-Use	The number of premium session licenses that are currently in use.

Viewing periodic statistics

Before you begin

Enable periodic statistics in **Network & Flows** > **Advanced Options**, and specify a collection interval.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Periodic Statistics**.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. Enter the date and time periods for which you want to search for statistics.
5. Click **Search**.
6. To view the statistics, click any of the following tabs:
   - **Summary**
   - **Subscriber Flow**
   - **Server Flow**
   - **Policy Group**
   - **To URI**
   - **From URI**

   Information for each of these tabs are shown in Periodic statistics field descriptions on page 412.

Periodic statistics field descriptions

Name	Description
Total Registrations	The number of active SIP registration requests received.

Table continues…

Name	Description
Total Subscriptions	The number of active subscription requests received.
Registrations Rejected	The number of rejected registrations.
Subscriptions Rejected	The number of rejected subscriptions.
Deregistrations	The number of de-registered requests.
Unsubscriptions	The number of unsubscribed requests.
Total Calls	The number of SIP calls received.
Calls Terminated	The number of terminated SIP calls.
Calls Rejected	The number of SIP calls rejected by Avaya SBC because of policy violation.
Calls Rejected by SBC	The number of SIP calls rejected by Avaya SBC.
Total Transferred Calls	The number of transferred SIP calls.
Calls Failed in Transfer	The number of SIP calls failed in transfer.
Total Redirected Calls	The number of redirected call.
Calls Failed in Redirection	The number calls failed in redirection.
Total SRTP Calls	The number of SRTP calls.
SRTP Calls Terminated	The number of terminated SRTP calls.
SRTP Calls Rejected	The number of rejected SRTP calls.
SRTP Calls Rejected by SBC	The number of SRTP calls rejected by Avaya SBC.
Total Video Calls	The number of video calls.
Video Calls Terminated	The number of terminated video calls.
Total Video Calls Rejected	The number of rejected video calls.
Video Calls Rejected by SBC	The number of video calls rejected by Avaya SBC.
Transcoded Sessions	The number of transcoded sessions.
Transcoded Sessions Terminated	The number of terminated transcoded sessions.
Failed Transcoded Session	The number of failed transcoded sessions.
Early Media Calls	The number of early media calls.
Audit/Media Inactivity Detected	The number of calls in which Avaya SBC detected any inactivity.
Media Relinquished Calls	The number of media relinquished calls.
Shared Control Calls	The number of shared control calls.
Shared Control Calls Terminated	The number of terminated shared control calls.
Info Sessions	The number of info sessions.
Info Sessions Rejected	The number of rejected info sessions.

User registration

You can view the list of users that are registered through Avaya SBC in the **Registrations State** column on the User Registrations page. You can also enter custom search criteria for the fields that are displayed on the system.

Viewing the list of registered users

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **User Registrations**.

   The EMS server displays the list of registered users, displaying information as shown in Registered user field descriptions on page 415.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. For complete details of a registered user, click the user details.

   The EMS server displays the following information:

   - User information:
     - Address of record of the user.
     - User Agent information related to the type of endpoint and SIP instance information.
     - Firmware type and the controller mode.
   - Servers:
     - The Avaya SBC device through which the user is registered to Avaya Aura®.
     - The subscriber flow and server flow that were used for registration.
     - Session Manager address, port, and transport used for registration.
     - Endpoint private IP, natted IP, and transport.
     - Endpoint registration state and last reported time.

Filtering registered users

About this task

Use this procedure to search for the required registered users.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **User Registrations**.

   The EMS server displays the list of registered users.
3. Click **Add Criteria**.

4. Select one of the following criteria from the drop-down list:
   - **AOR**
   - **SIP Instance**
   - **User Agent**
   - **Controller Mode**
   - **Firmware**
   - **SBC Device**
   - **Subscriber Flow**
   - **Server Flow**
   - **SM Address**
   - **SM Port**
   - **SM Transport**
   - **Endpoint Private IP**
   - **Endpoint Natted IP**
   - **Endpoint Transport**
   - **Registration State**
5. Select one of the following options and enter the required value in the text box:
   - **Contains**
   - **Starts with**
   - **Ends with**
   - **Exact Match**
6. To add more filter criteria, repeat Steps 3 to 5.
7. To remove a filter criteria, click **Remove**.
8. Click **Filter**.

   The EMS server displays the results based on the ANDing of the criteria.

Registered user field descriptions

The User Registrations screen displays the list of endpoints registered through Avaya SBC with the following details for each registration.

Name	Description
AOR	The SIP URI used by the endpoint to register to Session Manager.
SIP Instance	The MAC address of the endpoint.
Last Reported Time	The time when the user registration status was last updated.

When the endpoint tries to register to Avaya SBC, each call server uses the following information:

Name	Description
SBC Device	The Avaya SBC device that receives the REGISTER message.
SM Address	The Session Manager address of the call server with the primary or secondary status.
Registration State	The registration status of the endpoint.

Server status

You can view the current status of the configured SIP servers. The EMS server displays the connectivity status for trunk servers and enterprise call servers. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

Note:

For the servers to appear in the Status window, you must configure the server heartbeat in Server Configuration.

Configuring Avaya SBC real-time trunk status

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click the **Heartbeat** tab.
5. To enable the heartbeat, select the **Enable Heartbeat** check box.
6. Navigate to **Network & Flows** > **Endpoint flows** > **Server flows**.

   For more information about creating server flows, see “Creating Flow toward Call Server” in *Administering Avaya Session Border Controller*.

   Note:

   In a high availability failover scenario, the EMS server displays the actual status of the server after 5-10 seconds.

   To display the server status, the Avaya SBC must successfully resolve the FQDN used as the server address.

Viewing server status

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Server Status**.

The EMS server displays the Status screen, as shown in Server Status field descriptions on page 417.

Server Status field descriptions

Name	Description
Server Profile	The name of the server profile.
Server FQDN	The Fully Qualified Domain Name (FQDN) of the server.
Server IP	The IP address of the server.
Server Port	The port number of the server.
Server Transport	The transport protocol that the server uses.
Heartbeat Status	The heartbeat status of the server. **Note:** When the Heartbeat feature is disabled and the Registration feature is enabled on the Server Configuration page, the Server Status page displays the **Heartbeat Status** as UNKNOWN.
Registration Status	The registration status of the server. **Note:** When the Heartbeat feature is enabled and the Registration feature is disabled on the Server Configuration page, the Server Status page displays the **Registration Status** as UNKNOWN.
TimeStamp	The date and time when the server status was updated.

Viewing performance statistics

About this task

You can view the current performance status of several facets of the servers in your deployment. The system displays CPU usage, memory usage, total media ports, used media ports, queues, and quality of service (QoS).

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Performance Status**.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. Enter the date and time periods for which you want to search for statistics.
5. Click **Search**.

The system displays statistics for the following items. Information is shown in 5 minute intervals within the period of time selected in the search criteria.

- CPU usage for processes like SSYNDI, OAMP, and TURN-server, and threads like, HA, SIPCC, Transport, and Relay
- IPCS memory usage
- Resident memory usage for SSYNDI, OAMP, and TURN activity
- Number of available A1, A2, B1, and B2 media ports
- Number of A1, A2, B1, and B2 media ports in use during that time period
- Queue size for HA, SIPCC, Transport, and Relay threads
- Mean value of Jitter on the system

Viewing IP/URI Blocklist

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.

   You can view the **IP/URI Blocklist** page with a list of blocked IPs and URIs.
3. You can view the following options:
   - **Block Permanently** to block a IP/URI permanently.
   - **Block Subnet** to block a subnet.
   - **Unblock** to unblock an IP/URI.
   - **Propagate To** to propagate information to other Avaya SBCs managed by the EMS.

     Note:

     You can view the **Propagate To** option only when the EMS manages other Avaya SBCs.

Related links

System status on page 407

Enabling or disabling Telemetry reports

About this task

Telemetry reports contain the usage and performance data for a tenant configuration. These reports are summarized from the CDR data.

Before you begin

Ensure that you enable Telemetry reports to view them.

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. To enable Telemetry reports, run the following command:

   ```
   gui-feature-control.py enable teams_telemetry
   ```

3. To disable Telemetry reports, run the following command:

   ```
   gui-feature-control.py disable teams_telemetry
   ```

4. To check the status of Telemetry reports, run the following command:

   ```
   gui-feature-control.py status teams_telemetry
   ```

Related links

System status on page 407

Viewing Telemetry reports

About this task

You can view Telemetry reports only for cloud solutions that deploy MS Teams where the tenant is configured.

Before you begin

Ensure that you complete the following:

1. Create a tenant configuration profile. For more information, see Creating the tenant configuration profile on page 286.
2. Configure the **Tenant configuration profile** field on the server flow created for MS Teams. For more information, see Creating a server flow on page 515.
3. Enable the **Summarize Calls** check box on the Application rule created for the Server flow Endpoint Policy group where you have configured the tenant in Step 2. For more information, see Creating a new Application Rule on page 103.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **Telemetry Reports**.

   You can view the **Telemetry Reports** page.

3. Click one of the following:

   - **Usage**: To view the usage reports.
   - **Performance**: To view the performance reports.

4. In **Search Criteria**, enter the start date and time and the end date and time.

   The reports are generated based on the UTC zone.

5. **(Optional)** Do one of the following:
   - Select the **Collapse** check box to generate a report that contains a single row containing the data for all days selected in the search criteria. Each parameter in the report contains the sum of the values for each day.
   - Clear the **Collapse** check box to generate a report that contains a single row for each day selected in the search criteria.

   For example, in the **Search Criteria**, you select **Start Date** as `04/15/2024`, **Start Time** as `00:00`, **End Date** as `04/19/2024`, and **End Time** as `00:00`. If you clear the **Collapse** check box, the report will contain one row for each day, that is, overall five rows. If you select the **Collapse** check box, the report will contain a single row for all five days.
6. Click **Search**.
7. **(Optional)** Click **Export CSV (Filtered)** to export the data for the specified period in an Excel sheet.

   The Excel sheet contains usage and performance data.
8. **(Optional)** Click **Export CSV (All)** to export all the data in an Excel sheet.

   The Excel sheet contains usage and performance data.

Telemetry Reports field descriptions

Usage field descriptions

Name	Description
Overall Call Count	The total number of inbound and outbound calls.
Overall Total Call Duration In minutes	The total call duration of inbound and outbound calls in minutes.
Overall Average Call Duration In minutes	The average call duration of inbound and outbound calls in minutes. **Overall Average Call Duration In minutes** = (**Overall Total Call Duration In minutes**) / **Overall Call Count**
Inbound Call Count	The total number of inbound calls.
Inbound Total Call Duration In minutes	The total call duration of inbound calls in minutes.
Inbound Average Call Duration In minutes	The average call duration of inbound calls in minutes. **Inbound Average Call Duration In minutes** = (**Inbound Total Call Duration In minutes**) / **Inbound Call Count**
Outbound Call Count	The total number of outbound calls.
Outbound Total Call Duration In minutes	The total call duration of outbound calls in minutes.

Table continues…

Name	Description
Outbound Average Call Duration In minutes	The average call duration of outbound calls in minutes. **Outbound Average Call Duration In minutes** = (**Outbound Total Call Duration In minutes**) / **Outbound Call Count**
No of Users	The total number of users engaged in inbound and outbound calls only on the tenant configured.

Performance field descriptions

Name	Description
Join Reliability Success Calls In %	The percentage of successful conference calls.
Join Reliability Failure Reasons Reason Code - Count	The total number of conference call failures with reason codes. Refer to the table below on mapping SIP error responses to reason codes.
Transfer Reliability Success Calls In %	The percentage of calls transferred successfully.
Transfer Reliability Failure Reasons Reason Code - Count	The total number of call transfer failures with reason codes. For more information, see the following table for mapping SIP error responses to reason codes.

Note:

The inbound and outbound calls are made to and from MS Teams.

Failure reason code mapping

SIP Error Response Code	Reason Code
403	1
404	2
408	3
410	4
412	5
480	6
484	7
486	8
488	9
500	10
503	11
504	12
Other than above codes	13

Log files

Using the log collection feature you can:

- Collect log files for a 24 hour period of time.
- Download log files for investigating and troubleshooting an issue.
- Copy log files to a remote server for viewing and storage.
- Sort the collected log files by the file name, the file size, and the date the file was last modified.
- Sort the collected log files in ascending and descending order.
- Delete the log files no longer needed.

Viewing system logs

About this task

SysLog Viewer displays the syslog file according to certain user-definable filtering criteria, such as log type, time period, and severity. Use the following procedure to define and view syslog reports.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Select the **Logs** option from the toolbar, and click the **System Logs** menu.

   The EMS server displays the Syslog Viewer screen. On this screen, you can specify criteria in the **Query Options** section to filter the results displayed.
3. In the **Start Date** and **End Date** fields, filter the results displayed in a search report to fall within starting and ending dates and times. In previous Avaya SBC Syslog Viewer windows, there were four separate fields: **Start Date**, **Start Time**, **End Date**, and **End Time**.

   Note:

   The date and time entries are combined in a single field, mm/dd/yyyy [hh:mm], with the time entry, [hh:mm], being optional. An **End Date** or **End Time** entry is not required when you enter a **Start Date** or **Start Time**.

   You can also select additional search criteria in the **Query Options** section.
4. In the **Keyword** field, type one or more words to define the limits of the log report, and click **Search**.

   The system runs the report and displays the output.

   Note:

   Keyword searches are case-insensitive and tokenized. Each keyword term entered in the **Keyword** field is searched. However, for a log line to be included in a report, all keyword terms that are entered in the **Keyword** field must be found in that log line.

Syslog Viewer field descriptions

Query Options section

The Query Options section on the Syslog Viewer screen contains options for filtering the Syslog logs.

Name	Description
Keyword	Search keywords for viewing logs.
Start Date	Date and time from which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
End Date	Date and time up to which you want to view logs You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
Show	Number of entries to be displayed on a page.
Class	Class of the logs to be displayed. The options are: • **All** • **Platform** • **Trace** • **Security** • **Protocol** • **Incidents** • **Registration** • **Audit** • **GUI** • **Unknown**
Severity	Severity of the logs to be displayed. The options are : • **Unknown** • **Info** • **Notice** • **Warning** • **Error** • **Critical** • **Alert** • **Emergency**

Results section

Name	Description
Timestamp	Timestamp of the log message.
Host	Device for which the log is generated.
Severity	Severity of the message.
Class	Class of the message.
Summary	Summary of the message.

Viewing audit logs

About this task

Audit Log Viewer displays the contents of the audit log. The audit log contains a record of security related events, such as logins, session starts, session ends, new user additions, and password attempts/retries/changes. Use the following procedure to view the Audit Log Viewer information.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Logs** > **Audit Logs**.

   The EMS server displays the Audit Log Viewer page.
3. In the **Start Date** and **End Date** fields, you can filter the results that are displayed in a search report to fall within starting and ending dates and times.
4. In the **Keyword** field, type one or more words to define the limits of the log report, and click **Search**.

   In the Results section, the EMS server displays the report output.
5. To see additional details about a particular log line in a report, select the log line.

   The EMS server displays the Audit Log Details page.
6. On the **Monitoring & Logging** > **Syslog Management** page, you can set the log level rules for the Audit Log and other logs.

   Audit Logging is enabled in the Log Level row for the Audit class and Audit Facility as LOG_LOCAL6.

   The Log Level Facility name, LOG_LOCAL6, is reserved for Audit Logging and cannot be changed. The LOG_LOCAL6 file path destination cannot be changed either. The file path is `/archive/syslog/ipcs/audit.log`.

Audit Logs field descriptions

Query Options section

The Query Options section on the Audit Log Viewer screen contains options for filtering the audit logs.

Name	Description
Keyword	Search keywords for viewing logs.
Start Date	The date and time from which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
End Date	The date and time up to which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
Show	The number of entries to be displayed on a page.

Results section

Name	Description
Timestamp	The timestamp of the log message.
Host	The device for which the log is generated.
Summary	The summary of the message.

Collecting and downloading log files

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **Log Collection**.
4. **(Optional)** Select the SBC device for which you want to collect log files. For an EMS, there cannot be multiple devices.
5. Click the **Collect Logs** tab and do the following:
   a. Select the type of log files that you want to collect. For more information, see Collect Logs field descriptions on page 426.
   b. Select a “from” and “to” time frame for the collection. You can collect up to 24 hours of logs.
   c. Click **Collect Logs** to collect the selected logs.

   The system collects the logs into an archive file. Once finished, a link to the log file is displayed on the **Collect Logs** tab.
6. Do one of the following steps to download the log file:
   - Click the log file link displayed on the **Collect Logs** tab.
   - Click the **Log Archive** tab and click the file name you want to download. For more information, see Log Archive field descriptions on page 426.
7. Using your browser controls, open or save the log file.

8. When you want to delete a log file, click **Delete** next to the log file you want to delete. Click **OK** to delete the file.

Collect Logs field descriptions

Name	Description
All Logs	Collects the database, application, GUI (EMS only), and upgrade logs that show the status of the system and configuration information. Crash dumps logs are not included in the **All logs** option because of the large size. Crash dumps logs can be collected separately. **Note:** The remaining options are clear when you select the **All Logs** check box .
Database logs	Collects the database dump logs.
Application Logs	Collects the SSYNDI logs.
GUI Logs	Collects the web interface and jsp logs. **Note:** The **GUI logs** option is available for EMS only.
Upgrade Logs	Collects the upgrade related logs.
Crash Dumps	Collects the system crash dumps.
From Date & Time	Specifies the day and time of day when you want to start collecting log files.
To Date & Time	Specifies the day and time of day when you want to stop collecting log files. You can collect a maximum of 24 hours of logs in one file.

Log Archive field descriptions

Name	Description
File Name	The file name of the collected log file.
File Size	The size of the collected log file in bytes.
Last Modified	The date and time when the collected log file was last modified.

Button	Description
Delete	Deletes the selected log file.

Debugging logs

Enabling application debug logs

About this task

The debugging logs are located at `/archive/log/ipcs/ss/logfiles/elog/`. You can collect the logs from the console.

The **Subsystem Logs** tab displays a list of processes, each of which contains subsystems. You can select the required subsystems for which you want to enable logs.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
3. Click the **Subsystem Logs** tab.
4. Select the device on which you want to toggle the log settings.

   The EMS server categorizes the subsystem logs under the following processes:

   - **LogServer**
   - **OAMPSERVER**
   - **SYSMON**
   - **SSYNDI**
   - **TURNCONTROLLER**
5. Do one of the following:
   - To turn on all debug information on the device, select the **Debug**, **Info**, and **Warning** log level check boxes at the table header.
   - To select a specific log level for all subsystems, select the **Debug**, **Info**, or **Warning** log level check box at the table header.
   - To select log levels for a specific process, select the **Debug**, **Info**, or **Warning** log level check box next to the process name.
   - To select log levels for a specific subsystem, expand the process name and select the **Debug**, **Info**, or **Warning** log level check box next to the subsystem.

   By default, the **Warning** log level check box is enabled.
6. Click **Save**.

Debugging field descriptions

Subsystem Logs

Name	Description
Process Name	Specifies the process for which you want to enable logs. This field displays processes such as: • LogServer • OAMPSERVER • SYSMON • SSYNDI • TURNCONTROLLER Each process contains subsystems. You can select the required subsystems for which you want to enable logs.
Debug	Specifies that debug logs are enabled for a subsystem. If you select the **Debug** check box in the table header, the system selects debug logs for all processes.
Info	Specifies that informational logs are enabled for a subsystem. If you select the **Info** check box in the table header, the system selects informational logs for all processes.
Warning	Specifies that warning logs are enabled for a subsystem. If you select the **Warning** check box in the table header, the system selects warning logs for all processes.

GUI logs

Name	Description
GUI	Controls master log levels for all GUI logs. The options are: • Info • Warn • Error
SOAP	Includes detailed logs generated by a GUI SOAP client. SOAP handles communication with EMS and Avaya SBC Communication Manager servers, for example, restart application, reboot device, and uninstall device. This option is deprecated.
Statistics	Includes the trace logs for Statistics when this field is enabled.
HTTP	Includes the HTTP communication logs for REST API between EMS and SBCs when this field is enabled.

Table continues…

Name	Description
Shell Commands	Include detailed logs when you start any external process.
File Uploads	Includes detailed logs for user file uploads, for example, upgrade packages, scrubber packages, and certificates.
Licensing	Includes detailed logs generated by a GUI WebLM client.
Certificates	Includes the trace logs for TLS certificate installation when this field is enabled.
Backup / Restore	Includes the trace logs for backup and restore when this field is enabled.
Third Party Components	Controls a master log level for third-party logs. This log level covers any logs from third-party libraries that the GUI uses. The options are: • Debug • Info • Warn • Error
SSH	Controls log levels for a third-party SSH library used for backup or restore and remote actions. The options are: • Inherit • Debug • Info • Warn • Error
SNMP	Includes the SNMP logs based on the log level selected.
LDAP	Includes the LDAP logs based on the log level selected.
RADIUS	Includes the RADIUS logs based on the log level selected.
Spring	Includes the Spring framework logs based on the log level selected.
Square Utilities	Includes the Square Utilities logs based on log the level selected.

Third-Party Logs

Name	Description
Nginx	Controls log levels for nginx. The options are: • Info • Notice • Warn • Error • Crit • Alert • Emerg
Ldap	Controls log levels for LDAP. The options are: • Any • Packets • Config • Stats
Transcoding	Controls log levels for transcoding. The options are: • None • All
H248	Controls log levels for H248. The options are: • None • Error • Trace

Disabling application debug logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
3. Click the **Subsystem Logs** tab.
4. Do one of the following:
   - To disable all debug information on the device, clear the **Debug**, **Info**, and **Warning** log level check boxes at the table header.

- To disable a specific log level for all subsystems, clear the **Debug**, **Info**, or **Warning** log level check box at the table header.
- To disable log levels for a specific process, clear the **Debug**, **Info**, or **Warning** log level check box next to the process name.
- To disable log levels for a specific subsystem, expand the process name and clear the **Debug**, **Info**, or **Warning** log level check box next to the subsystem.

5. Click **Save**.

Enabling GUI debug logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
4. In the content area, click **Third-Party Logs** tab.
5. Select the required log levels.
6. Click **Save**.

Disabling GUI Logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
4. In the content area, click **Third-Party Logs**.
5. Clear the required log levels.
6. Click **Save**.

Location of debug log files

Debug logs can be viewed or collected from the console.

The elog files for processes running on SBC are available at:

`/archive/log/ipcs/ss/logfiles/elog/`

The elog files for processes running on EMS are available at:

`/archive/log/ipcs/sems/logfiles/elog/`

The traceSBC logs for SIP are available at:

`/archive/log/tracesbc/tracesbc_sip`

The traceSBC logs for PPM are available at:

`/archive/log/tracesbc/tracesbc_ppm`

Core dumps are generated at:

`/archive/crash`

Smdumps for each process is available at:

`/usr/local/ipcs/smdump/`

Table 16: Elog locations for processes

Process	elog Path	Purpose
EMS		
SYSMON	`/archive/log/ipcs/sems/logfiles/elog/SYSMON`	To debug connectivity issues between Avaya SBC and EMS, process restart due to ping failure, and HA issues
OAMPSERVER	`/archive/log/ipcs/sems/logfiles/elog/OAMPSERVER`	To manage SNMP configuration of EMS
LOGSERVER	`/archive/log/ipcs/sems/logfiles/elog/LogServer`	To debug issues related to logging for other processes
Avaya SBC		
SBC SYSMON	`/archive/log/ipcs/ss/logfiles/elog/SYSMON`	To debug connectivity issues between Avaya SBC and EMS, process restart due to ping failure, and HA issues
SSYNDI	`/archive/log/ipcs/ss/logfiles/elog/SSYNDI`	To debug SIP application and media issues
OAMPSERVER	`/archive/log/ipcs/ss/logfiles/elog/OAMPSERVER`	To debug SNMP and statistics
TURNCONTROLLER	`/archive/log/ipcs/ss/logfiles/elog/TURNCONTROLLER`	To debug issues with TURN/STUN

Troubleshooting

Use the **Troubleshooting** menu item to:

- View system information, installed packages, and application status.
- Run a quick diagnostics on links between servers within your deployment and ping specific servers.

Related links

Viewing system information on page 433

Viewing system information

About this task

You can view the system information, installed packages, and application status.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Troubleshooting** > **System Information**.

   The application pane displays the System Information page.

   The Overview tab displays information about the following:

   - CPU
   - Memory
   - NIC
   - BIOS/UEFI
   - OS
   - Kernel

   The Versions tab displays the list of installed packages along with the following information:

   - Name
   - Base Version
   - Patch Version

   The Process Status tab displays the list of services along with the following information:

   - Name
   - Type
   - Status: Up or Down
   - CPU Usage
   - Memory Usage
   - Uptime

Related links

Troubleshooting on page 432

Running diagnostics tests

About this task

The Diagnostic Tests screen provides a variety of tools to aid in troubleshooting Avaya SBC operation. Available tools include a full diagnostic test suite, and individual tabs to monitor certain functional aspects of Avaya SBC, such as TCP and TLS activity.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Troubleshooting** > **Diagnostic Tests**.

   The application pane displays the Diagnostic Tests page.
3. Click **Full Diagnostics**.
4. Click **Start Diagnostic**.

   The tests listed in the **Task Description** column of the display are sequentially run, with the results of the test displayed in the **Status** column. If an error is encountered while running a test, the test continues until all tests are run. The application pane displays the reason for the error in the **Status** column.
5. Click **Ping Test**.

   The ping test can be used to verify basic IP connectivity to elements beyond the gateways. For example, ASM or the trunk server.

Diagnostics field descriptions

Full Diagnostic tab

Name	Description
EMS Link Check	Checks the EMS link.
EMS to Radius	Sends a ping request from EMS to the Radius server.
Ping: SBC to EMS	Sends a ping request from Avaya SBC to EMS.
Ping: EMS to SBC	Sends a ping request from EMS to Avaya SBC.
SBC Link Check: A1	Checks the Avaya SBC A1 interface. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2
Ping SBC [A1] to Gateway	Sends a ping request from the Avaya SBC A1 interface to the Gateway. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2

Table continues…

Name	Description
Ping SBC [A1] to Primary DNS	Sends a ping request from the Avaya SBC A1 interface to the Primary DNS. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2
EMS to Radius	Sends a ping request from Avaya SBC to the Radius server.

Ping Test

Name	Description
Source Device / IP	The IP address of the device from where the ping originates.
Destination IP	The IP address to which the ping is sent.

Users

The **Users** menu item gives you a quick listing of which administrative users are logged on to the system.

Viewing administrative users

About this task

The Active Users page provides a summary of all active system administrative accounts currently logged on to the EMS web interface.

Note:

You can only view the users account information. You cannot modify the information.

Use the following procedure to view the system administrative accounts that are currently logged on to the interface.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Users**.

   The EMS server displays the Active Users page.

Active Users field descriptions

Name	Description
User Name	The name assigned to the user.
Role	The role of the user.
Real Name	The real name of the user.
Contact Info	The contact information of the user.
Time Logged In	The time when the user last logged in to EMS.

License usage

About this task

Use this procedure to monitor license usage and compliance with your purchased license limits. This information is useful to keep track of how often you are using and acquiring a license, and also the number of times you are exceeding your license limits. If you are exceeding your license limits regularly or excessively, it may indicate that you need to expand your licensing agreement or upgrade your system.

You can display license usage based on a range of dates and license types. The license types include:

- Standard
- Advanced
- Video
- Transcoding
- Client Enablement Services (CES)
- Premium

Licensing statistics are collected hourly and are displayed on a maximum per day basis.

You can export and save the license usage information into a CSV spreadsheet.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Device Management** > **License Compliance**.
4. Enter a start and end date for which you want to view license usage.
5. Click **Search**.

   The system displays a line chart that shows the license usage for the dates selected.

6. You can then do any of the following steps to view usage data:
   - Hover over a date on the chart to display the number of licenses used, the number of licenses acquired, and the number of times the license was used over the purchased limit for that date.
   - Using the **Select License** drop-down, you can select other license types to see the same values for different license types.
   - Click **Export Data** to download and save the license statistics into a CSV spreadsheet.

Command line monitoring tools

Avaya SBC provides several command line tools to help you monitor status of your system.

Related links

traceSBC on page 437
Trace on page 443
tcpdump on page 444
showflow on page 445
sbceinfo on page 447
clipcs on page 447
swversion on page 448
Hardware specifications report file on page 449
Command History file on page 450

traceSBC

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the non-encrypted private key of the Avaya SBC is needed to decrypt the TLS and HTTPS traffic.

The traceSBC tool offers solutions for both issues. traceSBC is a perl script that parses Avaya SBC log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBC. traceSBC can also process log files real time on Avaya SBC, so that you can check SIP and PPM traffic during live calls. The tool can also work in the noninteractive mode, which is useful for automation testing.

Note:

In Release 10.1.2, traceSBC tool can only be run as "root" user.

Log files

Avaya SBC can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files in real-time by opening the most recent

log files in the given directories. traceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size of the file reaches the limit of about 10 MBytes.

Log locations:

The traceSBC logs for SIP are available at:

`/archive/log/tracesbc/tracesbc_sip`

The traceSBC logs for PPM are available at:

`/archive/log/tracesbc/tracesbc_ppm`

Active files are of the following format:

```
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651
```

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33
tracesbc_sip_1408617250_1408620820_1
```
or

```
-rw-rw---- 1 root root 31706 Jul 10 13:34
tracesbc_sip_1436549674_1436553270_1.gz
```

SIP and PPM logging administration

SIP logging is always enabled by default. You can enable PPM, STUN, TLS, and AMS logging, if required.

Performance benefits

Memory

After 10000 captured messages, traceSBC stops processing the log files to prevent exhausting the memory. This check is done during the capture when the tool is parsing the log files. The tool counts the number of SIP and PPM messages in the logs. This number is not the number of messages sent or received on the interfaces. This counter is a summary of messages from all logs, not for each log. Note that this safeguard is present only for real-time mode. When the tool is used in non real-time mode, this counter does not stop processing the logs specified in the command line. The counter continues processing the logs specified in the command line to be able to process more files or messages in off-line mode.

Processor

A built-in mechanism is available to prevent high CPU usage. Throttling is not tied to CPU level. In the current implementation, throttling is done by releasing the CPU for a short period after each line of the file is processed. The result is that CPU occupancy is low on an idle system when the tool actively processes large log files. You can disable throttling by the –dt command line parameter which can be useful when processing large log files offline. However, in this case CPU occupancy might go up to 100%, and so you must not use this option on a live system.

Operational modes

Non real-time mode

The tool starts with at least one file in the command line parameters. The tool automatically detects the type of files, processes the files, and finally displays messages from the different files in one diagram ordered by the timestamp. If filters are set, only the messages that match the filters are displayed in the diagram. In this mode, enabling live capture is not an option.

Examples:

traceSBC tracesbc_sip_1408635251

traceSBC /archive/log/tracesbc/tracesbc_sip/tracesbc_sip_1408635251 archive/log/tracesbc/tracesbc_ppm/tracesbc_ppm_1408633429

Real-time mode

In this mode, traceSBC runs interactively. You must run traceSBC on the active SBC and without specifying a file in the command line parameters. When you run **traceSBC**, the tool opens, displaying a list of options at the bottom of the screen. Those options are described in User interface elements and options on page 440.

Once you start the trace, the system automatically starts processing the log files. The live capture can be started and stopped anytime without affecting service.

Automatic mode

In this mode, traceSBC must be on the SBC and the command is called with -a and -w parameters at a minimum.

Example:

traceSBC -a "sip|ppm" -w /tmp/trace.log

Use this mode for test automation. You can also use this mode to stop capture when a certain condition is met, and then save filtered messages automatically. Multiple stop triggers are present, such as number of packets, time, regular expression, and a combination of these. When a stop trigger fires, or when you press CTRL+C, the tool automatically saves the filtered messages and stops the captures.

Command line options

Use **traceSBC** to start the traceSBC tool from the command line interface. For command line help, use the “–h” parameter.

traceSBC [-h] [options *SBC_LOG_FILE*

Where options are

-u *URI|NUMBER*	Filter calls that contain URI|NUMBER in the **From** or **To** field.
-i *IP*	Filter messages from/to <IP> address.
-c *CALL-ID*	Filter based on the SIP 'Call-ID' header field.
-r *REGEXP*	Filter messages based on the regular expression.

-g *HEA=VALUE*	Filter SIP header field <HEA> for value <VALUE>.
-or	Use a logical OR operator instead of the implicit. Use AND when using multiple filter options.
-nr	Do not display REGISTER messages.
-ns	Do not display SUBSCRIBE/NOTIFY/PUBLISH messages.
-no	Do not display OPTIONS messages.
-np	Do not display PPM messages.
-uni	Use Unicode/UTF-8 characters. Display the arrows and other lines in graphic mode. Your terminal client has to support Unicode to display this correctly.
-m	Use to run multiple instances of traceSBC.
-k	Kill other traceSBC instances.
-w *FILE*	Set filename for saving filtered messages.
-a *TYPE*	Starts specific captures in non-interactive mode where <TYPE> can be `sip|ppm|callp`.
-st *SEC*	Stops capture after given seconds.
-sp *PACKET*	Stops capture after given number of captured messages.
-sr <REGEXP>	Stops capture if regular expression found a match.
-srt <SEC>	Run trace <SEC> more seconds after REGEXP match.
-srp <PACKET>	Collect <PACKET> more messages after REGEXP match.
SBC_LOG_FILE	File name of the SSYNDI file or files previously captured with traceSBC. More than one file can be specified. If no file is specified, then you can start or stop the capture using the **s** key.

User interface elements and options

Window header

The window header shows the hostname, the name of the script, the number of captured messages, and the number of displayed messages that matched the filters. The header also displays warning messages such as MAX NUM PACKETS 10000 EXCEEDED.

Status bar

The status bar on the bottom of the screen is the most important and most used part of the tool. The bottom line has two areas, and its content depends on which mode the tool is in. The left side of the status bar shows the filename in nonreal-time mode, or shows Multiple files when the tool

was called with more than one file. In real-time mode, this area shows which trace is active. Red means disabled, and green means enabled.

The rest of the status bar lists the available commands:

s=Start / s=Stop : Starts or stops live capture, which means the tool enables or disables the appropriate logging. Capture can be enabled for SIP and PPM individually. Stop disables all logging at the same time and stops processing the log files. This command shows only if the tool was started in real-time mode.

Note:

Depending on the traffic and the capture modes at the time of stopping the trace, the log files might contain more messages than the messages already captured by the tool.

q=Quit: Quit from the tool. If capture is running, the tool shows a pop-up to confirm the exit without stopping the logging.

w=Write: Export filtered messages to a file. The dialog prompts you for a filename. The system saves SIP messages in the specified file to the current directory. The system saves PPM messages in a separate file with a `.ppm` extension. The system also exports SIP messages in pcapng format to a file with a `.pcapng` extension. SIP messages can be exported if text2pcap and tshark utilities are available on the machine where you run traceSBC.

i=IP / i=Name: Toggle between IP and user name presentation of the hosts in the header of the ladder diagram.

r=RTP: Turn RTP simulation on or off. When a session is established early or confirmed, the tool inserts a line in the diagram. This line represents the RTP stream between the two hosts described by the SDP. The diagram also shows the negotiated codec type.

Note:

The RTP stream is created based on the negotiated information in SDP. However, there is no guarantee that these RTP streams come to the system.

u=Full Screen: Use the full screen for the message detail box without having the left and right side of the frame. This option is useful not only to see more about the message, but to easily copy or paste the content.

d=Calls: Shows the summary of all calls.

Ladder diagram

The ladder diagram displays the filtered messages. The arrow shows the direction of the message between the SBC and the host from where the message arrived or was sent to. The IP of the host is at the top of the column. If the host is an Avaya phone, traceSBC attempts to extract the user information from the message, and replaces the IP with the user handle. To navigate between the messages, use the UP/DOWN arrow keys. The message is highlighted. To see the details of the message, press `Enter`. The header of the message detail form shows the source and destination IP or port and the transport protocol.

Filter options

The **f=Filters** filter options set in the dialog window override the command line option settings. If no new filter is entered, the current filter will remain active. To clear all filters, type **e** or **erase** in the **New Filter** field. The following is an example of the available filters:

```
Display Filter Usage:
  -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in
                   the 'From' or 'To' field.
  -i <IP>          Filter messages from/to <IP> address.
  -port <PORT>     Filter messages from/to <PORT>.
  -noport <PORT>   Filter messages from/to any ports except <PORT>.
  -c <CALL-ID>     Filter on the SIP 'Call-ID' header.
  -r <REGEXP>      Filter messages based on regular expression.
  -s <GSID>        Filter on the SIP 'Av-Global-Session-ID' header.
  -g <HEA>=<VALUE> Filter SIP header field <HEA> for value <VALUE>.
  -or              Use a logical OR operator instead of the implicit
                   AND when using multiple filter options.
  -nr              Do not display REGISTER messages.
  -ns              Do not display SUBSCRIBE/NOTIFY/PUBLISH messages.
  -no              Do not display OPTIONS/PING messages.
  -ni              Do not display INFO messages.
  -np              Do not display PPM messages.
  -nu              Do not display STUN/TURN/ICE messages.
  -nt              Do not display TLS Handshake messages.
  -nh              Do not display HTTP/WEBRTC messages.
  -nm              Do not display AMS WEBUA messages.
  -nl              Do not display LDAP messages.
```

Usage examples

Start a new capture

To start a new capture, run **traceSBC** without arguments and then press `s`: **traceSBC**

Filter a GSID

The “s” filter provides a way to trace the Avaya Global Session Identifier (GSID) header to filter SIP call traces. A GSID is in a form similar to 16169a40-cfe2-11ea-aeb9-00505694198d.

Note:

To use the GSID filter, the **Extensions** option in server interworking must be set to **Avaya**.

Filter SIP messages

To filter SIP messages from/to 1.1.1.1 and 2.2.2.2, enter the following command:

traceSBC -i *"1.1.1.1|2.2.2.2”*

Analyze an SSYNDI file

To analyze a previously captured SSYNDI file named `my_sbc.log`, enter the following command:

traceSBC my_sbc.log

Note:

Enable the debug log setting before performing the analysis. traceSBC does not display the logs if the debug log settings are not enabled. To enable SSYNDI debug logs, log on to the

EMS and navigate to **Monitoring & Logging** > **Debugging**. Select the SBC device and then click the **SSYNDI debug logs**checkbox.

Trace

With the Trace function, you can trace an individual packet or group of packets comprising a call through Avaya SBC. The information shows how the call traversed the Avaya SBC-secured network.

Configuring Packet Capture

About this task

Use the following procedure to set the filtering options and to capture packets or message flow.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Monitoring & Logging** > **Trace**.
4. Click **Packet Capture** or the **Captures** tab for the required information.
5. Navigate to a directory for saving the Packet Capture (pcap) file and click **Save** to save the file to the new directory.
6. Use Wireshark or a similar application to open up the Packet Capture (pcap) file. If Wireshark is already installed, you can double-click the file to open it with Wireshark. Otherwise, start Wireshark first and then either open the file from within the Wireshark application or double-click the Packet Capture file.

Note:

You can view the file using Wireshark (originally named Ethereal), a free and open-source packet analyzer application used for network troubleshooting, analysis, and software protocol development. You can download and install Wireshark, or a similar network analyzer program, to view the Packet Capture (pcap) file.

Trace field descriptions

Packet Capture

Name	Description
Status	The current status of the system for capturing packets.
Interface	The interface used for packet capture.
Local Address	The local IP address and port. The default value for this field is All.

Table continues…

Name	Description
Remote Address	The remote IP address and port. The default value for this field is an asterisk (*).
Protocol	The protocol used for packet capture. The options are: • **All** • **UDP** • **TCP**
Maximum Number of Packets to Capture	The number of packets to capture data. You can enter a value between 1 and 10,000.
Capture Filename	The name of the file used to capture data. If you use the name of an existing capture file, the system overwrites the file.

Button	Description
Start Capture	Begins the packet capture.
Clear	Clears the values that you entered in the **Packet Capture** tab.

Captures tab

Name	Description
File Name	The name of the packet capture file.
File Size (bytes)	The size of the packet capture file.
Last Modified	The latest date and time at which the capture file was changed. The default value for this field is **All**.

In addition to these fields, the **Captures** tab has two additional fields for sorting the packet captures by file name, file size, or last modified date.

Button	Description
Sort	Sorts the list of packet capture files by file name, file size, or last modified date.
Reset	Clears the values that you selected for sorting the data.

tcpdump

The tcpdump tool is the main troubleshooting tool of Avaya SBC, which can capture network traffic. Using tcpdump is a reliable way to analyze the information arriving to and sent from Avaya SBC. However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

You can use tcpdump to capture packets from the CLI if you need to capture more than 10000 packets. After the captures are taken, ensure you stop the command.

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the Avaya SBC is needed to decrypt the TLS and HTTPS traffic.

For packet capture started through GUI, the output files are stored in `/archive/pcapfiles/IPCS2`.

Running tcpdump in CLI

Procedure

1. Log on to the EMS server through SSH with ipcs user credentials.
2. At the command prompt, type `cd /archive/pcapfiles/IPCS2`.
3. Type `tcpdump -ni any -s 0 -w '`*filename*`.pcap'`, where *filename* is the name of the packet capture file.
4. To run packet captures on a specific interface, type `tcpdump -i any -s 0 -w '`*filename*`.pcap'`

   To run packet captures on a specific interface, use **`tcpdump -I`** *data_interface*. Packet capturing on Avaya SBC negatively impacts packet latency.
5. Wait for the capture to end, and press `Ctrl+C`.
6. Type `chown ipcs:ipcs` *filename*`.pcap`.

   The system displays the packet capture file in the **Captures** tab in the EMS web interface.

showflow

A flow is a connection between an endpoint and Avaya SBC. Types of flows are:

- Static: A static flow is configured on the Avaya SBC only one time. Static flows do not change until the administrator changes the flows. Static flows are used, for example, for connections between endpoints and an Avaya SBC signaling address.
- Dynamic: A dynamic flow is a transient connection between an endpoint and Avaya SBC. Software creates, modifies, and deletes dynamic flows to support the transfer of media packets through Avaya SBC.

Many flows can exist on Avaya SBC simultaneously. To troubleshoot issues with Avaya SBC, you can use the **`showflow`** command to display flows with varying levels of detail.

Description

`showflow` is a root-level console command to display the flows that are currently active on Avaya SBC.

Syntax

`showflow` 310 *flow-type detail-levelfilter-ip*

flow-type The flow type can be:

- static: Shows all static flows.
- dynamic: Shows all dynamic flows.
- turn_client_side: Shows all TURN flows on the listen interface of Avaya SBC.
- turn_far_side: Shows all TURN flows on the relay interface of Avaya SBC.
- blacklist: Shows all IP addresses that are currently blacklisted. Packets from blacklisted addresses do not match any flows.
- whitelist: Shows only those static flows that require whitelisting of the endpoint IP address.

detail-level You can specify the detail level for dynamic flows. The detail level for all other flows is fixed. When levels exceed the default detail level 0, you can see the default flow information and also additional information for the flow. The detail levels for dynamic flows can be:

- 0: Shows the default level of information. If a detail level is not specified in the command, the system uses 0 detail level.
- 1: Adds more decrypt information to every flow.
- 2: Adds more encrypt information to every flow.
- 3: Adds the physical port number for the output of the flow. Packets matching this flow are sent out of this physical port.
- 4: Adds relay information. Packets matching this flow are changed according to this relay before they are forwarded.
- 5: Adds VLAN identifiers and flow statistics.
- 6: Adds SIPREC information. This option does not change non-SIPREC flows.
- 7: Adds encrypt information for a SIPREC flow. This option does not change non-SIPREC flows.
- 8: Adds decrypt information for a SIPREC flow. This option does not change non-SIPREC flows.
- 12: Shows RTCP-MUX actors applied on "dynamic flows".

filter-ip If you specify a filter IP address, the **`showflow`** command displays dynamic flows that use the IP address that you specified as:

- An input or a packet source
- An output or a packet destination

When you specify a filter IP address, the **`showflow`** command displays dynamic flows pertaining to an endpoint with that IP address. If you do not provide a filter IP address, the system displays all dynamic flows.

Example

The following example displays full details of all dynamic flows with 10.20.30.40 as a source or destination:

showflow 310 dynamic 8 10.20.30.40

The following example displays all static flows:

showflow 310 static

sbceinfo

Use the **sbceinfo** command options to obtain system version, application type, and hardware details.

Syntax

```
sbceinfo [options]
```

Where options are:

getversion	Displays Avaya SBC version information.
gethwtype	Displays Avaya SBC hardware information.
getemsip	Displays the EMS IP address.
getapptype	Displays the application type running on the server.

clipcs

About this task

The **clipcs** commands are used to display basic information about Avaya SBC system configuration and status. You can run the **clipcs** console commands by logging in as a root user. To run these commands, first enter **clipcs** at the root prompt.

Note:

clipcs commands are deprecated in Release 10.1.2.

The **clipcs** commands are grouped according to two modes of operation: Console and Instance. The Console mode is the top-level command structure from which basic Avaya SBC systemwide commands can be executed. The Instance mode is the next level of administrative control that provides direct access to a particular Avaya SBC functional node.

Use the following procedure to run the **clipcs** console commands.

Note:

All **clipcs** commands and arguments are case-sensitive.

Procedure

1. On the root level prompt (#), enter the following command:

clipcs

The system displays the Avaya SBC console.

```
[root@EMS ~]# clipcs
Starting SBC Console...Please wait.
SBC Version x.x.x (C) Avaya Inc.
SBC Status:
Installation    Status
--------------- ----------------------------------------
sems           Running since Jul 30 12:23:50
ss                Running since Jul 30 12:23:50
SBC#
```

2. At the `SBC#` prompt, enter the following command:

   help

   The system displays the list of available **clipcs** commands.

clipcs commands and descriptions

The following table contains a list of **clipcs** commands and descriptions of commands available at the console prompt (#):

Command	Description
clear	Clears the display screen.
clock	Displays, sets, and clears the internal system clock.
exit	Moves the command level from instance mode to console mode. Also closes the clipcs screen when the command level is in the Console mode.
quit	Closes the clipcs screen when the command level is in the Console mode.
help	Displays a list of available commands and their descriptions.
refresh	Refreshes the open session screen.
spool	Spools to file settings.
status	In the Console mode, this command displays the status of Avaya SBC nodes. In the Instance mode, this command displays the detailed operational status of the node being accessed.
select	Selects a particular Avaya SBC node for access and activates the Instance mode.

swversion

The **swversion** command displays the product name, instance name, software version, and product deployment. See the following example:

```
Product Name            : ASBCE-8.X
Product Instance Name   : IPCS ID=[2] NODE ID=[11]
Product Version         : 8.1.2.0-25-19490
Product Deployment      : VMware Virtual Platform
```

Note:

You must be logged on as superuser, such as root, to run this command.

Hardware specifications report file

When a system is deployed, Avaya SBC automatically creates the file `/usr/local/ipcs/etc/hw_specs_report.txt` that contains hardware-related information about the system. To view this file, you must be logged on as root.

The following are some examples of the information stored in this file:

```
Number of NICs: 6
Product Information: MicroSBC
HWModel: CAD0230
Number of CPUs: 2
CPU Type:               64-bit capable
Number of Disks: 1
Disk space: 476940 MB
RAM: 1819 MB
manufacturer:Portwell
Applications Supported: EMS+SBCE
Model:110
```

```
Number of NICs: 2
Product Information: VMware Virtual Platform
HWModel: UNKNOWN
CPU Type:               64-bit capable
Number of CPUs: 4
Number of Disks: 1
Disk space: 163840 MB
RAM: 7725 MB
manufacturer:VMware,Inc.
Applications Supported: EMS
Model:EMS
```

```
Number of NICs: 4
Product Information: VMware Virtual Platform
HWModel: UNKNOWN
CPU Type:               64-bit capable
Number of CPUs: 8
Number of Disks: 1
Disk space: 163840 MB
RAM: 7820 MB
manufacturer:VMware,Inc.
Applications Supported: EMS+SBCE
Model:110
```

```
Number of NICs: 6
Product Information: VMware Virtual Platform
HWModel: ESXi6.5
CPU Type:               64-bit capable
Number of CPUs: 4
Number of Disks: 1
Disk space: 163840 MB
RAM: 7821 MB
manufacturer:VMware,Inc.
Applications Supported: SBCE EMS+SBCE
Model:310
```

Command History file

Avaya SBC logs every attempted or completed change activity on OS/CLI level in the `commandhistory` log file in the /archive/log directory. The format of the `commandhistory` file is as follows:

```
timestamp | Session: xx.dd.yy.xx | User: xyz | IP: xxx.xxx.xxx.xxx | SID: xxx | PPID:
xxx | PID: xxx | Command: xxx | Result: SUCCESS or FAILED"
```

Note:

SID and PPID can be used for auditd logs search along with command and timestamp.

Related links

Command line monitoring tools on page 437

Instance commands

Instance commands are also referred to as **`top`** commands. These commands are used to display detailed information about a specific Avaya SBC node in the network and EMS node with multiple Avaya SBC nodes.

Instance commands are only available within the instance mode, which is enabled when you run the **`clipcs select`** command for a node or application instance. Instance commands communicate directly with the active Avaya SBC node or communicate with the selected EMS or Avaya SBC application instance that runs on a single platform. Instance commands provide output from the active node or instance only.

Screen displays for the presented instance commands are automatically refreshed at a rate determined by the **`refresh`** command. The default refresh rate is 5 seconds.

top command description

You can use the **`top`** command for troubleshooting.

Command	Description
top	Displays a detailed functional status of the selected Avaya SBC node. The display is automatically refreshed every 5 seconds.

Traps

To see Avaya SBC alarms on System Manager, you must upload the Avaya SBC common alarms definition file (cadf) to System Manager.

For information about the traps, see Trap descriptions on page 240.

SNMP MIBs

Avaya SBC supports the Management Information Base (MIB) for data interfaces as defined in RFC-1213, rfc1213.mib. This section describes the MIBs you can download and view using SNMP.

Downloading the Avaya SBC MIB

The latest Avaya SBC MIB file is available in the downloads section on the support website at:

http://support.avaya.com/downloads/.

Avaya SBC OID Descriptions

This section describes the key Object Identifiers (OIDs).

Private Enterprise OIDs

OID	Description
ipcs stats sip calls: .1.3.6.1.4.1.6889.2.77.1.3.1	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipcalls
ipcs stats sip protocol: .1.3.6.1.4.1.6889.2.77.1.3.3	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipprotocol
Ipcsincidencesinfo: .1.3.6.1.4.1.6889.2.77.4	.iso.org.dod.internet.private.enterprises.Avaya.ipcsincidencesinfo
Ipcsalarmsinfo: .1.3.6.1.4.1.6889.2.77.2	.iso.org.dod.internet.private.enterprises.Avaya.ipcsalarmsinfo

Key OIDs

Classification of Requests/Responses matching a particular Domain Policy Group at the node

OID	Description
ipcsTotalINVITES	Number of SIP INVITE messages
ipcsTotalINVITERetransmits	Number of SIP INVITE Retransmits
ipcsTotalINVITE100Responses	Number of SIP INVITE 100 Responses
ipcsTotalINVITE1XXResponses	Number of SIP INVITE 1XX class Responses excluding SIP 100 Response.
ipcsTotalINVITE200Responses	Number of SIP INVITE 200 Responses
ipcsTotalINVITE200ResponseRetransmits	Number of SIP INVITE 200 Response Retransmits
ipcsTotalINVITE4XX6XXResponses	Number of SIP INVITE 4XX 6XX Responses

Table continues…

OID	Description
ipcsTotalINVITE4XX6XXResponseRetransmits	Number of SIP INVITE 4XX 6XX Response Retransmits
ipcsTotalBYESent	Number of SIP BYE requests
ipcsTotalBYERetransmits	Number of SIP BYE Retransmits
ipcsTotalBYE200Responses	Number of SIP BYE 200 Responses
ipcsTotalCANCELSent	Number of SIP CANCEL requests
ipcsTotalCANCEL200Responses	Number of SIP CANCEL 200 Responses
ipcsTotalACK200Responses	Number of SIP ACK requests for INVITE 200 OK Response
ipcsTotalACK4XX6XXResponses	Number of SIP ACK requests for INVITE 4xx-6xx class Responses
ipcsTotalACKTimeOuts	Number of SIP ACK timeouts ie. Number of ACK requests missing for the INVITE 200 OK/4xx-6xx class responses
ipcsTotalNonInviteRequests	Number of NonInvite Requests
ipcsTotalNonInvite1xxResponses	Number of NonInvite 1xx Responses
ipcsTotalNonInvite2xxResponses	Number of NonInvite 2xx Responses. Also includes the 200 OK responses for BYE and CANCEL requests

Get system configuration

OID	Name	Examples of displayed output
1.3.6.1.4.1.6889.2.77.12.1	sbcVersionNumber	8.1.2.0-31-19756
1.3.6.1.4.1.6889.2.77.12.2	sbcApplianceType	SingleBox
1.3.6.1.4.1.6889.2.77.12.3	sbcDeploymentMode	DMZ_ONLY
1.3.6.1.4.1.6889.2.77.12.4	processorVendor	GenuineIntel
1.3.6.1.4.1.6889.2.77.12.5	processorVersion	Intel(R) Xeon(R) Gold 6154 CPU @ 3.00GHz
1.3.6.1.4.1.6889.2.77.12.6	baseboardProductName	440BX Desktop Reference Platform
1.3.6.1.4.1.6889.2.77.12.7	baseboardManufacturer	Intel Corporation
1.3.6.1.4.1.6889.2.77.12.8	sbcPlatformMemory	8009024kB
1.3.6.1.4.1.6889.2.77.12.9	sbcPlatformDisc	160G
1.3.6.1.4.1.6889.2.77.12.10	sbcKernelVersion	3.10.0-1062.37.1.el7.AV1.x86_64
1.3.6.1.4.1.6889.2.77.12.11	sbcOperatingSystem	Red Hat Enterprise Linux Server release 7.7 (Maipo)
1.3.6.1.4.1.6889.2.77.12.12	sbcNetworkDriver	vmxnet3
1.3.6.1.4.1.6889.2.77.12.13	sbcThirdPartySoftware	'C-Ares': 'c-ares-1.10.0-3.el7.x86_64'

Out of Dialog Requests dropped

OID	Description
ipcsTotalOutOfDialogReferMesFromNW	Number of Out of Dialog REFER requests dropped at the node
IpcsTotalAckMessageOutOfDialogue	Number of Out of Dialog ACK requests dropped at the node
IpcsTotalByeMessageOutOfDialogue	Number of Out of Dialog BYE requests dropped at the node
IpcsTotalCancelMessageOutOfDialogue	Number of Out of Dialog CANCEL requests dropped at the node
IpcsTotalNotifyMessageOutOfDialogue	Number of Out of Dialog NOTIFY requests dropped at the node
ipcsTotalReinviteMessageOutOfDialogue	Number of Out of Dialog RE-INVITE requests dropped at the node

Out of Dialog Responses dropped

OID	Description
ipcsTotal1XXMessageOutOfDialogue	Number of Out of Dialog 1XX class responses dropped by the node
ipcsTotal2XXMessageOutOfDialogue	Number of Out of Dialog 2XX class responses dropped by the node
ipcsTotal3XXMessageOutOfDialogue	Number of Out of Dialog 3XX class responses dropped by the node
ipcsTotal4XXMessageOutOfDialogue	Number of Out of Dialog 4XX class responses dropped by the node
ipcsTotal5XXMessageOutOfDialogue	Number of Out of Dialog 5XX class responses dropped by the node
ipcsTotal6XXMessageOutOfDialogue	Number of Out of Dialog 6XX class responses dropped by the node

Out of Transaction Responses dropped

OID	Description
ipcsTotal1XXMessageOutOfTransaction	Number of 1XX Messages received out of transaction dropped by the node
ipcsTotal2XXMessageOutOfTransaction	Number of 2XX Messages received out of transaction dropped by the node
ipcsTotal3XXMessageOutOfTransaction	Number of 3XX Messages received out of transaction dropped by the node
ipcsTotal4XXMessageOutOfTransaction	Number of 4XX Messages received out of transaction dropped by the node

Table continues…

OID	Description
ipcsTotal5XXMessageOutOfTransaction	Number of 5XX Messages received out of transaction dropped by the node
ipcsTotal6XXMessageOutOfTransaction	Number of 6XX Messages received out of transaction dropped by the node
ipcsTotalCancelMessageOutOfTransaction	Number of CANCEL requests received out of transaction dropped by the node

Status of SIP calls

ipcssipcTotalRegistrationRequests	Number of Registration Requests received at node. This number does not include the registration triggered by node for keeping the pinhole open.
ipcssipcTotalRegistrationsChallenged	Number of Registrations Challenged by node and also includes the number of challenges from the Call Server. The number of registrations challenged by IPCS node includes the SIP 401/407 based Radius Authentication Responses (AAA feature) and SIP 407 based SIV Authentication Responses (DOS feature).
ipcssipcTotalRegistrationsRejected	Number of Registrations Rejected by the node and also includes the failed registration responses observed from the call server at the node. Failed registration responses include the SIP 4xx-6xx class responses excluding SIP 400, SIP 401/407 Responses. The registrations are rejected by the node due to failed registration challenges, failed registration processing, and registrations blocked due to security features.
ipcssipcTotalCallsReceived	Total Number of SIP Calls received at the node. This number equals Calls Blocked + Calls Allowed.
ipcssipcTotalCallsBlocked	Number of SIP calls Blocked by the node due to SIP Parse errors, failed AAA challenges, and calls blocked due to security features.
ipcssipcTotalCallsAllowed	Number of SIP calls classified by the node as Legitimate.

WebRTC statistics

OID	Description
ipcswebrtcStunBindingSuccess	Number of successful STUN bindings
ipcswebrtcStunBindingFailure	Number of failed STUN bindings
ipcswebrtcAllocateSuccess	Number of successful TURN allocations
ipcswebrtcAllocateFailure	Number of failed TURN allocations
ipcswebrtcRefreshSuccess	Number of successful TURN allocation refreshes

Table continues…

OID	Description
ipcswebrtcRefreshFailure	Number of failed TURN allocation refreshes
ipcswebrtcChannelBindSuccess	Number of successful channel bindings
ipcswebrtcChannelBindFailure	Number of failed channel bindings

Other OIDs

OID	Description
ipcssipcTotalActiveRegistrations	The number of active SIP registrations.
ipcssipcTotalActiveCalls	The number of active SIP calls.
ipcssipcTotalActiveTCPRegistrations	The number of active SIP registrations with TCP transport.
ipcssipcTotalActiveUDPRegistrations	The number of active SIP registrations with UDP transport.
ipcssipcTotalActiveTLSRegistrations	The number of active SIP registrations with TLS transport.
ipcssipcTotalActiveSRTPCalls	The number of active calls using media as SRTP.
ipcssipcTotalRegistrations	The number of active SIP registration requests received.
ipcssipcTotalTCPRegistrations	The number of SIP registrations received with TCP transport.
ipcssipcTotalUDPRegistrations	The number of SIP registrations received with UDP transport.
ipcssipcTotalTLSRegistrations	The number of SIP registrations received with TLS transport.
ipcssipcTotalCalls	The number of SIP calls received.
ipcssipcTotalCallsFailed	The number of failed SIP calls.
ipcssipTtlCallsDeniedDueToPolicy	The number of SIP calls rejected by Avaya SBC because of policy violation.
ipcssipcTotalRegistrationsDroppedByMissingPolicy	The number of SIP registrations dropped by Avaya SBC because of missing policy.
ipcssipcTotalInvitesDroppedByMissingPolicy	The number of SIP invites dropped because of missing policy.
ipcssipTtlSessDroppedDueToMaxNumofConcSessExc	The number of SIP sessions dropped by Avaya SBC because the maximum number of concurrent sessions was exceeded.
ipcsTotalCANCELSent	The number of SIP CANCEL requests.
ipcsTotalCANCEL200Responses	The number of SIP CANCEL 200 responses.
ipcsTotalCANCELRetransmits	The number of SIP CANCEL retransmits.
ipcsTotalFromAndToHeaderMatchFailure	The number of From and To header match failures.
ipcsTotalRegMesWithMoreContacts	The number of registration messages with more contacts.

Table continues…

OID	Description
ipcsTotalMesWithAddrIncomplete	The number of messages with incomplete addresses.
ipcsTotalAuthHeaderMatchFailure	The number of Auth header match failures.
ipcsTotalContactSrcAddrMatchFailure	The number of Contact Source Address match failures.
ipcsTotalViaMatchFailure	The number of Via match failures.
ipcsTotal3XXMesFromNW	The number of 3XX messages from network.
ipcsTotalRegistrationMatchFailure	The number of Registration Match failures.
ipcsTotalContactSDPConnMatchFailure	The number of Contact SDP Match failures.
ipcsTotalSpoofedSipBye	The number of spoofed SIP Bye requests.
ipcsTotalSpoofedReinvite	The number of spoofed Reinvite requests.
ipcsTotalSpoofedCancel	The number of spoofed Cancel requests.
ipcsTotalSpoofedCancelToRemote	The number of spoofed Cancel To Remote requests.
ipcsTotalSpoofed200	The number of spoofed 200 responses.
ipcsTotalSpoofedErrorResp	The number of spoofed error responses.
ipcsTotalRegistrationFailed	The number of failed registrations.
sbcTotal1xMCesUserLoginFailed	The number of failed Avaya one-X® Mobile user logins.
sbcTotal1xMCesUserLoginSucceeded	The number of successful Avaya one-X® Mobile user logins.
ipcsTotalNumberofFirewallPacketsDropped .1.3.6.1.4.1.6889.2.77.1.3.5.12	The number of packets dropped by the Avaya SBC firewall.
ipcsTestAlarmNotification	The test alarm notification.
ipcsCPUUsageNotification	The notification sent when CPU usage exceeds 80%.
ipcsMemoryUsageNotification	The notification sent when memory usage exceeds 80%.
ipcsDiskUsageNotification	The notification for disk usage exceeding a set threshold.
ipcsDiskFailureNotification	The notification for disk failure.
ipcsNetworkFailureNotification	The notification for network failure.
ipcsHAFailureNotification	The notification for HA failure.
ipcsHAHeartBeatFailureNotification	The notification for failure to receive heartbeat from both HA servers.
ipcsProcessFailNotification	The notification for process failure.
ipcsDatabaseFailNotification	The notification for database failure.
ipcsRSAFailureNotification	The notification for RSA failure.
ipcsIncidenceNotification	The notification about incidents.
ipcsLicenseAmrSessionReservedCount	The number of licenses reserved for AMR sessions.
ipcsLicenseAmrSessionInUseCount	The number of licenses currently in use for AMR sessions.
ipcsLicenseStandardSessionReservedCount	The number of licenses reserved for standard sessions.

Table continues…

OID	Description
ipcsLicenseStandardSessionInUseCount	The number of licenses currently in use for standard sessions.
ipcsLicenseAdvancedSessionReservedCount	The number of licenses reserved for advanced sessions.
ipcsLicenseAdvancedSessionInUseCount	The number of licenses currently in use for advanced sessions.
ipcsLicenseScopiaVideoSessionReservedCount	The number of licenses reserved for video sessions.
ipcsLicenseScopiaVideoSessionInUseCount	The number of licenses currently in use for video sessions.
ipcsLicenseCesSessionReservedCount	The number of licenses reserved for CES sessions.
ipcsLicenseCesSessionInUseCount	The number of licenses currently in use for CES sessions.
ipcsLicenseTranscodingSessionReservedCount	The number of licenses reserved for transcoding sessions.
ipcsLicenseTranscodingSessionInUseCount	The number of licenses currently in use for transcoding sessions.
ipcsLicensePremiumSessionReservedCount	The number of licenses reserved for premium sessions.
ipcsLicensePremiumSessionInUseCount	The number of licenses currently in use for premium sessions.

Statistics details with examples

Call between two remote workers through Avaya SBC

In the following scenario, a call is made from A to B.

- Number of Registrations in Statistics: Counter increases by 2

  One registration per phone, so in total 2 registrations from both A and B

  In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if both phones A and B are configured for multi-Session Manager deployment, the counter increases by 4.

- Number of Invites in Statistics: Counter increases by 2

  The counter increases whenever Avaya SBC receives an INVITE
  First INVITE from phone A towards Avaya SBC, which is sent to the call server
  Second INVITE from Call Server towards Avaya SBC, which is sent to phone B

- Number of Invites 200 Responses in Statistics: Counter increases by 2

  The counter increases whenever Avaya SBC receives a 200 OK for INVITE sent
  First 200 ok response from phone B towards Avaya SBC which is sent to the call server
  Second 200 ok response from Call Server towards Avaya SBC which is sent to phone A

- Number of Bye in Statistics: Counter increases by 2

The counter increases whenever Avaya SBC receives a Bye
First Bye from phone A towards Avaya SBC which is sent to the call server
Second Bye from Call Server towards Avaya SBC which is sent to phone B

Call between a remote worker and an internal phone through Avaya SBC

In the following scenario, a call is made from A to C and the call is disconnected at A.

- Number of Registrations in Statistics: Counter increases by 1

  One registration per phone, so in total 1 registration

  Phone C registration will not be seen by Avaya SBC as this phone is an internal phone

  In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if phone A is configured for multi-Session Manager deployment, the counter increases by 2.

- Number of Invites in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives an INVITE
  INVITE from phone A towards Avaya SBC, which is sent to the call server

- Number of Invites 200 Responses in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives a 200 Ok for INVITE sent
  200 ok response from phone C towards Avaya SBC, which is sent to phone A

- Number of Bye in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives a Bye
  Bye from phone A towards Avaya SBC, which is sent to the call server

Chapter 11: CLI commands

About the Command Line Interface

The Avaya SBC Command Line Interface (CLI) provides a high-speed serial management interface for local or remote access to the Avaya SBC security device. With the CLI, you can access Avaya SBC for performing various administrative and operational tasks. These tasks are executed using a robust assortment of commands entered through a terminal emulator, such as SSH protocol over port 222 or 22.

Note:

If any firewall is present between the EMS and SBC, port 222 must be open in both directions.

Accessing Avaya SBC

Accessing Avaya SBC or EMS device using VGA connection

Before you begin

- Ensure that you connect the monitor to EMS through a VGA cable.
- Ensure that you connect a keyboard to EMS.

Procedure

1. Press `Enter` to establish a communication connection.
2. Enter your username and password, and press `Enter`.

Accessing Avaya SBC or EMS device through SSH

About this task

Establish a secure connection to the Avaya SBC device.

Before you begin

Ensure that you install an SSH application, such as PuTTY.

Procedure

1. Start an SSH session through PuTTY.

2. In the **Host Name (or IP Address)** field, type the IP address of the Avaya SBC device.

   Through SSH, you can access the EMS or M1 interface.
3. In the **Port** field, type `222`.
4. In the **Connection type** field, click SSH.
5. Click **Open**.

   Avaya SBC establishes the session and displays the Command Line prompt.
6. On the Command Line prompt, log in as ipcs.
7. In the **Password** field, type the password and press `Enter`.

   Avaya SBC displays the dollar ($) prompt.
8. To go to the root level or superuser privileges, type `sudo su` and press `Enter`.

   Avaya SBC displays the super user command line prompt (#).

Configuring Avaya SBC for HA deployment using CLI

Before you begin

- Ensure that the EMS server is functional and in the same network as Avaya SBC.
- Ensure that both Avaya SBCs in the HA pair are installed and functional.

Procedure

1. Log in to the primary Avaya SBC device.
2. Edit the `cli_sbce_config.sample` file in the following folder: `usr/local/ipcs/etc`.
3. Remove `#` from the `cli_sbce_config.sample` file and modify the respective parameters.
4. Rename the `cli_sbce_config.sample` file to `cli_sbce_config`.

   Primary and secondary Avaya SBCs are added to the EMS server in a commissioned state.

   Note:

   Do not change any configurations for secondary Avaya SBC when configuring Avaya SBC for HA deployment using CLI.
5. Check the `cli_sbce_config` file for successful configuration of Avaya SBC.

   If configuration is successful, the `cli_sbce_config` file is renamed to `cli_sbce_config.commissioned`.

Configuring Avaya SBC for single server deployment using CLI

Before you begin

- Ensure that you install Avaya SBC.
- Ensure that the EMS server is functional and in the same network as Avaya SBC.

Procedure

1. Log in to the Avaya SBC device.
2. Edit the `cli_sbce_config.sample` file in the following folder: `usr/local/ipcs/etc`.
3. Remove `#` from the `cli_sbce_config.sample` file and modify the respective parameters.
4. Rename the `cli_sbce_config.sample` file to `cli_sbce_config`.

   Avaya SBC is in a commissioned state.
5. Check the `cli_sbce_config` file for successful configuration of Avaya SBC.

   If configuration is successful, the `cli_sbce_config` file is renamed to `cli_sbce_config.commissioned`.

Reconfiguration command options

The **`sbceconfigurator.py`** command is used for many system-level reconfiguration tasks. This table summarizes the options available when reconfiguring your system.

Caution:

When using the **`sbceconfigurator.py`** command, you must use only the command options shown in this table. Do not use any other command options.

Description	Usage examples
The `change-dns-ip-fqdn` option changes the DNS configuration. When using this command, you must enter the DNS IP address, and you can optionally include the DNS FQDN (shown as *[FQDN]* in the examples). Depending on whether you have just a single server or both primary and secondary servers, you can use the command to make the following changes: • Change primary only – first two methods shown in the examples • Change primary and secondary • Change secondary only • Remove secondary – used when you have both a primary and secondary and you only want to retain the primary system	**sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN],Current Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *Current Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *Current Primary DNS IP Address [FQDN]*
The `change-ems-ip` option does the following: • Changes the primary or active EMS IP address on the secondary or standby EMS. • Changes the secondary or standby EMS IP address on the primary or active EMS and all the SBC servers connected to EMS. • Changes the primary or active EMS IP address on the connected SBC servers, which were not reachable while changing the primary or active EMS IP address.	**sbceconfigurator.py change-ems-ip** *Old EMS IP Address New EMS IP Address*
The `change-hostname` option changes the host name.	**sbceconfigurator.py change-hostname** *HOSTNAME*
The `change-ip-gw-mask` option changes the management IP address, gateway, and subnet mask.	**sbceconfigurator.py change-ip-gw-mask** *Management IP Address Gateway IP Address Subnet Mask*
The `change-ntp-ip` option changes the NTP IP address.	**sbceconfigurator.py change-ntp-ip** *New NTP IP Address <yes/no> <<if yes provide PASSWORD>*
The `change-nw-passphrase` option changes the network passphrase.	**sbceconfigurator.py change-nw-passphrase** *Passphrase*

Table continues…

Description	Usage examples
The `change-sbce-ip` option changes the SBC IP address on the EMS database. Use the following steps to use this command: 1. Change the management IP address, gateway, mask on the SBC server by using the **change-ip-gw-mask** option 2. Run the **change-sbce-ip** option on the EMS CLI to notify the EMS about the SBC IP change.	**sbceconfigurator.py change-sbce-ip** *Old SBC IP Address New SBC IP Address*
The `change-ssl-certs yes` option changes the self-signed certificate for EMS and single SBC servers. This is an interactive command that steps you through changing the self-signed certificate. The command prompts you for the following information: • First and Last Name: [Default=] • Organizational Unit: [Default=] • Organization: [Default=] • City or Locality: [Default=] • State or Province: [Default=] • Country Code (2 letter code): [Default=]	**sbceconfigurator.py change-ssl-certs yes**
The `view-timezone` option displays the administered time zones. This is an interactive command that steps you through viewing a time zone.	**sbceconfigurator.py view-timezone**
The `change-timezone` option assigns a new time zone. This is an interactive command that steps you through selecting a time zone. The command prompts you for the following information: • Location • Country • Time Zone	**sbceconfigurator.py change-timezone**
The `gen-system-ssh-keys` option generates system SSH keys.	**sbceconfigurator.py gen-system-ssh-keys**
The `exchange-ems-keys` option exchanges the SSH keys. Use this command to copy SSH keys from the primary (or secondary, if present) EMS to SBC. Do this to ensure proper function of passwordless SSH between servers.	**sbceconfigurator.py exchange-ems-keys**

Table continues…

Description	Usage examples
The `factory-reset` option resets the system to the factory default state. Use the following procedure: 1. To uninstall the SBC device in a multiple server deployment from GUI, click **Device Management** > **Devices** and click **Uninstall**. This operation clears the device-specific configuration and is not required on EMS and a single server deployment. 2. Run `sbceconfigurator.py factory-reset`. This operation clears the device-specific configuration on EMS or a single server deployment. **Important:** Run this command from either a serial console or VGA session. Do not run this command from an SSH putty session since network connectivity will be lost during this operation.	**`sbceconfigurator.py factory-reset`**
The `re-configure` option moves Avaya SBC from one EMS to other EMS. The option does the following: 1. Convert SingleBox deployment to Seperate Box deployment and added to EMS. Usage example: **`sbceconfigurator.py re-configure`** 2. Move Separate Box deployment from one EMS to other EMS. Usage example: **`sbceconfigurator.py re-configure`** 3. Move HA Pair deployment from one EMS to other EMS. Usage example: **`sbceconfigurator.py re-configure`** **Note:** Ensure to run **`sbceconfigurator.py re-configure`** command on the PEER Avaya SBC once the first Avaya SBC comes back up after re-configure.	**`sbceconfigurator.py re-configure`**

Table continues…

Description	Usage examples
The **join-ha** option converts Separate Avaya SBC to HA by adding another Avaya SBC device. Use the following procedure: 1. Deploy new Avaya SBC and add to the EMS. 2. Make the new Avaya SBC into Registered state. 3. Run the **sbceconfigurator.py join-ha** command from new Avaya SBC cli. Command usage: **sbceconfigurator.py join-ha**	**sbceconfigurator.py join-ha**
generate-rest-credentials option is used to create the rest credentials. This command is supported from Release 10.1.2. • If you run the command in EMS, it will generate the rest credentials for all Avaya SBC associated with it and other EMS incase of active active EMS. • If you run the command in HA setup, it will generate the rest credentials for other box in Pair: EMS and secondary EMS if configured. • If you run the command in separate box, it will generate the rest credentials for EMS and Secondary EMS. • Single Box (EMS+SBC) is not supported.	**sbceconfigurator.py generate-rest-credentials**

Enabling or disabling network interfaces using CLI

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Run the following command to enable or disable the network interfaces:

```
sbceconfigurator.py data-interface-enable <interface name>
sbceconfigurator.py data-interface-disbale <interface name>
```

Editing SIP server profile parameters using CLI

About this task

Use this following procedure to edit IP Address/FQDN, port and transport protocol for an existing SIP server profile.

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. Run the following command to list all the available SIP server profiles:

   ```
   sbceconfigurator.py server-config-show
   ```

3. Run the following command to export the SIP server profile configuration to your system:

   ```
   sbceconfigurator.py server-config-export <SIP server profile name>
   ```

4. Run the following command to edit the SIP server profile parameters:

   ```
   sbceconfigurator.py server-config-change <Old IP/FQDN> <New IP/FQDN> <Old Port>
   <New Port> <Old Transport> <New Transport> <SIP server profile>
   ```

Editing network management parameters using CLI

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. Run the following command to list all the configured network configurations:

   ```
   sbceconfigurator.py network-config-show
   ```

3. Run the following command to export the network configuration to your system:

   ```
   sbceconfigurator.py network-config-export <Network Name>
   ```

   Important:

   It is recommended not to rename the exported file. Renaming the file will fail the importing of the edited file.

4. Edit the required fields in the exported file.
5. Run the following command to import the updated network configuration back to the EMS server:

   ```
   sbceconfigurator.py network-config-import <NetworkConfig filename>
   ```

Creating and restoring configurable snapshot using CLI

Procedure

1. Log in to the EMS CLI interface using administrative privileges.
2. Run the following command to create a configurable snapshot:

   ```
   python /usr/local/ipcs/icu/scripts/SnapshotMain.py backup
   ```

3. Run the following commands to restore the configured snapshot:

```
/usr/local/ipcs/icu/scripts/bdrmon.py --breakreplication
```

```
python /usr/local/ipcs/icu/scripts/SnapshotMain.py restore <actual path of backup_file>
```

Deleting the secondary EMS

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command:

   sbceconfigurator.py delete-secondaryems-fromprimary

Changing management IP, gateway and network mask details for a single server deployment

Procedure

1. Log in to the server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The server restarts indicating that the management IP has been changed successfully.

Changing the management IP for an HA deployment

Changing management IP, gateway IP, and network mask details on primary EMS

Use the following command to change management IP, gateway, and network mask details on the primary EMS server.

sbceconfigurator.py change-ip-gw-mask *<MGMT_IP> <GW_IP> <NW_MASK>*

The script does the following:

1. Checks if the database is functional.
2. If the database is functional, proceeds with stopping application processes.
3. Checks if all the Avaya SBC servers connected to EMS are reachable. If any Avaya SBC server is unreachable, exits or proceeds with changing the EMS IP address on the

reachable Avaya SBC servers. Later, when the devices are reachable from EMS, users can regenerate or change the EMS IP addresses on the devices.

4. Prints out the log messages, which shows the current status on screen.
5. The EMS server then reboots. The user needs to ssh using the new EMS IP address.
6. EMS generates certificates automatically and sends it to all Avaya SBCs.

Change in management IP requires a change in the NTP address configuration on all Avaya SBC servers connected to EMS.

Note:

All Avaya SBC servers must have the changed EMS IP address.

Related links

Changing primary EMS IP on unreachable Avaya SBC on page 468
Changing the NTP IP address on Avaya SBC on page 468
Changing IP address of the primary EMS server on the secondary EMS server on page 469

Changing primary EMS IP on unreachable Avaya SBC

About this task

Use this procedure only when Avaya SBC is unreachable while changing the primary EMS IP address.

Procedure

1. Log in the EMS web interface as a super user.
2. Type **sbceconfigurator.py change-ems-ip** <*EMS_OLD_IP*> <*EMS_NEW_IP*> and press `Enter`.

Changing the NTP IP address on Avaya SBC

About this task

Changing the management IP address of EMS requires a change in the NTP IP address configuration on the Avaya SBC devices connected to EMS. For proper functioning of OpenVPN, ensure that the date and time on the Avaya SBC devices match those on the EMS device. Avaya recommends configuring the EMS IP address as the NTP IP address of the Avaya SBC devices.

Before you begin

If you plan to use the system password while running the command, ensure to have it ready.

Procedure

1. Log in to the Avaya SBC device as a super user.
2. Enter the following command:

   sbceconfigurator.py change-ntp-ip *NewNTPIPAddress* <*yes/no*> <*if yes provide PASSWORD*>

Where:

- *NewNTPIPAddress* is the new NTP IP address.
- *<yes/no> <if yes provide PASSWORD>* is either **yes** or **no**. If you type **yes**, you must enter the system password after running the command.

Example

```
INFO : Changing NTP Server IP..
INFO : Make sure your Date and Time matches EMS...
INFO : Updating NTP IP address IPV4 in sysinfo file...
INFO : Updating NTP Config File..
sh /usr/local/ipcs/icu3/scripts/setNTPAuth.sh 10.81.21.18 no
INFO : Restarting NTP Server..
Restarting ntp server
INFO : Syncing NTP time..
Connecting to NTP Server 10.81.21.18 to synchronize time
NTP Server Sync is successful
INFO : Sync Time To HWClock.
```

Changing IP address of the primary EMS server on the secondary EMS server

Procedure

1. Log on to the EMS device as a super user.
2. Type `sbceconfigurator.py change-ems-ip` *EMS_old_IP EMS_new_IP* and press `Enter`.

Changing management IP, gateway IP, and network mask details on secondary EMS

Procedure

1. Log on to the Avaya SBC server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBC restarts indicating a successful completion of the management IP change. After changing the management IP, the primary EMS and Avaya SBC devices must be notified about the new Avaya SBC IP address of the secondary EMS.
3. Log on to the primary EMS and Avaya SBC devices as a super user.
4. Type `sbceconfigurator.py change—ems-ip` *Old_EMS_IP New_EMS_IP*.

   The system changes the IP address of the secondary EMS.

   Note:

   Ensure that you change the IP address of the secondary EMS in the primary EMS and each Avaya SBC device.

Changing management IP, gateway IP, and network mask details on Avaya SBC

Procedure

1. Log on to the Avaya SBC server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBC restarts indicating successful completion of the management IP change. After changing the management IP, the EMS must be notified about the new Avaya SBC IP address.
3. Log on to the EMS server as a super user.
4. Type `sbceconfigurator.py change—sbce-ip` *Old_SBCE_IP New_SBCE_IP*.

   The system changes the IP address of the Avaya SBC in the EMS database.

Changing hostname

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Type `sbceconfigurator.py change-hostname Hostname`.
3. Restart the system.

   For the hostname change to take effect, you must perform a soft reboot of the Avaya SBC.

Changing network passphrase

About this task

Network passphrase is important for EMS-Avaya SBC authentication. If you change the network password for an Avaya SBC, ensure that you change the passphrase on all systems connected to the Avaya SBC.

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Type `sbceconfigurator.py change-nw—passphrase New Passphrase`.

   The server restarts for enabling the new passphrase. The server is either the EMS or its connected SBC's where the command is executed.

Regenerating self-signed certificates

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command:

   `sbceconfigurator.py change-ssl-certs yes`

Regenerating the rest credentials

About this task

External cases like certificate sync and upgrade package copy, and system tasks like application restart and reboot the system, might not work from GUI due to the rest credentials issues. In such cases, run the `generate-rest-credentials` command.

Procedure

1. Log in to the Avaya SBC or EMS CLI using administrative privileges.
2. Run the command: `sbceconfigurator.py generate-rest-credentials`
   - If you run the command in EMS, it will generate the rest credentials for all Avaya SBC associated with it and other EMS incase of active active EMS.
   - If you run the command in HA setup, it will generate the rest credentials for other box in Pair: EMS and secondary EMS if configured.
   - If you run the command on separate box, it will generate the rest credentials for EMS and Secondary EMS.
   - Single Box (EMS+SBC) is not supported.

   Note:

   The `sbceconfigurator.py generate-rest-credentials` command is supported from Release 10.1.2.

Changing DNS IP and FQDN

About this task

The `change-dns-ip-fqdn` option changes the DNS configuration. When using this command, you must enter the DNS IP address, and you can optionally include the DNS FQDN (shown as

[FQDN] in the examples). Depending on whether you have just a single server or both primary and secondary servers, you can use the command to make the following changes:

- Change primary only – first two methods shown in the examples
- Change primary and secondary
- Change secondary only
- Remove secondary – used when you have both a primary and secondary and you only want to retain the primary system

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Enter any of the following command options depending on which IP address or FQDN you want to change:.
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN],Current Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *Current Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *Current Primary DNS IP Address [FQDN]*

   The EMS server changes the DNS IP address and optionally, the FQDN.

Regenerating the rest credentials

About this task

External cases like certificate sync and upgrade package copy, and system tasks like application restart and reboot the system, might not work from GUI due to the rest credentials issues. In such cases, run the `generate-rest-credentials` command.

Procedure

1. Log in to the Avaya SBC or EMS CLI using administrative privileges.
2. Run the command: `sbceconfigurator.py generate-rest-credentials`
   - If you run the command in EMS, it will generate the rest credentials for all Avaya SBC associated with it and other EMS incase of active active EMS.
   - If you run the command in HA setup, it will generate the rest credentials for other box in Pair: EMS and secondary EMS if configured.

- If you run the command on separate box, it will generate the rest credentials for EMS and Secondary EMS.
- Single Box (EMS+SBC) is not supported.

Note:

The `sbceconfigurator.py generate-rest-credentials` command is supported from Release 10.1.2.

Resetting SNMP configuration

About this task

Perform this procedure to reset SNMP configuration when statistics viewer displays non-numeric values.

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command:

   `/usr/local/ipcs/icu3/scripts/ResetSnmpConfig.sh`

3. When the system prompts for confirming, press `Y`.

Restarting spiritAgent

About this task

Perform this procedure when:

- SNMP traps are not send outside.
- spiritAgent gets stopped if there is no SNMP user configured.

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command to restart spiritAgent:

   `systemctl restart spiritAgent`

3. Run the following command to ensure that spiritAgent is up and running:

   `systemctl status spiritAgent`

Chapter 12: Template Wizard

Template Wizard feature:

- Quickly provisions a newly-installed system to a working state.
- Supports provisioning of Trunk and Remote Worker flows.
- Is not a replacement for the traditional UI.

This feature accepts a minimum subset of the information required to create basic trunk or remote worker flows, such as listen addresses, ports, call/trunk server addresses, and X.509 certificate/keys (if applicable). This information is used in the backend to create the relevant profiles to support these basic flows.

For trunk deployments, this information includes:

- Networks & Addresses
- SIP Server (Trunk)
- SIP Server (Call Server)
- Signaling Interface
- Media Interface
- Server Flows
- Routing Profiles

For remote worker deployments, this information includes:

- Networks & Addresses
- SIP Servers (Primary Call Server + Optional Secondary Call Server)
- Signaling Interface
- Media Interface
- Server Flows
- Subscriber Flows
- Routing Profiles

DAT file

Additional information, such as interworking parameters or topology hiding settings, might be required for specific service providers or remote worker deployments. This information is provided through a DAT file (YAML format) which can define options for a Service Provider (Trunk) or Client Type (Remote Worker).

A DAT file can be used to define the following:

- Application Rule
- Media Rule
- Server Interworking Profile
- Topology Hiding Profile

All the rules/profiles provided in a DAT file are optional and revert to the default profiles if not specified inside a DAT file. By default, Avaya SBC is not bundled with any DAT files. However, Avaya provides documentation on how to create your own DAT files through Avaya DevConnect.

Managing DAT files

Prerequisites

Ensure that you have the following:

- A network diagram (or basic understanding of how you plan to layout your network)
- A DAT file (obtained separate or created on your own)
- An EMS with at least one COMMISSIONED but unconfigured Avaya SBC

Installing a DAT file

About this task

Once you obtain or create a DAT file, it needs to be installed in the GUI to be usable.

Procedure

1. Log in to the EMS GUI.
2. Ensure the EMS device is selected from the device selection widget at the top left of the screen.
3. Click **Templates** > **Dat Management link**.
4. Click **Add** for the desired deployment type:
   - If the DAT file is intended for use with Trunk deployments, click **Add** for Service Providers.
   - If the DAT file is intended for use with Remote Worker deployments, click **Add** for Clients.
5. **(Optional)** In the **Name** field, enter a custom name to use for this specific DAT file.

   If no name is provided, the default from the DAT file is used.
6. Click **DAT file** to browse and select the DAT file.

7. Click **Finish**.

Editing a DAT file

Procedure

1. Log in to the EMS GUI.
2. Ensure the EMS device is selected from the device selection widget at the top left of the screen.
3. Click the **Templates** > **Dat Management link**.
4. Select the DAT file and click **Edit**.
5. Make the required changes and click **Finish** to save the DAT file.

Deleting a DAT file

Procedure

1. Log in to the EMS GUI.
2. Ensure the EMS device is selected from the device selection widget at the top left of the screen.
3. Click the **Templates** > **Dat Management link**.
4. Select the DAT file and click **Delete**.
5. Click **OK**.

Using Template Wizard

About this task

Once you install at least one DAT file, you can use Template Wizard.

Procedure

1. Log in to the EMS GUI.
2. Ensure the EMS device is selected from the device selection widget at the top left of the screen.
3. Click the **Templates** > **Wizard**.
4. In the **Device Select** field, select the Avaya SBC device.

   Warning:

   Do not select a working device (especially if it is in production). Template Wizard is designed for a new configuration and can potentially break an existing configuration, requiring manual steps to restore the previous configuration.

5. In the **Deployment Type** field, select one of the following:
   - **Trunk**
   - **Remote Worker**
6. Fill in the appropriate fields depending on the deployment type.

   For information about the fields, see “Template Wizard field descriptions”.
7. Click **Submit**.

Related links

Template Wizard field descriptions on page 477

Template Wizard field descriptions

Name	Description
Device Select	The device that the Template Wizard should be run against. Select an Avaya SBC device. **Warning:** Do not select a working device (especially if it is in production). Template Wizard is designed for a new configuration and can potentially break an existing configuration, requiring manual steps to restore the previous configuration.
Deployment Type	The deployment type the Template Wizard should create: • **Trunk** • **Remote Worker**

Trunk deployment field descriptions

Name	Description
Call Server Details: OR **Trunk Server Details:**	
Use Call Server or **Use Trunk Server**	A box to select an existing call or trunk server or define a new call or trunk server. If an existing call or trunk server is selected, the server must contain exactly one server address. No additional information is needed. If a new call or trunk server is to be added, select **<Create New Call/Trunk Server…>** and fill out the fields.
Address or FQDN	The IP address or FQDN of the SIP call or trunk server.
Port	The SIP port of the SIP call or trunk server.

Table continues…

Name	Description
Transport	The transport type of the SIP call or trunk server. Select one of the following: **TCP**, **UDP**, or **TLS**. If **TLS** is selected, you must enter the certificate details.
Use Network	A box to select an existing network or define a new network. If an existing network is selected, only an IP address is prompted. If a new network is to be added, select **<Create New Network…>** and fill out the fields.
IP Address	The listen IP address to use when setting up the signaling and media interface. If an existing network is selected, this field enables selecting an existing IP address or entering a new IP address.
Gateway	The gateway for the network.
Subnet Mask/Prefix	The subnet mask or network prefix for the network.
Interface	The Avaya SBC interface to attach the network to.
Signaling Port	The Signaling Port to use on for SIP signaling.
Port Range Start	The Media Port Range to use for SIP media.
Port Range End	The Media Port Range to use for SIP media.
TLS: This section is visible only if TLS is selected as the Call or Trunk Server transport.	
Upload New Certificate / Use Existing Certificate	The certificate selection mode: • **Upload New Certificate** • **Use Existing Certificate**
Certificate	The TLS certificate. If **Upload New Certificate** is selected, upload a valid PEM-encoded X.509 certificate file. If **Use Existing Certificate** is selected, a field is available to select a certificate already installed on Avaya SBC.
Private Key	The private key file. If **Upload New Certificate** is selected, you must upload a valid PEM-encoded RSA private key file. If **Use Existing Certificate** is selected, this field is not required.

Table continues…

Name	Description
Private Key Passphrase	The passphrase for the Private Key file. If **Upload New Certificate** is selected, provide the passphrase for the Private Key file. Leave the field blank if the private key does not have encryption. If **Use Existing Certificate** is selected, this field is not required.
Upload New Certificate Authorities / Use Existing Certificate Authorities	Select the CA selection mode.
Peer Certificate Authorities	If **Upload New Certificate Authorities** is selected, you must upload one or more PEM-encoded X.509 certificate files to provide CA trust anchors. If **Use Existing Certificate Authorities** is selected, a field is available to select one or more CA certificates already installed on Avaya SBC.

Remote Worker deployment field descriptions

A Remote Worker Deployment is used to allow remote users access to the internal voice network, typically using secured communications. The fields under these sections are used to define the configuration including Networks, Signaling and Media Interfaces, Server Flows, Subscriber Flows, Routing Rules, and TLS profiles if necessary.

Name	Description
Use Call Server	A box to select an existing call server or define a new call server. If an existing call server is selected, the server must contain one server address. No additional information is needed. If a new call server is to be added, select **<Create New Call Server…>** and fill out the fields.
Address or FQDN	The IP address or FQDN of the SIP call server.
Port	The SIP port of the SIP call server.
Transport	The transport type of the SIP call server. Select one of the following: **TCP**, **UDP**, or **TLS**. If **TLS** is selected, you must enter the certificate details.
Use Network	A box to select an existing network or define a new network. If an existing network is selected, only an IP address is prompted. If a new network is to be added, select **<Create New Network…>** and fill out the fields.

Table continues…

Name	Description
IP Address	The listen IP address to use when setting up the signaling interface and media interface. If an existing network is selected, this field enables selecting an existing IP address or entering a new IP address.
Gateway	The gateway for the network.
Subnet Mask/Prefix	The subnet mask or network prefix for the network.
Interface	The Avaya SBC interface to attach the network to.
Signaling Port	The Signaling Port to use on for SIP signaling.
Port Range Start	The Media Port Range to use for SIP media.
Port Range End	The Media Port Range to use for SIP media.
TLS: This section is visible only if TLS is selected as the Call Server transport.	
Upload New Certificate / Use Existing Certificate	The certificate selection mode: • **Upload New Certificate** • **Use Existing Certificate**
Certificate	The TLS certificate. If **Upload New Certificate** is selected, upload a valid PEM-encoded X.509 certificate file. If **Use Existing Certificate** is selected, a field is available to select a certificate already installed on Avaya SBC.
Private Key	The private key file. If **Upload New Certificate** is selected, you must upload a valid PEM-encoded RSA private key file. If **Use Existing Certificate** is selected, this field is not required.
Private Key Passphrase	The passphrase for the Private Key file. If **Upload New Certificate** is selected, provide the passphrase for the Private Key file. Leave the field blank if the private key does not have encryption. If **Use Existing Certificate** is selected, this field is not required.
Upload New Certificate Authorities / Use Existing Certificate Authorities	Select the CA selection mode.

Table continues…

Name	Description
Peer Certificate Authorities	If **Upload New Certificate Authorities** is selected, you must upload one or more PEM-encoded X.509 certificate files to provide CA trust anchors. If **Use Existing Certificate Authorities** is selected, a field is available to select one or more CA certificates already installed on Avaya SBC.

Secondary Session Manager Details (Optional)

The fields in this section are identical to those in the Primary Session Manager Details fields except the following field:

Name	Description
Use Secondary Session Manager	A checkbox to determine if a secondary Session Manager should be configured. If the checkbox is cleared, only one Session Manager configuration is provisioned.

Verifying the configuration

About this task

Once the Template Wizard form is submitted, the profiles and rules are created in the backend on the Avaya SBC instance. You must verify that the configuration is valid for the defined template.

Procedure

1. Ensure that the following information in the Trunk screen matches with what was entered in Template Wizard:
   - Networks & Addresses
   - SIP Server (Trunk)
   - SIP Server (Call Server)
   - Signaling Interface
   - Media Interface
   - Server Flows
   - Routing Profiles
2. Ensure that the following information in the Remote Worker screen matches with what was entered in Template Wizard:
   - Networks & Addresses
   - SIP Servers (Primary Call Server + Optional Secondary Call Server)

- Signaling Interface
- Media Interface
- Server Flows
- Subscriber Flows
- Routing Profiles

Chapter 13: Configuring Remote Worker

Remote worker overview

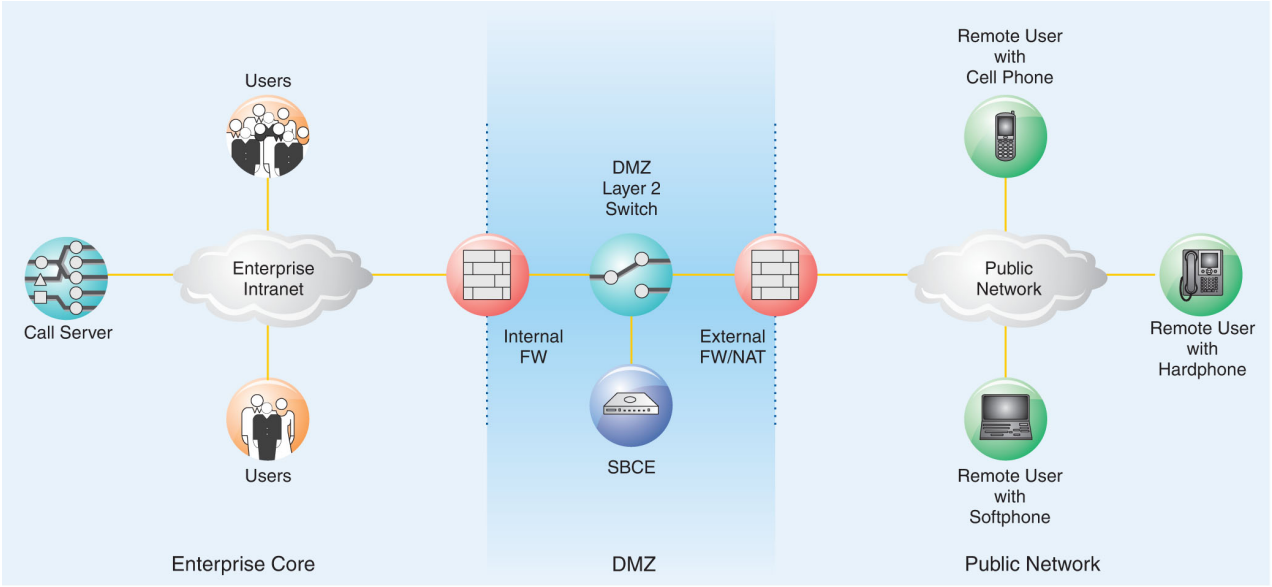
Avaya SBC delivers security to a SIP-based enterprise network. This chapter describes how to configure Avaya SBC for Avaya Aura® remote worker.

Remote Worker

The remote worker feature supports SIP deployments and extends access to the features of an internal enterprise Unified Communications (UC) and Call Center (CC) network. Therefore, a remote worker can also be a CC agent. The extended features include firewall/Network Address Translation (NAT) traversal, encryption, user authentication, and enforcement of session-endpoint call policies.

When a remote worker outside the enterprise network calls a user inside the core enterprise network, Avaya SBC decrypts the SRTP media, if present, coming to the enterprise from the external IP network, that is the internet. The SBC performs any required NAT, analyzes traffic for anomalous behavior, applies the relevant Unified Communications media policies, and then passes the RTP/SRTP stream to the intended recipient.

The following diagram shows a typical remote worker topology:



cysbdp1w LAO 021413

To configure IPv6 support for Remote Worker, you must have:

- IPv6 address provisioned in signaling address interface.
- Media interface must have primary and secondary interface publishing both IPv4 and IPv6 addresses.
- Tolerant field must be enabled in the server flow.

Remote Worker best practices

- Download the settings and firmware files using a proxy server, which requires a different external IP address.
- Configure the firewall on Avaya Aura® Session Manager to whitelist the Avaya SBC internal IP.
- Configure Media or Signaling QoS on Avaya SBC. Enable SIP Video specifically on Avaya SBC, if required.
- Add emergency numbers in the Emergency URI Group.
- Forward video/audio signaling and media ports for customer firewall configuration.
- Disable SIP Application Layer Gateway (ALG) on firewalls. As part of SIP ALG functionality, firewalls actively interpret SIP messages and modify them.
- For basic debugging of Avaya SBC, take a packet capture or run the **`traceSBC`** command to determine whether the issue is with Avaya SBC. If further debugging is required, enable debug logs and get the appropriate logs. For troubleshooting, see Viewing current system incidents on page 404 and Viewing current system alarms on page 380.
- Review the Avaya SBC, Avaya Aura® Session Manager, and endpoint release notes for fixes, limitations, and workarounds.

Note:

Avaya SBC supports maximum 512 active IPs. Avaya SBC can accept connections from 512 IP addresses simultaneously.

Limitations and interactions when administering the Remote Worker solution

Limitation for registering Remote Workers

While sending a 301 Moved Permanently response from Session Manager, Avaya SBC does not replace the Session Manager IP address with the external interface IP address. Therefore, endpoints receiving the 301 Moved Permanently response cannot register to the Session Manager.

For example, two Session Managers are configured in Avaya SBC for Remote Worker as follows:

- The first Session Manager is configured with Public interface as A1 and Private Interface as B1

- The second Session Manager is configured with Public interface as A2 and Private Interface as B2
- A user 1234 is configured with the second Session Manager as Primary Session Manager
- The endpoint is configured with IP address of A1 interface as a proxy or registrar server

In this configuration, when the endpoint attempts registration as Remote worker with user 1234, the endpoint sends the REGISTER message to Avaya SBC on the A1 interface. Then, Avaya SBC sends the REGISTER message to the first Session Manager. For this user, the second Session Manager is configured as the Primary Session Manager. Therefore, the first Session Manager sends a 301 Moved Permanently message with the IP address of the second Session Manager in the contact header to the Avaya SBC. However, Avaya SBC forwards the 301 Moved Permanently response to the endpoint without changing the IP address in the contact header. Therefore, the endpoint cannot REGISTER to the second Session Manager.

Limitation for using 96x1 phones as remote users

When a remote worker is behind a NAT, the source IP in the message is different from the media IP published in the SDP message. In such scenarios, Avaya SBC uses media latching to determine the media IP. However, when remote workers behind a NAT only receive media, but do not send media, media latching cannot be used to determine the media IP. To overcome this limitation, the STUN keep alive mechanism is used to determine the media IP. The 96x1 phones do not support STUN keep alive mechanism. Therefore, when a SIP 96x1 phone registers to Avaya SBC as a remote worker user, the phone cannot use the Group Page feature with which media is unidirectional.

Limitation for using third-party SIP endpoints

Avaya SBC does not officially support the registration of third-party SIP endpoints. When used in combination with Avaya applications such as Avaya Oceana®, Avaya Meetings Server, or Avaya Equinox® Meetings Online, Avaya SBC does not support third-party SIP endpoints unless validated by these Avaya offers or applications.

Interaction with Communication Manager administration for music on hold

For remote workers that are administered behind a NAT, the SIP trunks used for the remote workers must have the following Communication Manager options administered to provide music on hold:

- Using the **`change trunk-group XX`** command, the TRUNK FEATURES screen on Page 3, you must set the **Hold/Unhold Notifications** option to no.
- Using the **`change trunk-group XX`** command, the PROTOCOL VARIATIONS screen on Page 4, you must set the **Network Call Redirection** option to no.

Session Manager configuration for Avaya SBC

Configure Session Manager to whitelist internal IP of SBC and to disable PPM rate limiting.

Related links

Whitelisting Avaya SBC internal IP address on page 486
Adding the internal IP of Avaya SBC in System Manager on page 486
Disabling PPM rate limiting on page 487

Whitelisting Avaya SBC internal IP address

Procedure

1. Log on to the System Manager web interface.
2. In the **Elements** section, click Session Manager.
3. In the left navigation pane, click **Network Configuration** > **SIP Firewall**.
4. On the SIP Firewall Configuration page, click **New**.
5. On the Rule Set page, in the Rules tab, create a new rule.

   For more information about rule sets, see *Administering Avaya Aura® Session Manager*.
6. In the Whitelist tab, create a new entry.
7. In the Key section, select the **Remote IP Address** check box.
8. In the **Value** field, type the Avaya SBC internal IP address.
9. In the left navigation pane, click **Session Manager Administration**.
10. On the **Session Manager Administration** page, in the **Session Manager Instances** section, select Session Manager, and then click **Edit**.

    The system displays the Edit Session Manager page.
11. In the Security Module section, in the **SIP Firewall Configuration** field, select the rule set created in Step 4.
12. Click **Commit**.

Related links

Session Manager configuration for Avaya SBC on page 485

Adding the internal IP of Avaya SBC in System Manager

Procedure

1. Log on to the System Manager web interface.
2. In the **Elements** section, click Session Manager.
3. In the left navigation pane, click **Network Configuration** > **Remote Access**.
4. In the Remote Access page, click **New**.

   The system displays the Remote Access Configuration page.
5. In the **Name** field, type the name of the new access list.

   For more information about access lists, see *Administering Avaya Aura® Session Manager*.
6. In the **SIP Proxy Mapping Table** section, click **New**.
7. In the **SIP Proxy Public Address (Reference A)** field, type the public IP address for interface B1 used for remote worker.

8. In the **Session Manager (Reference C)** field, click the Session Manager instance being used.
9. In the **SIP Proxy Private IP Addresses** section, click **New**.
10. In the **SIP Private IP Address (Reference B)** field, type the internal IP address of Avaya SBC.
11. On the Remote Access page, click the remote access configuration name that you created.
12. Click **Commit**.
13. **(Optional)** Repeat Step 6 to Step 10 to add more internal IP addresses.

Related links

Session Manager configuration for Avaya SBC on page 485

Disabling PPM rate limiting

Procedure

1. Log on to the System Manager web interface.
2. In the left navigation pane, click **Session Manager Administration**.
3. On the **Session Manager Administration** page, in the **Session Manager Instances** section, click the Session Manager instance, and then click **Edit**.
4. On the **Edit Session Manager** page, in the **Personal Profile Manager (PPM) – Connection Settings** section, clear the **Limited PPM Client Connection** and **PPM Packet Rate Limiting** check boxes.
5. Click **Commit**.

Related links

Session Manager configuration for Avaya SBC on page 485

Remote worker configuration checklist

Task	Link	✔
Clone the Avaya-ru profile.	Cloning the Avaya-ru profile on page 488	
Create an Avaya call server profile.	Creating an Avaya call server profile on page 489 (advanced services only)	
Create an external signaling interface for the phone network.	Creating an external signaling interface for a phone network on page 490	
Create an internal signaling interface for the Avaya call server.	Creating an internal signaling interface for an Avaya call server on page 491	

Table continues…

Task	Link	✔
Create an external media interface for the phone network.	Creating an external media interface for a phone network on page 493	
Create an internal media interface for the Avaya call server.	Creating an internal media interface for an Avaya call server on page 493	
Create a PPM Mapping Profile.	Creating standard PPM mapping profiles on page 509 or Creating custom PPM mapping profiles on page 494	
Create a reverse proxy policy.	Creating a reverse proxy policy on page 498	
Create a reverse proxy service for PPM traffic.	Creating a reverse proxy relay service for PPM traffic on page 500	
Configure reverse proxy service for downloading a file or firmware.	Creating a reverse proxy relay service for file or firmware download on page 501	
Create a reverse proxy service for multi-tenant or IP Office powered deployments.	Creating reverse proxy service for multi-tenant or IP Office powered deployments on page 502	
Create a media rule.	Creating a media rule on page 512	
Configure application rules for concurrent sessions per endpoint and maximum concurrent sessions.	Creating application rules on page 513	
Create an endpoint policy group.	Creating an endpoint policy on page 563	
Create a routing profile to an Avaya call server.	Creating a routing profile towards Avaya Aura call server on page 514	
Create a server flow.	Creating a server flow on page 515	
Create a subscriber flow.	Creating a subscriber flow on page 516.	
If you are setting up an Avaya Meetings Server remote worker, administer BFCP and FECC.	Configuring Binary Floor Control Protocol on page 589	
Add a URI group for emergency numbers.	Creating a new URI group on page 178	
Enable the URI group by selecting the emergency URI group in the **E911 URI Group** field from **Network & Flows** > **Advanced Options** > **SIP Options**.	Managing SIP options on page 225	

Cloning the Avaya-ru profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

The EMS server displays the Interworking Profiles page.

4. Click an Avaya-ru profile, and then click the **Clone** button.
5. In the Clone Profile window, type the profile name.
6. Click **Finish**.

Creating an Avaya call server profile

Before you begin

Clone the avaya-ru interworking profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.
4. In the application pane, click **Add**.

   The EMS server displays the Add Server Configuration Profile window.
5. Enter a name for the server profile.
6. Click **Next**.

   The EMS server displays the Add Server Configuration Profile – General window.
7. In the **Server Type** field, click **Call Server**.
8. In the **IP Address/Supported FQDNs** field, enter the IP address or FQDN of Session Manager.
9. In the **Transport** field, click transport protocol of Session Manager.

   Note:

   - Avaya recommends the use of TLS as TLS is secure and supports Presence Services.
   - If the call server uses a different IP or FQDN, protocol, and port, click **Add** to add a new entry.
10. Depending on the selected **Transport** option, enter the relevant port number. For example, if you select TLS as the transport mode, then in the **TLS Port** field, type the TLS port number.

    Note:

    - The default port number for TCP and UDP is 5060.

- The default port number for TLS is 5061.

11. Click **Next**.

    The EMS server displays the Add Server Configuration Profile – Authentication window.

12. If you use server authentication, type the related information in the Add Server Configuration Profile – Authentication window.

    Note:

    For remote workers that use an Avaya Aura® network, leave these fields blank.

13. Click **Next**.

    The EMS server displays the Add Server Configuration Profile – Heartbeat window.

14. Select the **Enable Heartbeat** check box to establish a heartbeat.
15. Select appropriate values in the **Method**, **From URI**, and **To URI** fields for sending heartbeat messages towards the server.

    For a single Session Manager instance, leave these fields blank.

16. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.

17. In the **Interworking Profile** field, select the interworking profile as `avaya-ru-multism`.
18. Select the **Enable Grooming** check box.
19. In the **TLS Client Profile** field, click the default TLS profile.
20. For the other fields, do not change the default parameters.
21. Click **Finish** to save and exit.

Related links

Cloning the Avaya-ru profile on page 488

Creating an external signaling interface for a phone network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The application pane displays the list of signaling interfaces, and the content pane displays the parameters of the selected signaling interface.

4. In the upper-right corner of the content pane, click **Add**.

   The EMS server displays the Add Signaling Interface window.

5. Enter the required information in the appropriate fields.
6. Click **Finish** to save and exit.

   Note:

   To configure multi-Session Managers, repeat these steps to add the second signaling interface.

Related links

Signaling interface field descriptions on page 273

Creating an internal signaling interface for an Avaya call server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The application pane displays any existing signaling interfaces, and the content pane displays the parameters of the selected signaling interface.

4. In the right-corner of the content pane, click **Add**.

   The EMS server displays the Add Signaling Interface window.

5. Enter the required information in the appropriate fields and click **Finish**.

Result

The EMS server displays the new internal signaling interface.

Related links

Signaling interface field descriptions on page 273

Add Signaling Interface field descriptions

Name	Description
Name	A descriptive name for one of the following: • External signaling interface for the phone network. • Internal signaling interface for the Avaya call server.
IP Address	IP address of the internal or external signaling interface.
TCP Port	TCP port number. The default TCP port number is 5060.
UDP Port	UDP port number. The default UDP port number is 5060. If your call server uses a different protocol, type the appropriate port numbers in the **TCP Port** /**UDP Port** fields, as applicable.
TLS Port	TLS port number. The default TLS port number is 5061. **Note:** • Avaya recommends the use of TLS as this protocol is secured and supports presence. • Use the B1 interface as the external signaling interface. • To use Avaya one-X® Communicator for shared control, configure the shared control port in the internal signaling interface.
TLS Profile	Profile name of TLS. You can also use third-party certificates. If you specify the TLS port number, then you must select a TLS profile. Otherwise, leave this field blank.
Enable Shared Control	To use Avaya one-X® Communicator in the shared control mode, select the **Enable Shared Control** check box.
Shared Control Port	Shared control port number, for example, 5063. For an internal firewall between Avaya SBC and Session Manager, you must open the Shared Control Port, for example, port 5063. The Shared Control port must not be used anywhere else on the Avaya SBC.

Creating an external media interface for a phone network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.
4. On the Media Interface page, click **Add**.

   The EMS server displays the Add Media Interface window.
5. Enter the required information in the appropriate fields and click **Finish**.

Creating an internal media interface for an Avaya call server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.
4. On the Media Interface page, click **Add**.

   The EMS server displays the Add Media Interface window.
5. Enter the required information in the appropriate fields.
6. **(Optional)** To change the port range settings, go to **Network & Flows** > **Advanced Options** > **Port Ranges** page.
7. **(Optional)** To make **TLS Profile** and **Buffer Size** fields visible in **Media Interface** tab, select the **Media Tunneling** feature in **Network & Flows** > **Advanced Options** > **Feature Control**.
8. In the **TLS Profile** field, select the profile name of the TLS.
9. In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
10. Click **Finish**.

Result

Avaya SBC displays the new external and internal media interfaces.

Related links

Add Media Interface field descriptions on page 494

Add Media Interface field descriptions

Name	Description
Name	A descriptive name for one of the following: • External media interface for the phone network. • Internal media interface for the Avaya call server.
IP Address	IP address of the external or internal media interface.
Port Range	Starting and ending port range numbers. The port range is from 35000 to 40000. To change the port range settings, change the values in the **Port Range** field on the Edit Media Interface page.

Related links

Creating an internal media interface for an Avaya call server on page 493

Creating custom PPM mapping profiles

About this task

Use this procedure to create custom PPM mapping profiles for the following server types:

- Presence
- Session Manager
- Branch Session Manager

For example, you must create a mapping profile for each group of remote workers who use the same pair of Session Manager systems as the primary Session Manager and the secondary Session Manager.

With custom PPM mapping profiles, you can administer server IP addresses, FQDNs, and ports that are not available with the standard set of pre-defined server properties. For example, if you have a geo-redundant deployment and the server that you want to connect to is not in the local network, you can use the custom options to link the servers.

Note:

- When PPM Mapping profile configured with custom option, Avaya SBC expects exact configured Session Manager FQDN from Session Manager in PPM responses to rewrite with the configured mapping of Avaya SBC IP.
- When PPM Mapping profile configured without custom option, Avaya SBC maps the resolved IP of FQDN in server configuration with the PPM response to rewrite with configured mapping of Avaya SBC IP.

  Use IP addresses instead of FQDN if custom PPM profile is required.

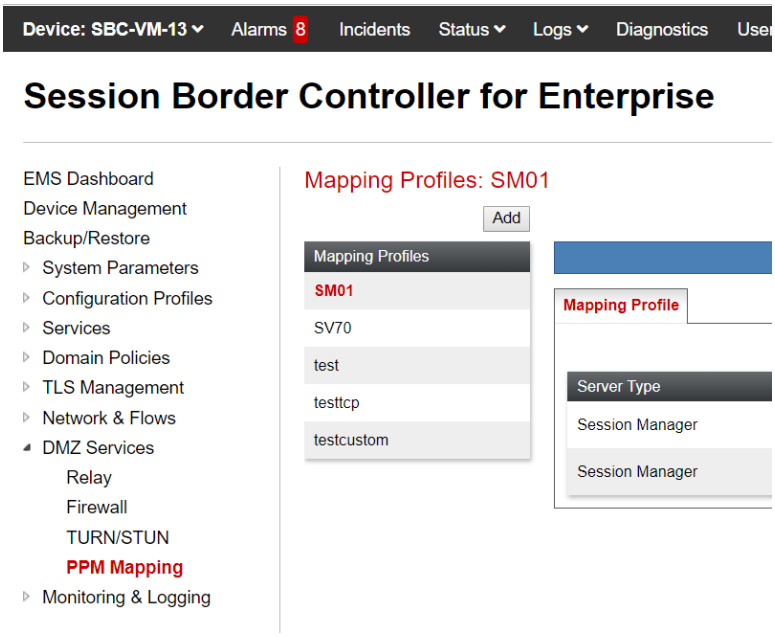
When creating PPM mapping profiles, consider the following:

- Within a mapping profile, you can create multiple profile entries.
- You can administer both standard and custom PPM profile entries in the same mapping profile.
- If you need to convert a profile entry from standard to custom or custom to standard, record the current settings of the profile entry, delete the profile entry, and readminister the profile entry using the standard or custom options.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **PPM Mapping**.
4. Click the **Add** button that is above the **Mapping Profiles** list.

   The system displays a screen similar to the following example:



5. In the **Profile Name** field, type the profile name.
6. Click **Next**.
7. In the **Server Type** field, click one of the following options:
   - **Presence**
   - **Session Manager**
   - **Branch Session Manager**
8. Select the **Custom** check box. For the Session Manager or Branch Session Manager server types, you can click either check box.

   The Mapping Profile window changes to show different options.

For **Presence**, the system displays options for **Server Address** and **Mapped IP**.

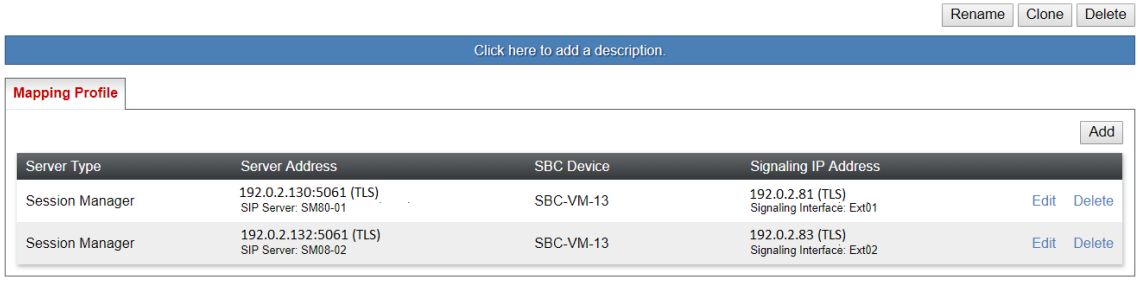
For **Session Manager** or **Branch Session Manager**, the system displays options for **SIP Server Profile**, **Server Address/Port**, **Server Transport**, **Mapped IP/Port**, and **Mapped Transport**.

Important:

You must use the FQDN of the server in the **Server Address** option for Presence, Session Manager, and Branch Session Manager servers.

9. Enter the required information for each option.
10. Click **Finish**.

    The system adds the new mapping profile in the **Mapping Profiles** list and displays the settings for the profile entry that you created in the **Mapping Profile** tab.



11. After adding a new mapping profile, you can do any of the following operations for a mapping profile:
    - (Optional) Click **Click here to add a description** to add a description of the mapping profile. After you add a description, click **Finish**. To change the description, click the displayed description.
    - Click **Rename** to change the name of the mapping profile.
    - Click **Clone** to duplicate the selected mapping profile under a new name. All profile entries assigned to the original mapping profile are copied over to the new mapping profile with the same options. You can then change those options as needed.
    - Click **Delete** to delete the mapping profile and all of its profile entries.
12. For a mapping profile, you can do any of the following operations for the profile entries under the **Mapping Profile** tab:
    - Click the **Add** button to create a new profile entry within the selected mapping profile. The options for a new profile entry are the same as when you created a mapping profile the first time. When you add multiple profile entries to a mapping profile, the entries can be either standard or custom profiles.
    - Click **Edit** to change the options within a profile entry.

- Click **Delete** to delete the individual profile entry within the selected mapping profile.

Related links

Custom PPM mapping profile field descriptions on page 497

Custom PPM mapping profile field descriptions

Name	Description
Profile Name	The name of the PPM mapping profile.
Server Type	The type of server. The options are: • Presence • Session Manager • Branch Session Manager
SIP Server Profile	For Session Manager or Branch Session Manager, select the **SIP Server Profile** that you want to use before you click the **Custom** option. After you click **Custom**, this becomes a display-only field. SIP Server Profile is not used with Presence.
Server Address	**Important:** You must use the FQDN of the server in the **Server Address** option for Presence, Session Manager, and Branch Session Manager servers. Server Address is not used with Session Manager or Branch Session Manager.
Server Address/Port	**Important:** You must use the FQDN of the server in the **Server Address** option for Presence, Session Manager, and Branch Session Manager servers. For Session Manager or Branch Session Manager, the IP address or FQDN and port number of the server. You must manually enter these values. Server Address/Port is not used with Presence.
Server Transport	For Session Manager or Branch Session Manager, the transport protocol used for the server. Server Transport is not used with Presence.
SBC Device	This is a display-only field that shows the SBC server selected when adding a PPM mapping profile.
Mapped IP	For Presence, the IP or FQDN for the mapped device. You must manually enter these values. Mapped IP is not used with Session Manager or Branch Session Manager.

Table continues…

Name	Description
Mapped IP/Port	For Session Manager or Branch Session Manager, the IP or FQDN and the corresponding port for the mapped device. You must manually enter these values. Mapped IP/Port is not used with Presence.
Mapped Transport	For Session Manager or Branch Session Manager, the transport protocol used for the mapping profile. Mapped Transport is not used with Presence.

Related links

Creating custom PPM mapping profiles on page 494

Creating a reverse proxy policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Reverse Proxy Policy**.

   The system displays the Reverse Proxy Policy window.
4. Administer the options described in Reverse Proxy Policy field descriptions on page 498.
5. Click **Finish**.

Related links

Reverse Proxy Policy field descriptions on page 498
Creating a reverse proxy relay service for PPM traffic on page 500
Creating a reverse proxy relay service for file or firmware download on page 501
Creating reverse proxy service for multi-tenant or IP Office powered deployments on page 502
Relay Services field descriptions on page 504

Reverse Proxy Policy field descriptions

Name	Description
General	
Allow Web Sockets	Permits Web Sockets if selected.
Request Max Body Size (in MB)	Indicates the maximum size of the client request body.
Timeout	
Client Body Timeout	Indicates the timeout for reading the client request body.

Table continues…

Name	Description
Client Header Timeout	Indicates the timeout for reading the client request header.
DNS Resolver Timeout	Indicates the timeout for resolving domain name of server address.
TLS/SSL Session Timeout	Indicates the time for which the client can reuse the SSL session parameters.
Server Read Timeout	Indicates the maximum time for which reverse proxy waits to read data from the server before marking it as unavailable
Rate/Connection Limiting	
Enable Rate Limiting	Enables rate limiting. With rate limiting, you can restrict excessive SIP requests from a host and avoid a DoS attack.
Total Number of Clients	Indicates the size of the shared memory zone from which SIP requests will be monitored . This field is available only when you select the **Enable Rate Limiting** check box.
Maximum simultaneous Connections (per client)	Indicates the simultaneous connections per client.
Average Request Rate	Indicates the number of requests permitted per second or minute. If the number of requests exceed the rate specified in this field, the requests are processed at a defined rate. This field is available only when you select the **Enable Rate Limiting** check box.
Burst per Client	Indicates the maximum burst size. Excessive requests are delayed until the number of requests exceed the maximum burst size, after which the request is stopped with an error. This field is available only when you select the **Enable Rate Limiting** check box.
Custom Headers	
Name	Specifies the name of the custom header that you want to add to reverse proxy relay services. Custom headers can be used to specify security headers for the nginx relay service.

Value	Specifies the value of the custom header that you want to add to reverse proxy relay services. The value must be ended with `;` and when it contains `"`, it must be prepended with a backslash (`\`).
	For example, the following value:
	`"max-age=31536000; includeSubDomains" always`
	must be configured as:
	`\"max-age=31536000; includeSubDomains\" always;`

Creating a reverse proxy relay service for PPM traffic

About this task

Use the following procedure for each Avaya SBC.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **Relay**.

   The EMS server displays the Relay Services page.
4. In the **Reverse Proxy** tab, click **Add**.
5. On the Add Reverse Proxy Profile page, administer the following options using Relay Services field descriptions on page 504 for reference:
   a. In the **Service Name** field, type the reverse proxy profile name.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, click the external SBC IP address.
   d. In the **Listen Protocol** field, select the protocol published towards remote workers.

      If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
   e. In the **Listen TLS Profile** field, click the TLS profile you created.

      The default TLS profiles, such as AvayaSBCServer have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.
   f. In the **Listen Port** field, type the port for remote workers.

      The default value is 443 for HTTPS and 80 for HTTP.
   g. In the **Server Protocol** field, click the protocol used for the Avaya SBC server.

      For security reasons, Avaya recommends the use of HTTPS.
   h. In the **Server TLS Profile** field, click the TLS profile that you created.
   i. In the **Connect IP** field, click the IP address that Avaya SBC must use for communicating with the file servers.
   j. In the **PPM Mapping Profile** field, click the mapping profile.

      For information about creating PPM Mapping Profile, see Creating PPM Mapping Profile.
   k. In the **Server Addresses** field, type the PPM server IP address and port number.
   l. In the **IP / URI Blocklist Profile** field, select desired profile.
   m. In the **IP / URI Blocklist Trusted Address** field, enter the trusted server IP address.

6. Click **Finish**.

Creating a reverse proxy relay service for file or firmware download

About this task

You must create a reverse proxy service to download a file or firmware for endpoints on an Avaya SBC device.

You can configure multiple reverse proxy services using the same IP address if the listen ports used are different. If the same port needs to be reused, then configure a different IP address through Network Management.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **Relay**.

   The EMS server displays the Relay Services page.
4. In the **Reverse Proxy** tab, click **Add**.
5. On the Add Reverse Proxy Profile page, administer the following options using Relay Services field descriptions on page 504 for reference:
   a. In the **Service Name** field, type the reverse proxy profile name.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, select the external SBC IP address.

      The IP address must be different from the IP address used for SIP signaling and media interfaces.
   d. In the **Listen Protocol** field, click the protocol published towards remote workers for downloading the file or firmware.

      If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
   e. In the **Listen TLS Profile** field, click the TLS profile that you created.

      The default TLS profiles such as AvayaSBCServer have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.
   f. In the **Listen Port** field, type the port for remote workers.

      For HTTPS, the default value is 443. For HTTP, the default value is 80.
   g. In the **Server Protocol** field, click the protocol used for the Avaya SBC server.

      For security reasons, Avaya recommends the use of HTTPS. If you select the HTTPS protocol, the system enables the **Server TLS Profile** field.

h. In the **Server TLS Profile** field, click the TLS profile that you created.

i. In the **Connect IP** field, click the IP address that Avaya SBC uses to communicate with the file servers.

j. In the **Server Addresses** field, type the server IP address and port number.

Note:

Using the same IP address, you can configure multiple reverse proxy services for different listen ports. To reuse a port, configure a different IP address through Network Management.

6. In the **Reverse Proxy Policy Profile** field, click a reverse proxy policy profile.
7. To enable rewriting URL for the Converged Conference feature, do the following:
   a. To redirect the URL to a different URL, select the **Rewrite URL** field.
   b. In the **URL Replace** field, type the URL that the system must use to replace the current URL.
8. Click **Finish**.

Creating reverse proxy service for multi-tenant or IP Office powered deployments

About this task

You can configure multiple tenants using the same listen IP and different listen domain for the each tenant.

Before you begin

Create TLS server profiles for all the tenants.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **Relay**.

   The EMS server displays the Relay Services page.
4. In the **Reverse Proxy** tab, click **Add**.
5. On the Add Reverse Proxy Profile page, administer the following options using Relay Services field descriptions on page 504 for reference:
   a. In the **Service Name** field, type the reverse proxy profile name.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, select the external SBC IP address.

      The IP address must be different from the IP address used for SIP signaling and media interfaces.

d. In the **Listen Protocol** field, click the protocol published towards remote workers for configuring the multi tenant.

   If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.

e. In the **Listen TLS Profile** field, click the TLS profile that you created.

   The default TLS profiles such as AvayaSBCServer have demonstration certificates. For optimum security, Avaya recommends that you do not use demonstration certificates.

f. In the **Listen Port** field, type the port for remote workers.

   For HTTPS, the default value is 443. For HTTP, the default value is 80.

g. In the **Server Protocol** field, click the protocol used for the Avaya SBC server.

   For security reasons, Avaya recommends the use of HTTPS. If you select the HTTPS protocol, the system enables the **Server TLS Profile** field.

h. In the **Server TLS Profile** field, click the TLS profile that you have created for all the tenants and associate the TLS server profile with the reverse proxy profile.

   The **SNI Options** field for the TLS server profiles must be **None**. The number of TLS server profiles configured must be same as the number of tenants.

6. **(Optional)** Create an **SNI Group** with all tenant's TLS server profiles except tenant one TLS server profile.
7. Create TLS server profile using tenant one certificate with **SNI options** as **OPTIONAL** or **MANDATORY**. Associate the tenant one TLS server profile with the SNI group created in the previous step and with the signaling interface.
8. To enable rewriting URL for the Converged Conference feature, do the following:
   a. To redirect the URL to a different URL, select the **Rewrite URL** field.
   b. In the **Received Server Host** field, select the SAN or CN field of the certificate associated with the TLS server profile.

      Note:

      For any mismatched or non-SNI request with Reverse Proxy Profile configured, Avaya SBC and Avaya Workplace Client works as follows:

      - Without "Any" option in **Received server host**: Avaya SBC serves the first server configured with the received server host, with TLS server profile configured with **SNI Options** as **Optional** or **Mandatory**.
      - With **Any** option in **Received server host**: Avaya SBC serves the server TLS profile certificate configured with the received server host, with TLS server profile configured with **SNI Options** as **Optional** or **Mandatory**.

   c. In the **URL Replace** field, type the URL that the system must use to replace the current URL.
9. Click **Finish**.

Related links

Creating a reverse proxy policy on page 498

Relay Services field descriptions

Application Relay tab

Field	Description
General Configuration	
Name	Specify a name for the application relay.
Service Type	Specify a service type. The options are: XMPP, RTCP, LDAP, SCEP, HTTP, CES, and Other.
Remote Configuration	
Remote IP/FQDN	Specify the server IP address or FQDN as follows: • For RTCP (Core Avaya SBC): Monitoring Server IP address. • For IM (DMZ Avaya SBC): Core Avaya SBC external IP address. • For Avaya SBC at remote site: DMZ Avaya SBC external/public IP.
Remote Port	Specify the port as follows: • For RTCP (Core Avaya SBC): RTCP monitoring port. • For IM (DMZ Avaya SBC and remote site): 5222.
Remote Transport	Specify the remote protocol. **Note:** IM messages are sent to Presence over TCP, while other messages, such as Publish messages are sent to Presence using TLS. The options are: TCP, UDP, and TLS.
Device Configuration	
Listen IP	Specify the network name and IP address as follows: • For RTCP (Core Avaya SBC): Core Avaya SBC external IP address. • For RTCP (DMZ Avaya SBC): DMZ Avaya SBC external IP address. • For IM (DMZ Avaya SBC) and Avaya SBC at remote site: Remote Avaya SBC external IP address.

Table continues…

Field	Description
Listen Port	Specify the port as follows: • For RTCP (Core Avaya SBC): RTCP monitoring port. • For IM (DMZ Avaya SBC and remote site): 5222.
Connect IP	Specify the network name and IP address as follows: • For RTCP (Core Avaya SBC): Core Avaya SBC internal IP1 address. • For RTCP (DMZ Avaya SBC): DMZ Avaya SBC internal IP address. • For IM (DMZ Avaya SBC) and Avaya SBC at remote site: Remote Avaya SBC internal IP address.
Listen Transport	Specify the listen protocol. The options are: TCP, UDP, and TLS.
Additional Configuration	
Whitelist Flows	Select to whitelist flows for XMPP traffic.
Use Relay Actors	Select to use relay actors while configuring Application Relay for RTCP monitoring.
Options	Specify an option: • For RTCP (Core Avaya SBC): End-to-end Rewrite, Hop-By-Hop Traceroute, and Bridging. • For RTCP (DMZ Avaya SBC): Hop-By-Hop Traceroute. • For RTCP (Remote Avaya SBC): End-to-end Rewrite and Hop-By-Hop Traceroute. **Note:** These options are available only when you select the **Use Relay Actors** check box.

The remote port must be configured to the port of the file server. If port 443 is required, TCP should be used. Both Remote port and Listen port, must be the same. To support firmware downloads, use port 80 for listen port and remote port fields. If the ports used are different, configure multiple relays using the same IP address. If the same port needs to be reused, then a different external IP address must be configured using the Network Management feature.

Reverse Proxy tab

Name	Description
Service Name	Reverse proxy file name.
Enabled	Enables the reverse proxy service.

Table continues…

Name	Description
Listen IP	External Avaya SBC IP address and network name. **Note:** Use a different IP address for SIP signaling and media.
Listen Port	80 for HTTP. 443 for HTTPS.
Listen Protocol	Protocol published towards remote workers for downloading the file,
Listen TLS Profile (TLS Server Profile)	TLS profile to be used if HTTPS listen protocol is selected.
Server protocol	Protocol used for the Avaya SBC server.
Server TLS Profile (TLS Client Profile)	TLS profile to be used if HTTPS server protocol is selected.
Listen Domain	Listen domain for the Avaya SBC server.
Connect IP	Network name and IP address that Avaya SBC uses to communicate with file servers.
Load Balancing Algorithm	Algorithm used for load balancing for the reverse proxy. Available options include: • Round-Robin • IP Hashing • Least # of Connections **Note:** When you select the load balancing algorithms for Reverse Proxy, you must configure Avaya SBC services to ensure that no other service is listening on port 80. For example, the **Load Monitoring** service (**Network flows** > **Advanced options** > **Load Monitoring**) to monitor Turn services traffic listens on port 80 by default. You must ensure that these conflicting services should not be used simultaneously.
PPM Mapping Profile	Specifies a PPM Mapping profile.
Reverse Proxy Policy Profile	Reverse proxy profile to be used for this reverse proxy entry.
Rewrite URL	Enables rewriting URL.
Whitelisted IPs	Specifies up to five IPs to be whitelisted.
Server Addresses	Server IP address and port number.

Table continues…

Name	Description
Received Server Host	**Received Server Host** field, select the SAN or CN field of the certificate associated with the TLS server profile. **Note:** For any mismatched or non-SNI request with Reverse Proxy Profile configured: • Without “Any” option in **Received server host**: Avaya SBC serves the first server configured with the received server host, with TLS server profile configured with **SNI Options** as **Optional** or **Mandatory**. • With **Any** option in **Received server host**: Avaya SBC serves the server TLS profile certificate configured with the received server host, with TLS server profile configured with **SNI Options** as **Optional** or **Mandatory**.
Whitelisted URL	Whitelisted URL for the server.
URL Replace	URL to replace the whitelisted URL. This field is available only when you select the **Rewrite URL** check box.

XMPP tab (Applicable to multi-tenant or IP Office powered deployments)

Name	Description
Service Name	XMPP profile name.
Listen IP	External Avaya SBC IP address and network name. **Note:** Use a different IP address for SIP signaling and media.
Listen Port	80 for HTTP. 443 for HTTPS.
Remote FQDN/IP	FQDN or IP address that Avaya SBC uses to communicate with remote workers.
XMPP Domain	XMPP domain name.
DNS/SRV	Option to specify whether DNS priority will be used to route the message.
Remote port	Port used to connect to the remote side of the network.
Connect IP	Network name and IP address that Avaya SBC uses to relay XMPP messages.

H248 Relay tab

Field	Description
General Configuration	
Service Name	Specify a name for the H248 relay.
Media Anchoring	Select the check-box to enable media to pass through SBC.
Listen IP	Select the Avaya SBC IP address and network name.
Listen Port	The default Listen Port is 2944.
Listen Transport	The transport protocol used for communication between the endpoint and interface at Avaya SBC. By default, it is set to TLS.
Listen TLS Profile	Select a TLS profile that is configured with the H248 relay.
Connect IP	The IP address for communicating with the prognosis server. • Type the remote Avaya SBC internal signaling IP for configuring application relay for RTCP monitoring in remote Avaya SBC. • Click the network name, and select the interface that prognosis can reach for configuring application relay for RTCP monitoring in core and DMZ Avaya SBC.
Connect Transport	The transport protocol used for communication between the endpoint and interface at Avaya SBC. By default, it is set to TLS.
Connect TLS Profile	The interface that Communication Manager or Media Gateway Controller can reach. Select the **Connect TLS Profile** from the list.
Remote Server Configuration	
Media Gateway	Select the type of **Media Gateway** from the list.
H248 Media	
Media Gateway Controller	Select the type of **Media Gateway Controller** from the list.
Listen Media Interface	Select the type of **Listen Media Interface** from the list.
Connect Media Interface	Select the type of **Connect Media Interface** from the list.
H248 Management	
H248 Profile	Select the relay name to configure the H248 relay for RTCP monitoring.

Creating standard PPM mapping profiles

About this task

Use this procedure to create standard Personal Profile Manager (PPM) mapping profiles for the following server types:

- Presence
- Session Manager
- Branch Session Manager

For example, you must create a mapping profile for each group of remote workers who use the same pair of Session Manager systems as the primary Session Manager and the secondary Session Manager.

Standard PPM mapping profiles use the set of SIP server profiles, server addresses, signaling interfaces, and mapped transport values that are pre-defined in your system administration. For most deployments, you can use standard PPM mapping profiles.

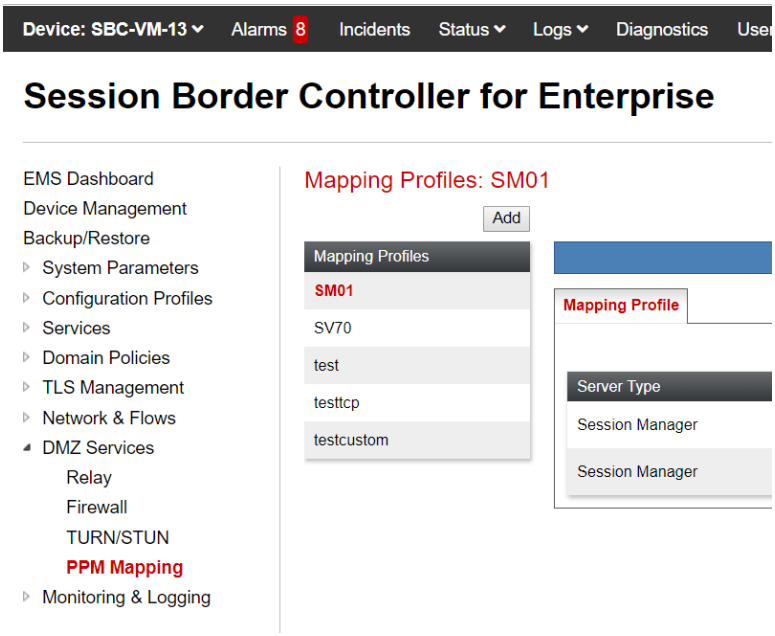
When creating PPM mapping profiles, consider the following:

- Within a mapping profile, you can create multiple profile entries.
- You can administer both standard and custom PPM profile entries in the same mapping profile.
- If you need to convert a profile entry from standard to custom or custom to standard, record the current settings of the profile entry, delete the profile entry, and readminister the profile entry using the standard or custom options.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **PPM Mapping**.
4. Click the **Add** button that is above the **Mapping Profiles** list.

   The system displays a screen similar to the following example:



5. In the **Profile Name** field, type the profile name.
6. Click **Next**.
7. In the **Server Type** field, click one of the following options:
   - **Presence**
   - **Session Manager**
   - **Branch Session Manager**

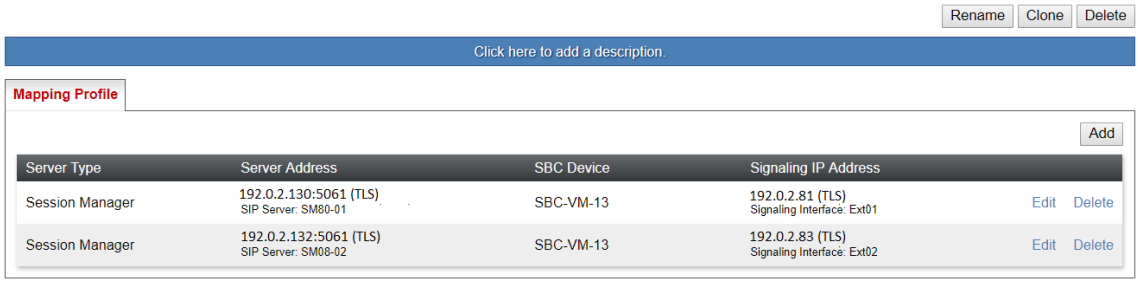
   For **Presence**, the system displays the Mapping Profile window, which has options for **Server Address** and **Signaling Interface** for the SBC Device. For each option, select one of the pre-defined set of values.

   For **Session Manager** or **Branch Session Manager**, the system displays the Mapping Profile window, which has options for **SIP Server Profile**, **Server Address**, **Signaling Interface**, and **Mapped Transport**. For each option, select one of the pre-defined set of values.

   Important:

   You must use the FQDN of the server in the **Server Address** option for Presence, Session Manager, and Branch Session Manager servers.
8. Click **Finish**.

   The system adds the new mapping profile in the **Mapping Profiles** list and displays the settings for the profile entry that you created in the **Mapping Profile** tab.



9. After adding a new mapping profile, you can do any of the following operations for a mapping profile:
   - (Optional) Click **Click here to add a description** to add a description of the mapping profile. After you add a description, click **Finish**. To change the description, click the displayed description.
   - Click **Rename** to change the name of the mapping profile.
   - Click **Clone** to duplicate the selected mapping profile under a new name. All profile entries assigned to the original mapping profile are copied over to the new mapping profile with the same options. You can then change those options as needed.
   - Click **Delete** to delete the mapping profile and all of its profile entries.
10. For a mapping profile, you can do any of the following operations for the profile entries under the **Mapping Profile** tab:
    - Click the **Add** button to create a new profile entry within the selected mapping profile. The options for a new profile entry are the same as when you created a mapping profile the first time. When you add multiple profile entries to a mapping profile, the entries can be either standard or custom profiles.
    - Click **Edit** to change the options within a profile entry.
    - Click **Delete** to delete the individual profile entry within the selected mapping profile.

Related links

Standard PPM mapping profile field descriptions on page 511

Standard PPM mapping profile field descriptions

Name	Description
Profile Name	The name of the PPM mapping profile.

Table continues…

Name	Description
Server Type	The type of server. The options are: • Presence • Session Manager • Branch Session Manager
SIP Server Profile	For Session Manager or Branch Session Manager, the profile that you want to assign to the **Server Type**. SIP Server Profile is not used with Presence.
Server Address	**Important:** You must use the FQDN of the server in the **Server Address** option for Presence, Session Manager, and Branch Session Manager servers. For Session Manager or Branch Session Manager, the pre-defined IP address and port number of the Session Manager system for which you are creating a profile.
SBC Device	This is a display-only field that shows the SBC server selected when adding a PPM mapping profile.
Signaling Interface	The signaling interface used for the profile.
Mapped Transport	For Session Manager or Branch Session Manager, the transport protocol used for the mapping profile. Mapped Transport is not used with Presence.

Related links

Creating standard PPM mapping profiles on page 509

Creating a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Media Rules**.
4. Create a new media rule.

   Note:

   When you use SRTP as preferred format, disable **Encrypted RTCP** as Avaya Aura® does not support encrypted RTCP.

5. Click **Finish**.

Related links

Creating a media rule on page 110

Creating application rules

Before you begin

Clone an existing application rule as a starting point or create a new one. Do not change the default application rule.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.
4. On the applications rule page, create a new application rule.

Note:

- Repeat the steps to create an application rule for Subscriber Flow End Point Policy Group.
- Type the number of concurrent sessions required for the customer license. As a best practice, type a number that is more than the number specified in the customer license. For example, if you have a license for 300 concurrent sessions, type 500 for each, audio and video.
- If you clone the default application rule, Audio is already enabled. However, you must adjust the values and then enable Video, if required.

Creating an endpoint policy group

Before you begin

Create a media rule to associate the endpoint policy group with the subscriber flow and the server flow.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The application pane displays the defined policy groups, and the content pane displays the parameters of the selected policy group.

4. Create a new policy group.
5. Click **Finish**.

Note:

Create two endpoint policy groups, one for server flow, and one for subscriber flow.

- Create a new subscriber flow and associate the new endpoint policy to the subscriber flow.
- Create a new server flow and associate the new endpoint policy to the server flow.

Creating a routing profile towards Avaya Aura® call server

About this task

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing** .
4. On the Routing Profile page, click **Add**.
5. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
6. Click **Next**.

   The system displays the second Routing Profile page.
7. **(Optional)** In the **URI Group** field, select the URI group for the routing profile.

   For example, if you have a routing profile *Test1* and URI Group *user 1234@test.com*, any request message to user 1234@test.com will resolve profile Test1.
8. **(Optional)** In the **Time of Day** field, enter the time-of-day profile.

   Note:

   Remote users must not use the time-of-day profile for the routing profile.
9. In the **Load Balancing** field, click one of the options. You can configure up to 20 next hop addresses with the available load balancing.
   - Priority: From the list of next-hop addresses, request messages take the first priority. If a request message fails to reach the first next-hop address, the request message takes the second priority.
   - Round Robin: Request messages are delivered to the next-hop address on a round-robin basis. Any request message is processed sequentially, beginning again with the first next-hop address, in a circular manner.

- Weighted Round Robin: Each configured next-hop address is assigned a weight. Request messages route to the next-hop address on the basis of the assigned weight.
- DNS/SRV: Used for configuring multiple domain names. If selected, you can enable or disable NAPTR. Avaya SBC uses DNS priority to route the message. If you disable NAPTR, specify the transport type.

10. In the **Transport** field, click **TCP**, **UDP**, or **TLS**.

    If you define the transport type in the **Transport** field, the system deactivates the common **Transport Type** field.

11. Select the **Next Hop Priority** check box.

    If you enable this setting, Avaya SBC processes the configured next-hop address in the event of failure routing.

12. Select the **Ignore Route Header** check box to enable the system to ignore the message route header while resolving message routing.
13. Click **Add** to configure the next-hop address.
14. Click **Finish**.

Creating a server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   The application pane displays the list of existing devices, and the content pane provides the subscriber flow and server flow information about the selected device.

4. In the **Server Flows** tab, click **Add**.

   The EMS server displays the Add Flow window.

5. In the **Flow Name** field, type a flow name.
6. In the **Server Configuration** field, select the server profile created earlier.
7. Keep the default value for the **URI Group**, **Transport**, and **Remote Subnet** fields.
8. In the **Received Interface** field, select the external interface towards the endpoints.
9. In the **Signaling Interface** field, select the internal interface towards the Avaya call server, for example, Sig_Intf_Int_to_Call_Server.
10. In the **Media Interface** field, select the interface towards the Avaya call server, for example, Med_Intf_1.
11. In the **End Point Policy Group** field, click the created endpoint policy.

12. In the **Routing Profile** field, keep the default value.
13. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
14. Select **FQDN Support** checkbox to use the FQDN for ASBC address instead of IP address for headers added by ASBC. By default **FQDN support** is disabled.
    - If checkbox is not selected, ASBC adds IP address in message
    - If checkbox is selected, ASBC adds FQDN value to message instead of IP.
15. In the **FQDN** field, type a FQDN value. **FQDN** field is applicable only when **FQDN support** is enabled.
16. In the **Tenant Configuration Profile** field, select the tenant configuration profile.

    The default value is **None**.

    For Cloud solutions that deploy MS Teams, you must create a customer tenant configuration profile to generate telemetry reports for the customer. For more information, see Tenant configuration on page 286.
17. Click **Finish** to save and exit.

Creating a subscriber flow

About this task

Use the following procedure to create a subscriber flow. The procedure is explained by using Subscriber_Flow_1 as a sample.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.

   The EMS server displays the End Point Flows page.
4. In the **Subscriber Flows** tab, click **Add**.

   The EMS server displays the Add Flow window.
5. Create a User Agent.
6. In the **Flow Name** field, type `Subscriber_Flow_1`.
7. Unless the customer has special requirements, use the default values for the **URI Group**, **User Agent**, **Source Subnet**, **Via Host**, and **Contact Host** options.
8. In the **Signaling Interface** field, select the external interface towards the endpoint.
9. Click **Next**.

The system displays the second Add Flow window.

10. Set the **Source** option to **Subscriber**.
11. Do not administer the **Methods Allowed before REGISTER** option.
12. In the **Media Interface** field, select the corresponding media interface towards the endpoint.
13. In the **Secondary Media Interface** field, select **None**.
14. In the **End Point Policy Group** field, select the endpoint policy created earlier.

    Note:

    If RTP is needed use default low or avaya-def-low-encoding (for SRTP) depending on the endpoints.
15. In the **Routing Profile** field, click the name of the routing profile that points toward the Avaya call server.
16. Select **FQDN Support** checkbox to use the FQDN for SBC address instead of IP address for headers added by SBC. By default **FQDN support** is disabled.
    - If checkbox is not selected, SBC adds IP address in message
    - If checkbox is selected, SBC adds FQDN value to message instead of IP.
17. In the **FQDN** field, type a FQDN value. **FQDN** field is applicable only when **FQDN support** is enabled.
18. If you require TLS transport, select the desired TLS profile in the **TLS Client Profile** field.
19. In the **Presence Server Address** field, enter the Presence server IP address or FQDN.

    Avaya SBC does not rewrite the Presence Subscription URI if Remote Workers use FQDN instead of the external Avaya SBC IP address in the **Presence Server Address** field. This change is required to support the endpoints that implement Presence Services Communication Profile, such as Avaya Workplace Client 3.0. For these endpoints, Request-URI of a presence SUBSCRIBE request is in the form user@domain.com and must not be changed by the Subscriber Flow. This change permits the concurrent deployment of older and new endpoints in the same solution. Presence service to the Remote Workers does not work if the private FQDN used to reach Avaya SBC is not resolvable in the enterprise network.
20. **(Optional)** If you type an FQDN instead of an IP address in the **Presence Server Address** field, do one of the following:
    - Configure Split DNS to ensure that the private FQDN can be resolved within the enterprise network.
    - Create a Regular Expression in Session Manager for Presence, and use the Regular Expression in the Routing Policy for the Presence Server.

    This step is relevant only to older endpoints that are administered with an FQDN for Presence Services address. This step is not required for Avaya Workplace Client 3.0.

21. In the **IP / URI Blocklist Profile** field, select desired profile.
22. In the **Trusted Address** field, enter the trusted server IP address.

    The trusted IP address identified by the Admin are not blocked.
23. Click **Finish**.

Related links

Adding a new user agent (Advanced Services only) on page 270
Add URI Group field descriptions on page 179
User agents (Advanced Services only) on page 270

Configuring application relay for IM

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **Relay Services**.

   The following endpoints support Presence Server configuration by using PPM Mapping:

   - Avaya one-X® Communicator for Windows: Release 6.2 SP 11 Patch 3.
   - 96x1 phones: Release 6.5.
   - Avaya Workplace Client for all platforms: Release 3.0.

     Avaya Workplace Client was earlier known as Avaya Communicator.
3. On the Relay Services page, click **Application Relay** > **Add**.
4. On the Add Application Relay page, do the following:
   a. In the **Name** field, type the name of the application relay.
   b. In the **Service Type** field, click **XMPP**.
   c. In the **Remote IP/FQDN** field, type the prognosis server IP.
   d. In the **Remote Port** field, type the port number 5222.
   e. In the **Remote Transport** field, click **TCP**.
   f. In the **Listen IP** field, click the network name, and click the IP to which endpoint sends packets or the interface facing the endpoint.
   g. In the **Connect IP** field, click the network name, and select the interface that prognosis can reach.
   h. In the **Listen Transport** field, click **TCP**.

Note:

Whitelist Flows and **Use Relay Actors** fields are not applicable to **Service Type** as **XMPP** selection.

5. Click **Finish**.

Checklist for configuring Presence server

Endpoints get presence information from the Presence server. To ensure that presence information is available to the endpoints in the network, you must add the Presence server IP address in:

- The subscriber flow
- The PPM mapping profile

Task	Description	Reference	✔
Add Presence server IP to the subscriber flow.	All endpoints support Presence server configuration by using the subscriber flow.	Creating a subscriber flow on page 516	
Create PPM Mapping Profile for Presence server.		Creating standard PPM mapping profiles on page 509 or Creating custom PPM mapping profiles on page 494	

Monitoring RTCP for a single Session Manager deployment

About this task

The primary function of RTCP is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information to participants in a streaming multimedia session.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**
4. On the Advanced Options page, click the **RTCP Monitoring** tab.

5. Select the **RTCP Monitoring Relay** check box.

   Note:

   For relay settings, do not use an IP address that is already in use for SIP signaling and media bandwidth efficiency.

6. In the **Node Type** field, click **Core**.
7. In the **Relay IP** field, click the internal IP address of Avaya SBC.

   This IP address is used to relay the traffic received from the DMZ SBC and core phones towards the monitoring server.

8. In the **Port** field, type the port number used for RTCP monitoring.
9. Click **Save**.

Application relay settings for RTCP monitoring using single Session Manager

An application relay must be configured on CORE Avaya SBC for RTCP traffic received from DMZ Avaya SBC and core phones. Another application relay must be configured for RTCP traffic received from media gateway.

Relay 1: For RTCP traffic coming from DMZ Avaya SBC and core phones

RTCP traffic received on Core Avaya SBC external IP Address is sent out to a monitoring server using Core Avaya SBC internal IP1 address.

Relay 2: For RTCP traffic coming from media gateway

RTCP traffic received on Core SBC internal IP1 address is sent out to a monitoring server using Core Avaya SBC internal IP2 address.

For more information about application relay settings, see the Application relay field descriptions section.

Related links

Relay Services field descriptions on page 504

Configuring call support for unregistered endpoints

About this task

Use this task to configure call support for unregistered endpoints. For example, unregistered endpoints might still require support in case of an emergency call or when someone is using a click to call feature.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **URI Groups**.
4. In the application pane, click **Add**.

   The EMS server displays the Add URI window.
5. In the **Group Name** field, type the name of the URI group.

   The group name must indicate that the URI group is for emergency calls from unregistered numbers.

   For example, in the **Group Name** field, type `911_Anonymous`. If configuring a group for the click to call feature, type `Click2Call`.
6. Click **Next**.
7. In the **URI Type** field, click **Plain**.
8. In the **URI** field, type `anonymous@ucaas`.

   This URI group is applied to a subscriber to allow unregistered Avaya SIP endpoints to dial an emergency number or use click to call.
9. Click **Finish**.
10. In the navigation pane, click **Network & Flows** > **End Point Flows**.

    In the content area, the EMS server displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBC security devices.
11. Click the **Subscriber Flows** tab.
12. Click **Add**.

    The EMS server displays the Add Flow window.
13. In the **Flow Name** field, type the name of the endpoint flow.
14. In the **URI Group** field, click the URI group that you created for emergency calls from unregistered SIP endpoints.
15. In the **Signaling Interface** field, click the external interface for this Avaya SBC.
16. Click **Next**.
17. In the **Source** field, click **Click To Call**.
18. In the **Media Interface** field, click the external interface for this Avaya SBC.
19. In the **End Point Policy Group** field, click the policy for remote endpoints.
20. In the **Routing Profile** field, click the routing profile that is mapped to the required Session Manager.
21. Click **Finish**.

Checklist for back-to-back configuration with a single Session Manager

No.	Task	Reference	Notes	✔
1.	Configure core Avaya SBC.	Remote worker configuration checklist on page 487.		
2.	Configure DMZ Avaya SBC.	Remote worker configuration checklist on page 487.		
2a.	Configure the server interworking profile.	Creating Interworking Profiles on page 529	1. Clone avaya-ru server interworking profile and name the profile as avaya-ru-b2b. 2. In **Advanced** tab, in the **Record Routes** field, click **None**.	
2b.	Configure the server.	Creating an Avaya call server profile on page 489.	Ensure that the server configuration points to corresponding external IP address of core Avaya SBC. **Note:** Select the server interworking profile created in Step 2a.	
2c.	Configure the subscriber flow.	Creating a subscriber flow on page 516.		
2d.	Creating a reverse proxy service for file or firmware download.	Creating reverse proxy service for file or firmware download on page 501.		
2e.	Configure application relay settings for IM.	Application relay settings for IM on page 504.		

Checklist for back-to-back-to-back configuration with a single Session Manager

No	Task	Reference	Notes	✔
1.	Configure core Avaya SBC.	Remote worker configuration checklist on page 487.		
2.	Configure DMZ Avaya SBC.	Remote worker configuration checklist on page 487.		
2a.	Configure the server interworking profile.	Creating Interworking Profiles on page 529.	1. Clone avaya-ru server interworking profile and name it as avaya-ru-b2b. 2. In **Advanced** tab, in the **Record Routes** field, click None.	
2b.	Configure the server.	Creating an Avaya call server profile on page 489.	Ensure that the server configuration points to the corresponding external IP address of core SBC. **Note:** Select the server interworking profile created in Step 2a.	
2c.	Configure the subscriber flow.	Creating a subscriber flow. on page 516		
2d.	Configure reverse proxy for file download.	Creating reverse proxy service for file or firmware download. on page 501		
2e.	Configure application relay settings for IM.	Configuring application relay for IM. on page 518		
3.	Configure remote Avaya SBC.			
3a.	Do not configure public IP address in the **Network Management** feature.			

Table continues…

No	Task	Reference	Notes	✔
3b.	Configure the server inter-working profile.		1. Clone avaya-ru server interworking profile and name it as avaya-ru-b2b. The server interworking profile configuration is same. Therefore, you can use the same profile between the two SBCs. 2. In **Advanced** tab, in the **Record Routes** field, click None.	
3c.	Configure server.		When the Avaya SBC is facing the internet directly, the server configuration for Session Manager must point to the corresponding WAN IP address of the enterprise network or the external IP address of the SBC in DMZ. Do not configure the server configuration for the Presence server.	
3d.	Configure default topology profile.			
3e.	Configure an application relay to support IM for remote workers.	Application relay settings for IM on page 504		

Monitoring RTCP for back-to-back-to-back deployment

About this task

The primary function of RTCP is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information to participants in a streaming multimedia session.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**
4. On the Advanced Options page, click the **RTCP Monitoring** tab.

5. Select the **RTCP Monitoring Relay** check box.

   For relay settings, do not use an IP address that is already in use for SIP signaling and media bandwidth efficiency.

6. In the **Node Type** field, perform the following:
   - For DMZ Avaya SBC configuration, click **DMZ**.
   - For CORE Avaya SBC configuration, click **Core**.
   - For remote Avaya SBC configuration, click **Remote**.

7. In the **Relay IP** field, click **None**.

   For Core Avaya SBC configuration, in the **Relay IP** field, click the IP address of the core Avaya SBC Internal IP1.

   Note:

   Core Avaya SBC Internal IP1 address is the address used to send RTCP traffic received from DMZ Avaya SBC and core phones towards a monitoring server.

8. For Core Avaya SBC configuration, in the **Port** field, type `5005`.

   For other configurations, do not change the values.

9. Click **Save**.

Next steps

Configure application relay settings specific to the Core Avaya SBC configuration, remote worker configuration, or DMZ configuration.

Application relay settings for monitoring RTCP using back-to-back-to-back deployment

Configure application relay for monitoring RTCP (DMZ Avaya SBC).

Configure two application relays for the Core Avaya SBC as follows:

Relay 1 : For RTCP traffic coming from DMZ Avaya SBC and core phones

RTCP traffic is received on Core Avaya SBC external IP address and is sent out to a monitoring server using Core Avaya SBC internal IP1 address.

Relay 2: For RTCP traffic coming from media gateway

RTCP traffic is received on Core SBC internal IP1 address and is sent out to a monitoring server using Core Avaya SBC internal IP2 address.

Note:

If there are multiple Core Avaya SBC, repeat the RTCP configuration steps on each Avaya SBC.

For more information about application relay settings, see the Application relay field descriptions section.

Related links

Relay Services field descriptions on page 504

Chapter 14: Configuration of server flows for SIP trunking

About SIP trunking

With the SIP Trunking feature of Avaya SBC security devices, SIP trunk-enabled enterprises can completely secure SIP connectivity over the Internet. This security is achieved through SIP trunking services obtained through an Internet Telephony Service Provider (ITSP).

SIP trunking ensures the privacy of all calls traversing the enterprise network, while maintaining a well-defined demarcation point between the core and access network. In addition, with the SIP Trunking feature in Avaya SBC, an enterprise can maintain granular control through well-defined domain policies. These domain policies secure SIP implementations or servers of customers from known SIP and Media vulnerabilities.

Because the Avaya SBC security device is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the SBC device for processing. See Figure 6: Avaya SBC deployed in the enterprise DMZ on page 528. If the signaling traffic is encrypted, the Avaya SBC device decrypts all TLS encrypted traffic and looks for anomalous behavior. Then, Avaya SBC forwards the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

Example

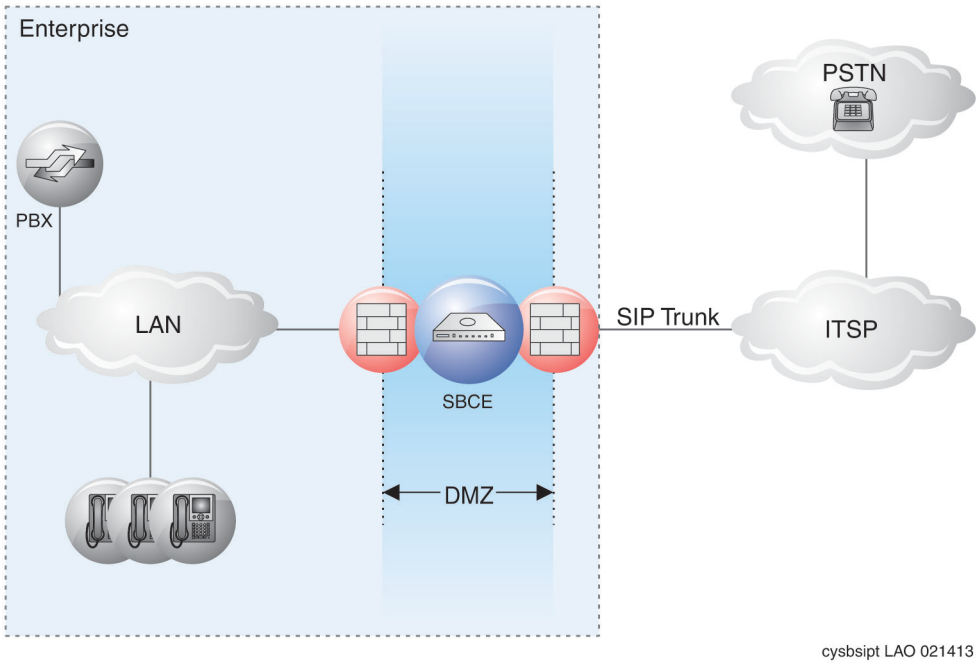


Figure 6: Avaya SBC deployed in the enterprise DMZ

SIP trunk configuration checklist

Use this checklist while configuring a generic Avaya SBC SIP trunk with the generic call server or trunk server. Based on the call server options, configure the signaling manipulation and interworking. For more information about signaling manipulation, see specific call server or trunk server Application Notes.

Task	Reference	✔
Create interworking profiles.	Creating Interworking Profiles on page 529.	
Create server profiles for call server and trunk server.	Creating Server Profile for Call Server on page 530 and Creating Server Profile for Trunk Server on page 531.	
Create routing profile for call server and trunk server.	Creating Routing Profile for Call Server on page 532 and Creating a Routing Profile for a Call Server on page 532.	
Create Topology Hiding Profile.	Creating a Topology Hiding profile on page 535	
Create signaling interfaces.	Creating External Signaling Interface toward Trunk Server on page 536 and Creating Internal Signaling Interface Toward Call Server on page 537.	

Table continues…

Task	Reference	✔
Create media interfaces.	Creating External Media Interface toward Trunk Server on page 538 and Creating Internal Media Interface Toward Call Server on page 538.	
Create server flows.	Creating call server flow on page 539 and Creating a trunk server flow on page 540.	
Perform server-specific configuration for trunking.	Configuring Avaya SBC for SIP Trunk on page 541 and Configuring Avaya SBC for other trunks on page 542.	

Creating Interworking Profiles

About this task

Interworking Profile features are configured based on different Trunk Servers, for example, Avaya and Nortel. You can use the available default profiles as is or after modification, or configure new profiles.

Note:

The procedures before and after this section provide generic instructions for SIP trunking configuration that apply to all implementations.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The existing interworking profiles are displayed. You can use a default Trunk Server Profile, modify the default Trunk Server Profile, or create a new Trunk Server Profile.
4. Click **Add**.
5. In the **Profile Name** field, type a name for the new profile.
6. Enter required information in the Interworking profile screens, and click **Finish**.

   The system displays the newly created interworking profile.
7. Click the **Advanced** tab, and click **Edit**.
8. Select appropriate fields on the Editing Profile screen, and click **Finish**.

Next steps

To configure trunks servers used in your network, see Configuring Avaya SBC for SIP Trunk on page 541 and Configuring Avaya SBC for SIP Trunk on page 541.

Creating Server Profile for Call Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.
4. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.
5. In the **Profile Name** field, type a call server name and click **Next**.

   The system displays the second Server Configuration Profile window.
6. In the **Server Type** field, click **Call Server**.
7. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or of the FQDN.
8. In the **Transport** field, select the transport protocol that you want to use.

   For integration with Teams, you must select **TLS**.
9. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.

   For integration with Teams, you must select `5061` when using TLS.
10. Click **Next**.

    The system displays the Add Server Configuration Profile – Authentication screen.
11. **(Optional)** If you use server authentication, type the related information on this screen.
12. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.
13. **(Optional)** If you use the heartbeat feature, select the **Enable Heartbeat** check box and type relevant details in the **Method**, **Frequency**, **From URI**, and **To URI** fields.

    If you enable the heartbeat, a message is sent periodically to the server to help monitor the connectivity status of the server. When a primary and secondary server are available in the network, this server status is useful to determine which server is active.
14. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.
15. **(Optional)** If the Call Server is Session Manager, select the **Enable Grooming** check box.

    With Grooming enabled, the system can reuse the same connections for the same subscriber or port.

16. In the **Interworking Profile** field, select the profile name for the type of call server.

    For the Avaya Call Server Profile, you can clone the default `avaya-ru` profile. You can use the cloned profile to make any changes in the interworking profile.
17. In the **TLS Client Profile** field, select the client profile to be used for the server.
18. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.
19. In the **Connection Type** field, click a connection type.
20. Click **Finish**.

Creating Server Profile for Trunk-side server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.
4. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.
5. In the **Profile Name** field, type a trunk server name and click **Next**.

   The system displays the second Server Configuration Profile window.
6. In the **Server Type** field, click **Trunk Server**.
7. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or its FQDN.
8. In the **Transport** field, select the transport protocol that you want to use.
9. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.
10. Click **Next**.

    The system displays the Add Server Configuration Profile – Authentication screen.
11. **(Optional)** If you use server authentication, type the related information on this screen.
12. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.
13. **(Optional)** If you use the heartbeat feature, select the **Enable Heartbeat** check box and type relevant details in the **Method**, **Frequency**, **From URI**, and **To URI** fields.

If you enable the heartbeat, a message is sent periodically to the server to help monitor the connectivity status of the server. When a primary and secondary server are available in the network, this server status is useful to determine which server is active.

14. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.

15. **(Optional)** If you use the TCP or TLS transport protocol, select the **Enable Grooming** check box.

    With Grooming enabled, the system can reuse the same connections for the same subscriber or port.

16. In the **Interworking Profile** field, select the profile name for the type of trunk server.

    For the Avaya Call Server Profile, you can clone the default `avaya-ru` profile. You can use the cloned profile to make any changes in the interworking profile.

17. In the **TLS Client Profile** field, select the client profile to be used for the server.
18. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.
19. In the **Connection Type** field, click a connection type.
20. Click **Finish**.

Creating a Routing Profile for a Call Server

About this task

Use this procedure to create a routing profile with the next hop as a call server address.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.
4. In the application pane, click **Add**.

   The application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.

5. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
6. Click **Next**.

   The system displays the second Routing Profile window.

7. **(Optional)** In the **URI Group** field, select the URI group of the routing profile. For example, if you have a routing profile *Test1* and URI Group *user 1234@test.com*, any request message to user 1234@test.com will resolve profile Test1.
8. **(Optional)** In the **Time of Day** field, enter the time-of-day profile.

   Remote users must not use the time-of-day profile for the routing profile.
9. In the **Load Balancing** field, enter one of the following options. You can configure up to five next hop addresses with the available load balancing.
   - Priority: From the list of next-hop addresses, request messages take first priority. If a request message fails to reach the first next-hop address, the request message takes the second priority.
   - Round Robin: Request messages are delivered to the next-hop address on a round-robin basis. Any request message is processed sequentially, beginning again with the first next-hop address, in a circular manner.

     Note:

     You must create another routing profile for the next hop as a SIP trunk address.
   - Weighted Round Robin: Each configured next-hop address is assigned a weight. The request messages routes to the next-hop address on the basis of the assigned weight.
   - DNS/SRV: Multiple domain names can be configured. If selected, you can enable or disable NAPTR. Avaya SBC uses DNS priority to route the message. If you disable NAPTR, specify the transport type.
10. In the **Transport** field, enter **TCP** or **TLS**.

    If you define the transport type here, the system deactivates the common **Transport Type** field.
11. Select the **Next Hop Priority** check box.

    If you enable this setting, Avaya SBC processes the configured next-hop address when routing fails.
12. Select **Call Server** from **Server Configuration**.
13. Click **Add** to configure the next-hop address.
14. Click **Finish**.

Creating Routing Profile for Trunk Server

About this task

This procedure will create a routing profile with next hop as a Trunk side Server IP address.

Note:

Use the following profile name: `Route_to_Trunk_Svr`.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Configuration Profiles** > **Routing**.
4. In the Application pane, click **Add**.

   The Application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.
5. In the **Profile Name** field, type the profile name in the `Route_to_Trunk_Svr` format.
6. Click **Next**.

   The system displays the second Routing Profile window.
7. Log in to the EMS web interface with administrator credentials.
8. In the navigation pane, click **Configuration Profiles** > **Routing**.
9. In the Application pane, click **Add**.

   The Application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.
10. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
11. Click **Next**.

    The system displays the second Routing Profile window.
12. **(Optional)** In the **URI Group** field, select the URI group of the routing profile. For example, if you have a routing profile *Test1* and URI Group *user 1234@test.com*, any request message to user 1234@test.com will resolve profile Test1.
13. **(Optional)** In the **Time of Day** field, enter the time-of-day profile.

    Note:

    Remote users must not use the time-of-day profile for the routing profile.
14. In the **Load Balancing** field, enter one of the options. You can configure up to five next hop addresses with the available load balancing.
    - Priority: From the list of next-hop addresses, request messages take the first priority. If a request message fails to reach the first next-hop address, the request message takes the second priority.
    - Round Robin: Request messages are delivered to the next-hop address on a round-robin basis. Any request message is processed sequentially, beginning again with the first next-hop address, in a circular manner.

Note:

You must create another routing profile for next hop as a SIP trunk address.

- Weighted Round Robin: Each configured next-hop address is assigned a weight. The request messages routes to the next-hop address on the basis of the assigned weight.
- DNS/SRV: Multiple domain names can be configured. If selected, you can enable or disable NAPTR. Avaya SBC uses DNS priority to route the message. If you disable NAPTR, specify the transport type.

15. In the **Transport** field, enter **TCP** or **TLS**. If you define the transport type here, the system deactivates the common **Transport Type** field.
16. Select the **Next Hop Priority** check box. If you enable this setting, Avaya SBC processes the configured next-hop address in the event of failure routing.
17. Select **Trunk Server** from **Server Configuration**.
18. Click **Add** to configure the next-hop address.
19. Click **Finish** to save the configuration and exit.

    This displays the Routing Profile screen, showing the newly created `Route_to_Trunk_Svr` Routing Profile along with the `Route_to_Call_Svr` Routing Profile created by the procedure described in Creating Routing Profile for Call Server on page 532.
20. For a failover trunking configuration, select the Next Hop priority checkbox.
21. Specify the priorities for the configured trunking servers.
    - Priority 1: the primary server
    - Subsequent priorities: secondary server(s)

    The following are the ways in which Avaya SBC can failover from one trunking server to the next. The ways in which Avaya SBC detects whether the server is reachable.
    - **Heartbeat**: Enable this setting on the Server Profile setting.
    - **SIP Timer**: SIP RFC 3261 Timer. By default, this functionality is available for all the request messages. If you want to overwrite RFC 3261 timer, use the **server interworking profile** timer configuration
    - **Server Error Message**: If the server sends a 5xx message, Avaya SBC considers the server as currently unavailable.

Creating a Topology Hiding profile

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the left navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The left Application pane displays the Topology Hiding profiles, and the Content pane displays the parameters of the selected profile.
3. In the Application pane, click the default profile.
4. In the Content pane, click **Clone**.

   The system displays the Clone Profile window.
5. In the **Clone Name** field, type the name in the `SBCE_to _Call_Svr` format and click **Finish**.

   The system displays the cloned profile in the application pane.
6. To modify the cloned profile, in the left navigation pane, click the cloned profile.
7. In Content pane, click **Edit**.
8. After you have modified the values, click **Finish** to save, submit, and exit.

Creating external signaling interface toward Trunk-side server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Signaling Interface**.

   The left Application pane displays the list of signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
4. In the upper-right corner of the Content pane, click **Add**.

   The system displays the Add Signaling Interface window.
5. In the **Name** field, type a descriptive name for the external signaling interface for the phone network.
6. In the **IP Address** field, select the IP address of the external signaling interface.
7. Depending on the transport protocol you are using for your network, do the following:
   - If you use TCP, in the **TCP Port** field, type the TCP port number. The default TCP port number is 5060.
   - If you use UDP, in the **UDP Port** field, type the UDP port number. The default UDP port number is 5060.
   - If you use TLS, in the **TLS Port** field, type the TLS port number. The default TLS port number is 5061.

When you specify the TLS port, the system enables the **TLS Profile** and **Enable Shared Control** fields.

Note:

- TLS is a secure protocol. To use TLS, you must have advanced session licenses and encryption licenses.
- Use the B1 interface as the external signaling interface.
- Enable only the transport protocols that you want to use.

8. From the **TLS Profile** field, select the appropriate Avaya SBC TLS profile name.

   You can also use third-party certificates.

   If you specify the TLS port number, then you must select a TLS profile. Otherwise, leave this field blank.

9. Click **Finish**.

Note:

To configure multiple Session Managers, repeat this task to add the second signaling interface.

Creating Internal Signaling Interface toward Call Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Signaling Interface**.

   The left Application pane displays any existing signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.

4. In the right-corner of the Content pane, click **Add**.
5. In the Add Signaling Interface window, add the following parameters:
   a. In the **Name** field, type a name for the internal signaling interface for the Avaya call server.
   b. From the **IP Address** field, select the IP address of the internal signaling interface.
   c. Configure the transport that you want to use.

Note:

- TLS is a secure protocol. To use TLS, you must have advanced session licenses and encryption licenses. In the **TLS Port** field, type the port number `5061`.

- If your call server uses a different protocol, type the appropriate port numbers in the **TCP Port** or **UDP Port** fields, as applicable.
- The default port number for TCP and UDP is 5060.
- Do not select the **Enable Stun** check box.

d. **(Optional)** From the **TLS Profile** field, select the profile name for TLS.

You can select a TLS profile only when you add a TLS port. If the **TLS Port** field is empty, the **TLS Profile** field is unavailable.

e. Click **Finish** to save and exit.

The system displays the new internal signaling interface.

Creating External Media Interface toward Trunk Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.
4. In the upper-right corner of the Application pane, click **Add**.

   The system displays the Add Media Interface window.
5. In the **Name** field, enter a descriptive name for the external media interface toward the phone network.
6. In the **IP Address** field, click the IP address of the external media interface.
7. In the **Port Range** fields, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.
8. Click **Finish**.

Creating Internal Media Interface toward call server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the left navigation pane, click **Network & Flows** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.

4. In the Applications pane, click **Add**.

   The system displays the Add Media Interface window.

5. In the **Name** field, type a descriptive name for the internal media interface of the Avaya call server.
6. In the **IP Address** field, click the IP address of the internal media interface.
7. In the **Port Range** field, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.

8. Click **Finish**.

Creating call server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **End Point Flows**.

   The left Application pane displays the list of existing devices, and the Content pane provides the subscriber flow and server flow information about the selected device.

4. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow window.

5. In the **Flow Name** field, enter a flow name.
6. In the **Server Configuration** field, click the name of the Avaya call server profile.
7. Keep the default value for the **URI Group**, **Transport**, and **Remote Subnet** fields.
8. In the **Received Interface** field, click the name of the interface pointing toward the SIP trunk, for example, Sig_Intf_Ext_to_Trunk_Net.
9. In the **Signaling Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Sig_Intf_Int_to_Call_Server.
10. In the **Media Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Med_Intf_1.
11. In the **End Point Policy Group** field, click the created endpoint policy.
12. In the **Routing Profile** field, choose the routing profile towards SIP trunk.

13. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
14. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.
15. In the **Remote Branch Office** field, keep the default value **Any** or select another remote branch office.
16. Click **Finish** to save and exit.

Creating a trunk server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.

   The system displays the End Point Flows page.
4. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow page.
5. In the **Flow Name** field, type a name for the server flow.
6. Unless the customer has special requirements, use the default (*) values for the **URI Group**, **Transport**, and **Remote Subnet** options.
7. In the **Signaling Interface** field, click the name of the interface that receives all of the SIP traffic from the trunk server.
8. In the **Media Interface** field, select the name of the interface that receives all media traffic from the trunk.
9. In the **End Point Policy Group** field, use the default value: default-low.

   Note:

   If the phones use TLS/SRTP, select the appropriate end policy group.
10. In the **Routing Profile** field, click the name of the routing profile that points toward the trunk server.
11. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
12. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.

13. In the **Remote Branch Office** field, keep the default value **Any** or select another remote branch office.

    The **Remote Branch Office** field lists all servers configured for remote branch office.

14. Enable the **Link Monitoring from Peer** option to enable handling of incoming SIP OPTIONS messages.

    The **Link Monitoring from Peer** option is used to support the Avaya Aura® SIP Resiliency feature. Avaya SBC must support the SIP Resiliency feature in the OPTIONS response Contact header. Session Manager should know the SIP Resiliency supported for neighboring elements to change the call/message sequence behavior for the Session Manager failover/failback scenarios.

    When **Link Monitoring from Peer** is enabled, Avaya SBC sends a success (200OK) response if the OPTIONS request is matched to that server flow.

    When **Link Monitoring from Peer** is disabled, the OPTIONS request is relayed to the destination server.

15. Click **Finish**.

Configuring Avaya SBC for SIP Trunk

Before you begin

Perform all the steps needed for trunk configurations, including configuration of a SIP trunk with Avaya.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The system displays the Server Configuration screen.

4. In the **General** tab, ensure that you see the servers created in earlier steps.
5. Click the **Advanced** tab, and ensure that the **Interworking Profile** field displays the correct profile selected for the Avaya server.
6. **(Optional)** If the correct **Interworking Profile** name for Avaya is not selected in the **Advanced** tab screen, click the **Edit** button to display the Advanced Edit pop-up screen, and select the profile name for the Avaya Interworking Profile.
7. Click **Finish** to save and exit.
8. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.
9. In the **Interworking Profiles** list, click an Interworking profile.

You can clone the default `avaya-ru` profile, or create a new interworking profile.

10. Click the **Advanced** tab.
11. Click the **Edit** button at the bottom of the screen.

    The system displays the Advanced Edit window.
12. In the **Extensions** field, select **None**.
13. Click **Finish** to save and exit.
14. In the Server Interworking screen, click the **General** tab.
15. In the lower-center section of the screen, click the **Edit** button.
16. In the **Hold Support** field, click **RFC2543**.
17. Click **Next**, and then click **Finish** to save and exit.

Configuring Avaya SBC for other trunks

Before you begin

Perform all steps needed for all trunk configurations, including parameter settings that are specific to the type of trunk server being configured.

Procedure

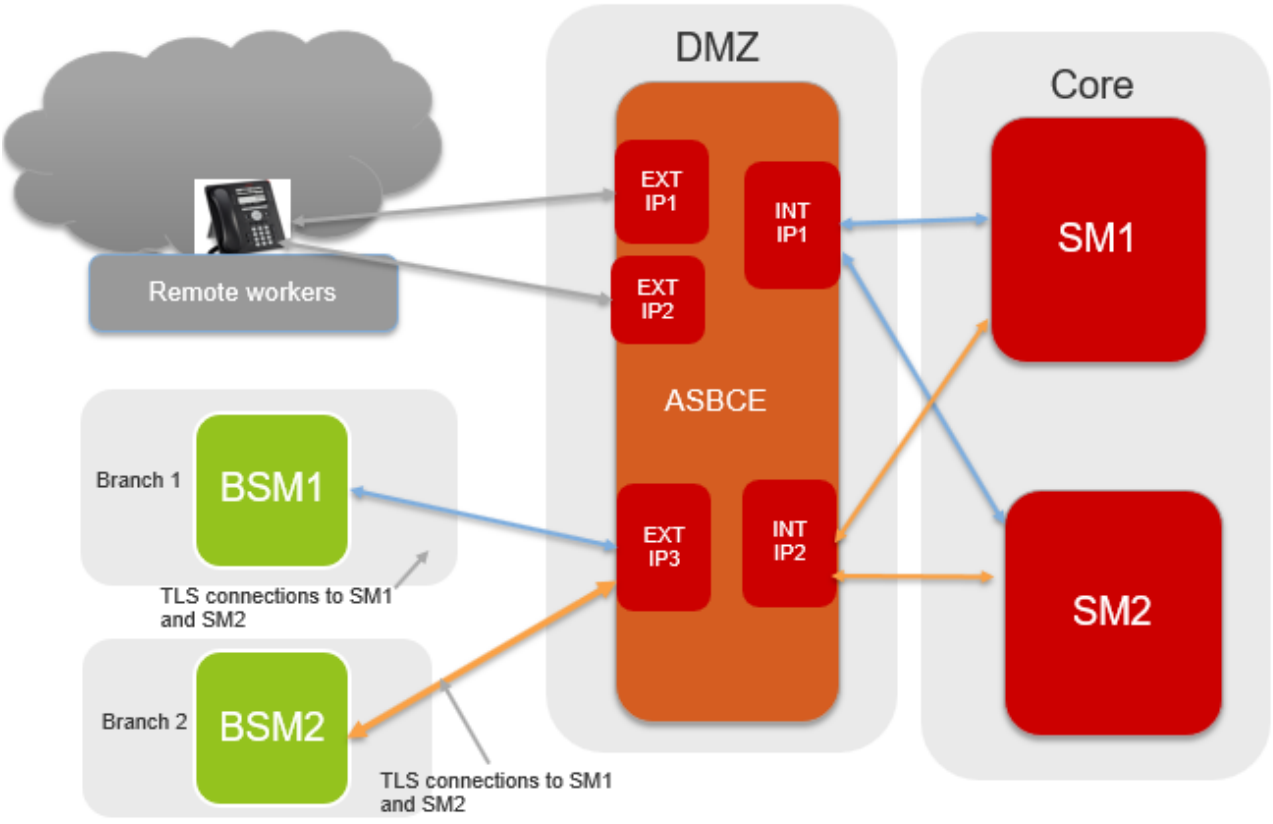
1. Enable server interworking features for different trunk servers, based on the customer requirements.
2. If a default interworking profile is unavailable, then create a new profile.

   Refer Application Notes on https://support.avaya.com for specific interworking configuration.

Chapter 15: Branch Survivability

Avaya Enterprise Cloud (AEC) is cloud service provides UC and CC SIP solutions or customers. It provides an alternative for existing Avaya Aura® customers that want to move their existing Avaya Aura® premises service to more a cloud experience while maintaining much of their existing setup and system experience. The subscription service is hosted and managed by Avaya in Azure Data Centers. The AEC Branch Survivability feature provides survivability to remote workers in branches.

This feature is used in a configuration that provides survivability to remote workers in branches. The following diagram shows a setup where a remote worker maintains connectivity to both Session Manager in the core and Session Manager in branches. When core Session Manager is available all connectivity is to core Session Manager through Avaya SBC. When there is a failure, Remote worker will use branch Session Manager and hence survives locally within the branch.



Remote side (Workers): Connections are always initiated from remote workers to Avaya SBC. An external IP is configured on Avaya SBC for each core Session Manager for redundancy configurations.

Remote side (Branches): Connections are always initiated from Branch Session Manager to Avaya SBC and there is a single external IP on Avaya SBC that all Branch Session Managers connect to. A connection established from a Branch Session Manager to a Session Manager is reused for the messages from Session Manager to Branch Session Manager.

Core side: An internal IP is assigned for each Branch Session Manager. In Avaya SBC, each Session Manager is configured with a server for each IP.

When there is a failure between core and branches, Remote Workers detect the failure and uses Branch Session Manager for local survivability. It connects multiple Branch Session Managers to core Session Manager through Avaya SBC using a single external IP. This in turn minimizes cost to customers as external IPs in cloud environment are expensive. Single External IP is the key advantage of this feature.

The SIP trunk connectivity established from Branch Session Manager to Session Manager through Avaya SBC can be used to route calls.

Checklist for configuring Branch Survivability

No.	Task	Reference	✔
1	Create a TLS server profile.	Creating a TLS server profile on page 545	
2	Create an external signaling interface for all Branch Session Managers to connect.	Adding a new signaling interface on page 545	
3	Create an internal signaling interface for Avaya SBC to connect to Session Managers. **Note:** One signaling interface should be created for each Branch Session Manager.	Adding a new signaling interface on page 545	
4	Create a Branch Session Manager server profile.	Creating a Branch Session Manager server profile on page 546	
5	Create a Session Manager server profile.	Creating Server Profile for Call Server on page 530	
6	Create a routing profile for Branch Session Manager server flow.	Creating a routing profile on page 547	

Table continues…

No.	Task	Reference	✔
7	Create a routing profile for Session Manager server flow.	Session Manager server flow uses the default routing profile.	
8	Create a server flow for Branch Session Manager.	Creating a server flow for Branch Session Manager on page 547	
9	Create a server flow for Core Session Manager.	Creating a server flow for Core Session Manager on page 548	

Creating a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.

   The application pane displays the Server Profiles screen.
4. Click **Add**.

   The application pane displays the New Profile window.
5. In the **Certificate** field, select the required certificate.

   This certificate is used to verify the common name of Session Manager.
6. In the **SNI Options** field, select **Mandatory**.
7. **(Optional)** In the **SNI Group** field, select an SNI group.

   If this interface checks multiple SNIs, you can create an SNI group and add all the TLS server profiles to this group.
8. In the **Peer Verification** field, select **Required**.

   This field enables mutual authentication.
9. Configure the remaining fields.

   For more information, see TLS server profile screen field descriptions on page 368.
10. Click **Finish**.

Adding a new signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the Avaya SBC instance to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The application pane displays the Signaling Interface screen.

4. In the content pane, click **Add**.

   The application pane displays the Add Signaling Interface pop-up window.

5. Configure the fields.

   For more information, see Signaling interface field descriptions on page 273.

6. Click **Finish**.

Creating a Branch Session Manager server profile

About this task

Creating a Remote Branch Office server to route messages to the Branch Session Manager.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, select the Avaya SBC instance.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The EMS server displays the SIP Servers page.

4. In the application pane, click **Add**.

   The EMS server displays the Add Server Configuration Profile window.

5. In the **Profile Name** field, enter a name for the server profile.
6. Click **Next**.

   The EMS server displays the Add Server Configuration Profile window.

7. In the **Server Type** field, select **Remote Branch Office**.
8. Select the **Verify TLS Common Name** check box.
9. In the **TLS Common Name** field, common name must be unique for each remote Branch Server.

   You must create an end point certificate with a unique common name for each remote Branch Server.

10. In the **IP Address/Supported FQDNs** field, enter the IP address of the Branch Session Manager.
11. In the **Transport** field, select **TLS**.
12. In the **Port** field, enter the TLS port number.

    The default port number for TLS is 5061.

13. Click **Next**.

    The EMS server displays the Add SIP Server Profile – Authentication window.

14. If you use server authentication, type the required information in the Add Server Configuration Profile – Authentication window.

15. Click **Next**.

    The EMS server displays the Add SIP Server Profile - Advanced window.
16. In the **Interworking Profile** field, select the interworking profile.
17. Select the **Enable Grooming** check box.
18. Leave the remaining fields to the default values.
19. Click **Finish**.

Related links

Server configuration profile field descriptions on page 319

Creating a routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, select the Avaya SBC instance.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules that comprise a selected routing profile.
4. In the application pane, click **Add**.
5. In the **Profile Name** field, type a distinctive name for the new routing profile, and click **Next**.
6. Select the **Server Name Indication (SNI)** check box.
7. In the **Server Name** field, enter the common name for Session Manager.

   Branch Session Manager sends this common name in TLS handshake to indicate the connection to Session Manager. This certificate common name is from TLS server profile associated to the external signaling interface.
8. Enter the requested information into the remaining fields.

   For more information, see Routing profile field descriptions on page 186.
9. Click **Finish**.

   The application pane displays the new routing profile.

Related links

Routing profile field descriptions on page 186

Creating a server flow for Branch Session Manager

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, select the Avaya SBC instance.

3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   The application pane displays the list of existing devices, while the content pane provides subscriber flow and server flow information about the selected device.

4. Click the **Server Flows** tab and click **Add**.

   The application pane displays the Add Flow window.

5. In the **Flow Name** field, enter a name for the server flow.
6. In the **SIP Server Profile** field, select the Remote Branch Office server.
7. In the **Received Interface** field, select the interface configured for the Branch Session Manager.
8. In the **Routing Profile** field, select the routing profile that contains SNI rules for each core Session Manager.

   When multiple Branch Session Managers are used, all Branch Session Manager server flows use the same routing profile.

9. In the **Topology Hiding profile** field, set the appropriate value depending on the server.

   This field changes the SIP message headers sent to the next hop server.

10. Leave the remaining fields to the default values.
11. Click **Finish**.

Related links

Add Subscriber Flow field descriptions on page 164

Creating a server flow for Core Session Manager

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, select the Avaya SBC instance.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   The application pane displays the list of existing devices, while the content pane provides the subscriber flow and server flow information about the selected device.

4. Click the **Server Flows** tab and click **Add**.

   The application pane displays the Add Flow window.

5. In the **Flow Name** field, enter a name for the server flow.
6. In the **SIP Server Profile** field, select the core server.
7. In the **Received Interface** field, select the interface all Branch Session Managers connect.
8. In the **Signaling Interface** field, select the signaling interface.

   A unique signaling interface should be created for each Branch Session Manager.

9. In the **Media Interface** field, select the media interface.
10. In the **Routing Profile** field, select the routing profile that routes to Branch Session Manager.
11. In the **Remote Branch Office** field, select the the next hop Branch Session Manager.

    This field is the key to route the messages from Session Manager to Branch Session Manager. Avaya SBC uses SNI information in route and this field to route the message to correct Branch Session Manager.
12. In the **Topology Hiding profile** field, set the appropriate value depending on the server.

    This field changes the SIP message headers sent to the next hop server.
13. Leave the remaining fields to the default values.
14. Click **Finish**.

Related links

Add Subscriber Flow field descriptions on page 164

Chapter 16: Multiple Session Manager

Multiple Session Manager support for Avaya SBC in Remote Worker deployment

After Avaya SBC installation, Avaya SBC is ready for configuration and is available for administration through the web console.

Avaya SBC must be configured with one-to-one mapping of signaling and media interfaces. Signaling and media interface configuration is explained in the following sections.

The network configuration must have a unique set of external and internal IP addresses on Avaya SBC corresponding to the primary and secondary Session Manager.

Note:

Avaya SBC supports only two Session Managers. Ensure that the Management interface, or the IP used to access GUI, is not in the same subnet as the internal or external interface.

The following sections describe how to use Avaya SBC in a multiple Session Manager environment.

Note:

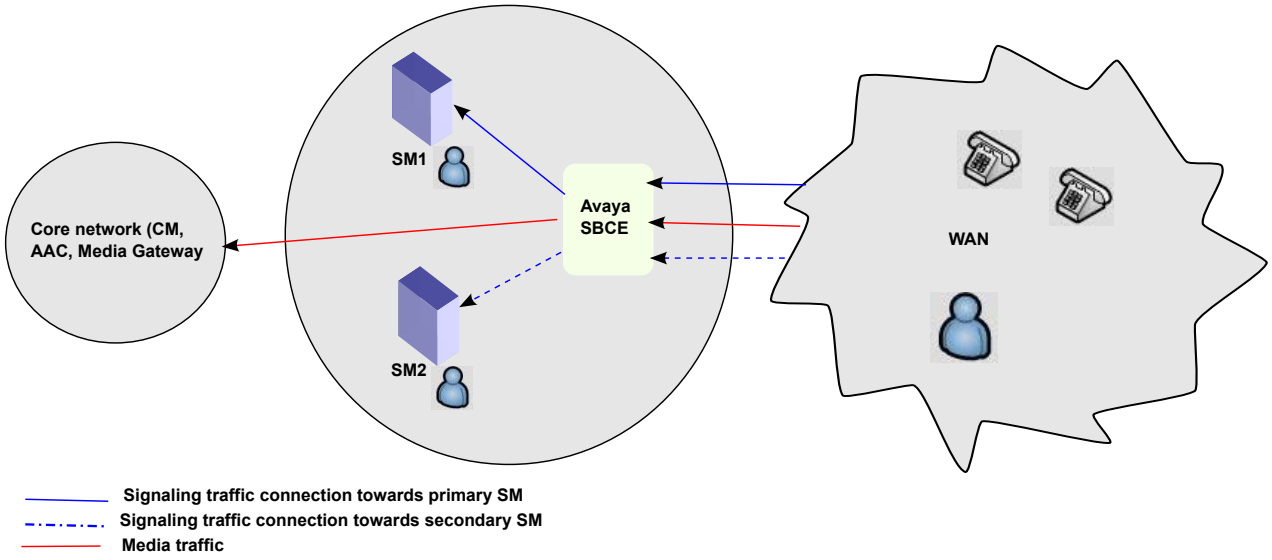
In the following sections:

- The IP address on Avaya SBC towards the internet is referred to as an external address.
- The IP address on Avaya SBC towards the core network or call server is referred to as an internal address.

Single Avaya SBC connected to two Session Managers

In the following scenario, the phones in the network maintain two socket connections to Avaya SBC, at two different IP addresses hosted by Avaya SBC:

- One socket for traffic to primary Session Manager 1
- Second socket for traffic to secondary Session Manager 2



Multiple Session Manager configuration checklist

Task	Notes	Reference	✔
Configure internal and external addresses, corresponding to the primary and secondary Session Managers for the A1 and B1 interfaces.		Configuring internal and interfaces on page 553	
Create two external signaling interfaces and two internal signaling interfaces.		Creating an external signaling interface toward phone network on page 490 Creating an internal signaling interface toward Avaya call server on page 491	
Create two external media interfaces and two internal media interfaces.		Creating an external media interface toward phone network on page 493 Creating internal media interface toward Avaya call server on page 493	
Create a media rule.		Creating a media rule on page 512	
Create a server interworking profile.		Creating a server interworking profile on page 553	

Table continues…

Task	Notes	Reference	✔
Ensure that voice sessions are set as per the user license in the application rules and enable video.		Creating application rules on page 513	
Create an endpoint policy group.		Creating an endpoint policy group on page 513	
Create two server profiles, one for the primary and another for the secondary Session Manager.	Ensure that you enable heartbeat so that Avaya SBC sends heartbeats to Session Manager. The heartbeats are used to detect whether a Session Manager is available.	Creating an Avaya call server profile on page 489	
Create a reverse proxy for file download.		Creating a reverse proxy relay service for file or firmware download on page 501	
Create two routing profiles for primary and secondary Session Managers.	Do not use alternate routing in a multiple Session Manager deployment. Do not configure the **Next Hop Server 2** field. Remote worker uses its algorithm to determine when to reach the secondary Session Manager. Avaya SBC does not require alternate routing in this type of deployment if the primary Session Manager goes down.	Creating a routing profile to Avaya call server on page 514	
Create two subscriber endpoint flows corresponding to the primary and secondary Session Managers.	If you require RTP, use default low or avaya-def-low-encoding (for SRTP) depending on the endpoints. **Note:** If RTP and SRTP are both used, select capability negotiation.	Creating a subscriber flow on page 516	

Table continues…

Task	Notes	Reference	✔
Create a server flow.	Create two server flows, one for Session Manager 1 and another for Session Manager 2.	Creating a server flow on page 167	
Configure an application relay for IM.		Configuring application relay for IM on page 518	

Note:

For more information about remote worker configuration, see Remote worker configuration checklist on page 487.

Configuring the Avaya SBC IP addresses corresponding to the primary and secondary Session Managers

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   Avaya SBC displays the Network Management page.
4. Click **Networks** > **Add**.
5. In the Add Network dialog box, type the following:
   - An External IP address for signaling towards endpoints to support the corresponding Session Manager.
   - An External IP address for configuration of the file or firmware download.
   - An internal IP address for signaling towards the corresponding Session Manager. This address can be reused for configuration file/firmware download.
6. Select **Interface Configuration** and enable the interfaces.
7. Repeat Step 2 to Step 5 for each Avaya SBC system.
8. Click **Finish**.

Creating a server interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.

   Avaya SBC displays the Interworking Profiles page.

4. Select the **avaya-ru** profile, and click **Clone**.

   Avaya SBC displays the Clone Profile window.
5. In the **Clone Name** field, type `avaya-ru-multism`.
6. Click **Finish**.
7. Click the new **avaya-ru-multism** profile, and click **Timers**.
8. Click **Edit**.
9. In the **Trans Expire** field, type `4`.

   This setting supports Fast response timeout towards Session Manager.
10. Click **Finish**.

Configuring application relay settings for multiple Session Manager

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **Relay Services**.

   Note:

   - Set all the other parameters under general configuration to default values.
   - Define application relay on both SBCs in HA pair to connect to the file server.

   For information about downloading the firmware, see *Creating a reverse proxy service for file or firmware download*.

   For configuring application relay settings for IM, see *Configuring application relay for IM*.

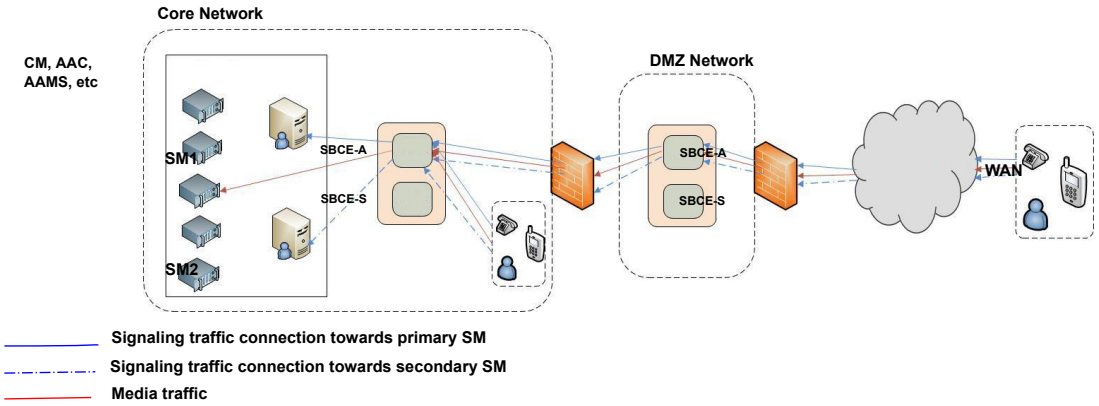
Multiple Session Manager support with back-to-back Avaya SBCs

Avaya SBCs are deployed back-to-back in a multiple Session Manager remote worker solution. In the solution, one Avaya SBC is deployed in the DMZ network and another Avaya SBC in the CORE network.

You can manage both Avaya SBCs by using a single EMS web console or different EMS web consoles.

Ideally, there must be a firewall between the CORE and DMZ network, but the firewall is not mandatory for the Avaya SBC deployment.

In the following diagram, the core and DMZ Avaya SBCs have been deployed in HA mode.



Back-to-back configuration checklist

In the following table, the first task refers to the configuration of Avaya SBC in the Core network. The rest of the tasks refer to the configuration of Avaya SBC in the DMZ network.

For more information, see *Multiple Session Manager configuration checklist*.

Note:

Remote workers must register to IP address of Avaya SBC in DMZ.

No.	Task	Notes	✔
1.	Configure Avaya SBC in the Core network.	Use the multiple Session Manager configuration checklist.	
2.	Configure Avaya SBC in the DMZ network.	For more information about configuring SBC in DMZ, see the previous section. If there are no remote workers configured to get the service from DMZ SBC directly, the **Enable heartbeat** field in the **Server Configuration** feature corresponds to Core SBC 1 and Core SBC 2.	
2a.	Configure server interworking profile.	Clone the avaya-ru server interworking profile and name it `avaya-ru-multism`. The server interworking profile configuration is same if you are using the same EMS to manage Avaya SBC in remote location and Avaya SBC in DMZ. In **Timers** tab, set the **Trans Expire** field to 4 seconds. This is to support FAST RESPONSE TIMEOUT. In Advanced tab, set **Record Routes** to None.	

Table continues…

No.	Task	Notes	✔
2b.	Configure server.	Server configuration corresponding to primary Session Manager and secondary Session Manager point to the corresponding external IP address of the Core Avaya SBC. **Note:** Repeat this step for each Core Avaya SBC that you deploy. Do not configure server configuration for Presence server. Ensure that you enable heartbeat so that Avaya SBC sends heartbeats to Session Manager. The heartbeats are used to detect whether a Session Manager is available.	
2c.	Configure topology hiding profile.		
2d.	Configure a reverse proxy for file download.	See Creating a reverse proxy relay service for file or firmware download on page 501.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Configuring application relay for IM on page 518.	

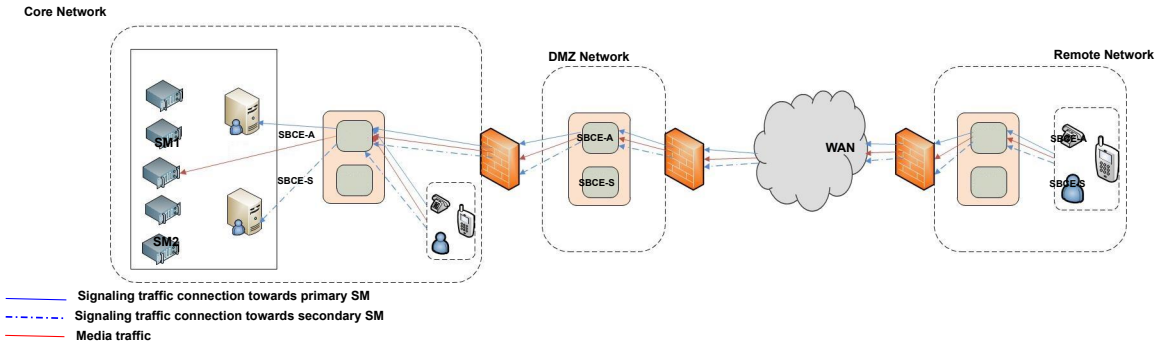
Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBC systems

Avaya SBC systems are deployed at three levels in a multi-Session Manager remote worker solution. In this solution, one Avaya SBC is deployed in the DMZ network, one or more Avaya SBC systems are deployed in the CORE network, and another Avaya SBC is deployed in the remote site.

There is no restriction on the number of EMS web consoles used to manage the Avaya SBC. The only requirement is to manage all core Avaya SBC systems using a single EMS web console.

Note:

Ensure that the EMS can reach the Avaya SBC that it manages through the network.



Related links

Back-to-back-to-back configuration checklist on page 557

Back-to-back-to-back configuration checklist

No.	Task	Details	✔
1.	Configure core Avaya SBC.	Use the multi-Session Manager checklist in the previous section. **Important:** Task 1 refers to configuring Core Avaya SBC. However, the other tasks given below, that is 2, 2a, 2b, 2c, 2d, and 2e refer to configuration of Avaya SBC in DMZ network and 3, 3a, 3b, 3c, 3d, 3e, and 3f refer to configuration of SBC in remote network	
2.	Configure Avaya SBC in the DMZ network.	For more information about configuring Avaya SBC in DMZ, see the previous section. If there are no remote workers configured to get the service from DMZ Avaya SBC directly, the **Enable heartbeat** field in the **Server Configuration** feature corresponds to Core Avaya SBC 1 and Core Avaya SBC 2.	
2a.	Configure server interworking profile.	Clone the avaya-ru server interworking profile and name it `avaya-ru-multism`. The server interworking profile configuration is same, if using the same EMS to manage Avaya SBC in remote location and Avaya SBC in DMZ. In **Timers** tab, set the **Trans Expire** field to 4 seconds. This is to support FAST RESPONSE TIMEOUT. In Advanced tab, set **Record Routes** to None.	

Table continues…

No.	Task	Details	✔
2b.	Configure server.	Server configuration corresponding to primary Session Manager and secondary Session Manager point to the corresponding external IP address of the Core Avaya SBC. **Note:** Repeat this step for each Core Avaya SBC that is deployed. Ensure that you enable heartbeat so that Avaya SBC sends heartbeats to Session Manager. The heartbeats are used to detect whether a Session Manager is available. Do not configure server configuration for Presence server.	
2c.	Configure topology hiding profile.		
2d.	Configure a reverse proxy for file download.	See Creating a reverse proxy relay service for file or firmware download on page 501.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Relay Services field descriptions on page 504.	
3.	Configure the remote Avaya SBC.		
3a.	Do not configure public IP address in the **Network Management** feature.		
3b.	Configure server interworking profile.	Clone the avaya-ru server interworking profile and name it `avaya-ru-multism`. The server interworking profile configuration is same, therefore you can use the same profile between the two SBCs. In **Timers** tab, configure Trans Expire to 4 seconds. This is to support FAST RESPONSE TIMEOUT towards Session Manager. In Advanced tab, set **Record Routes** to None.	
3c.	Configure server.	When Avaya SBC is facing the internet directly, the server configuration for primary Session Manager and secondary Session Manager must point to the corresponding WAN IP address of the enterprise network or the external IP address of the SBC in DMZ.	
3d.	Configure default topology profile.		
3e.	Configure a reverse proxy for file download.	See Creating a reverse proxy relay service for file or firmware download on page 501.	

Table continues…

No.	Task	Details	✔
3f.	Configure an application relay to support IM for remote workers.	See Configuring application relay for IM on page 518.	

Related links

Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBC systems on page 556

Geographic-redundant deployment

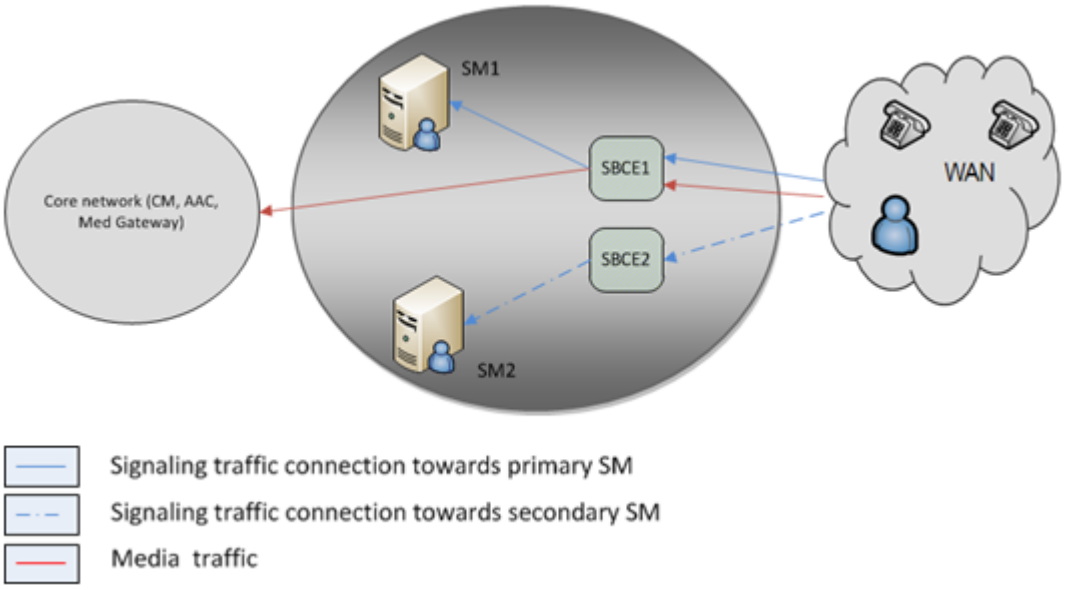
In a Geographic-redundant deployment, you can deploy two different Avaya SBC devices in two different data centers. You can deploy the devices as individual Avaya SBC devices or devices managed by their own EMS. You can deploy these Avaya SBC devices in a High Availability mode or a non-High Availability mode. You can deploy EMS in High Availability mode in different data centers only if layer 3 connectivity is available between the two data centers.

Related links

Geographic-redundant deployment in the non-HA mode on page 559
Geographic-redundant deployment in the HA mode on page 560
Checklist for configuring Geographic-redundant deployment on page 561
Creating an endpoint policy on page 563
Configuring Avaya SBC for web collaboration on page 564
Configuring Presence Server on page 565

Geographic-redundant deployment in the non-HA mode

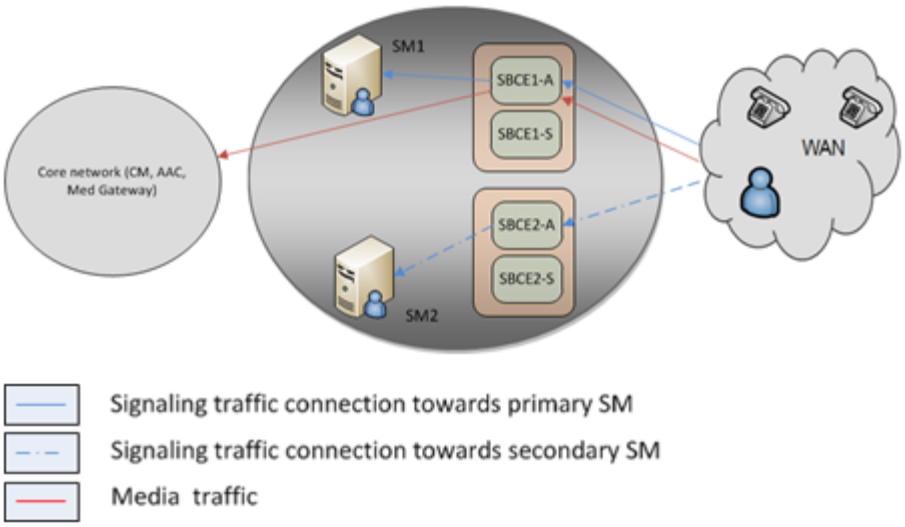
In the following diagram, SBC1 and SBC2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBC1 corresponding to the primary Session Manager, SM1. The second connection with SBC2 corresponds to the secondary Session Manager, SM2.



Geographic-redundant deployment in the HA mode

In the following diagram, SBC1 and SBC2 are two different physical devices that are deployed in an HA mode in different data centers. The endpoints have one connection with SBC1-A, that is Active SBC corresponding to the primary Session Manager, SM1. The second connection is with SBC2-A, Active SBC corresponding to the secondary Session Manager, SM2.

During an SBC1-A fail over, SBC1-S, which is the standby Avaya SBC, handles the media of the active calls. During an SBC2-A fail over, SBC2-S, which is the standby Avaya SBC, handles the media of the active calls.



Checklist for configuring Geographic-redundant deployment

Use the following checklist to configure the Geographic-redundant Avaya SBC deployment.

Note:

All Avaya SBC devices in a Geographic-redundant Avaya SBC deployment must be controlled by the same external EMS.

In the following checklist:

- The IP address on Avaya SBC towards the internet is referred to as external address.
- The IP address on Avaya SBC towards the core network or call server is referred to as internal address.
- The primary Session Manager is referred as SM1 and the secondary Session Manager is referred as SM2.

Task	Reference	Notes	✔
Configure internal and external addresses corresponding to primary and secondary Session Manager devices for the A1 and B1 interfaces.	Configuring internal and external IP addresses on page 553		
Create two external signaling interfaces.	Creating an external signaling interface toward phone network on page 490		
Create two internal signaling interfaces.	Creating an internal signaling interface toward Avaya call server on page 491		
Create two external media interfaces.	Creating an external media interface toward phone network on page 493		
Create two internal media interfaces.	Creating internal media interface toward Avaya call server on page 493		
Create a server interworking profile.	Creating a server interworking profile on page 553		
Create two server profiles, one for the primary and another for the secondary Session Manager.	Creating an Avaya call server profile on page 489		
Create PPM Mapping Profiles for each group of remote workers that has the same pair of Session Managers as primary and secondary Session Manager.	*Administering Avaya Session Border Controller*		

Table continues…

Task	Reference	Notes	✔
Configure reverse proxy service for downloading file or firmware.	Creating reverse proxy service for file or firmware download on page 501		
Create an endpoint policy.	Creating an endpoint policy on page 563		
Create two routing policies for SM1 and SM2.	Creating a routing profile to Avaya call server on page 514		
Create two subscriber endpoint flows corresponding to the primary and secondary Session Managers.	Creating a subscriber flow on page 516.	If you require RTP, use the default low or avaya-def-low-encoding (for SRTP) depending on the endpoints. **Note:** If RTP and SRTP are both used, select capability negotiation.	
Create two server flows corresponding to the primary and secondary Session Managers..	Creating a new server endpoint flow on page 167		
Create application rules.	Creating application rules on page 513	Ensure that voice sessions are set as per the user license in the application rules and enable video.	
Configure application relay for IM.	Configuring application relay for IM on page 518		
Create a reverse proxy service for PPM traffic.	Creating a reverse proxy service for PPM traffic on page 500		
Configure web collaboration.	Configuring Avaya SBC for web collaboration on page 564		
If the Session Manager Firewall is enabled, add the Avaya SBC Internal IP in the Whitelist.			
Configure Presence Services.	Configuring Presence Server on page 565		

Creating an endpoint policy

About this task

You must create an endpoint policy to support SDP Capability Negotiation and to disable Fingerprint security feature.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. To create a Media Rule for SDP capability negotiation support, do the following:
   a. In the navigation pane, click **Domain Policies** > **Media Rules**.
   b. Click **Add**.
   c. In the **Name** field, enter the name and click **Next**.
   d. Enter the appropriate details in the **Audio Encryption** and **Video Encryption** sections.
   e. In both the sections, clear the **Encrypted RTCP** check box and select the **Interworking** check box.
   f. In the Miscellaneous section, select the **Capability Negotiation** check box. Click **Next**.
   g. Disable the Media Anomaly detection. Click **Next**.
   h. Disable Media silencing and click **Next**.
   i. If required, select DSCP on Media QoS Marking.

      The recommended default values are DSCP-EF for audio and video.
3. To disable Fingerprint feature, do the following:
   a. In the navigation pane, click **Domain Policies** > **Security Rules**.
   b. Click the **Fingerprint** tab.
   c. Clear the **Fingerprinting** check box.
   d. In the left navigation pane, click **Domain Policies** > **End Point Policy Groups**.
   e. Click **Add**.
   f. In the **Group Name**, enter a name.
   g. In the **Policy Group** field, change media rule to the one created earlier and security rule to the one created earlier.
   h. Click **Finish**.
   i. Associate this endpoint policy to the subscriber flow in use and to the server flow in use.

Configuring Avaya SBC for web collaboration

Procedure

1. Create a TLS server certificate with `CN` or `SubAltName` as web collaboration server.
2. On the EMS web interface, click **SBC** and navigate to **TLS Management** > **Server profiles**, and select the TLS server certificate created in Step 1.

   For more information, see “Installing Non-Avaya certificates”.
3. Create a reverse proxy service for web collaboration traffic on a different listen IP than the reverse proxy service created for PPM services:
   a. On the EMS web interface, navigate to **DMZ Services** > **Relay** > **Reverse Proxy**.
   b. In the **Service Name** field, type a name.
   c. Select the **Enabled** check box.
   d. In the **Listen IP** field, type the Avaya SBC external IP address that should be different than the IP address used for PPM services.
   e. In the **Listen protocol** field, select `HTTPS` or `HTTP`.
   f. In the **Listen TLS profile** field, select the profile created earlier.
   g. In the **Listen Port** field, type `443`.
   h. In the **Server Protocol** field, type select `HTTPS` or `HTTP`..
   i. In the **Server TLS profile** field, select **Server TLS profile** only for HTTPS.
   j. In the **Connect IP** field, type the IP address to be used by Avaya SBC for communication towards server.
   k. Leave the **Load Balancing Algorithm** and **PPM Mapping Profile** fields blank.
   l. Select the **Allow Web sockets** check box.
   m. In the **Server Addresses** field, type the web collaboration server address and port.
4. For windows flare, additional configuration of application relay is needed on Avaya SBC:
   a. In the navigation pane, click In the navigation pane, click **DMZ Services** > **Relay**
   b. On the Relay page, click **Application Relay** > **Add**.
   c. In the **Name** field, type the name of the application relay.
   d. In the **Remote Domain** field, add the domain.
   e. In the **Remote IP/FQDN** field, type the web collaboration server IP.
   f. In the **Remote Port** field, type the port number 843.
   g. In the **Remote Transport** field, click **TCP**.
   h. In the **Published Domain** field, type the domain.
   i. In the **Listen IP** field, type the Avaya SBC external IP which is the same IP address as used in web collaboration reverse proxy configuration.

j. In the **Listen Port** field, type the port number 843.
k. In the **Connect IP** field, type the internal Avaya SBC IP address.
l. In the **Listen Transport** field, click **TCP**.
m. Click **Finish**.

Configuring Presence Server

Procedure

1. Log into the System Manager web interface.
2. Navigate to **Routing** > **Regular Expressions**.
3. Add a regular expression for `sips:list-.*@multism.com` and route that to the Presence Server.
4. Click **Commit**.

Chapter 17: Signaling manipulation

About signaling manipulation

This section provides an overview of the Avaya SIP signaling header manipulation (SigMa) feature for the Avaya SBC product. This feature provides the ability to add, change, and delete any of the headers and other information in a SIP message. You can also configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language.

- SigMa Scripting Language: The proprietary scripting language, known as “Sigma”, developed by Avaya to define any SIP message manipulation that will be performed by Avaya SBC.
- Packet Path and Hook Points: The packet path where a message transverses through the Avaya SBC stack and the hook points within the path where actions defined in a SigMa script can be acted upon.
- Avaya SBC GUI SigMa Editor: Access to the SigMa Editor for creating SIP signaling manipulation scripts that is provided through the standard Avaya SBC Configuration/ Management Graphical User Interface.

If you configure a Sigma profile in server configuration without configuring a server flow Sigma profile, the server configuration Sigma profile is always used.

If you configure a Sigma profile in server configuration and server flow, the system applies the server flow Sigma profile at the PRE-ROUTING and POST_ROUTING stages. The system applies server configuration Sigma profile at the AFTER_NETWORK stage.

You must not configure a Sigma profile in server configuration and then add new Sigma profiles created for that server configuration in server flows. In this scenario, The system does not apply server configuration Sigma profile because the server flow Sigma profile takes priority.

SigMa scripting language

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBC. Using this language, one can write a script and tie it to a given flow through the EMS GUI. The Avaya SBC appliance then interprets this script at the given hook point. For more information, see Hook points on page 573.

SigMa primer

A SigMa script consists of one or more **Within Session** statements. Each statement represents transformations to be applied to signaling messages in a given session. A Session is defined as a SIP dialog and has the same lifetime as that of a dialog. These transformations can be applied on

any given header including SDP elements. The transformations also include addition and deletion of headers, not just the ability to update the headers.

There are two types of Within session statements:

- Generic: `within session "all"`, which applies the transformation to all dialogs.
- Specific to a dialog: `within session "invite"`, which applies the transformation to the specified dialog. In this example, for the “invite” dialog.

SigMa script size limitations

SigMa scripts are limited in size to 8,000 bytes. To work within this limitation, use generic Regular Expression (regex) pattern matching whenever possible instead of plain URI matching. This can reduce the size of the script.

Session statement

This session statement has three parts: Method, Where Clause, and Code Block.

```
within session "<method>" where <condition> { <codeblock> }
```

- Method: Where you specify the SIP request method that starts the session.
- Where Clause: Where you specify the Session selection criteria on top of the Method for which the Code Block must be executed. The Session selection criteria can be augmented using AND / OR conjunctions.

  The variables that can be used within the Where Clause are given in the table: Where Clause Variables on page 567.
- Code Block: Where the operations are written and encapsulated with a set of braces {}. The operations might include further selection criteria and actual operations on headers themselves.

  Three different statements can be written within the code block:

  - act on message where <extra criteria> { <code> } – Tells the interpreter to run the given code on all messages within the SigMa session that match the criteria.
  - act on request where <extra criteria> { <code> } – Tells the SigMa interpreter to run the given code on all request messages within the session that match the criteria.
  - act on response where <extra criteria> { <code> } – Tells the interpreter to run the given code on all response messages within the session that match the criteria.

Note:

Many of the above statements can be written in a given session code block as needed for a given script.

Where clause variables

Variable	Description
%INITIAL_REQUEST	A Boolean variable (“TRUE” or “FALSE”) denoting if the code applies to the first request within a session.

Act on statements

Act On request and response statements tell the interpreter to execute the given code for all requests and responses respectively if the given criteria in the Where Clause has matched. The Where Clause specifies this criteria. Much like Where Clause of the Session, several Session Variables can be checked to specify the matching criteria. The Session Variables that are valid in this clause are given in the following table.

Session variables

Variable	Description	Applicable For
%DIRECTION	Value can be: • INBOUND: For incoming messages • OUTBOUND: For outgoing messages from SBC	act on message act on request act on response
%ENTRY_POINT	Values can be: • PRE_ROUTING • POST_ROUTING • AFTER_NETWORK The AFTER_NETWORK variable value is valid only within server configuration and not within server flow.	act on message act on request act on response
%METHOD	Values can be: • INVITE • REGISTER • ACK • PRACK • BYE • CANCEL, and • etc The method name can be any method either already part of standards or proprietary.	%METHOD
%IN_DIALOG	Values can be: TRUE or FALSE. This value indicates if the given message is a in-dialog message or a dialog creating message.	act on request
%RESP_CODE	Values can be from 100 to 600. This value represents a valid SIP response code.	act on response
%REQ_METHOD	Same as METHOD. But this value represents the method that the given response corresponds to.	act on response

Code blocks

The code blocks for the act on statements contain the code necessary to carry out actions. Four kinds of statements can go into the code block: Assignment Statement, Conditional Statement, Function Call, and Print Statement.

Code Blocks

A list of statements that can go into a code block is provided below.

- Assignment Statement. For example:
  - %var = “1”;
  - %var = HEADERS[“From”][0];
  - HEADERS[“From”][0] = “From: Alice <sip:alice@atlanta.com>;tag=1928301774”
  - HEADERS[“To”][0] = %val;
- Conditional Statement. For example:

```
if (%var = “value”) then
{
…Code…
}
else
{
…Code…
}
```

- The operators can be:
  - = for equality
  - != for negation of equality

  Either side of the operators can be a variable, a quoted string, any of the built-in arrays’ values or a regular expression get()/match() call.

  If the condition is true then the code in the then {} block is executed otherwise the else {} block will be executed.
- Function Call. Usually called on a built-in function. For example:
  - remove(): To remove a header
  - append(): To append a string to a header
  - regex_replace(): To replace text within a header using a regular expression
- Print Statement. Prints the parameters given in the log file of the process as an INFO level log. The parameters must be separated by commas and can be any of the following free string in quotes, variables, or any built-in variable.
  - print “foo”, “bar”

- print “Body(1) is – “, %BODY[1]

Built-in variables and arrays

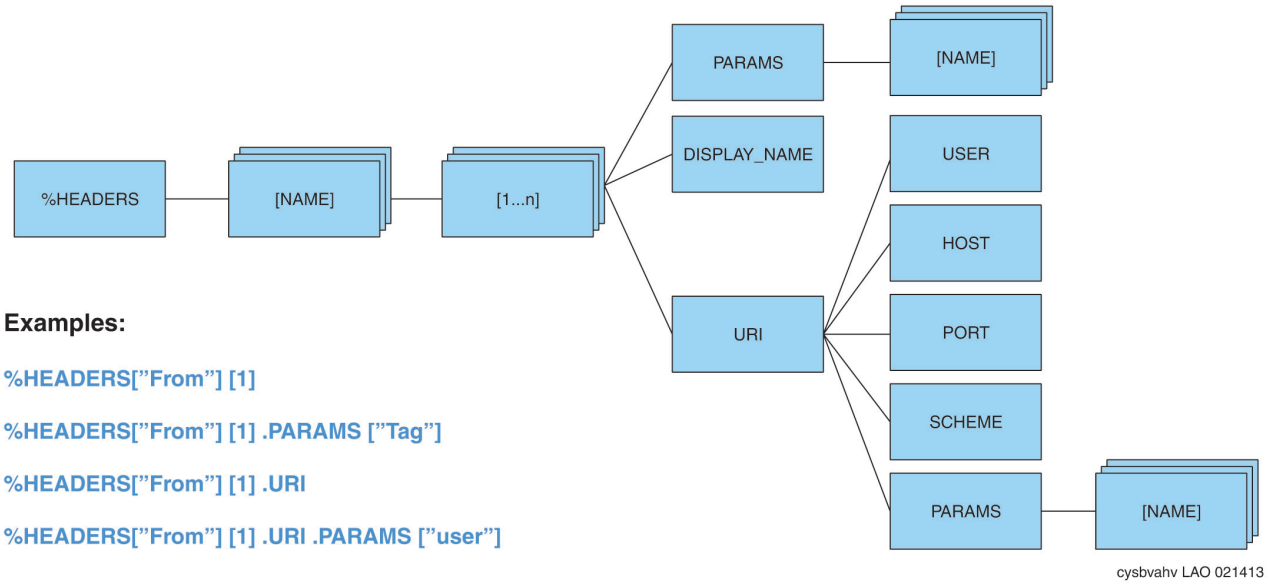
SigMa has several built-in variables and arrays, each representing a data element concerning the session and its messages. The most important ones are the %HEADERS[] and %SDP[] arrays that are used to retrieve the headers and SDP elements for a given message. The built-in variables and arrays also have a built-in hierarchy to represent the various elements within headers and SDP specification.

This section shows the lists of built-in variables and arrays, with their valid forms, descriptions, and illustrations.

HEADERS Variable

Variable	Valid Forms	Description
%HEADERS[]	%HEADERS[“Name”][n]	Used to retrieve an entire header. The second dimension ‘n’ denotes the nth instance of the header in the message. Value of n can be 1...∞
	%HEADERS[“Name”][n].PARAMS[“Name”]	Used to retrieve parameters within a header.
	%HEADERS[“Name”][n].DISPLAY_NAME	Refers to the display name within a header.
	%HEADERS[“Name”][n].URI	Refers to the URI within a header.
	%HEADERS[“Name”][n].URI.USER, %HEADERS[“Name”][n].URI.HOST, %HEADERS[“Name”][n].URI.PORT, %HEADERS[“Name”][n].URI.SCHEME, %HEADERS[“Name”][n].URI.PARAMS[“Name”]	Refers to various elements within a URI.

Example



Examples:

%HEADERS[”From”] [1]

%HEADERS[”From”] [1] .PARAMS [”Tag”]

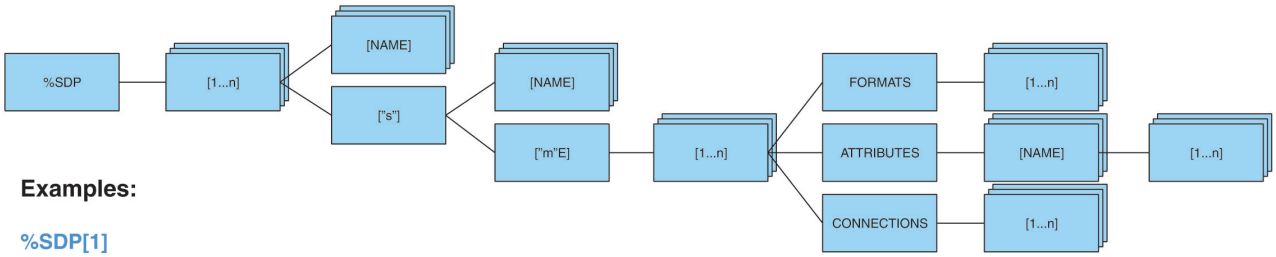
%HEADERS[”From”] [1] .URI

%HEADERS[”From”] [1] .URI .PARAMS [”user”]

SDP Variable

Variable	Valid Forms	Description
%SDP[]	%SDP[n]	Refers to an entire nth SDP specification. Index n can be 1… ∞.
	%SDP[n][“Name”]	Refers to a header within an SDP.
	%SDP[n][“Name”][“SessionHdrName”]	Refers to a session header (like media) within an SDP session.
	%SDP[m][“s”][“m”][n]	Refers to nth media specification.
	%SDP[l][“s”][“m”][n].FORMATS[n]	Refers to nth media format specification.
	%SDP[j][“s”][“m”][k].ATTRIBUTES[“Name”][n]	Refers to nth instance of “Name” attribute in the kth media specification.
	%SDP[m][“s”][“m”][n].CONNECTIONS[k]n]	Refers to the kth connection from nth media specification.

Example



Examples:

%SDP[1]

%SDP[1] [”v”]

%SDP[1] [”s”] [”t”]

%SDP[1] [”s”] [”m”] [k] . FORMATS[1]

%SDP[1] [”s”] [”m”] [k] . ATTRIBUTES{”fmtp”] [1]

cysbvasv LAO 021413

Other Variables

Variable	Valid Forms	Description
%INITIAL_REQUEST		Set to “TRUE” or “FALSE” based on the request being the first one in the session or not.
%REMOTE_IP		Set to the remote IP within the message.
%BODY	BODY[n]	Returns the n^{th} mime from the body of the message. Returns the entire body (by mime instance) of the message.

Built-in functions

Several built-in functions are available mostly for regular expression operations.

Built-In Functions table

Variable	Valid Forms	Description
exists()	exists(%HEADERS[“Header”])	Returns “TRUE” or “FALSE” based on the existence of a header, or a param in the message.
	exists(%HEADERS[“Header”].PARAMS[“Param”])	
remove()	remove(%HEADERS[“Header”])	Removes a header or a parameter from the message.
	remove(%HEADERS[“Header”].PARAMS[“Param”])	
regex_match()	%HEADERS[“Header”].regex_match(“regex”)	Returns “TRUE” or “FALSE” based on whether the regular expression found a match in the text or not.
	%HEADERS[“Header”].PARAMS[“Param”].regex_match(“regex”)	
regex_get()	%HEADERS[“Header”].regex_get(“regex”)	Returns the extracted string by the regular expression. The return value will be an empty string if no match was found.

Table continues…

Variable	Valid Forms	Description
	%HEADERS[“Header”].PARAMS[“Param”].regex_get(“regex”)	
regex_replace()	HEADERS[“Header”].regex_replace(“regex”, “string”)	Replaces a given match with the provided string within the header string or a param.
	%HEADERS[“Header”].PARAMS[“Param”].regex_replace(“regex”, “string”)	

User-defined variables

User-defined variables are simply a storage area for holding a certain string. These variables can be used within assignment and conditional statements. All user-defined variables are of string type. The variables names must all start with a ‘%’ sign and can include alpha numeric characters. The only other valid extra character allowed within the variable name is the ‘_’ (underscore).

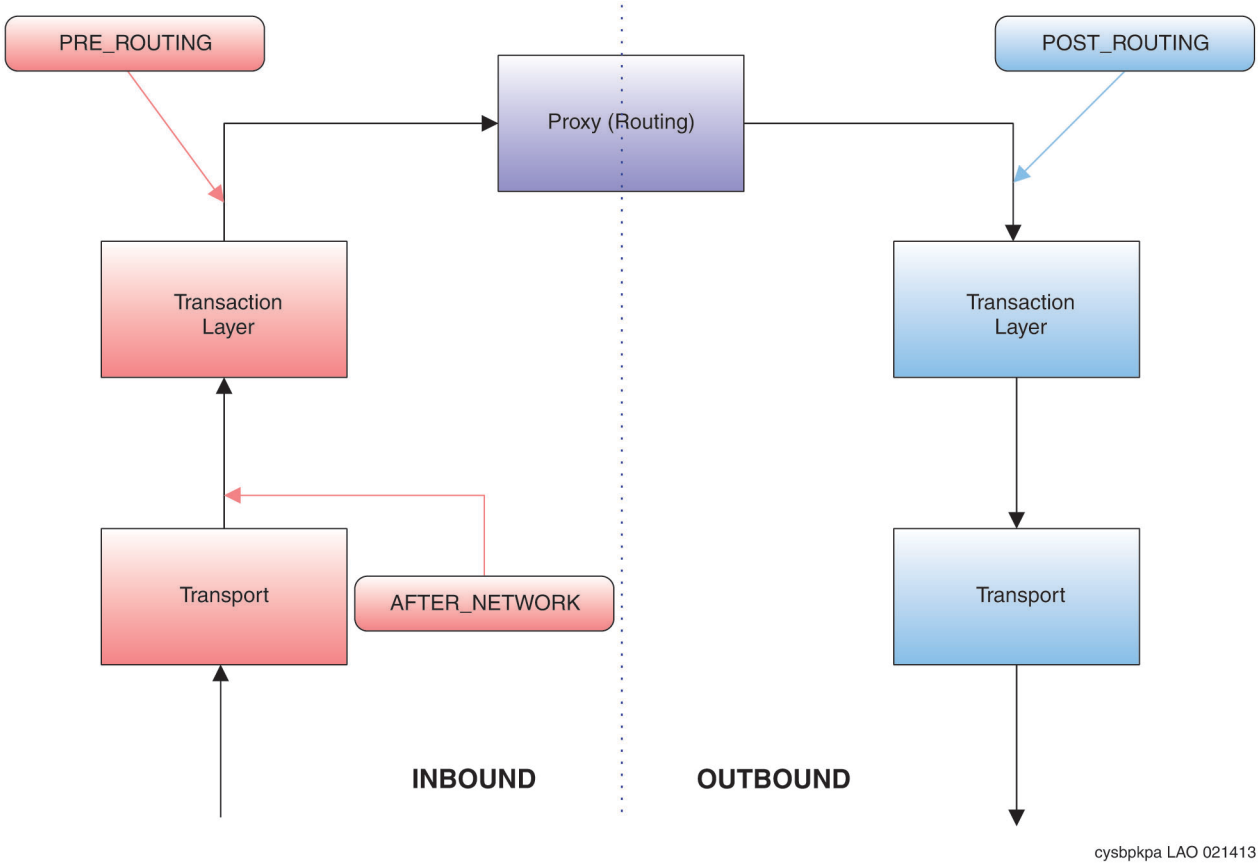
Hook points

Several hook points are illustrated in the figure and table.

Hook points are points within the Avaya SBC processing from where given actions can be executed. These hook points can be specified by using the `%ENTRY_POINT` built-in variable within the Where Clause.

Hook Point	Description
AFTER_NETWORK	A point in the packet path soon after the packet is received from the network. The AFTER_NETWORK hook point can be used to modify some parameters related to SIP dialog matching. For example, when elements send messages with dialog parameters that do not conform to RFC standards, the messages can be corrected with the AFTER_NETWORK hook. Any manipulation required for Avaya SBC before matching the dialog is applied at this hook. This hook takes the configuration of the source of the message. You cannot use the AFTER_NETWORK hook point in the server flow.
PRE_ROUTING	After the transaction layer, before target destination for the packet is determined. The PRE-ROUTING hook point can be used to influence the routing decisions and deliver the messages to different elements with required message modifications. This hook takes the configuration of the source of the message.
POST_ROUTING	After target destination is determined, before the transaction layer. The POST-ROUTING hook point can be used to modify the message based on the destination element requirements. This hook takes the configuration of the destination of the message.

Example



SigMa Scripting examples

The SigMa scripting language is best demonstrated using some examples. This table provides some use cases and how they can be represented in a SigMa script.

Description	Scripting Example

Reverting From and To tags in all responses to REGISTER method.	`within session "REGISTER"`
	`{`
	`act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"`
	`    {`
	`        %from_tag = %HEADERS["From"][1].PARAMS["Tag"];`
	`        %HEADERS["From"][1].PARAMS["Tag"] = %HEADERS["To"][1].PARAMS["Tag"];`
	`        %HEADERS["To"][1].PARAMS["Tag"] = %from_tag;`
	`    }`
	`}`

Table continues…

Description	Scripting Example

Updating the p-asserted-identity field with the value of From header if P-Asserted-Identity field value is anonymous	`within session "ALL"`
	`{`
	`act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        if (%HEADERS["P-Asserted-Identity"][1].URI.USER = "anonymous") then`
	`        {`
	`            %aor = %HEADERS["From"][1].URI;`
	`            %HEADERS["P-Asserted-Identity"][1] = %aor;`
	`        }`
	`    }`
	`}`

Adding a media attribute in SDP	`within session "ALL"`
	`{`
	`    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        %SDP[1]["s"]["m"][1].ATTRIBUTES["fmtp"] = "101 0-16";`
	`    }`
	`}`

Adding a header	`within session "ALL"`
	`{`
	`    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        %HEADERS["SLiC-Version"][1] = "3.2.2";`
	`    }`
	`}`

Trunking: Removing phone_context param from Request Uri, To and From headers	`within session "ALL"`
	`{`
	`act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        remove(%HEADERS["Request_Line"][1].PARAMS["phone-context"]);`
	`        remove(%HEADERS["From"][1].PARAMS["phone-context"]);`
	`        remove(%HEADERS["To"][1].PARAMS["phone-context"]);`
	`    }`
	`}`

Trunking: For all new calls, add diversion header if it does not exist	`within session "INVITE"`
	`{`
	`    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`    if (%INITIAL_REQUEST = "TRUE") then`
	`        {`
	`            %HEADERS["Diversion"][1] = "sip:333444555@";`
	`            append(%HEADERS["Diversion"][1], %REMOTE_IP);`
	`        }`
	`    }`
	`}`

Table continues…

Description	Scripting Example

Learn P-Asserted-Identity from INVITE and use this value to replace From URI in every Request	`within session "INVITE"`
	`{`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        If (%INITIAL_REQUEST = "TRUE") then`
	`        {`
	`            %passert_val = %HEADERS["P-Asserted-Identity"][1].URI;`
	`        }`
	`        else`
	`        {`
	`            %HEADERS["From"][1].URI = %passert_val;`
	`        }`
	`    }`
	`}`

Changing Max-Forwards from 0 to 45 from carriers	`within session "INVITE"`
	`{`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        if (exists(%HEADERS["Max-Forwards"][1])) then`
	`        {`
	`        %HEADERS["Max-Forwards"][1] = "45";`
	`        }`
	`    }`
	`}`

Changing the CLID to a specific number 3134657809 when a 1800-xxx-xxxx or 1877-xxx-xxxx number is dialed
 	
This script changes the from number without changing the display name.
	`within session "INVITE"`
	`{`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        if (%HEADERS["To"][1].URI.USER.regex_match("1800(.*)")) then`
	`        {`
	`        %HEADERS["From"][1].DISPLAY_NAME = "3134657809";`
	`        }`
	`        if (%HEADERS["To"][1].URI.USER.regex_match("1877(.*)")) then`
	`        {`
	`        %HEADERS["From"][1].DISPLAY_NAME = "3134657809";`
	`        }`
	`    }`
	`}`

Removing display name	`within session "INVITE"`
	`{`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`        remove(%HEADERS["From"][1].DISPLAY_NAME);`
	`        remove(%HEADERS["Contact"][1].DISPLAY_NAME);`
	`        remove(%HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME);`
	`    }`
	`}`

Table continues…

Description	Scripting Example

Changing Inactive to RecvOnly	`within session "ALL"`
	`{`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="AFTER_NETWORK"`
	`    {`
	`        /*The "a=" field contains attributes to provide more information on the codecs. Change from inactive to recvonly in all Response Msg*/`
	`%BODY[1].regex_replace("a=inactive\r\n","a=recvonly\r\n");`
	`        //add(%BODY[1]["a=recvonly\r\n"]);`
	`    }`
	`}`

Removing duplicate in ACK	`within session "INVITE"`
	`{`
	`/*Look only for ACK messages from SM and process the message immediately after receiving the message. */`
	`act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="ACK"`
	`    {`
	`        /*If in the request line of ACK, a duplicate of transport=tcp;transport=tcp occurs, remove one of the duplicates. */`
	`        if(%HEADERS["Request_Line"][1].regex_match("transport=tcp;transport=tcp")) then`
	`        {`
	`        %HEADERS["Request_Line"][1].regex_replace("transport=tcp;transport=tcp", "transport=tcp");`
	`        }`
	`    }`
	`}`

Checking the user portion of the URI for a specific prefix 50833 and replacing the prefix with an empty string when a match is found	`within session "INVITE"`
	`{`
	`/*Look for INVITE messages only.*/`
	`act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`
	`    {`
	`    /* The User portion of the URI in the To header is checked to see if it starts with the prefix 50833.  If it does, then it is replaced with an empty string. If URI.USER does not match the regex, then the action is ignored and the message is left intact.*/`
	`        %HEADERS["To"][1].URI.USER.regex_replace("^.....","");`
	`        %HEADERS["Request_Line"][1].URI.USER.regex_replace("^.....","");`
	`    }`
	`}`

SigMa Scripting Tutorial

The following are some additional examples of test cases and use cases with their associated SigMa scripts and explanations of what the scripts do.

Any limitations of each script are also included.

Test Case 1: Manipulation of P-Asserted-Identity Header

Use case

The P-Asserted-Identity header field can be used to present the identity of the originator of a request within a trusted network. Since the From header field is populated by the originating User-Agent, the From header field might not contain the actual identity. The P-Asserted-Identity header is established by means of authentication between the originating User-Agent and its outgoing proxy. The outgoing proxy then adds a P-Asserted-Identity header field to assert the identity of the originator to other proxies.

1. If the P-Asserted-Identity header field is not present, a proxy might add one containing at most one SIP or SIPS URI, and at most one telephone URL.
2. If the proxy received the message from an element that it does NOT trust and if there is a P-Asserted-Identity header present, the proxy MUST replace the SIP URI or remove it.

Script

```
within session "ALL"  //Looks into all the messages
{
    /* Message should be a request "act on request" and the messages coming towards
the SBCE should be considered, i.e. the destination of the message should be SBCE
"%DIRECTION="INBOUND". The actions are invoked as soon as the message comes from the
wire(%ENTRY_POINT="AFTER_NETWORK") */
         act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
            {
            /*Checks if the first P-Asserted-Identity header is present/exists in
            the message. Each header is represented as %HEADERS[“<Header-name>”]
            [<Header position>].For headers such as From and Contact, the Header
            Position is always 1.For headers like Via and P-Asserted-Identity,
            the positions can range from 1 to n*/

                    if(exists(%HEADERS["P-Asserted-Identity"][1]))then
                    {
                        remove(%HEADERS["P-Asserted-Identity"][1]); //Remove the header
                    }
                /*If the P-Asserted-Identity header is not found in the message*/
                    else
                    {
                                    /* Add a SIP and a telephone URI.*/
                            %HEADERS["P-Asserted-Identity"][1] =
"12345<sip:12345@192.168.150.150>";
                            %HEADERS["P-Asserted-Identity"][2] = "tel:+14085264000";
                    }
                    }
            }
```

Description

The script looks into each message that comes in since the script acts on all sessions and checks if:

1. The message is a request message.
2. The message is coming to Avaya SBC.

When the above conditions are fulfilled and when the message comes from the wire, the basic sanity checks and DoS checks are performed on the message. The script checks if a P-Asserted-Identity header exists. If P-Asserted-Identity header exists, the script removes the header, else the script adds the header.

Limitations

To remove all the P-Asserted-Identity headers, you must know the maximum number of headers that must be present in the messages. You do not need to know the exact number of headers that come in because if you try to perform an operation on a header that does not exist, the operation is ignored.

Note:

If `%HEADERS["<Header-Name>"][<Header Position>]` is already present, then the operation `%HEADERS["<Header-Name>"][<Header Position>] = <VAL>` will modify the header.

If the header is not present in the message, `%HEADERS["<Header-Name>"][<Header Position>] = <VAL>` adds the header to the message.

Test Case 2: Adding a Media Attribute in SDP

Use case

You must add or modify the SDP attributes or the connection parameters for interoperability.

Script

```
/*Looks into messages in the INVITE session only (It includes all messages in the
INVITE dialog)

within session "INVITE" {
*/act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {

            /*The "m=" field in SDP contains information about the type of media
session.    It includes the format-list parameter for specifying the codecs. Assuming
that the message comes in with 2 codecs, we add a third codec as 101 */

            %SDP[1]["s"]["m"][1].FORMATS[3]="101";

            /*The "a=" field contains attributes to provide more information on the
codecs.            Assuming that the message does not have any fmtp attribute,we add
the first one as 101 0-16*/           %SDP[1]["s"]["m"][1].ATTRIBUTES["fmtp"][1]="101
0-16";
    }

}
```

Description

The script processes all the messages of the INVITE session. A session is defined as a SIP dialog and has the same lifetime as that of a dialog. A new format-type and an attribute is added corresponding to fmtp.

Limitations

You must know the number of codecs and the number of formats in format list parameter and attributes. Else, you might replace an existing format type.

Test Case 3: Changing Calling Party Presentation to Restricted

Use Case

Required to change Calling Party Presentation to Restricted.

Script

```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {

            /*Checks if the privacy header value matches with the regular expression
            given(“none”). If it matches, then the privacy header value is changed to
“id”*/

            if(%HEADERS["Privacy"][1] = "none")then

            {
            %HEADERS["Privacy"][1] = "id";
            }
    }
}
```

Description

The script processes all the messages of a session. A session is defined as a SIP dialog and has the same lifetime as that of a dialog consisting of Request and Responses. The script changes the Privacy header if the header exists in the message, so that the calling party is shown as restricted to the called party.

Limitations

None.

Test Case 4: Replace From Header For a Set of Users

Use case

In an organization, several phones used by the employees and each of them might have a unique From URI associated with phones. The organization might require that all outgoing calls have the same From URI. For this purpose, the following script can be used.

Script

```
within session "INVITE"{
/* For users whose Uri begins with the prefix 10, when the message comes towards the
SBCE, the Uri is changed to “9000”<sip:9000@domain>. So, when the receiver answers the
call, the From is 9000. */
        act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
        {
                /*A Uri can be
represented as “<diplay_name>”<scheme>:<user>@<host>:<port>",
eg: ”shalini”<sip:shalini@Avaya.com:5060>. "URI.USER" extracts the user portion of the
URI.  "regex_match"tries to match the string against the regular expression. It is of
the form <string>.regex_match(“<regular expression>”).In this example,it is checked if
the "USER" portion in the “From” Header starts with the prefix 10 */

                if(%HEADERS["From"][1].URI.USER.regex_match("^10"))then
                {
                /*The uri and display name of the actual user is stored in temporary
variables*/
                %OriginalFromUri = %HEADERS["From"][1].URI.USER;
```

```
                %OriginalFromName = %HEADERS["From"][1].DISPLAY_NAME;

                /* The display name and uri is changed to the new values.*/
                %HEADERS["From"][1].DISPLAY_NAME = "9000";
                %HEADERS["From"][1].URI.USER = "9000";
                }
        }

/* When the response comes back, we need to change the URI USER and DISPLAY NAME to the
actual user. So,before the message is sent out to the wire from the SBC, it is checked
if the URI.USER is 9000.  If yes, then change it back to the original user's details. */
/* Message should be a response "act on response" and the messages going out from the
SBC should be considered (\"%DIRECTION="INBOUND"). The actions are invoked before the
message goes out (%ENTRY_POINT="BEFORE_NETWORK") */

        act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="BEFORE_NETWORK"
        {
                /*Check if the user portion of the From URI is 9000*/
                if(%HEADERS["From"][1].URI.USER = "9000")then
        {
        /*Change the URI.USER and display name to the original user's details, which
are saved in the temporary variables*/
        %HEADERS["From"][1].URI.USER = %OriginalFromUri;
        %HEADERS["From"][1].DISPLAY_NAME = %OriginalFromName;
        }
    }
}
```

Description

The previous example shows how to modify a message (request) on its way out and also modify a message (response) when it comes in.

Limitations

The example illustrates the use of `regex_match`. The regular expression provided within the parentheses, that is, `regex_match(<regular expression>)`, can be any valid Perl regular expression. However, the symbol can not be used in the regular expression.

Test Case 5: Editing the "Allow" Header

Use case

The Allow header indicates the methods supported by the user agent. For example, Allow: INVITE, ACK, BYE, INFO, OPTIONS, CANCEL. The OPTIONS method is used to query a user agent or server about its capabilities and discover its current availability. The response to the request lists the capabilities of the user agent or server. This listing might not be desired probably due to security reasons. In this case, the SBC can strip the OPTIONS method from the Allow header before sending out the message.

Script

```
within session "INVITE"
{
    /*Look for INVITE messages only.  This is specified with the extra condition
%METHOD="INVITE" in the "where" clause*/

act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
%METHOD="INVITE"
{

/*There could be i.multiple methods in Allow or ii. OPTIONS could be the only method in
Allow.  If there are multiple methods in Allow, OPTIONS could be i. in the beginning 2.
```

```
in the middle/the end */

/*If OPTIONS is in the middle/end in Allow, it would be of the form
Allow:<Methods>,OPTIONS,<More methods> or Allow:<Methods>,OPTIONS. So, we try to match
"Allow"  against the regex ,OPTIONS */
                if(%HEADERS["Allow"][1].regex_match(", OPTIONS"))then
                {
                /*<string1>regex_replace("<regex1>","<string2>") looks for
regex1(regular expression)  in string1 and replaces it with string2(plain string). Here
we replace ,OPTIONS with  an empty string, indirectly removing ,OPTIONS*/
                        %HEADERS["Allow"][1].regex_replace(", OPTIONS","");
                    }
                                else
                                {
                                /*Nested if-else*/
                                /*If OPTIONS is in the beginning in Allow, it would be
of the form
                                Allow: OPTIONS,<More methods>. So, we try to match
"Allow" against the regex OPTIONS, */
                                        if(%HEADERS["Allow"][1].regex_match("
OPTIONS,"))then
                                        {
                                /* We replace OPTIONS, with an empty string, indirectly
removing OPTIONS,*/
                                                %HEADERS["Allow"][1].regex_replace("
OPTIONS,", "");
                                        }
                                        else
                                        {
                                /*If OPTIONS is the only method in Allow, it would be
of the form
Allow: OPTIONS. So, we try to match "Allow" against the regex OPTIONS */
                                                 if(%HEADERS["Allow"]
[1].regex_match(" OPTIONS"))then
                                                {
                                                /*Since OPTIONS is the only method
in Allow, we remove the entire header*/
                                                /*remove(%HEADERS["<Header-name>"]
[<Posn>] removes the header specified in
                                                <Header-name> in Position
<Posn>.Here we remove the Allow header*/
                                                            remove(%HEADERS["Allow"]
[1]);
                                                }
                                        }
                                }
                }
}
```

Description

This script is useful while operating on headers such as Allow, Supported, Content-Type, whose values can not be extracted individually as compared to headers like From, To, or Contact.

Limitations

The regular expression in `regex_replace` can not include the $ symbol.

Test Case 6: Prefix Stripping

Use case

Phone numbers might contain a prefix. Sometimes, this prefix needs to be stripped off before the call is routed. This prefix is useful in scenarios where a call transfer is made and the number to which the call must be transferred is entered with a prefix.

Script

```
within session "INVITE"
{
/*Look for REFER messages only.  This is specified with the extra condition
%METHOD="REFER" in the "where" clause*/
             act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
and %METHOD="REFER"
            {
        /* The User portion of the URI in the "Refer-To"  header is checked to see if
it starts with the prefix 011.  If it does, then it is replaced with an empty string.
If URI.USER does not match the regex, then the action is ignored and the message is
left intact.*/
                      %HEADERS["Refer-To"][1].URI.USER.regex_replace("^011","");
            }
}
```

Description

Messages that have the Refer-To method are checked for a prefix in the URI. If so, the prefix is stripped before sending the message out.

Limitations

The regular expression in `regex_replace` can not have the $ symbol.

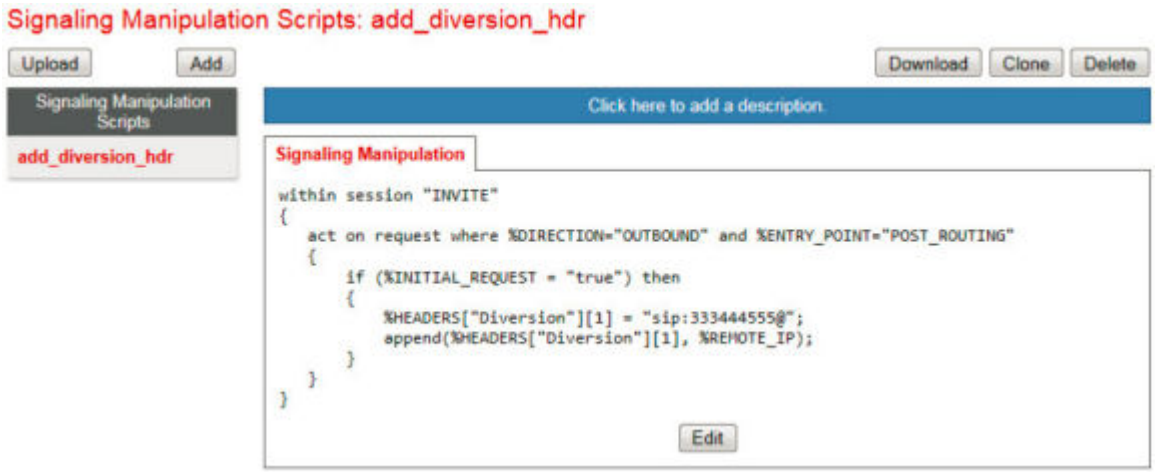
Signaling Manipulation Scripts field descriptions

The Signaling Manipulation scripts pane lists all scripts that are stored on the device. Clicking on a script name in the list displays the script in the SigMa Editing window to the right, where the script can be modified.

Button	Description
Edit	To make modifications to the existing script.
Save	To save the changes to the script after making modifications to the script. **Note:** After **Save Button** is clicked, the script will be transparently submitted to the backend and validated before it is saved to the disk. If the script fails validation, error messages are displayed to the user to correct any syntax errors in the script.
Add	To create a new script by opening up a blank SigMa Editing window to the right.

Table continues…

Button	Description
Upload	To upload the selected script to a remote location.
Download	To download a script to the device from a remote location.
Clone	To copy the selected script to a new script name to modify the newly named script for a different functionality.
Delete	To delete the selected script.



Sigma Design Overview

A Sigma Process Flowchart is provided below.

Note:

After you create a SigMa script, you must specify the script in a Server Configuration before you can run the script.

Specifying a SigMa script in a server configuration

About this task

Use the following sample procedure to specify a SigMa script in a server configuration.

Note:

Ensure that no server configurations have been created yet. If you are specifying a SigMa script in an existing server configuration, proceed to Step 9 of this procedure.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.
4. In the Server Configuration screen, click **Add**.
5. In the first Add Server Configuration Profile screen, type a name in the **Profile Name** field, and click **Next**.
6. In the second Edit SIP Server Profile screen, type the appropriate information, and then select **Next**.
7. In the third Edit SIP Server Profile — Authentication screen, type the appropriate information, and then select **Next**.
8. In the fourth Edit SIP Server Profile — Heartbeat screen, type the appropriate information, and then select **Next**.
9. In the fourth Edit SIP Server Profile — Registration screen, type the appropriate information, and then select **Next**.
10. In the Edit SIP Server Profile — Advanced screen, type the appropriate information, and then select **Finish**.

    The system saves the configuration, and the updated Server Configuration screen is refreshed showing the newly-added profile.
11. Select the profile name and then click the **Advanced** tab button.
12. In the SIP Servers Advanced Tab screen, select the **Edit** button.
13. In the Edit SIP Servers Profile Advanced screen, select the name of the SigMa script that you want to specify from the drop-down list in the **Signaling Manipulation Script** field.
14. Click **Finish**.

Chapter 18: Remote access

Secure Access Link

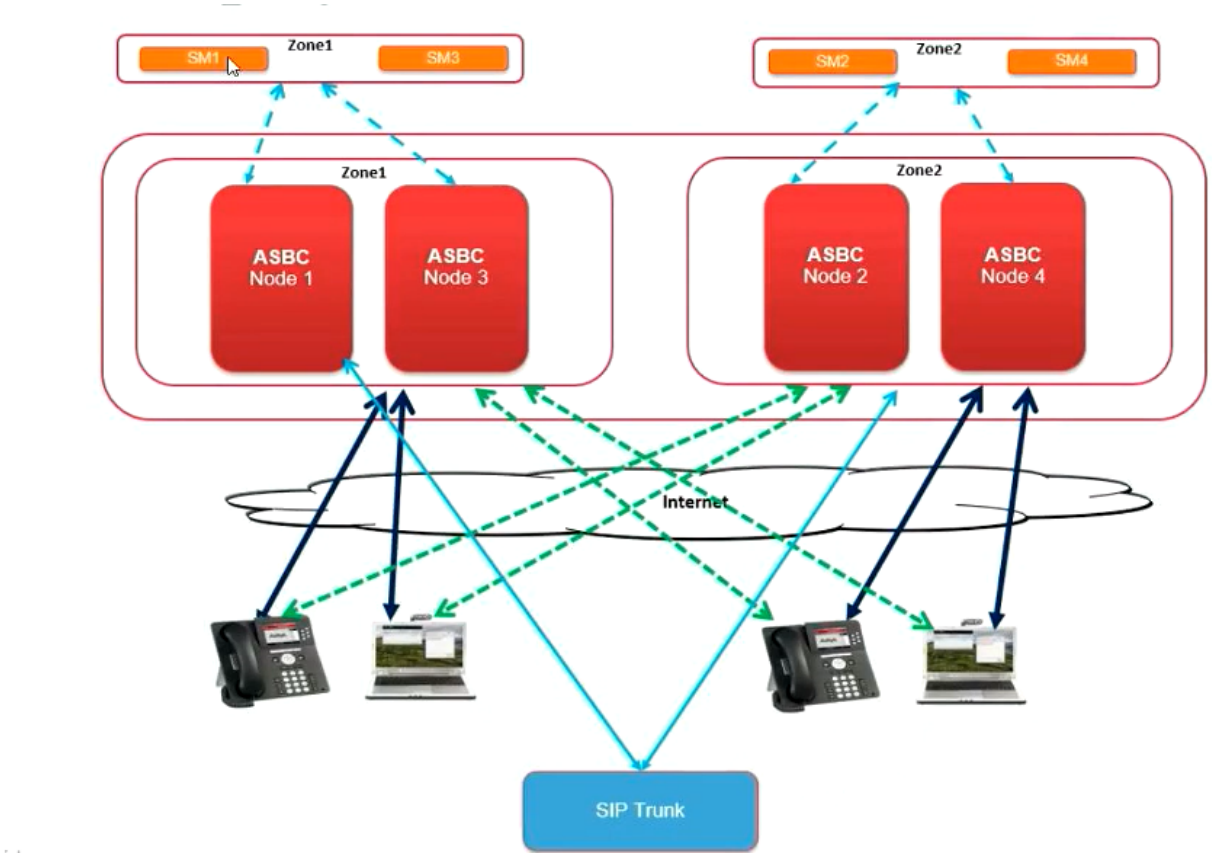
Use Secure Access Link (SAL) for remote access to Avaya SBC systems in non-IP Office environments. Register Avaya SBC for remote access with the customer SAL. For information about configuring SAL, see *Implementing Secure Access Link Gateway*.

Chapter 19: Zero Down Time support

Zero Down Time support for AEC deployments

For Avaya Enterprise Cloud (AEC) deployments, Avaya SBC supports upgrades without any maintenance window and with minimal service disruption.

The following shows a typical setup of AEC deployment with Zero Down Time support:



The AEC deployment has two zones. Each zone has single or multiple Avaya SBCs based on the customer requirement.

Users are distributed across zones. For example, if a customer deployment has 1000 users, 500 users are registered in zone 1 as primary and zone 2 as secondary. And, the other 500 users are registered in zone 2 as primary and zone 1 as secondary.

This process provides seamless upgrade for both remote worker and SIP trunk calls.

You can upgrade a single Avaya SBC at a time or all Avaya SBCs in a zone at once. However, it is recommended to upgrade a single Avaya SBC at a time. Other Avaya SBCs in the same zone continue to function.

Users with no call activity are drained immediately from the current Avaya SBC that is being upgraded to the Avaya SBC in the other zone. Active call users are drained once they complete the call. Users will be able to perform all mid-call operations across the upgrade process.

SIP trunks distribute incoming calls using the DNS-SRV method. DNS SRV records are manipulated by Cloud Orchestrator to redirect SIP trunk traffic from the Avaya SBC that is being upgraded to Avaya SBC in the other zone. New calls are redirected to the other zone whereas active calls continue on the same zone till complete.

Cloud Orchestrator is used for scheduling upgrades for AEC deployments. Cloud Orchestrator monitors the active call count and starts the upgrade process when the active call count becomes zero.

For more information, refer to AEC Application Notes.

Avaya SBC supports registrations of Third-party endpoints such as FlyingVoice endpoints. It also supports Zero Down Time workflows.

Chapter 20: Video devices interoperability

Binary Floor Control Protocol

To provide continuous presence during video conferencing, applications use the switched video or the mixed and switched video technique.

Avaya Aura® Conferencing uses the switched video technique to provide continuous presence. Video streams are relayed to all participants so that each participant receives the corresponding multiple video streams from the far ends. Avaya Meetings Server uses the mixed video technique where a single video media stream is mixed for all participating users.

Through the video channel, one of the continuous presence streams provides information about the presentation apart from the main video. The presentation channel is through the web and not through a video channel. Switched video streams use only one presentation video channel for multiple main video media streams for each participant. Mixed video devices use one video media stream for presentation. The main video media stream displays participants in one frame. The floor control of this presentation video channel is by Binary Floor Control Protocol (BFCP) messages.

BFCP messages control how multiple video streams access and use the shared video channel.

Configuring Binary Floor Control Protocol

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. On the dashboard, click **Domain Policies** > **Media Rules**.
4. On the Media Rules page, click the **Advanced** tab.
5. Select the **BFCP Enabled** check box.

   The media rule included in the endpoint policy group must be applied to the subscriber side and server side.
6. In the navigation pane, click **Network & Flows** > **Media Interface**.
7. On the Media Interface page, click **Add**.

The EMS server displays the Add Media Interface dialog box.

8. In the **Name** field, type the name of the media interface.

   The **IP Address** field is pre-populated with the Media Interface IP address.

9. In the **Port Range** field, enter the TCP port range.

   The default range is 35000 to 40000.

SRTP overview

Avaya SBC supports encrypted audio and multiple video media such as main video, video presentation, and Far End Camera Control (FECC) based on SDP capability negotiation.

If the far-end entity does not support SRTP encryption, Avaya SBC converts one leg of the call as RTP and the other leg as SRTP by using the SDP negotiation. The conversion between the originating and terminating legs depends on the cipher policy administered on Avaya SBC.

Avaya SBC does not use Master Key Identifier (MKI) and encrypted RTCP for Avaya Meetings Server interoperability. Avaya SBC negotiates the SDP session by using non-encrypted RTCP.

Note:

Avaya SBC supports SRTP calls over SIP, but Avaya Aura® supports SRTP calls only when the call uses the TLS protocol.

Considerations for SRTP after failover

- Due to the bandwidth limitation or change in the call toplogy, such as a media server not supporting SRTP and application of music-on-hold, fallback from SRTP to RTP call is supported.
- Upgrade from RTP to SRTP is allowed.
- Any conversion from RTP to SRTP between incoming and outgoing legs is applicable after failover.
- Media using SRTP flows after failover.
- Modification of keys using REINVITE is applicable after failover.
- Fallback from RTP to SRTP is applicable after failover.

Forward Error Correction

Video over IP requires high bandwidth. Transmission of video data over unreliable communication channels might result in packet loss and error. Forward Error Correction (FEC) is a mechanism to control packet loss and errors in data transmission over the IP network. The sender encodes the

messages in a redundant way by using the error-correcting code. The redundancy feature enables the receiver to detect errors and correct the errors without retransmission. This mechanism is useful when communication is one way and has multiple receivers.

The FEC mechanism uses the FEC schemes defined in RFC 5445, the FEC building block defined in RFC 5052, and the SDP signaling defined in RFC 5109. Avaya Workplace Client uses the proprietary SDP signaling and FEC building blocks and schemes, which are not compatible with the IETF standard.

FEC detects errors and protects the principal video but does not protect the data for audio channels. FEC is also applicable for H264/SVC video codecs.

Far End Camera Control

Avaya SBC supports FECC Offer and Answer in SDP. Avaya SBC checks if the media application line uses the H.224 codec. Any other media application line without an H.224 codec type is ignored.

Avaya SBC does not negotiate Offer and Answer SDP for the Far End Camera Control (FECC) media application line. Offer and Answer exchange and negotiation is done end-to-end between the sender and receiver. Avaya SBC does not support mixed encryption because FECC is tied to Media Rules. Therefore, FECC is encrypted if main video is encrypted. Similarly, FECC is on RTP if the main video is on RTP. If FECC is not negotiated in Offer and Answer end-to-end, the principal video channel works without FECC.

Avaya SBC applies encryption according to SDP Capability Negotiation and SDES by Avaya SBC policy.

Configuring Far End Camera Control

About this task

When you enable the FECC feature, Avaya SBC supports SRTP policy settings for the FECC media application line.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation, click **Domain Policies** > **Media Rules**.
4. On the Media Rules page, select a media rule, and click the **Advanced** tab.
5. Select the **FECC Enabled** checkbox.

Chapter 21: WebRTC-enabled call processing

WebRTC-enabled call handling

Avaya SBC supports incoming calls from WebRTC-enabled web browsers to an internal Avaya Aura® network with SIP at the core. For example, a consumer can call an Avaya Aura® network by using a WebRTC-enabled browser from an external network. This WebRTC call is possible if the organization discloses the organization website to real-time multimedia calls and enables the browser with APIs for real-time multimedia communication. The signaling and media traverse the border edge of the enterprise network that contains the firewall and Avaya SBC in DMZ. In this scenario, Avaya SBC, Avaya Breeze® platform, and Avaya Aura® Media Server together function as the WebRTC-SIP gateway. The signaling and media must traverse the border edge of the enterprise network. Avaya SBC relays HTTP signaling by using the Reverse Proxy feature and the media relay by using TURN Server relay functionality. Additionally, for a WebRTC call, STUN binding, STUN reflexive address discovery, and ICE connectivity checks are required. All these aspects are implemented within the TURN/STUN server functionality built into Avaya SBC.

A WebRTC-enabled browser supports symmetric NAT and multiple IP addresses.

Avaya SBC supports TURN using SEND or DATA indication and TURN signaling on TCP, TLS and UDP.

For information about WebRTC performance and capacity, see *Avaya WebRTC Connect Reference*.

WebRTC considerations

- WebRTC to SIP multimedia calls is not supported.
- WebRTC solution does not provide HA survivability, therefore, the existing calls do not work after the primary Avaya SBC becomes non-functional. A solution is configured with High Availability (HA) functionality so that new WebRTC calls can be started from the HA pair if the active or primary Avaya SBC is nonfunctional.
- Avaya does not support incoming calls from an external network to an internal network between WebRTC-enabled browsers.
- WebRTC solution supports only audio with G711 codec.

- Select the **Media Learning** check box in TURN/STUN Profiles only for deployments with TURN on AMS or MCU. Clear the **Media Learning** check box for TURN/STUN profile deployment on browser.

Turntop

The **turntop** command is used to learn statistics on a WebRTC call.

Description

Use this command to get the following details:

- total turn allocation success
- total turn allocation failure
- total channel bind success
- total channel bind failure
- total stun binding success
- total stun binding failure

Related links

Running the turntop command on page 593

Running the turntop command

Procedure

1. Log in to the Avaya SBC server.
2. Type `sudo su`.

   The system prompts for a password.
3. At the **password** prompt, type the ipcs password.
4. At the root prompt, type `clipcs` and press `Enter`.
5. Type `select ss` and press `Enter`.
6. Type `turntop` and press `Enter`.

Related links

Turntop on page 593

Configuring the TURN/STUN profile for WebRTC calls in Avaya SBC

Before you begin

In the navigation pane, click **Device Management** and verify the following details:

- The Avaya SBC name and the management IP address.
- The Element Management System (EMS) name and the management IP address.
- The **Status** column of Avaya SBC EMS displaying `Commissioned`.

About this task

Use this procedure to verify that the Avaya SBC configuration settings match the settings in Avaya Breeze® platform and Avaya Media Server.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service**.

   The Application pane lists the registered Avaya SBC security devices for which the new TURN/STUN profile is applied. In the content area, the system displays an ordered list for TURN/STUN Profiles and TURN Relay configuration, for the selected Avaya SBC security devices.
4. From the application pane, select the Avaya SBC Device for which the new TURN/STUN profile will be created.

   The system displays the TURN/STUN Service screen showing the TURN/STUN profiles that are currently defined for that Avaya SBC device.
5. Click the **TURN/STUN Profiles** tab.
6. Click **Add**.

   The system displays the Add TURN STUN Profile window.
7. Enter the requested information in the appropriate fields, and click **Finish** to save and exit.

   Note:

   You must create and add the TURN Relay associated with that TURN/STUN profile, to save any change in existing TURN/STUN profile.

Related links

Add TURN STUN Profile field descriptions on page 595

Add TURN STUN Profile field descriptions

Name	Description
Profile Name	Name of TURN/STUN profile.
UDP Listen Port	Listen port number for UDP.
TCP/TLS Listen Port	Listen port number for TCP/TLS. **Note:** If the type is selected as TLS in load monitoring then you must change the **Transport** protocol to TCP before configuring TURN STUN relay to avoid port conflicts.
TLS Server Profile	TLS server profile used for TCP/TLS listen port. **Note:** Ensure that atleast one TLS server profile is configured in **TLS Management** > **Server Profiles** . You can configure TURN/STUN profile without any TLS Server profile, by removing the entry from **TCP/TLS Listen Port** field.
Media Relay Port Range	Port range for the media relay. This range must not overlap with the port ranges used by Avaya SBC for other protocols such as SIP. Avaya recommends that you type the port range as 50000 to 55000. If you use a different port range, verify that there is no clash between other media port ranges for SIP calls.
Authentication	Option to enable authentication for TURN/STUN profile.
Client Authentication	Option to enable token based authentication for client when browser is enabled with TURN.
Server Authentication	Option to enable the use of static username and password for server authentication.
UserName	User name for server authentication.
Password	Password for server authentication.
Confirm Password	Password confirmation for server authentication.
Realm	Realm used for TURN server authentication.
Fingerprint	Option to enable fingerprint.
UDP Relay	Option to enable UDP relay.
TCP Relay	Option to enable TCP relay. **Note:** If you change the transport protocol from TCP to UDP or from UDP to TCP, the WebRTC service is affected. For any change in the transport protocol, you must restart the application.

Table continues…

Name	Description
DTLS	Option to enable DTLS. This field is unavailable by default.
Media Learning	Option to enable the learning of remote media source on TURN/STUN profile
Alternate Server 1 to 3	IP address of an alternate server. Configured **Listen IP** in **TURN Relay** has a load factor threshold. When the load factor threshold is exceeded, the load is redirected to an alternate TURN server address as configured in **Alternate Server 1 to 3**.

Related links

Configuring the TURN/STUN profile for WebRTC calls in Avaya SBC on page 594

Configuring the TURN relay service for WebRTC calls in Avaya SBC

Before you begin

In the navigation pane, click **Device Management** and verify that the Device Management page displays the following details:

- The Avaya SBC name and the management IP address
- The Element Management System (EMS) name and the management IP address
- The **Status** column of Avaya SBC EMS displaying `Commissioned`
- In the navigation pane, click **Network & Flows** > **Network Management** and configure A1 and B1 interfaces in the **Networks** tab.

  Ensure that a minimum of two IP addresses are configured in **Network Management** for configuring TURN relay service.

About this task

Use this procedure to verify that the Avaya SBC configuration settings match the settings in Avaya Breeze® platform and Avaya Media Server.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service**.

   The Application pane lists the registered Avaya SBC security devices for which the new TURN relay profile is applied. In the content area, the system displays an ordered list for TURN/STUN Profiles and TURN Relay configuration, for the selected Avaya SBC security devices.

4. From the application pane, select the Avaya SBC Device for which the new TURN relay service will be created.

   The system displays the TURN/STUN Service screen showing the **Listen IP** and **Media Relay IP** pair for TURN/STUN profiles, if already created in **TURN/STUN Profiles** tab that are currently defined for that Avaya SBC device.

5. Click the **TURN/STUN Relay** tab.
6. Click **Add**.

   The system displays the Add TURN STUN IP Pairing window.

7. Enter the requested information in the appropriate fields, and click **Finish** to save and exit.

Related links

Add TURN Relay field descriptions on page 597

Add TURN Relay field descriptions

Name	Description
Listen IP	Listen IP of TURN server. The system supports IPv4 and IPv6.
Media Relay IP	Media relay IP of TURN server. The system supports IPv4 and IPv6.
Service FQDN	TURN server listen FQDN
TURN/STUN Profile	Displays the TURN/STUN profiles

Related links

Configuring the TURN relay service for WebRTC calls in Avaya SBC on page 596

Chapter 22: Configuring SIPREC integration

About configuring Avaya SBC for recording media sessions

Avaya SBC supports a SIPREC-based solution to enable recording media sessions between Avaya SBC and a SIP Recording Server for SIP calls between remote workers and SIP trunk calls. The SIPREC configuration for remote worker and SIP trunking are the same, except for differences in server flow configuration towards the recorder. Audio recording supports IPv6, IPv4, and ANAT addressing on the SIPREC interface.

In a conference call recording scenarios, some recording vendors require additional information to identify mixed media streams coming from the conference bridge. Hence, conference media stream participant information is updated with configured conference URI. Avaya SBC and the recording vendor use this conference URI to identify the mixed media streams.

For Hairpin calls, Avaya SBC records the media only once and optimizes the subsequent SIPREC sessions. Avaya SBC provides an option to enable or disable this optimization. Optimization should be disabled where customer is looking for each individual participant media (stereo recording) for participants involved in a call.

In Lineside SIPREC solution, Avaya SBC avoids creating SIPREC sessions for unauthenticated SIP calls.

For SIPREC capacities, see *Avaya Session Border Controller Overview and Specification*.

Avaya SBC supports SIPREC with transcoding when the main call is transcoded. Avaya SBC does not support transcoding to the Recorder. You must ensure that G.729AB or G.711 is configured on either side of the media rules, although transcoding can happen with different codecs.

This chapter contains procedures for administering the SIPREC recording configuration. Before adding configurations for SIPREC recording, you must first configure SIP trunking on Avaya SBC.

Licensing for SIPREC sessions

A single SIPREC session requires one standard license and one advanced license for every non-encrypted recorded call. A single SIPREC session on an encrypted call also requires one standard license and one advanced license. However, an encrypted call with multiple SIPREC sessions requires one standard license and multiple advanced licenses depending on the number of SIPREC sessions.

For example, a SIP trunk call that is being recorded across three destinations requires one standard license and one advanced license for the SIP trunk call, plus two additional advanced licenses, for a total of one standard license and three advanced licenses. The same rules apply for an encrypted SIP trunk being recorded across three destinations: one standard license and three advanced licenses.

Checklist for configuring Avaya SBC for SIPREC

Task	Reference	✔
Configure one or more recording servers.	Configuring a recording server on page 600	
Create a routing profile for the Recording Server.	Adding a routing profile on page 259	
Configure one or more recording profiles and assigning the recording profile to a routing profile.	Configuring one or more recording profiles and assigning the recording profile to a routing profile on page 602	
Enable UCID for the signaling rules used on the Session Manager endpoint policy group.	Enabling UCID for the signaling rules used on the Session Manager endpoint policy group on page 603	
Create a Session Policy for the recorder, enable the recording server, and attach the recording profile.	Creating a new session policy for the Recording Server on page 604	
Create an application rule for the Recording Server.	Creating a new Application Rule on page 103	
Create a media rule with appropriate codec prioritization for the Recording Server. **Note:** For SRTP calls, ensure interworking is enabled. Avaya SBC does not support SIPREC video for this release. If video is enabled at Communication Manager for video calls, and if monitoring of stations is enabled, video time division multiplexing features might have impact on IPv6.	Creating a media rule for the Recording Server on page 604	
Create an endpoint policy group for the Recording Server.	Creating a new endpoint policy group on page 144	

Table continues…

Task	Reference	✔
Ensure that you provision enough RTP ports for the media interface towards the enterprise network. **Note:** For example, if you require 1000 ports for calls, you must provision 2000 ports for RTCP-used even ports and RTCP-used odd ports. To add SIPREC, you must provision another 4000 ports inside and outside RTP to the Recording Server.		
Create a session flow for the Recording Server. If you have a hairpin between remote worker and trunk, ensure that you create three session flows: • Session Flow 1 between trunk and Session Manager1. • Session Flow 2 between Session Manager2 and remote worker. • Session Flow 3 for hairpin flow between trunk and remote worker.	Adding a session flow for the Recording Server on page 606	
Create server flow for each Recording Server. For remote worker configuration, create a server flow for remote worker. Ensure that remote worker A1 interface is set as the received interface, and Avaya SBC interface towards recorder is set as the signaling interface for the server flow.	Creating a server flow on page 167	

Configuring a recording server

Before you begin

Ensure that configurations are done for SIP trunking between Session Manager and the carrier.

About this task

Session recording is a critical requirement for some businesses. Use this procedure to set up session recording by using SIPREC.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click **Add**.

The system displays the Add Server Configuration Profile window.

5. Enter a name for the recording server.
6. Click **Next**.

   The system displays the Edit SIP Server Profile - General window.
7. Administer the following options:
   - In the **Server Type** field, click **Recording Server**.
   - The **SIP Domain** field is optional, but you can enter the name of the enterprise side domain.
   - In the **TLS Client Profile** field, select the TLS client profile created for the recorder.
   - In the **IP Address/FQDN** field, type the IP address of the recording server.
   - In the **Port** field, type the port number.
   - In the **Transport** field, select a transport protocol.
8. **(Optional)** Click **Add** to add more IP addresses or FQDNs to the profile.
9. Click **Next**.

   The system displays the Add Server Configuration Profile - Heartbeat window.
10. Enable heartbeat for load balancing solutions. No other options are required..
11. Click **Next**.

    The system displays the Add SIP Server Profile - Registration window. No option settings are required.
12. Click **Next**.

    The system displays the Add SIP Server Profile - Ping window. No option settings are required.
13. Click **Next**.

    The system displays the Add Server Configuration - Advanced window.
14. Ensure that the **Enable Grooming** check box is selected.

    Important:

    For a recording server, the system selects the **Enable Grooming** field by default. Do not clear the **Enable Grooming** check box.
15. To select the interworking profile, perform one of the following actions:
    - In the **Interworking Profile** field, click the **avaya-ru** profile.

      The avaya-ru profile is the default interworking profile.
    - Clone the default avaya-ru interworking profile and select the cloned interworking profile.
16. **(Optional)** If the Transport type is TLS, select the appropriate TLS client profile.

17. Click **Finish**.

Next steps

Configure a routing profile. For more information, see Routing profiles on page 257.

Related links

Adding a routing profile on page 259

Configuring one or more recording profiles and assigning the recording profile to a routing profile

Before you begin

Verify that you have created a recording server as described in Configuring a recording server on page 600.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Recording Profile**.
4. Click **Add**.

   The system displays the Recording Profile window.
5. Enter a name for the policy.
6. Click **Next**.

   The system displays the Recording Profile window.
7. Administer the following options:
   - Select the **Call Termination on Recording Failure** option if you want the system to terminate the main call if any of the multiple recording sessions fail.
   - Select the **Play Recording Tone** option if you want the system to play a tone when recording starts.
8. Do one of the following:
   - If you do not want to add more profiles to this recording server, click **Finish**. You can add profiles later by clicking **Edit** for any administered recording server.
   - If you want to add more profiles to this recording server, click **Add** and continue with this procedure.

Note:

You are not required to create multiple recording profiles to use the multiple simultaneous SIPREC recording feature.

9. Administer the following options:
   - In the **Routing Profile** drop-down, select the profile you want to use for this recording server. Routing profiles are defined in Adding a routing profile on page 259.
   - In the **Recording Type** drop-down, decide whether you want selective recording or full-time recording.

     When using full-time recording, every communication session established using Avaya SBC is recorded by Avaya SBC end to end. When using selective recording, a portion of the communication session shall be recorded as the recording server cuts through the media stream.
   - The **Video Recording** option is not enabled in this release.
10. Click **Finish**.

    The system displays the administered profiles for the selected recording server.

Enabling UCID for the signaling rules used on the Session Manager endpoint policy group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.
4. Click the Signaling Rule that the Avaya SBC must use for the Recording Server.
5. Click the **UCID** tab.
6. Click **Edit**.
7. Select the **Enabled** check box.
8. In the **Node ID** field, enter a node ID.

   Every entity that generates a UCID has a node ID. The node ID must be unique across a solution.
9. In the **Protocol Discriminator** field, click **0x00**.

   The protocol discriminator configured on Avaya SBC must match the value configured for Communication Manager. If the Communication Manager CTI application requires the protocol discriminator 0x04 for the legacy Interaction Center application, you can set the protocol discriminator to 0x04.

10. Click **Finish**.

Creating a media rule for the Recording Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Media Rules**.

   The application pane displays the existing Media Rule sets, and the Content pane displays the parameters of the selected Media Rule set.
4. **(Optional)** If the recorder you use supports only specific codecs, in the **Audio Codec** section, select the **Codec Prioritization** check box.

   AWE supports only PCMU, PCMA, and G729 audio codecs, and DTMF dynamic codecs such as Dynamic 101. Therefore, you must select codec prioritization and select preferred codecs if you use a WFO recording server.
5. **(Optional)** Select the **Allow Preferred Codecs Only** check box.
6. **(Optional)** If you require media transcoding, select the **Transcode When Needed** check box

   For transcoded calls, you must configure the transcoded codec as G729AB and/or G711 or set codec prioritization as G729AB or G711MU. For SIPREC, one side of the call is transcoded, and the other side must be on G729AB or G711 or vice-versa. Media streamed to the Recorder must be on either a G729AB or G711 codec.
7. **(Optional)** In the **Available** column, select the preferred audio and DTMF dynamic codecs that the recorder supports, and click **>**.
8. **(Optional)** If the recording tone is enabled, select the **telephone-event**, **G729**, and **PCMU** preferred codecs.

   Recording tone is not supported for the PCMA preferred codec.
9. Click **Next**.
10. **(Optional)** Enable BFCP, FECC, and ANAT if required.
11. Click **Finish**.

Creating a new session policy for the Recording Server

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. In the application pane, click **Add**.

   The system displays the Session Policy window.
5. In the **Policy Name** field, enter a name that describes the purpose of the new policy.
6. Click **Next**.

   The system displays another Session Policy window.
7. Select the **Media Anchoring** check box.
8. Select the **Recording Server** check box.
9. In the **Recording Profile** field, select a recording profile that you have administered in Configuring one or more recording profiles and assigning the recording profile to a routing profile on page 602.
10. Select the **Optimize Hairpin Calls** check box to optimize SIPREC sessions on Hairpin calls.

    By default:

    - This field is disabled for new session policy.
    - This field is enabled for an existing session policy after Avaya SBC upgrade or migration.
11. Click **Next**.
12. Click **Finish**.

Related links

Adding a custom wave file for the recording tone on page 605
Creating a server flow on page 167
Adding a session flow for the Recording Server on page 606
Session Policy field descriptions on page 149

Adding a custom wave file for the recording tone

About this task

The default recording tone is the `CONNECTING_CALL` wave file . If required, you can change the recording tone to a new, short duration wave file that supports the G729 and PCMU codecs.

Procedure

1. Log in to the Avaya SBC server.
2. Type `sudo su`.

The system prompts for a password.

3. At the **password** prompt, type the ipcs password.
4. At the root prompt, type `/etc/init.d/ipcs-init stop`.

   The Avaya SBC server stops.
5. Copy the new wave file to `/usr/local/ipcs/prompt/pcmu` and `/usr/local/ipcs/prompt/g729`.
6. Rename the file as CALL_CONNECTING.

   The name of the default wave file is CALL_CONNECTING. By renaming the file, you replace the default file with the wave file you copied.
7. At the root prompt, type `/etc/init.d/ipcs-init start`.

   The Avaya SBC server starts.

Related links

Creating a new session policy for the Recording Server on page 604

Adding a session flow for the Recording Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Session Flows**.

   The content area displays the currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flows screen.
5. In the **Flow Name** field, type the name of the session flow.
6. In the **URI Group #1** and **URI Group # 2** field, select the URI group policy to identify the source or destination of the call.

   You can use the **URI Group #1** and **URI Group # 2** fields to restrict the calls that Avaya SBC records.

   For recording all calls, leave the default value * in the **URI Group #1** and **URI Group # 2** fields.
7. In the **Subnet #1** and **Subnet #2** fields, type the subnet addresses.

   You can specify the source and destination subnet addresses in the **Subnet #1** and **Subnet #2** fields.

   For recording all calls, leave the default value * in the **Subnet #1** and **Subnet # 2** fields.

8. In the **SBC IP Address** field, select the network name and IP address of the Avaya SBC.
9. In the **Session Policy** field, select the session policy that you created for the Recording Server.
10. Click **Finish**.

Chapter 23: Secure CES proxy

Secure Client Enablement Services proxy configuration

Client Enablement Services (CES) provides access to many Avaya Unified Communications (UC) capabilities, including telephony, mobility, messaging, conferencing, and Presence Services through a single application. Avaya one-X® Mobile communicates with the CES server by using the CES protocol. To provide CES services to Avaya one-X® Mobile clients outside the enterprise network, Avaya SBC provides a secure proxy that must be deployed in the enterprise DMZ. Avaya SBC checks all traffic from Avaya one-X® Mobile clients outside the enterprise network to the CES server.

The following sections describe the configuration required to use CES proxy.

Client Enablement Services CA certificate

Client Enablement Services (CES) uses the Avaya SIP CA certificate on IBM HTTP Server (IHS) and a custom self-signed certificate on Handset Server (HSS). To prevent login failure for Avaya one-X® Mobile clients, you must install the CES CA certificate and create a TLS profile in the following order:

1. Install Avaya SIP CA or third-party certificate on the CES client.
2. If you want to use System Manager CA certificates on IHS/HSS, run scripts on CES. This step is optional if you use other certificates.
3. Extract the CES CA certificate.
4. Install the CES CA certificate.
5. Create a TLS client profile.

For information about putting an identity certificate on the CES server, see *Implementing Avaya one-X® Client Enablement Services* at https://support.avaya.com.

Extracting the Client Enablement Services CA certificate

Procedure

1. Log on to the Client Enablement Services server.
2. Go to **CES Admin** > **Servers** > **Presence**, and extract the certificate.

Running scripts on a Client Enablement Services server to use the certificates signed by System Manager CA

About this task

The Client Enablement Services (CES) CA certificates are hardcoded. If you want to use System Manager CA certificates on IHS/HSS, use this procedure to run scripts when the CA certificate and the CES are from Release 6.2.3 or Release 6.2.4.

Before you begin

Install Avaya SIP CA or third-party certificate on a Client Enablement Services (CES) client.

Procedure

1. Log on to the CES server as root.
2. At the root prompt, type `cd /opt/avaya/IHS`.
3. Type `./migrate_smgr_ca_key_trust_store_to_ihs.pl`.

   The system migrates the CA keystore files to IHS.
4. Type `./activate_smgr_ca_certs.pl`.

   The system activates the CA certificates
5. Type `./migrate_ihs_keystore_to_handset_server.pl`.

   The system migrates the IHS keystore files to a handset server. The IHS and HSS servers now have the same keystore files.
6. Type `service 1xp restart`.

   The system restarts.

Creating a client TLS profile

Before you begin

Extract the CES CA certificate from the CES server and install the CES CA certificate on Avaya SBC.

For more information, see the Installing certificates section.

Procedure

1. From the **Device** menu, click the **SBC** name to administer.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the New profile screen.
4. In the **Profile Name** field, type `AvayaCESClient`.
5. In the **Certificate** field, click a certificate.
6. In the **Peer Verification** field, click **Required**.

7. In the **Peer Certificate Authorities** field, click a certificate.
8. In the **Verification Depth** field, type `1`.
9. In the **Renegotiation Time** field, type `0`.
10. In the **Renegotiation Byte Count** field, type `0`.
11. In the **Ciphers** field, click **Default**.
12. Click **Finish**.

Configuring CES proxy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **Relay Services**.

   The following endpoints support Presence Server configuration by using PPM Mapping:

   - Avaya one-X® Communicator for Windows: Release 6.2 SP 11 Patch 3.
   - 96x1 phones: Release 6.5.
   - Avaya Workplace Client for all platforms: Release 3.0.

     Avaya Workplace Client was earlier known as Avaya Communicator.
3. On the Relay Services page, click **Application Relay** > **Add**.
4. In the **Name** field, type a name for the CES proxy.
5. In the **Service Type** field, click **CES**.
6. In the **Remote IP/FQDN** field, type the CES server IP address or FQDN.
7. In the **Remote Port** field, type `8888`.
8. In the **Remote Transport** field, click **TLS**.
9. In the **Client TLS Profile** field, click a client TLS profile.
10. In the **Listen IP** field, click a network and the Avaya SBC external IP address.

    The Listen IP must be the IP that is used for SIP signaling.
11. In the **Listen Port** field, type `7777`.
12. In the **Connect IP** field, click a network and the Avaya SBC internal IP address.

    Avaya SBC requires a signaling interface for the IP address used in the **Connect IP** field. If the Connect IP is used only for CES, you must create a signaling interface for the internal IP.

Important:

TCP connection is not established with the CES server till you create a dummy signaling interface with:

- the same IP configured as Connect IP in CES relay configuration.
- a dummy port.

13. In the **Listen Transport** field, click **TLS**.
14. In the **Server TLS Profile** field, click a server TLS profile.
15. Click **Finish**.

Chapter 24: Call preservation

About the Avaya SBC configuration for Call Preservation

With the Call Preservation feature, the dialog context of the SIP user agent can survive a Session Manager failure even when the Session Manager context is lost. The dialog continues with end-to-end signaling of the intact user agent through an alternate Session Manager. The Call Preservation feature is available for SIP Routing Element (SRE) flows.

For the Call Preservation, a Session Manager Failover Group comprising a pair of Session Manager servers is associated with peer entities. The peer entities, such as Avaya SBC, use enhanced SIP timing and recovery techniques to provide signaling path continuity during Session Manager failure. When Avaya SBC detects that a Session Manager is unreachable, it uses the Failover Group Domain Name (FGDN) in the Session Manager through and Record-route headers to route the SIP traffic through the alternate Session Manager. The FGDN is a fully qualified domain name (FQDN) that resolves to an ordered set of Session Manager servers within a Session Manager Failover Group that provides a high availability SRE service. When the preferred Session Manager becomes unresponsive, the peer SIP entity uses the Session Manager Failover Group Domain resolution to identify and communicate with the alternate Session Manager.

Avaya SBC supports the following features of Call Preservation:

- Multiple Device Access (MDA)
- Call Bridging
- Call Transfer

  Note:

  The Call Transfer feature to preserve the call transactions during a flight will not work.
- Ad-hoc conference hosted by Communication Manager
- Ad-hoc conference hosted by a conference server
- Call Pickup
- Conference call hosted on the conference server

Checklist for configuring Avaya SBC for Call preservation

No.	Task	Reference	✔
1	Create an FGDN group and add FGDNs administered in Session Manager.	Creating FGDN groups on page 613	
2	Enable FGDN configuration for every Session Manager in the FGDN group. Ensure that all instances of Session Manager in the FGDN group have heartbeat configuration.	Creating FGDN groups on page 613	
3	Create a routing rule with an FGDN from the FGDN group as the next hop address.	Creating a routing rule for Call preservation on page 615	
4	Add the routing rule to the trunk server flow.	Creating a routing rule for Call preservation on page 615	
5	Change the interworking profile of Session Manager instances in the FGDN to set the **Transaction Expire** time to 4 seconds.	Creating a routing rule for Call preservation on page 615	
6	Administer DNS SRV for FGDN routing in the DNS server.		

Creating FGDN groups

About this task

The Call preservation feature uses configured FGDNs to route SIP traffic through an alternate Session Manager when a Session Manager fails.

Before you begin

Administer an Avaya Aura® for the Session Manager Call preservation feature.

Procedure

1. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **FGDN Groups**.
4. Do one of the following:
   - To add a new FGDN group, click **Add** at the top of the list of FGDN groups.
   - To add FGDNs to an existing FGDN group, click **Add** in the **FGDN Group** tab.
5. In the **Group Name** field, type a name for the group.

6. In the **FGDN(s)** field, type the FGDNs as administered in Session Manager.
7. Click **Finish**.

FGDN Group field descriptions

Name	Description
Group Name	The name of the FGDN group.
FGDN(s)	The failover group domain name. For call preservation, domain names must be the same as those configured in Session Manager.

Enabling FGDN for a Session Manager in the FGDN group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP servers**.
4. Click the server profile for the Session Manager in the FGDN group.
5. Click the **Heartbeat** tab.
6. Select the **Enable Heartbeat** check box and provide appropriate values in the **Method**, **Frequency**, **From URI**, and **To URI** fields.

   For the Call preservation feature to work, you must enable heartbeat for all Session Manager instances in the FGDN group.
7. Click the **Advanced** tab.
8. Click **Edit**.
9. Select the **Enable FGDN** check box.
10. **(Optional)** If Session Manager is configured for ports other than the default ports,type appropriate port numbers in the **TCP Failover Port** and the **TLS Failover Port** fields.
11. Click **Finish**.

Related links

Server configuration profile field descriptions on page 319

Creating a routing rule for Call preservation

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.

   The application pane displays the existing routing profiles. The content area displays the routing rules comprising a selected routing profile.
4. In the application pane, Click **Add**.
5. Type a distinctive name for the new routing profile, and click **Next**.
6. In the **Load Balancing** field, click **DNS/SRV**.
7. In the **Server Configuration** field, click **Custom**.
8. In the **Next Hop Address** field, type the FGDN configured in the FGDN group.

   The FGDNs you provide must be based on the preferred Session Manager order.
9. Click **Finish**.

Related links

Routing profile field descriptions on page 186

Adding the routing rule to the trunk server flow

Procedure

1. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.
4. Click the device for which you want to change the trunk server flow.
5. Click the **Server Flow** tab.
6. In the row corresponding to the server flow that you want to change, click **Edit**.
7. In the **Routing Profile** field, click the routing rule you created.
8. Click **Finish**.

Related links

Add Subscriber Flow field descriptions on page 164

Changing transaction expiry time in Server Interworking

Procedure

1. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. Click the interworking profile for the Session Manager instances in the FGDN.
5. Click the **Timers** tab.
6. Click **Edit**.
7. In the **Trans Expire** field, type `4`, and click **Finish**.

Next steps

Administer DNS SRV for FGDN routing in the DNS server.

Related links

Interworking profile field descriptions on page 332

Chapter 25: SIP resiliency

Avaya Aura® SIP Resiliency

User agents cannot exchange signaling messages when the SIP signaling path for a call between user agents is disconnected. Reasons for disconnection can be:

- SIP element failure
- Network unavailability
- Non-functioning of one or more SIP elements, such as proxy or location server, if the user switches the network from WiFi to 4G and from 4G to WiFi
- Failure of Session Manager

Using the SIP Resiliency feature, Avaya SBC preserves the call by using Session Manager to reconstruct the call between disconnected endpoints. Avaya recommends using the same domain names for signaling groups to support call reconstruction.

The SIP Resiliency feature is applicable for non Avaya Aura® Failover Group Domain Name (FGDN) segments, whereas for FGDN segments the Call Preservation feature of the previous release is applicable.

Note:

- Avaya SBC does not require SIP Resiliency or call reconstruction for HA failovers. You can deploy Avaya SBC in HA mode to preserve active calls.
- Avaya supports IPv6 addressing for Session Manager reconstructed calls.
- Session Manager uses “+” sign as a prefix in the From header user part for all the reconstructed calls. The “+” in the From header user part causes URI group mismatch on Avaya SBC when the server flows are configured with URI groups. To avoid this, Avaya SBC must be able to configure URI groups with or without “+” sign as a prefix.

Enabling SIP Resiliency

About this task

Use this procedure to enable SIP resiliency for call reconstruction.

Procedure

1. On the home page of System Manager web console, in **Elements**, click **Session Manager** > **Global Settings**.

2. Select the **Enable SIP Resiliency** check box.
3. Click **Commit**.

Chapter 26: Transcoding

About configuring Avaya SBC for transcoding and transrating

Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBC performs transcoding when the inbound and outbound entities have incompatible codecs. The Session Description Protocol (SDP) offer contains information about the codecs that the device sending the message prefers. The device that receives the message responds to the SDP offer by using the set of codecs that the receiving device supports.

Transrating reduces the bit rate of the media while retaining the original media format. Transrating is required where bandwidth is a constraint, for example, on the Wide Area Network (WAN). Enabling transrating results in a lesser number of packets and packet overhead because the packetization period is increased. For example, the packetization period (ptime) is 40 ms on WAN and 10 ms on an internal enterprise network for the same codec. For this example, transcoding is not required, but transrating is required because the packetization period for the same codec is different between inbound and outbound streams.

Codecs supported for transcoding

The following codecs are supported for transcoding:

- G711
- G711A
- G711MU
- G711U
- G722
- G726-32

  This codec is available only when **AMS Offloading** is enabled.
- G729
- G729AB
- H224
- H264/SVC
- OPUS Constrained Narrow Band

- OPUS Narrow Band
- OPUS Wide Band
- PCMA
- PCMU
- AMR-WB
- AMR-NB

The following codecs are supported specifically for Teams:

- G711A
- G711U
- G722
- G729
- OPUS

Any codecs not listed here that are used for calls passing through Avaya SBC do not receive any transcoding treatment from Avaya SBC and are simply relayed through the system.

Note:

Avaya SBC does not support the SILK codec, and it can be filtered if required.

Checklist for configuring Avaya SBC for transcoding

Task	Description	✔
Enable the transcoding and tranrating features.	Enabling transcoding and transrating on page 620	
Administer codec prioritization.	Configuring codec prioritization on page 621	
Add the media rule, which has transcoding enabled, to an endpoint policy group.	Configuring endpoint policy group on page 622	
Add the endpoint policy group to a server flow.	Configuring a server flow for transcoding on page 622	

Enabling transcoding and transrating

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.

3. In the left navigation pane, click **Network & Flows** > **Advanced Options**.
4. Click the **Feature Control** tab.
5. Select the **Transcoding** check box.

   Active transcoding calls are lost when the transcoding feature is disabled.
6. If transrating is required, select the **Transrating** check box.
7. If Avaya Aura® Media Server offloading is required, select the **AMS_OFFLOADING** check box.
8. Click **Save**.

Configuring codec prioritization

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Media Rules**.

   The application pane displays the existing Media Rule sets, and the content pane displays the parameters of the selected Media Rule set.
4. Click **Codec Prioritization** tab and click **Edit**.
5. Select the **Codec Prioritization**, **Transcode When Needed**, and **Transrating** check boxes.

   The system displays `[Transcodable]` next to the codecs that can be transcoded.

   In the Video Codecs section, the **Transcode When Needed** field is unavailable. Video codecs cannot be transcoded.

   You can select **Transrating** and **Transcode When Needed** fields independently.
6. **(Optional)** To remove all codecs that are not included in the Preferred Codecs list , select the **Allow Preferred Codecs Only** check box.
7. In the **Available** column, select the transcodable codecs, and click the right arrow button (**>**) to move them to the **Selected** column in the order of preference.
8. In the **Ptime** column, select a packetization time.

   You can select a packetization time only if you have selected the **Transrating** field.
9. Click **Next**.
10. **(Optional)** If required, enable BFCP, FECC, and ANAT.
11. Click **Finish**.

Configuring endpoint policy group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The EMS server displays the existing End Point Policy Groups.
4. From the application pane, select the Policy Group with the policy sets you want to edit.

   The EMS server displays the policy sets currently assigned to the selected Policy Group.
5. In the content pane, click **Edit**.

   The EMS server displays the Edit Policy Set window.
6. In the **Media Rule** field, click the transcode-enabled media rule.
7. Click **Finish**.

Configuring a server flow for transcoding

About this task

You must attach the endpoint policy group containing the transcode-enabled media rule to the server flow. This ensures that the codec policy is applied for network messaging coming from or going to the server.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.
4. Click the device for which you want to change the trunk server flow.
5. Click the **Server Flow** tab.
6. In the row corresponding to the server flow that you want to change, click **Edit**.
7. In the **End Point Policy Group** field, click the endpoint policy group with the transcode-enabled media rule.
8. Click **Finish**.

Chapter 27: CDR measurement and media statistics

The Call Detail Recording (CDR) and media statistics reporting framework is embedded in the CDR report and made available at the end of the call. The reporting framework provides a RADIUS interface to send CDR messages to the third-party RADIUS Server. If the interface does not exist or the RADIUS interface is nonfunctional because of network outage or a maintenance window, Avaya SBC saves the CDR records locally. Avaya SBC periodically sends data to the CDR adjunct using SFTP. You can configure the frequency when Avaya SBC sends data to the CDR adjunct.

The following types of configurations are available:

- The CDR adjunct is configured through the management interface.

  Data is pushed from Avaya SBC to SFTP. In this case, CDR adjunct and Avaya SBC validate each other based on a shared username and password.

  Avaya SBC raises a CDR alarm if `/archive/cdr` usage crosses the 70% threshold. The `/archive/cdr` directory can use 50% of the `/archive/` partition.

  For example, if the `/archive/` size is 20 GB, `/archive/cdr/` can use up to 10 GB. Avaya SBC raises a CDR alarm if `/archive/cdr/` uses more than 7 GB space.

  Avaya SBC begins purging CDR when `/archive/cdr/` usage crosses the 80% threshold. For example, if `/archive/cdr/` usage crosses the 8 GB threshold, Avaya SBC deletes files older than 3 days.
- RADIUS interface is used to send the CDR and media statistics event messages to the RADIUS Server. Vendor Specific Attributes are used to include CDR information that is not available with the standard RADIUS session information. Third party RADIUS servers need to upload the RADIUS dictionary from `/usr/local/ipcs/etc/rdictionary/dictionary.avayasbce` to analyze the CDR messages from Avaya SBC.
- CDR data can be stored on locally. To store locally, in the **CDR Support** field, select **CDR Adjunct**, but do not configure the CDR adjunct in the **Monitoring & Logging** > **CDR Adjunct** section.

CDR adjunct

Creating a CDR adjunct

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Monitoring & Logging** > **CDR Adjunct**.
4. Configure the following options:
   - In the **Address** field, type the address of the sftp server.
   - In the **Username** field, type the SFTP user name.
   - In the **Password** and **Confirm Password** fields, type the password for accessing the SFTP server.
   - In the **Location** field, type the directory path on the SFTP server where Avaya SBC must store the CDR files.
   - In the **Update Interval** field, click the interval at which Avaya SBC pushes data to the CDR adjunct.
5. Click **Save**.

CDR adjunct field descriptions

Name	Description
Address	The address of the SFTP server.
Username	The username for the SFTP server.
Password	The password to access the SFTP server.
Confirm Password	The field to confirm the password for the SFTP server.
Location	The directory path on the SFTP server where Avaya SBC stores CDR files.
Update Interval	The interval at which Avaya SBC sends data to the CDR adjunct.

When GDPR is enabled, Avaya SBC encrypts the CDR files.

Related links

GDPR on page 312

Radius profile

A Radius profile is used to configure communication between Radius Server and Avaya SBC. A Radius profile can be configured to use either TLS or UDP protocol for communication between Radius server and Avaya SBC. When TLS is used, Avaya SBC uses mutual authentication. So, you must configure a TLS client profile. For more information, see About TLS client profile management on page 372.

Creating a Radius profile

Before you begin

Before you set the **Communication Protocol** field to **TLS**, ensure that you have configured the TLS Client profile. For more information, see About TLS client profile management on page 372.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **RADIUS**.
4. On the Radius Profile page, click **Add**.
5. Enter the values in the fields and click **Finish**.

Radius profile field descriptions

Name	Description
Rule name	The Radius profile name.
Server Address & Port	The Radius server IP address and port number provided in the format: *IP_address:port* **Note:** If you leave the port number blank and: • Set the **Communication Protocol** field to **TLS**, the default port number **2083** is populated. • Set the **Communication Protocol** field to **UDP**, the default port number **1813** is populated.

Table continues…

Name	Description
Alternate Server Address & Port	The Radius server IP address and port number to reach when the primary server is down provided in the format: *IP_address:port* **Note:** If you leave the port number blank and: • Set the **Communication Protocol** field to **TLS**, the default port number **2083** is populated. • Set the **Communication Protocol** field to **UDP**, the default port number **1813** is populated.
Shared Secret	The shared password for Avaya SBC and Radius server.
Confirm Shared Secret	The field to confirm the shared password for Avaya SBC and Radius server.
Number of Retries	The number of attempts that Avaya SBC must try to connect to the Radius server.
Retry Timeout	The time interval for which Avaya SBC must wait for a response from the Radius server.
Connect Port	The Avaya SBC client port number used to send the Radius request messages.
Health Check Interval	The time interval for sending a health check signal to the Radius server when the Radius server is down.
Communication Protocol	The protocol used for communication between Avaya SBC and the Radius server: • **UDP** • **TLS** The default value is **UDP**.
TLS Client Profile	The TLS client profile configured for the Radius server. The default value is **None**. This field is available only when you set the **Communication Protocol** field to **TLS**.

Editing the Radius profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **RADIUS**.
4. Under the RADIUS profile parameters, click **Edit**.
5. Make the appropriate edits, and click **Finish**.

Result

The application pane displays the newly edited Radius profile.

Related links

Radius profile field descriptions on page 625

Renaming the Radius profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **RADIUS**.
4. At the top-right corner of the Radius profile parameters, click **Rename**.
5. In the Rename profile screen, in the **New Name** field, enter a new name for the profile.
6. Click **Finish**.

Result

The application pane displays the renamed Radius profile.

Deleting the Radius profile

Before you begin

Ensure that you delete any application rules associated with this profile. For more information, see Deleting an Application Rule on page 106.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **RADIUS**.
4. At the top-right corner of the Radius profile parameters, click **Delete**.
5. Click **OK** to confirm.

Result

The application pane no longer displays the deleted Radius profile.

Enabling CDR in an application

About this task

You must enable CDR in an application rule by selecting CDR adjunct or the Radius profile. Otherwise, CDR data is not collected for that application.

You can also create or modify an application rule to select the CDR adjunct or Radius profile with the rule.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Domain Policies** > **Application Rules**

   The application pane displays the existing application rule sets, and the content pane displays the parameters for the selected application rule.
4. In the application pane, click **Add**.
5. In the **CDR Support** field, click one of the following:
   - **Radius**: To send CDR events to the Radius server.
   - **CDR Adjunct**: To send CDR files to the CDR adjunct.

   Note:

   If you select **CDR adjunct** and have not configured the CDR adjunct parameters, Avaya SBC stores the CDR data locally.
6. If you chose **Radius** in the **CDR Support** field, in the **Radius Profile** field, select a Radius profile.
7. **(Optional)** If media statistics are required in CDR, select the **Media Statistics Support** check box.
8. In the **Call Duration** field, click one of the following:
   - **Setup**: Record data from the time an INVITE is processed.
   - **Connect**: Record data from the time Avaya SBC receives an ACK for the INVITE.
9. Click **Finish**.

Related links

Application Rule screen field descriptions on page 103

Enabling periodic statistics

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**.

   The system displays the Advanced Options page with the available devices.

4. **(Optional)** If you have multiple devices set up, select the device for which you want to enable periodic statistics.
5. In the **Devices** pane, click a device.
6. Select the **Collect Periodic Statistics** check box.
7. In the **Collection Interval** field, select the duration for which statistics must be made available.
8. Click **Save**.

Chapter 28: Media tunneling

The media tunneling feature provides uniform client messaging and signaling from team engagement and customer engagement client SDKs.

Avaya SBC supports media tunneling through HTTP proxy which acts as a medium that may change the TLS certificate of the media stream.

Media tunneling provides uninterrupted service when:

- A direct media connection path is unavailable between clients and the enterprise infrastructure.
- The corporate firewall of the remote customer enterprise blocks media packets and connection to a specific enterprise infrastructure from within another customer enterprise infrastructure.

Avaya SBC does not provide any interworking functionality for media tunnel calls so the topology must be homogenous.

Media tunneling supports:

- SHA1 and SHA2 hash algorithms.
- The maximum concurrent capacity of tunneled calls supported by Avaya SBC, if you select the **Media Tunneling** check box under **Advanced Options** > **Feature Control** in the EMS web interface.

Remote users that use the HTTPS proxy with SSL inspection mode must whitelist the conferencing server domains in the HTTPS proxy.

In case of a heterogenous environment where HTTPUA clients are behind MIM proxies like Zscalar, SSL Proxy Mode needs to be configured at HTTPUA clients. This triggers a proprietary mechanism of media tunneling which is transparent to any MIM proxies like Zscalar. There is no configuration requirement at Avaya SBC and is adapted dynamically based on client signaling.

Media tunneling checklist

No.	Task	Notes	✔
1	Enable converged conferencing.	See Enabling media tunneling on page 631.	
2	Add a media interface.	See Adding a media interface on page 631.	

Table continues…

No.	Task	Notes	✔
3	Create a TLS server profile.	See Creating a TLS server profile on page 368.	

Enabling media tunneling

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Advanced Options** > **Feature Control** tab.

   The system displays a list of features and a check box for respective feature.
4. Select the **Media Tunneling** check box to enable the Media Tunneling feature.
5. Click **Save**.

Disabling media tunneling

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Advanced Options** > **Feature Control** tab.

   The system displays a list of features and a check box for respective feature.
4. Clear the **Media Tunneling** check box to disable the Media Tunneling feature.
5. Click **Save**.

Adding a media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Click **Add**.
3. In the **Name** field, type a descriptive name for the media interface.
4. In the **IP address** field, select an IP address.

5. In the **Port Range** field, type the port range.
6. Select the **Media Tunneling** feature in **Network & Flows** > **Advanced Options** > **Feature Control** to make **TLS Profile** and **Buffer Size** fields visible in **Media Interface** tab.

   In the **TLS Profile** field, select the profile name of the TLS.

   In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
7. Click **Finish**.

Creating a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click **Add**.

   The EMS server displays the New Profile window.
5. Administer the options as described in TLS server profile screen field descriptions on page 368.
6. Click **Finish**.

   The EMS server creates, installs and lists the TLS server profile in the application pane.

Chapter 29: Configuring Avaya SBC to work with an external Avaya Aura Media Server

About configuring Avaya SBC and an external Avaya Aura® Media Server

Avaya SBC supports an external Avaya Aura® Media Server, which supports both transrating and transcoding, and also supports Avaya Aura® Media Server in high availability mode. For setting up Avaya Aura® Media Server with high availability, configure at least two Avaya Aura® Media Server instances. If you require load balancing, choose **Round Robin** or **Load Factor** in the **Load Balancing** field when configuring the routing profile.

Note:

External Avaya Aura® Media Server is not supported in Release 10.1.2.

Checklist for configuring an external media server

Task	Reference	✔
When using TLS (optional) for the connection to Avaya Aura® Media Server, verify that you are using TLS Version 1.2. Avaya Aura® Media Server requires TLS Version 1.2.	About TLS parameter management on page 351	
Enable Avaya Aura® Media Server offloading.	Enabling Avaya Aura Media Server offloading on page 634	
Configure a Media Server.	Configuring a media server on page 635	

Table continues…

Task	Reference	✔
Create a routing profile for the Media Server. If you require load balancing, add at least two Avaya Aura® Media Server instances, and in the Load Balancing field on the Routing Profile page, select **Round Robin** or **Load Factor**.	Adding a routing profile on page 259	
Assign the media type and routing profile in Session Policies.	Creating a session policy for a media server on page 635	
Create an application rule for the Media Server.	Creating a new Application Rule on page 103	
Create an endpoint policy group for the Media Server.	Creating a new endpoint policy group on page 144	
Create a session policy for a Media Server.	Creating a session policy for a media server on page 635	
Create a session flow for the Media Server.	Adding a session flow for a media server on page 636	
Create a server flow for each Media Server. You must assign the media and signaling interfaces created for Avaya Aura® Media Server to this server flow. The receive interface can be any interface. You must assign the default endpoint flow to this server flow.	Creating a server flow on page 167	

Enabling Avaya Aura® Media Server offloading

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Advanced Options**.
4. Click the **Feature Control** tab.
5. Select the **AMS_OFFLOADING** check box.

   Note:

   You must restart the SBC after enabling AMS Offloading.
6. Click **Save**.

Configuring a media server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click **Add**.

   The system displays the Add Server Configuration Profile window.
5. Enter a profile name.
6. Click **Next**.
7. In the **Server Type** field, select **Media Server**.
8. In the **IP Address** field, type the IP address of the media server.
9. In the **Port** field, type `7150` for TCP or `7151` for TLS (recommended defaults).
10. If you selected TLS, select a profile in the **TLS Client Profile** field, if required.
11. Click **Next**.
12. In the rest of the Add Server Configuration Profile windows, type the requested information in the appropriate fields, and click **Next** after each one.
13. After entering data in each screen, click **Finish**.

Next steps

Create a routing profile as described in Adding a routing profile on page 259.

Creating a session policy for a media server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Domain Policies** > **Session Policies**.

   The application pane displays the existing session policies, and the content pane displays the parameters of the selected session policy.
4. Click **Add**.

   The EMS server displays the Session Policy window.
5. In the **Policy Name** field, type a name for the new session policy, and click **Next**.

   The EMS server displays the second Session Policy window.

6. Select the **Media Anchoring** and **Media Server** check boxes.
7. In the **Routing Profile** field, select the routing profile that you created for Avaya Aura® Media Server.
8. Click **Finish**.

Next steps

- Create a new application rule as described in Creating a new Application Rule on page 103.
- Create an endpoint policy group as described in Creating a new endpoint policy group on page 144.
- Create a session flow.

Adding a session flow for a media server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **Session Flows**.

   The content area displays the currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flows screen.
5. In the **Flow Name** field, type the name of the session flow.
6. Use the default values for the following fields:
   - **URI Group#1**
   - **URI Group#2**
   - **Subnet #1**
   - **Subnet #2**
7. In the **SBC IP Address** field, select the network name and IP address of the Avaya SBC.
8. In the **Session Policy** field, select the session policy that you created for the media server.
9. Click **Finish**.

Next steps

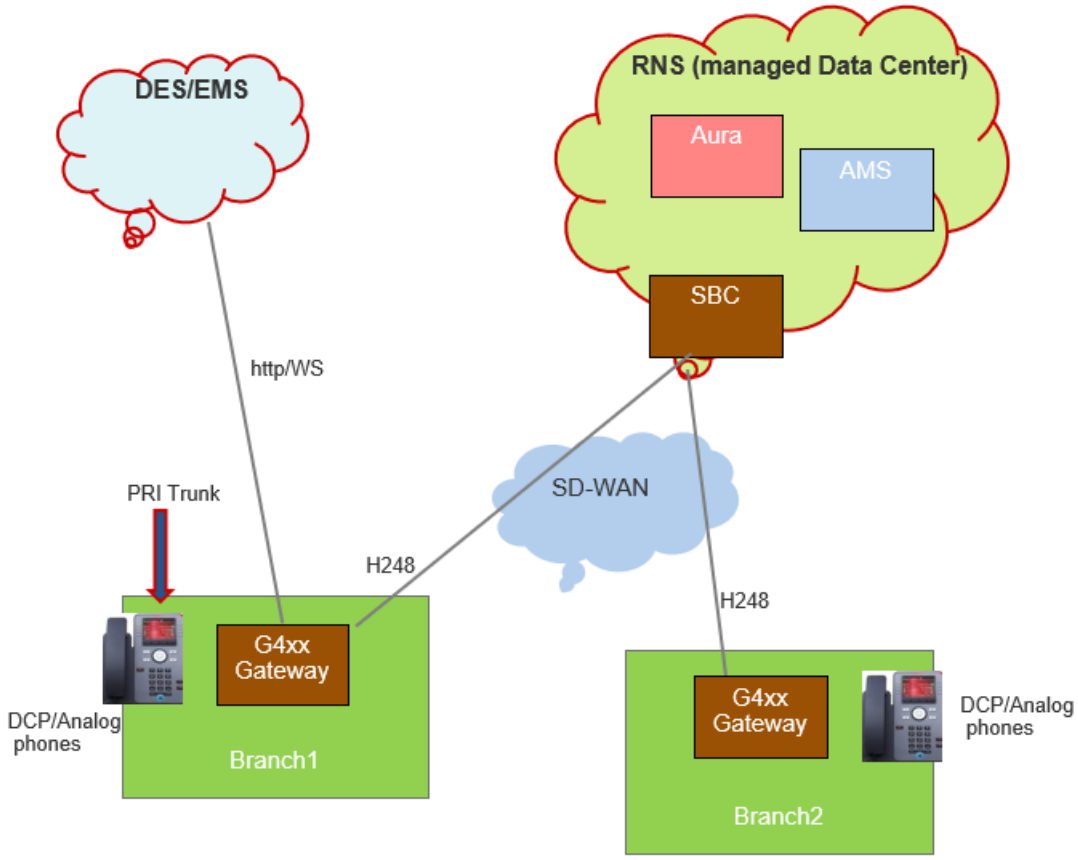
Create a server flow for every media server. In the server flow, assign the media interface, signaling interface, and endpoint flow created for Avaya Aura® Media Server.

Chapter 30: Edge Gateway support

Edge Gateway

The Avaya Ready Now® is a cloud-based service offer that requires Avaya products to be deployed in a distributed architecture. The endpoints and gateways operate in local NAT address domains at the branch office sites, while the Avaya server products remain in the data centers. The data centers also operates in a private address space. The Avaya SBC supports end-to-end communication from the data centers to reach out across public service provider networks and ultimately serve the branch office sites.

You can use Avaya SBC to access PRI trunk, DCP phones, Analog phones from branch to One Cloud Private core through public internet or SD-WAN. The feature should keep media optimized and local to branch for all cases of PRI trunk. DCP phones, Analog phones, and SIP phones from within the same branch or across branches with a common NAT. Avaya SBC provides media access to the One Cloud Private core if any media treatment is required from the One Cloud Private data center.



The G4xx gateways operating as an Edge Gateway are on the public network side of the Firewall from the Avaya SBC. While Avaya Products within the Data Center communicates with IP Addresses. The Edge Gateway tunnels H248 signaling into a TCP/TLS connection toward port 2944 on the Avaya SBC. The Avaya SBC acts as H248 Proxy server to modify the address fields and forward these messages on toward TCP port 2944 on the Communication Manager.

The Single IP support mechanism is developed to ensure that the same listen IP can talk to a unique connect IP towards Avaya Aura®Communication Manager. To identify each gateway uniquely, Avaya SBC is provisioned with a unique gateway serial ID. This gateway serial ID is configured from H248 Servers. The existing real IP of the gateway is replaced with the gateway serial ID. This support essentially allows all gateways to talk to one public IP of Avaya SBC on the public side. On the internal side, the feature has two functionality based on:

- If multiple private IPs are used for gateway registration on Avaya Aura®Communication Manager, then the Avaya SBC must perform multiplexing and de-multiplexing.
- If a single IP is used that requires changes on Avaya Aura®Communication Manager side to manage the gateway registrations using media gateway ID. The gateway sends TPKT0 packet with gateway serial ID, which Avaya SBC uses to identify connect interface towards Avaya Aura®Communication Manager. On each relay, there must be a unique gateway attached.

Note:

Serial ID is a unique 12 characters alphanumeric identity of a gateway. You can locate the serial ID by running `show system` command on the gateway console.

Checklist for configuring Avaya SBC for Edge gateway

No.	Task	Description	Notes	✔
1	Configure the Edge Gateway SNMP trap destination.	Configuring the Edge Gateway SNMP trap destination on page 639		
2	Create a new H248 server.	Creating a new H248 server on page 640		
3	Add a new media interface.	Adding a new media interface on page 274		
4	Configure H248 relay service.	Configuring H248 relay on page 642		
5	Configure application relay for Edge Gateway.	Configuring application relay for Edge Gateway on page 643		

Configuring the Edge Gateway SNMP trap destination

About this task

Add the H248 profile to configure the the Edge Gateway SNMP trap destination.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **H248 Profile**.
4. In the application pane, click **Add**.

   The EMS server displays the Add H248 Profile window.
5. In the **Profile Name** field, type the name of the new H248 profile.
6. In the **IP Address** field, enter the IP Address of the SNMP server.
7. From the **Server Type** drop-down list, select **SNMP**.
8. Click **Finish**.

The content pane displays the new H248 profile.

H248 Profile field descriptions

Name	Description
Profile Name	Specify a descriptive name for the H248 profile.
Server Type	Select **SNMP** from the drop-down list.
IP Address	Enter the IP address for the SNMP server.

Creating a new H248 server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **H248 Servers**.
4. In the application pane, click **Add**.

   The EMS server displays the Add Server Configuration Profile window.
5. In the **Profile Name** field, type the name of the new H248 server profile.
6. Click **Next**.
7. In the **Server Type** drop-down, select the media gateway.
8. In the **Serial ID** field, type the serial ID.
9. Click **Finish**.

   The content pane displays the new H248 server.

Add H248 server field descriptions

Name	Description
Profile Name	Specify a descriptive name for H248 Server.

Table continues…

Name	Description
Server Type	Select the type of H248 server for the profile. The options are: • Media Gateway • Media Gateway Controller
Serial ID	Enter the Serial ID for Media Gateway. **Note:** • You can locate the serial ID by running `show system` command on the gateway console. • After updating the serial ID for Media Gateway, you must restart the system.
IP Address	Enter the IP address for Media Gateway Controller.

Adding a new media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface screen.
4. In the content pane, click **Add**.

   The EMS server displays the Add Media Interface pop-up window.
5. Enter the requested information in the appropriate fields and click **Finish**.

Result

The EMS server displays the new configuration in the Media Interface display.

Add Media Interface field descriptions

Name	Description
Name	A descriptive name for one of the following: • External media interface for the phone network. • Internal media interface for the Avaya call server.

Table continues…

Name	Description
IP Address	IP address of the external or internal media interface.
Port Range	Starting and ending port range numbers. The port range is from 35000 to 40000. To change the port range settings, change the values in the **Port Range** field on the Edit Media Interface page.

Related links

Creating an internal media interface for an Avaya call server on page 493

Configuring H248 relay

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **DMZ Services** > **Relay**.
4. On the Relay Services page, click **H248 Relay** > **Add**.

   The EMS server displays the Add H248 Profile window.
5. In the **General Configuration** section, do the following:
   a. In the **Service Name** field, type the name of the service.
   b. Select the **Media Anchoring** check box.
   c. In the **Listen IP** field, click the network name, and click the IP to which Gateway sends packets or the interface facing the Gateway.
   d. In the **Listen Port** field, type the port number `2944`.
   e. In the **Listen Transport** field, click **TLS**.
   f. In the **Listen TLS Profile** field, click the network name to which Gateway sends packets or the interface facing the Gateway.
   g. In the **Connect IP** field, click the network name, and click the IP to which Communication Manager or Media Gateway Controller can reach.
   h. In the **Connect Transport** field, click **TLS**.
   i. In the **Connect TLS Profile** field, click the network name, and select the interface that Communication Manager or Media Gateway Controller can reach.
6. In the **Remote Server Configuration** section, do the following:
   a. In the **Media Gateway** drop-down, select the media gateway.

b. In the **Media Gateway controller** drop-down, select the media gateway controller.

7. In the **H248 Media** section, do the following:
   a. In the **Listen Media Interface** drop-down, select the listen media interface.
   b. In the **Connect Media Interface** drop-down, select the connect media interface.
8. In the **H248 Management** > **H248 Profile** drop-down, select the H248 profile.
9. Click **Finish**.

Configuring application relay for Edge Gateway

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **Relay Services**.
3. On the Relay Services page, click **Application Relay** > **Add**.
4. On the Add Application Relay page, do the following:
   a. In the **Name** field, type the name of the application relay.
   b. In the **Service Type** field, click **Other**.
   c. In the **Remote IP/FQDN** field, type the logging server IP.
   d. In the **Remote Port** field, type the logging server syslog port number .
   e. In the **Remote Transport** field, click **TCP**.
   f. In the **Listen IP** field, click the network name, and click the IP to which Edge Gateway sends the syslog messages. The default listen port for TLS is 6514.
   g. In the **Connect IP** field, click the network name, and select the media gateway address.
   h. In the **Listen Transport** field, click **TLS**.
5. Click **Finish**.

Back to back H248 Proxy

The back to back H248 a proxy establishes proxy connection between one or multiple branches over a public network, while the datacenter is located in different networks. To support this mechanism, the SBC is set to function in two modes:

- Branch-Edge Mode
- Core Mode

By default, SBC is set to the Core mode. These modes can be changed after installation.

SBC in branch-edge mode

In this mode, the gateway connects to the core mode SBC over a public network and set up a connection with datacenter.

Note:

To ensure the media anchors on the branch-edge SBC, you must select the **Media Anchoring** check-box, while configuring H248 relay.

The back to back H248 proxy un-anchors the media between the two branch-edge SBCs, while the media connectivity is not certain. When media is not anchored on the core SBC, it is either placed on the local branch SBC or connected to remote branch SBC. The branch SBC maintains a connection per gateway with the core SBC and each connection on TLS.

SBC at core

In this mode, the media is transferred within a NAT region. The usage of branch SBC is not mandatory and can be eliminated. In this design, the core SBC communicates with the gateway directly. If core SBC fails, the branch SBC also drops the connections towards the gateway.

Related links

Configuring back to back H248 Proxy on page 644

Configuring back to back H248 Proxy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network Management** > **Advanced Options** > **H248 options**.
4. On the **Advanced H248 Options**, select the device mode from the options.

   The possible values are:

   - Core
   - Branch Edge

   Note:

   If an SBC is set to branch-edge mode, it is not possible to change to core mode. The functionality of related relays in these modes is different and is not interchangeable. To convert an SBC from branch-edge to core mode, you must reconfigure it from scratch.
5. Click **Save**.

Related links

Back to back H248 Proxy on page 643

Chapter 31: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Design		
Avaya Session Border Controller Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBC.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller on a Hardware Platform	Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Google Cloud Platform	Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBC system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller	Describes how to upgrade to the latest release of Avaya SBC.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller	Describes troubleshooting and maintenance procedures for Avaya SBC.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.

  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
20600W	Avaya Session Border Controller 8.1 Technical Delta
21098W	Session Border Controller 8.0 Technical Delta
20660W	Administering the Avaya Session Border Controller for Enterprise - SIP Trunk
60660W	Administering Avaya SBC Release 8 for Remote Worker
20660T	Administering Avaya SBC Release 8 Test
20800C	Implementing and Supporting Avaya SBC — Platform Independent
20800T	Avaya SBC Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBC — Platform Independent
26160W	Avaya SBC Fundamentals
7008T	Avaya SBC for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBC for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

Table continues…

Course code	Course title
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Solution for simultaneous downloads of config and firmware files

Simultaneous downloads of config/firmware files

Solution for downloading configuration and firmware files simultaneously

Environment:	Remote worker
Components:	File server, Avaya SBC, Endpoint.
Requirements:	Required two external IP addresses on Avaya SBC. Endpoint must be able to reach both the external interfaces of Avaya SBC.

This solution is an alternate solution to support the simultaneous downloads of configuration and firmware files from different endpoints through Avaya SBC. In this case, Avaya SBC does not rewrite the content of the configuration file. The file server must serve the configuration file with Avaya SBC content by using GROUPS in configuration file. Avaya SBC requires two IP addresses, one for downloading configuration/firmware files and another interface used for PPM and SIP signaling. Avaya SBC creates a relay between the endpoints and file server.

GROUP identifier in endpoint administration

The GROUP Identifier feature of endpoints enables associating a group of remote worker endpoints with specific SBCs. This feature enables the maintaining of a single configuration file, for the entire enterprise, with individual Avaya SBC access address administered to each GROUP ID. Using GROUP Identifier with the settings file, you can apply administration changes to a specific group of telephones, which takes effect with the next telephone boot-up.

The GROUP is an integer ranging from 0 to 999 with 0 as the default. After the GROUP assignments are set, edit the configuration file and enable each telephone of the appropriate group to download its proper settings. You can administer the GROUP system variable for each individual telephone using the Craft (local administrative) interface.

In staging the remote worker endpoints, the customer must plan according to the enterprise network topology. The technician must assign the endpoint, based on the access Avaya SBC, to a specific GROUP and configure the GROUP ID on the set before deploying to the end-user.

See *Administering Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones*.

File server configuration example

Example: 46xxsettings.txt File with GROUPS.

In this example GROUP_554 and GROUP_555 are for remote workers.

GROUP_554 non secure group

GROUP_555 secure group (TLS/SRTP)

```
 ##############################################################
 ##
# GROUP_SETTINGS
##
##############################################################
##
## Parameter values can be set for specifically-designated groups of
## telephones by using IF statements based on the GROUP parameter.
##
## The value of GROUP can be set manually in a telephone by using the
## GROUP local craft procedure or, for H.323 telephones, it can be set
## remotely by CM based on the telephone's extension number.
## The default value of GROUP in each telephone is 0,
## and the maximum value is 999.
##
## To create a group of settings, use one of the templates below,
## or create others just like them.
##
##############################################################
IF $GROUP SEQ 1 GOTO GROUP_1
IF $GROUP SEQ 2 GOTO GROUP_2
IF $GROUP SEQ 3 GOTO GROUP_3
IF $GROUP SEQ 3 GOTO GROUP_3
IF $GROUP SEQ 5 GOTO GROUP_4
IF $GROUP SEQ 5 GOTO GROUP_5
IF $GROUP SEQ 555 GOTO GROUP_555
IF $GROUP SEQ 554 GOTO GROUP_554
GOTO END
:
:
:
##############################################################
# GROUP_554
########## Add SET Statements for GROUP 554 below ############
### SETTINGS for TCP remote worker #######
SET SIP_CONTROLLER_LIST 10.0.196.251:5060;transport=tcp
SET CONFIG_SERVER_SECURE_MODE 1
SET MEDIAENCRYPTION "9"
SET PRESENCE_SERVER 1.0.197.251
SET ENABLE_PRESENCE 0
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1
```

```
SET HTTPSRVR 10.0.198.251
SET HTTPPORT 80
SET SIPDOMAIN "qames.com"
SET FAILBACK_POLICY auto
SET SIPREGPROXYPOLICY alternate
################ END OF GROUP 554 SETTINGS ####################
GOTOEND
GOTO END
#############################################################
# GROUP_555
########## Add SET Statements for GROUP 555 below ############
### SETTINGS for TLS remote worker #######
SET SIP_CONTROLLER_LIST 10.0.197.251:5061;transport=tls
SET CONFIG_SERVER_SECURE_MODE 2
SET MEDIAENCRYPTION "1"
SET PRESENCE_SERVER 1.0.197.251
SET ENABLE_PRESENCE 1
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1
SET HTTPSRVR 10.0.198.251
SET HTTPPORT 80
SET SIPDOMAIN "qames.com"
SET FAILBACK_POLICY auto
SET SIPREGPROXYPOLICY alternate
################ END OF GROUP 555 SETTINGS ####################
GOTO END
```

Phone configuration

Configure the GROUP identifier and file server address.

GROUP Identifier	The identifier used to load/apply the appropriate configuration from a downloaded configuration file.
File Server Address	The Avaya SBC external IP address used for config/firmware files download.

Configuring Avaya SBC

Before you begin

Ensure that a minimum of two signaling interfaces are present. Dedicate one of the interfaces to the phone firmware download.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the task pane, click **Network & Flows** > **Network Management**.

   The system displays the Network Management screen. From this screen, you can create a new IP address for use with Relay Services and Application Relay.

4. In the Devices list in the Application Pane, click the Avaya SBC device.
5. Click the **Networks** tab.
6. In the **Networks** tab, click **Add.**

   The system displays the Add Network screen.
7. Type the IP address information, and click **Finish**.
8. Create a reverse proxy service for file or firmware download.

Related links

Adding a new signaling interface on page 272
Creating a reverse proxy relay service for file or firmware download on page 501

Appendix B: EMS web interface

EMS web interface

The EMS web interface is a fully integrated, web-accessible operations and administration platform for Avaya SBC UC security products. GUI centralizes and simplifies the provisioning, administration, control, and monitoring of Avaya SBC.

The EMS web interface contains a Postgres database to store configuration and subscriber information, which is updated by each of the deployed Avaya SBC security elements.

The following functions can be performed by using the EMS web interface:

- Configuration
- Alarm and fault management
- SIP statistics monitoring
- Administration and maintenance

Related links

EMS screen elements on page 655

EMS screen elements

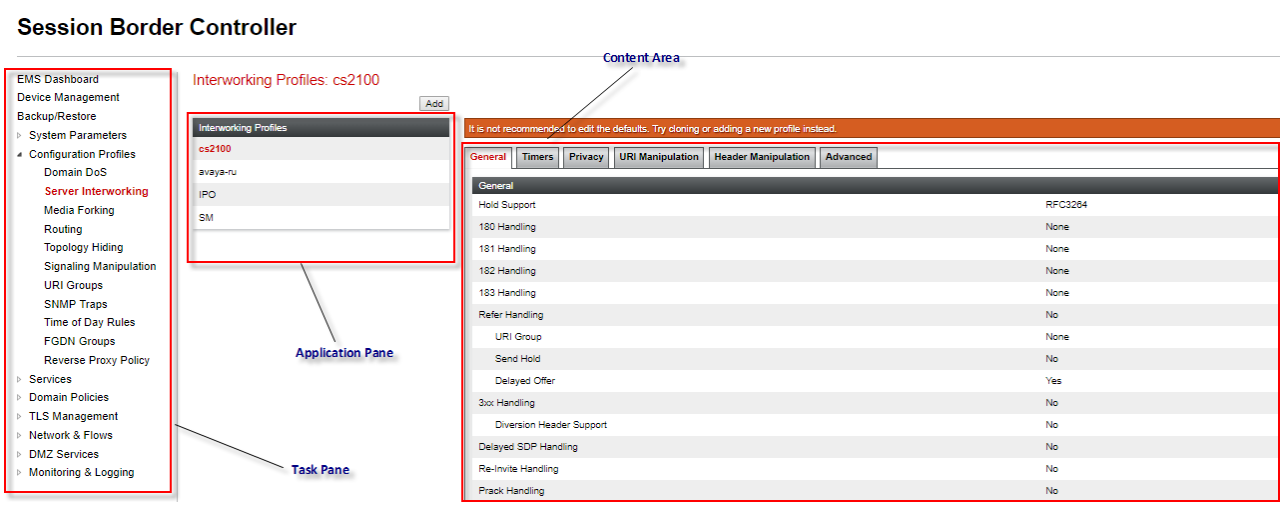
Use the EMS web interface for the administration and configuration of the Avaya SBC security system.

The main sections of the EMS web interface are:

- Tool bar
- Task pane
- Content area

The system displays the application pane between the task pane and the content area when you select any option from the task pane.

Example



Related links

[EMS web interface](#) on page 655
[Tool bar field descriptions](#) on page 656
[Display settings field descriptions](#) on page 657
[Application pane](#) on page 657
[Dashboard screen content area](#) on page 657
[EMS web interface button descriptions](#) on page 668

Tool bar field descriptions

The toolbar provides options to view the security status of the monitored IP network in real time.

Name	Description
Alarms	To access the Alarm Viewer window. The system displays the alarm count next to the server name.
Incidents	To access the Incident Viewer window.
Status	To access the Statistics Viewer, the User Registrations, or the Server Status window.
Logs	To access the Syslog Viewer or the Audit Log Viewer window.
Diagnostics	To access the Diagnostic Test Selection window. The system displays the following tests: • Full Diagnostic • Ping Test
Users	To access the Active User Account window.
Settings	To access the Display Settings or Change Password window.
Help	To access the system help.
Log Out	To log out of the system.

Related links

EMS screen elements on page 655

Display settings field descriptions

Name	Description
Menu Style	Selects the display style for the navigation menu. The options are: • Tree • Dropdown
Signaling Manipulation Syntax Highlighting	Specifies whether the system highlights the Signaling Manipulation syntax.

Related links

EMS screen elements on page 655

Application pane

When you select a security feature from the task pane, the system displays a list of available items to which the feature can be applied in the application pane. When the desired item is selected from the list in the application pane, the system displays the feature parameters assigned to the item in the content area.

Related links

EMS screen elements on page 655

Dashboard screen content area

This screen displays the contents of the selected features or functions. The content area of the Dashboard screen is different from the content area that is displayed when other features are selected from the task pane. This content area contains summary areas that display top-level, system-wide information such as which alarms and incidents are currently active, a list of installed Avaya SBC security devices, Avaya SBC device deployment information, and an area for viewing and exchanging notes with other administrators.

Area Descriptions

Name	Description
Information	Displays the system time, version, build date, license state, licensing overages, peak licensing overage, date on which you last logged in, and the number of failed login attempts.
Installed Devices	Displays a list of all the Avaya SBC security devices which are installed and provisioned in the enterprise VoIP network

Table continues…

Name	Description
Alarms	Displays a streaming feed which displays currently active system alarms, parsed according to the Avaya SBC device type which generated it. More information on the listed alarms can be accessed by clicking the Alarms link (top-left on the Tool Bar). A separate Alarms window will be opened from which the alarm can be viewed and manually cleared.
Incidents	Displays a streaming feed which displays currently active system incidents. It is parsed according to the Avaya SBC device type which generated it. More information on the listed incidents can be accessed by clicking the Incidents push-button from the Tool Bar. A separate Incidents window will be opened from which the incident can be viewed and manually cleared. Incidents are associated with security issues while alarms are associated with hardware/connectivity issues.
Notes	Enables viewing and exchanging text messages with other Avaya SBC administrative users to ensure that important system, security, or administrative information is relayed when necessary. This feature allows you to edit existing messages posted by other users, add new messages of your own, or delete outdated or expired messages. Only administrative level users can edit or delete other users' notes. All users can edit and delete their own notes. Messages posted in this area are stored in the EMS database and are retained when the system is powered down. Messages are continually displayed until such time as they are explicitly deleted by an administrative user.

Related links

EMS screen elements on page 655

Task pane

The task pane is located on the left side of the EMS web interface. Users can access the sections depending on the administrative privileges.

Task pane for EMS

EMS Dashboard

Use this screen to:

- View the software build version, license state, system time, build number, and copyright information.
- View active, up-to-the-minute alarm, incident, and statistical information.

Software management

Use this page to view the details of the installed packages. You can also delete a package using the **Delete** button.

Device Management

Use this screen to view, install, configure, shut down, or restart the Avaya SBC security devices. You can also restart the EMS and SBC devices from the Device Management screen.

This screen displays the **Devices**, **Updates**, **Licensing** and **Key Bundles** tabs.

System Administration

This screen displays the following tabs:

- **Users**
- **AAA**

The **Users** tab displays a comprehensive list of all users with administrative privileges. You can add, edit, and delete user accounts.

Backup/Restore

Use this screen to create a backup file containing the snapshot of the Avaya SBC system configuration. You can also restore the system files through this screen.

Monitoring & Logging

The Monitoring & Logging task pane provides options that are useful for troubleshooting problems.

Monitoring & Logging field descriptions

Name	Description
SNMP	Displays the SNMP information screen, which is used to create access accounts for granting certain users access to the SNMP information. This section has the following tabs: • **SNMP v3** • **Management Servers** • **Trap Severity Settings**
Syslog Management	Contains Log Level and Collectors tabs. The Log Level tab specifies the level of information that is logged for a specific class. The Collectors tab lists the log files where the syslog data is stored.

Table continues…

Name	Description
Debugging	Displays the debugging screen for EMS and devices. This screen contains **Subsystem Logs**, **GUI Logs**, and **Third-Party Logs** tabs. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller*.
Trace	Displays the Trace screen on which you can define the parameters necessary to trace a media packet traversing the network. This screen contains **Packet Capture** and **Captures** tabs. From the **Packet Capture** tab, you can specify an Interface, the local and remote IP, and the maximum number of packets, to capture packets for troubleshooting. The captured packets are available in the **Captures** tab.
Logs Collection	Collects and downloads logs from a web interface for investigating and troubleshooting an issue.
DoS Learning	Displays the Learned Information screen on which you can select a time slot for which DoS-related information is displayed, providing a snapshot of potential threats and anomalies which might be targeting the network. **Note:** This learns *Server DoS/DDoS* only, and the learning applies to: **Services** > **SIP Servers** > **Advanced**.
CDR Adjunct	Call detail records are sent to the configured CDR Adjunct.

Task pane for SBC

EMS Dashboard

Use this screen to:

- View the software build version, license state, system time, build number, and copyright information.
- View active, up-to-the-minute alarm, incident, and statistical information.

Software management

Use this page to view the details of the installed packages. You can also delete a package using the **Delete** button.

Device Management

Use this screen to view, install, configure, shut down, or restart the Avaya SBC security devices. You can also restart the EMS and SBC devices from the Device Management screen.

This screen displays the **Devices**, **Updates**, **Licensing** and **Key Bundles** tabs.

Backup/Restore

Use this screen to create a backup file containing the snapshot of the Avaya SBC system configuration. You can also restore the system files through this screen.

System Parameters

System Parameters field descriptions

Name	Description
DoS/DDos	Displays the **DoS/DDos** screen. This screen contains five tabs: **Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Whitelist**, and **Call Walking**. Using these tabs, you can set the actions the Avaya SBC security system must perform when the DoS, DDoS, or Call Walking attacks are detected.
Scrubber	Displays the **Scrubber** screen. This screen contains two tabs: **Packages** and **Rules**. Using these tabs, you can determine the scrubber rules that the system uses when analyzing the SIP signaling messages for anomalies.
User Agents	Displays the **User Agents** screen. Use this screen to define the trusted SIP user agents that can be used in Subscriber Flows.

Configuration profiles

Configuration Profiles field descriptions

Name	Description
Domain DoS	Displays the Rate Limit screen. Using this screen, you can determine the Avaya SBC security solution that responds to suspected DoS attacks. These responses include Alert Only, Enforce Limit, Enforce Limit with Response, SIP Challenge, and White List.
Server Interworking	Displays the Interworking Profiles screen. This screen contains the following tabs: **General**, **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation**, and **Advanced**. Using these tabs, you can edit the SIP signaling message parameters to facilitate interoperability between various endpoints and SIP implementations within the enterprise.
Media Forking	Displays the Media Forking Profiles screen. The media forking profile has parameters for sending a duplicate stream of media packets to a call recorder.
Routing	Displays the Routing Profile screen. Using this screen, you can manage the parameters related to routing SIP signaling messages to configured routing profiles.
Topology Hiding	Displays the Topology Hiding screen. Using this screen, you can manage how the source, destination and routing information in SIP and SDP message headers must be substituted or changed to maintain the integrity of the network. Use this screen to hide the topology of the enterprise network from external networks.
Signaling Manipulation	Displays the Signaling Manipulation screen. Use this screen to add, change, or delete the header and other information in a SIP message. You can also configure manipulation at each flow level flexibly, by using a proprietary scripting language.

Table continues…

Name	Description
URI Groups	Displays the URI Group screen. The system displays the configured URI groups in the application pane and the pattern for the URI group in the content area. A URI group is a logical group of SIP users that is referenced by call flows that are identified by various endpoints and session policies. You can add, view, edit, clone, and delete a URI group by using the corresponding buttons in the application pane and the content area. **Note:** You cannot edit default profiles available in the system.
SNMP Traps	Displays the SNMP Traps Profiles screen. The system displays the existing SNMP trap profiles. An SNMP trap profile specifies which SNMP traps are monitored and sent to the Serviceability Agent. You can add, view, edit, clone, and delete a profile. The SNMP traps are classified in the following categories on the SNMP Traps Profiles screen: System: • ipcsCPUUsage: CPU usage exceeded a set threshold • ipcsMemoryUsage: Memory usage exceeded a set threshold • ipcsDiskUsage: Disk usage exceeded a set threshold • ipcsDiskFailure: Hard disk failed • ipcsNetworkFailure: Network failed • ipcsProcessFail: Process in use failed • ipcsDatabaseFail: Database failed • ipcsHAFailure: High Availability failed • ipcsHAHeartBeatFailure: Heartbeat from secondary HA server failed • ipcsRSAFailure: RSA algorithm failed • ipcsIncidenceNotification: Notification for incidence occurring in Avaya SBC **Note:** You cannot edit default profiles available in the system.
Time of Day Rules	Displays the Time of Day Rules screen.
FGDN Groups	Displays the FGDN Groups screen. A Failover Group Domain Name (FGDN) group must be configured to support failover to an alternate Session Manager for Call preservation.
Reverse Proxy Policy	Displays the Reverse Proxy Profiles screen. The reverse proxy profile indicates the number of requests permitted per second.
URN Profile	Displays the URN Profiles screen.

Table continues…

Name	Description
Recording Profile	Displays the Recording Profiles screen.
H248 Profile	Displays the H248 Profiles screen.
IP/URI Blocklist	Displays the IP / URI Blocklist Profiles screen. Using this section you can unblock an IP, block a subnet and permanently block an IP/URI.
Tenant Configuration	Displays the Tenant Configuration Profiles screen.

Domain policies

Use the Domain Policies screen to configure, apply, and manage the rule sets or policies to control unified communications based on the criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies that activate the security features of the Avaya SBC security device to aggregate, monitor, control, and normalize call flows.

Domain policies field descriptions

Domain Policies field descriptions

Name	Description
Application rules	Displays a list of application rules in the application pane. You can add, view, edit, clone, or delete the application rules by using the corresponding buttons in the application pane and content area. The system also displays the audio and video application states along with the number of maximum concurrent sessions and the maximum sessions for each endpoint. You can change these parameters in a window accessible from the content area.
Border rules	Displays the **NAT Traversal** tab. Use this tab to manage the operation of Avaya SBC security device when deployed at the edge of the network.
Media rules	Displays a list of media rules in the application pane. You can add, view, edit, clone, or delete media rules by using the corresponding buttons in the application pane and content area. For a media rule, the system displays following parameters related to: • Media Encryption • Codec Prioritization • Media Silencing • Media BFCP • Media FECC • ANAT • transcoding

Table continues…

Name	Description
Security rules	Displays a list of security rules in the application pane. You can add, view, edit, clone, or delete media rules by using the corresponding buttons in the application pane and content area. The options are: • **Compliance** • **Scrubber** • **Domain DoS**
Signaling rules	Displays a list of signaling rules in the application pane. You can add, view, edit, clone, or delete signaling rules by using the corresponding buttons in the application pane and content area. The options are: • **General** • **Requests** • **Responses** • **Request Headers** • **Response Headers** • **UCID**
Charging rules	Displays a list of charging rules in the application pane. You can add, view, edit, clone, or delete charging rules by using the corresponding buttons in the application pane and content area.
End Point Policy Groups	Displays a list of policy group rules in the application pane. You can add, view, edit, or delete policy group rules by using the corresponding buttons in the application pane and content area. A Policy Group is a user-defined combination of the following rules applied to server flows and subscriber flows: • **Application** • **Border** • **Media** • **Security** • **Signaling** • **Charging**
Session Policies	Displays the **Media** tab. Use this tab to control how Avaya SBC processes the media streams. You can add, view, edit, clone, or delete session policies by using the corresponding buttons in the application pane and content area. **Caution:** You must change the Session Policies parameters only after consulting the Avaya technical support staff.

TLS Management

With the TLS Management screen to manage the parameters defined by the Transport Layer Security (TLS) protocol. You must configure the parameters to efficiently administer the security services that establish and maintain a secure TCP/IP connection between two communicating entities.

Implementing TLS within an enterprise VoIP network ensures communications session confidentiality, message integrity, and user authentication.

For a successful TLS management, the client and the server must be certified, so that the identities can be verified and trusted. The mechanism used to authenticate subscriber identities are certificates that are issued by a trusted Certificate Authority (CA).

Use the TLS Management screen to manage each facet of the TLS connection: certificates, clients, and servers. By selecting the desired TLS function (**Certificates**, **Client Profiles**, and **Server Profiles**) from the **Task Pane** and setting the corresponding parameters to precisely define how you want the TLS feature to function.

Use the TLS Management screen to manage the following facets of the TLS connection: certificates, clients, and servers. You can manage the facets by selecting a TLS function from the task pane.

TLS management field descriptions

Feature	Description
Certificates	Displays a certificates tab. Use this tab to handle the installation of certificates, CA root certificates, and Certificate Revocation Lists (CRL).
Client Profiles	Displays a list of available client profiles in the application pane. You can also define additional client profiles using automated field requests to solicit the information necessary to authorize a client to participate in a secure TLS session.
Server Profiles	Displays a list of available server profiles in the application pane. You can also define additional server profiles using automated field requests to solicit the information necessary to authorize a server to participate in a secure TLS session.
SNI Group	An SNI group is a collection of TLS profiles. The functionality of SNI group depends on Avaya SBC, if it is acting as a client or as a server during the communication.

Network & Flows

By Network & Flows task pane options, you can view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, endpoint and session call flows, as well as the ability to manage system logs and control security features.

Network & Flows field descriptions

Name	Description
Network Management	Displays the Network Management screen containing two tabs: **Interface** and **Networks**. From the **Interface** tab you can manage the internal and external IP addresses assigned to a particular Avaya SBC security device. The **Networks** tab allows you to enable or disable Avaya SBC Ethernet interfaces.
Media Interface	Displays the **Media Interface** screen which allows you to designate which server and port range will be used for media traffic.
Signaling Interface	Displays the **Signaling Interface** screen which allows you to designate which server and port range will be used for SIP signaling traffic (TCP, UDP, and TLS).
End Point Flows	Displays the **Subscriber Flows** and **Server Flows** tabs in the Content Area which allow you to determine how calls will be handled by Avaya SBC. These flow descriptions determine which security actions will be applied to the message packets identified by these combined policies. The End Point Flows determine the End Point Policy Group, which includes a security rule set (domain policy).
Session Flows	Displays the **Session Flows** screen, which contains a prioritized list of all currently defined media Session Flows. The Session Flow dictates what session policy to use.
Advanced Options	Contains **Periodic Statistics**, **Feature Control**, **Network Options**, **SIP Options**, **Port Ranges**, **RTCP Monitoring**, **HA Pair**, and **Load Monitoring** tabs. **Note:** The **HA Pair** tab is not displayed unless an HA pair is configured.

DMZ Services

Use this screen to create different profiles and firewall rules for each group of remote users. This screen contains following tabs:

Name	Description
Relay Services	Enables Web conferencing for Mobile Workspace Users. Displays **Application Relay** , **Reverse Proxy**, and **XMPP** tabs. **Application Relay** enables PSOM NAT traversal.

Table continues…

Name	Description
Firewall	Contains **Blacklist**, **Whitelist**, **Services**, and **Source Rate Limiting** tabs. • Blacklist: Provides options to prevent receiving packets from an external source IP or network. Entries included in the Blacklist take priority over entries in the Whitelist. Therefore, ensure that entries to be Whitelisted must not be added to the Blacklist. • Whitelist: Provides options for allowing all packets from an external source IP • Service Feature: Provides an option to allow or block PING for an Avaya SBC. As blocking Ping is a global setting, Ping on all the IPs on A1/B1 interfaces, except EMS management IP, is blocked when you select the Block option. • Source Rate Limiting: Provides options to increase the number of packets permitted from a source every second. The number of packets are set depending on the traffic type.
TURN/STUN Service	Displays the TURN STUN Configuration page. Contains **TURN/STUN Profiles** and **TURN RELAY** tabs.
PPM Mapping	Use this tab to create mapping profiles for each group of remote users. The mapping profiles are used to map the Avaya SBC external IP or name to the Call Server IP or name. With this mapping, the system changes the IP or names in the PPM messages flowing to or from the remote worker endpoint and the Call Server. This translation ensures that messages are exchanged correctly through intended SBC interfaces.

Monitoring & Logging

The Monitoring & Logging task pane provides options that are useful for troubleshooting problems.

Monitoring & Logging field descriptions

Name	Description
SNMP	Displays the SNMP information screen, which is used to create access accounts for granting certain users access to the SNMP information. This section has the following tabs: • **SNMP v3** • **Management Servers** • **Trap Severity Settings**
Syslog Management	Contains Log Level and Collectors tabs. The Log Level tab specifies the level of information that is logged for a specific class. The Collectors tab lists the log files where the syslog data is stored.
Debugging	Displays the debugging screen for EMS and devices. This screen contains **Subsystem Logs**, **GUI Logs**, and **Third-Party Logs** tabs. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller*.
Trace	Displays the Trace screen on which you can define the parameters necessary to trace a media packet traversing the network. This screen contains **Packet Capture** and **Captures** tabs. From the **Packet Capture** tab, you can specify an Interface, the local and remote IP, and the maximum number of packets, to capture packets for troubleshooting. The captured packets are available in the **Captures** tab.
Logs Collection	Collects and downloads logs from a web interface for investigating and troubleshooting an issue.
DoS Learning	Displays the Learned Information screen on which you can select a time slot for which DoS-related information is displayed, providing a snapshot of potential threats and anomalies which might be targeting the network. **Note:** This learns *Server DoS/DDoS* only, and the learning applies to: **Services** > **SIP Servers** > **Advanced**.
CDR Adjunct	Call detail records are sent to the configured CDR Adjunct.

EMS web interface button descriptions

Name	Description
Activate Feature	Enables the currently selected features or parameters.
Add / New	Create a new element, rule, or policy depending upon the screen currently being displayed.
Alarm Status Indicator	Displays a red rectangle and the current number of alarms if there are any active alarms.
Cancel	Cancels the current operation and closes the window without saving any changes.
Checkbox	Selects or deselects specific items, features, parameters, or actions.
Clone	Copies the currently selected rule or parameter to a new record to facilitate defining new rules.

Table continues…

Name	Description
Close	Cancels the current operation and closes the window without saving any changes.
Delete	Deletes the selected element or item from the currently displayed list.
Display Statistics	Displays the Statistics screen in a new window.
Edit	Edits the currently displayed row or object.
Expand Collapse	Expands the current selection to display nested items. Collapses the currently expanded category display list.
Help	Activates system help.
Incidents	Activates a separate incidents pop-up window to display all recently reported system-wide incidences.
Logout	Logs you out of the EMS web interface and re-displays the login screen.
Radio Button	Selects or deselects the corresponding item.
Reboot Device	Reboots the associated Avaya SBC security device.
Shutdown Device	Shuts down the associated Avaya SBC security device. **Warning:** Before you shut down the Avaya SBC device, ensure that someone is available on site to turn on the Avaya SBC device after shutting down.
Restart Application	Restarts an SBC application.
View Configuration	Displays the configuration of the associated Avaya SBC security device.
Install Device	Installs the associated Avaya SBC security device into the network.
Save	Saves information for the element associated with the Save icon.
Select All	Selects all the items in the current list.
Show Calendar	Displays a monthly calendar, where the month, day, and year are user-selectable.
Statistics	Activates a separate Statistics window that displays cumulative Call, Policy, and Protocol statistics.
Undo / Cancel	Allows you to undo changes made to an element after it has been edited. Undo reverts the element back to its pre-edit state.
Users	Opens a separate Logged-in Users window that displays all active Administrator accounts.
Swap Device	Substitutes one Avaya SBC security device for another, thereby placing a new device into service with the same provisioning information as the one being replaced.
Uninstall	Uninstalls the selected item from the network.

Related links

EMS screen elements on page 655

Appendix C: RFC support

RFC support

The following table lists how Avaya SBC complies with supported Request for Comment (RFC) specifications.

RFC	Support
RFC 2046 (MIME, obsoletes 1590)	Complies
RFC 2246 (TLS v1)	Complies
RFC 2833 (DTMF in RTP payload)	Complies
RFC 2976 (SIP INFO method)	Complies
RFC 3261 (SIP, obsoletes 2543)	Complies
RFC 3262 (SIP provisional responses)	Complies
RFC 3263 (SIP resource location)	Complies
RFC 3264 (SDP offer / answer model)	Complies
RFC 3265 (SIP event notification)	Complies
RFC 3311 (SIP UPDATE method)	Complies
RFC 3323 (SIP privacy)	Partially complies – no service disruption
RFC 3325 (SIP privacy extensions)	Partially complies – no service disruption
RFC 3327 (SIP header extension)	Does not comply
RFC 3515 (SIP REFER method)	Complies
RFC 3581 (SIP symmetric response)	Complies
RFC 3605 (SDP with RTCP)	Complies
RFC 3665 (SIP Basic Call Flow)	Complies
RFC 3680 (SIP registration events)	Complies – relayed
RFC 3711 (SRTP)	Complies
RFC 3842 (SIP message waiting)	Complies – relayed
RFC 3856 (SIP presence)	Complies – relayed
RFC 3857 (SIP watcher mechanism)	Complies – relayed
RFC 3891 (SIP replaces header)	Complies

Table continues…

RFC	Support
RFC 3892 (SIP referred-by mechanism)	Complies – relayed
RFC 3911 (SIP join header)	Complies – relayed
RFC 3951 (Internet Low Bit Codec)	Complies – relayed
RFC 4028 (SIP session timers)	Complies
RFC 4103 (Real-time text)	Complies
RFC 4122 (UUID to support GSID tracing)	Complies
RFC 4235 (SIP event dialogs)	Complies
RFC 4346 (TLS 1.1)	Complies
RFC 4566 (SDP, obsoletes 2327, 3266)	Complies
RFC 4568 (SDP security with SRTP)	Complies
RFC 4573 (Far End Camera Control)	Complies – relayed
RFC 4575 (SDP conference events)	Complies – relayed
RFC 4582 (Binary Floor Control Protocol)	Complies – relayed
RFC 4662 (SIP resource list events)	Complies – relayed
RFC 4730 (SIP key press events)	Complies – relayed
RFC 5031 (SIP URN for Emergency and other services)	Complies
RFC 5245 (Interactive Connectivity Establishment)	Complies
RFC 5246 (TLS 1.2)	Complies
RFC 5389 (TURN/STUN for WebRTC)	Complies
RFC 5806 (Diversion Indication in SIP	Complies
RFC 5853 (Requirements for Enterprise SBC Deployments)	Complies
RFC 5905 (Network Time Protocol V4)	Complies
RFC 5923 (Connection Reuse for SIP)	Complies
RFC 6062 (TURN on TCP)	Complies
RFC 7064 (Session Traversal Utilities for NAT – STUN)	Complies
RFC 7065 (Traversal Using relays around NAT) – TURN)	Complies
RFC 7245 (An Architecture for Media Recording Using the SIP)	Complies
RFC 7865 (SIPRec Metadata)	Complies
RFC 7866 (SIPRec Protocol)	Complies

Appendix D: CDR file field description

CDR file field descriptions

Name	Description	Field size in bytes
Ipcs Id	The unique ID that identifies Avaya SBC.	4
Session Id	The unique ID that identifies the call.	4
Leg Id	The unique ID for each leg of the call.	4
RURI Domain	The 32 last characters of host part that is IP address or Domain in Request URI.	32
RURI Username	The 16 last digits of the numeric user portion (Called Number) in Request URI.	16
From Domain	The 32 last characters of the host part of the From header.	32
From Username	The 16 last digits of the numeric user portion of the From header identifying the calling number.	16
To Domain	The 32 last characters of the host part of the To header.	32
To Username	The 16 last digits of the numeric user portion of the To header identifying the called number.	16
Outgoing PAI Domain	The 32 last characters of the host part of the P-Asserted-Identity header.	32
Outgoing PAI Username	The 16 last digits of the numeric user portion in the P-Asserted-Identity header.	16
Call Id	The CALL ID of the call leg.	128
UCID	The UCID, which is unique across Avaya solution for a call and can be used by other adjuncts for reporting, monitoring, and call recording. For recording in CDR, UCID must be administered in Avaya SBC or must come in signaling. The User-To-User header must contain the UCID portion. The User-To-User header containing user information is not part of this field.	24

Table continues…

Name	Description	Field size in bytes
Calling Party Address	The 32 last characters of the host part of contact of the far end calling User Agent (UA).	32
Called Party Address	The 32 last characters of the host part of contact of the far end called UA.	32
Endpoint group policy	The first 10 characters of the SIP Endpoint Policy administered on the Avaya SBC.	10
Server Flow	The first 10 characters of the SIP Server or Subscriber Flow administered on the Avaya SBC.	10
Session Policy	The first 10 characters of the session flow administered on the Avaya SBC.	10
Routing Profile	The first 10 characters of the Routing profile administered on the Avaya SBC.	10
Alternate routes attempted	The number of times Avaya SBC performs alternate routing.	4
Redirected to domain	The last 32 characters of the host part of the Contact header when Avaya SBC services enable redirection.	32
Redirected to Username	The last 16 digits of the numeric user portion of the User part from the Contact header when Avaya SBC services enable redirection.	16
Refer to Domain	The last 32 characters of the host part of the REFER-TO header.	32
Refer to Username	The 16 right-most digits of the numeric user portion of user part from the REFER-TO header.	16
Refer from Domain	The 32 right-most characters of host part of Referred-by header.	32
Refer from Username	The last 16 digits of the numeric user portion of the User part of the Referred-by header.	16
Duration	The duration of the call. The value is controlled by an administered flag so that duration is calculated from the connected to terminated time, or the initiated to terminated time. The administration is as per the policy of the operator. A seven-digit number indicates the duration of the call in hours, minutes, and seconds. First three digits indicate hours, the next two digits indicate minutes, and the last two digits indicate seconds .	8

Table continues…

Name	Description	Field size in bytes
Setup time	The timestamp of Initial INVITE ingressing / egressing from Avaya SBC. DO NOT use the slash	8
Connect time	The timestamp of ACK to Initial INVITE ingressing or egressing from Avaya SBC.	8
Disconnect time	The timestamp of the ingress BYE or any other session terminating message such as 4xx, 5xx, 6xx, and CANCEL.	8
VLAN tag	VLAN ID differentiates between traffic or calls coming from different tenants mapped with different VLAN IDs.	4
Codec	The codec negotiated for the call. The negotiated codec is obtained from the first common intersect between offer and answer messages.	4
Bandwidth	The highest bandwidth used by the call. The bandwidth values are rounded to the nearest multiple of 64000. The options are: • 0: Less than 32 kbps • 1: 64 kbps, less than or equal to 32 kbps • 2: 128 kbps, less than or equal to 32 kbps • 16: 1024 kbps, less than or equal to 32 kbps. This covers 1Mbps • 31: 1984 kbps, less than or equal to 32 kbps .This covers 2Mbps • 32: 2048 kbps, less than or equal to 32 kbps • 94: 6106 kbps, less than or equal to 32 kbps. This includes 6 Mbps • 96: 6144 kbps, less than or equal to 32 kbps • 99: 6304 kbps or greater	1

Table continues…

Name	Description	Field size in bytes
Endpoint type	The type of Endpoint. The options are: • 1: Trunk Server • 2: Call Server • 3: Subscriber • 4: Click to Call • 5: Recording Server • 6: Media Server	1
Feature flag	The feature invoked at Avaya SBC, such as Transfer, Redirection, and SIPREC. This is set as bit mask with the following options: • Bit 0: Call Recording • Bit 1: Call Transfer • Bit 2: Call Redirection • Bit 3: MS Teams call • Bit 4: Local Media Optimization (LMO) call	1
Media flag	The protocol used for media transport and media-related features. This field is set as bit mask with the following options : • Bit 0: Media Type RTP • Bit 1: Media Type SRTP • Bit 2: Media Inactivity Detected • Bit 3: Media Unanchor • Bit 4: Transcoding • Bit 5: Transrating • Bit 6: Hairpin	1

Table continues…

Name	Description	Field size in bytes
Reason code	The code for identifying the reason for call disconnect . The options are: • 1: Successful call .Originator hung up. • 2: Successful call. Terminator hung up. • 3: Unsuccessful call. Caller hung up when ringing. • 4: Unsuccessful call. Callee busy. • 5: Unsuccessful call. Originator hung up. • 6: Unsuccessful call. Terminator hung up. • 7: Unsuccessful call. Media not acceptable. • 8: Unsuccessful call. Forbidden. • 9: Unsuccessful call. User was not found. • 10: Unsuccessful call. Temporarily unavailable. • 11: Unsuccessful call. CAC and bandwidth limitations. • 12: Unsuccessful call. Resource limitation or service unavailable at remote site. • 13: Unsuccessful call. Resource limitation or unavailable at Avaya SBC. • 14: Unsuccessful call. Server failure on remote site. • 15: Unsuccessful call. Server failure at Avaya SBC • 16: Unsuccessful call. Any other failure at remote site. • 17: Unsuccessful call. Any other failure at Avaya SBC. • 18: Unsuccessful call. Timeout. • 65: Partial CDR or long call CDR	1

Table continues…

Name	Description	Field size in bytes
Media Type	Identifies the type of media used for the call leg. This field is set as bit mask with the following options: • Bit 0: Audio • Bit 1: Video • Bit 2: Application • Bit 3: Text • Bit 4: Message • Bit 5: Image	1
End to end secure signalling	The status of security of the signaling of the call . If the originating and terminating call is SIPS, the call is assumed to be secured end-to-end on signaling. The options are: • 1: Call has end-to-end secured signaling. • 0: Call is not end-to-end secured.	1
Failover Detected	Indicates, if Avaya SBC failover happened during call.	1
Latency Progress	Latency in 100 Trying for Avaya SBC timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Alert	Latency in 180 or 183 for Avaya SBC timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Connect	Latency in 200 OK for Avaya SBC timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Ack	Latency in ACK for Avaya SBC timestamp from 200 OK. Applicable to UAC and UAS	4
Incoming PAI Domain	The 32 last characters of the host part of the P-Asserted-Identity header.	32
Incoming PAI Username	The 16 last digits of the numeric user portion in the P-Asserted-Identity header.	16
Mean TTL	The mean TTL value of data packets in the sequence number range, rounded off to the nearest integer.	1
Begin Seq Num	The first sequence number of the RTP data packets.	2
End Seq Num	The last sequence number of the RTP data packets.	2

Table continues…

Name	Description	Field size in bytes
SSRC	The SSRC of the RTP data packet source.	4
Lost Pkt	The number of lost packets in the sequence interval.	4
Duplicate Pkt	The number of duplicate packets in the sequence interval.	4
Min Jitter	The minimum relative transit time between two packets in the sequence interval.	4
Max Jitter	The maximum relative transit time between two packets in the sequence interval.	4
Mean Jitter	The mean relative transit time between two packets in the sequence interval.	4
Loss Rate	The fraction of RTP data packets lost from the source since the packets were received. It is expressed as a fixed point number.	4
Discard Rate	The fraction of RTP data packets discarded from the source since the packets were received, due to late or early arrival, under-run or overflow at the receiving jitter buffer.	4
Round Trip Delay	The round trip time between the RTP instance and the voice application in milliseconds.	4
IsJoin	Identifies if the call leg is part of conference.	-
JoinStatus	The success or failure codes while joining the conference.	-
IsTransfer	Identifies if the call leg is part of call transfer.	-
TransferStatus	The success or failure codes on call transfer.	-
CallDirection	The direction of the call. The possible values are `Inbound` and `Outbound`.	-
ExportMode	The **CDR mode** configuration. The possible values are `3` for **Radius** and `4` for **Radius with Summary**.	-
PartnerId	The **Microsoft Partner Id** configured.	-
CustomerId	The **Microsoft Customer Id** configured.	

Note:

The P-Asserted Identity (PAI) in the SIP INVITE from the Call Server towards the Trunk will get stored in **Outgoing PAI** fields. Also, if the INVITE is from the Trunk Server, the response for this call from the Call Server will get stored in the **Outgoing PAI** fields.

The P-Asserted Identity (PAI) in the SIP INVITE from the Trunk Server towards Call Server will get stored in **Incoming PAI** fields. Also, If the INVITE is from the Call Server, the response for this call from the Trunk Server will get stored in **Incoming PAI** fields.

Glossary

AAA	Authentication, Authorization, and Accounting
ARP	Address Resolution Protocol
Authentication Tag (AT)	The Secure Real-Time Transport Protocol (SRTP) field that carries message authentication data.
CA	Certificate Authority
CDR	Call Detail Record
Certificate (Digital)	A digital certificate is akin to an electronic "credit card" that establishes a client's credentials and authenticity when establishing a communication session and is issued by a certification authority (CA). It contains various information used for encrypting messages and digital signatures. In addition, the certificate contains the digital signature of the certificate-issuing authority so that it can be verified as being real. Some digital certificates conform to a standard, such X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. See also "Certificate Authority (CA)".
Certificate Authority (CA)	The CA is a trusted body that confirms the validity and identity of entities involved in public key exchange. As a user's digital certificate is the only means by which entities may trust each other, the CA must be a legitimate, regulated, and officially recognized entity. An example of a well known CA that is used by many commercial organizations, is Verisign.
Certificate Signing Request (CSR)	In a Public Key Infrastructure (PKI) systems, a CSR is a message sent from an applicant to a certificate authority to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information.

	If the request is successful, the certificate authority will send back an identity certificate that has been digitally signed with the private key of the certificate authority.
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
Client Authentication	Refers to the process of authenticating a client identity by using the client certificate (in TLS).
Codec	Coder/Decoder
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTI	Computer Telephony Integration or Computer-Telephone Integration
Day Zero Attack	See Zero-Day Attack.
DDoS	Distributed Denial-of-Service
Demilitarized Zone (DMZ)	A computer network-related term that refers to the “neutral zone” between an enterprise’s private network and outside public network. Typically, a computer host or small network is inserted into this neutral zone to prevent outside users from getting direct access to the internal network.
Denial-of-Service (DoS)	The objective or end-result of certain types of malicious attacks or other activities against a network, where access to network services, resources, or endpoints is prohibited.
DH	Diffie-Hellman
Diffie-Hellman (D-H) Key Exchange	The process in which “session keys” are distributed between parties that have no prior knowledge of each other across an unsecure public network. This involves setting-up a secure tunnel using Public Key Encryption (PKE), through which session keys are passed.
DiffServ	Differentiated Services
Digest Authentication (DA)	A Hypertext Transport Protocol (HTTP) authentication scheme whereby user passwords are encrypted prior to being sent across the Internet, thus certifying the integrity of the Uniform Resource Locator (URL) data. The downside of DA is that although passwords are encrypted, the data being exchanged is not; it is sent in the clear.
Directory Harvest Attack (DHA)	DHA is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a SPAM database.

	A directory harvest attack can use either of two methods for harvesting valid e-mail addresses. The first method uses a brute force approach to send a message to all possible alphanumeric combinations that could be used for the username part of an e-mail address at the server. The second and more selective method involves sending a message to the most likely user names - for example, for all possible combinations of first initials followed by common surnames. In either case, the e-mail server generally returns a Not found reply message for all messages sent to a nonexistent address, but does not return a message for those sent to valid addresses. The DHA program creates a database of all the e-mail addresses at the server that were not returned during the attack. This explains how a new e-mail address can start receiving spam within days or hours after its creation.
Distributed Denial-of-Service (DDoS)	A more sophisticated type of DoS attack where a common vulnerability is exploited to first penetrate widely dispersed systems or individual end-points, and then use those systems to launch a coordinated attack. Much more difficult to detect than simple DoS attacks.
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DoW	Day-of-Week
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
Eavesdropping	The unauthorized interception and monitoring of voice packets or media streams.
EMS	Element Management System
Encapsulating Security Payload (ESP)	The ESP header normally forms part of an extension to the IP header, and is denoted in the IP type field by the value 50. The header itself is used to indicate the SPI Security Parameter Index (SPI) value that has been employed which, in turn, is associated to the key and algorithm that has been used to encrypt the IP payload. Only those entities privy to the Security Association (SA) have the mapping between the SPI and the key, consequently they are the only users who can decrypt the data. The ESP protocol is defined in RFC 2406.
ENUM	E Number Working Group or Electronic Numbering
ESP	Encrypted Security Payload
False negative	A malicious message that is erroneously treated as a legitimate message.

False positive	A legitimate message that is erroneously treated as a malicious message.
FCAPS	Faults, Configuration, Accounting, Performance, and Security
FQDN	Fully-Qualified Domain Name
FW	Firewall
GARP	Gratuitous Address Resolution Protocol
Global Cluster	Two or more nodes of a SBCAE functional element, such as Signaling or Intelligence.
Global Node	One logical SBCAE functional entity (Signaling or Intelligence) that is deployed in a network.
GUI	Graphical User Interface
HA	High-Availability or Harvest Attack
High-Availability	The Avaya SBC feature that allows two Avaya SBC security devices to be deployed as an integral pair, wherein one of the devices functions as the Primary and the other as an Alternate or Standby. Connected by a heartbeat signal and shared database, the two Avaya SBC security devices provide failover protection in the event one of the devices malfunctions.
HTTP	Hypertext Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ICMP	Internet Control Message Protocol
IM	Instant Messaging
Internet Protocol Security (IPSec)	IPSec is a general framework of open standards which provide for the integrity, confidentiality, and authentication of data exchanged between two peers.
Intrusion	A malicious user or process deliberately masquerading as a legitimate user or process.
IP	Internet Protocol
IPS	Intrusion Protection System
ITSP	Internet Telephony Service Provider
JITC	For products sold into the U.S. and Canadian Government and sector, Joint Interoperability Test Command (JITC) certification is a mandatory

	requirement. Based on the operating system and the capabilities of the product, each product must adhere to the respective standard specified at http://iase.disa.mil/stigs/checklist/index.html. Verification of JITC functionality includes execution of the scripts for the respective operating system on the product. The scripts are specified at http://iase.disa.mil/stigs/SRR/index.html.
Key Agreement Protocol	A type of cryptographic protocol whereby two or more parties to a communications exchange agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third-parties from forcing a key choice on the agreeing parties. Protocols which are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon.
Key Establishment	The process of establishing a shared secret key to be used for encrypting data exchanged between a client and a server over a Transport Layer Security (TLS) connection. Key establishment is also referred to as “key exchange”. In some key exchanges (e.g., RSA), the client generates a random key and sends it to the server. In other schemes (e.g., Diffie-Hellman, or DH) the server generates some random data, sends it to the client, the client generates additional random data, combines it with the server’s random data, and the resulting “key” is sent to the server to be used as a secret key. This latter scheme is an example of a “key agreement” type of key establishment because the two sides together agree on the key. See also “Diffie-Hellman (D-H) Key Exchange” and “Rivest, Shamir, & Adleman (RSA)”.
LAN	Local Area Network
Latency	The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination.
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MAD	Media Anomaly Detection
Man-in-the-Middle Attack (MIM)	A type of network security attack wherein an attacker takes control of an established communications session and masquerades as one of the participating end points. In this type of attack, the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other directly.

	The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them. (See also “public key infrastructure”).
Master Key Identifier (MKI)	That field of the Secure Real-Time Transport Protocol (SRTP) that identifies the master key from which the session keys were derived that authenticate and / or encrypt a particular packet. The MKI can also be used by key management to re-key and to identify a particular master key with the cryptographic text.
MCD	Machine Call Detection
MD5	Message Digest 5
Media Release	See “Anti-tromboning”. See also “Tromboning”.
Message Integrity	The ability to ensure that the message that was received is same as the message that was sent.
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extension
MKI	Master Key Identifier
Mobile Extension (MOBX)	An extension assigned to a mobile user on a Mobile Service Provider (MSP).
MSA	Message Sequence Analysis
Multipurpose Internet Mail Extension (MIME)	A technical standard that describes the transmission of non-text data (or data that cannot be represented in plain ASCII code). It is often used in email to deal with foreign language text as well as for audio and video data. MIME is defined in Request For Comments (RFC) 2045.
MWI	Message Waiting Indicator
Naming Authority Pointer (NAPTR)	A type of Domain Name Service (DNS) record that supports regular expression (regex)-based rewriting. See *Regular Expression (Regex).*
NAT	Network Address Translation
Network Address Translation (NAT) Device	A “barrier” device placed between two networks that translates an IP address used in one network to a different address known within the other network. One of these networks is designated the inside network (for example, an enterprise LAN) and the other is the outside network (for example, the Internet). Users on the inside network can “see” the outside network, but the outside can’t see the inside users, as all communication with the outside network is through the NAT device.

Nonce

A parameter that varies with time. A nonce can be a time stamp, a visit counter on a web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file.

Because a nonce changes with time, it is easy to tell whether or not an attempt at replay or reproduction of a file is legitimate; the current time can be compared with the nonce. If it does not exceed it or if no nonce exists, then the attempt is authorized. Otherwise, the attempt is not authorized.

In SSL / TLS, a nonce is a 32-bit timestamp and a 28-byte random field that is used during key exchange to prevent replay attacks.

NSAP

Network Service Access Point

NTP

Network Time Protocol

P-Asserted-ID

A private extension used in the Session Initiation Protocol (SIP). The P-asserted-id is a Sip header field that contains a SIP Uniform resource Identifier (URI) and an optional display name such as:

```
"Joe Brown" <sip:topengr@avaya.com>
```

A SIP proxy server can insert a P-asserted-id header into a message and forward it to another trusted proxy. However, if the user requests that this information be kept private, then the SIP proxy must remove this field prior to forwarding it to an untrusted proxy.

Packet Spoofing

Impersonating a legitimate user transmitting data.

PAP

Protected Authentication Protocol

Passphrase

A sequence of words or other text used to control access to a protected network or system, program, or data. A passphrase is similar to a password, but generally longer and with more restrictions for added security. Passphrases are often used to control both access to and operation of cryptographic programs and systems. Passphrases are particularly application to systems that use the passphrase as an encryption key.

PKI

Public Key Infrastructure

POP

Point-of-Presence or Post Office Protocol

Port Scanning

A method used by individuals to break into a network to see which assets or services they can hi-jack for their own use or sabotage to limit their use by someone else.

A port scan essentially consists of sending a message to each port, one at a time, and monitoring what kind of response, if any, is received. The

	type of response indicates whether the port is used and can therefore be exploited further. Since network services are normally associated with a “well-known” port number which provides access to it, a port scan can effectively identify which network resources can be exploited further.
PSOM	Persistent Shared Object Model
Public Key Infrastructure (PKI)	PKI is a digital certificate that enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and other information through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
QoS	Quality-of-Service
RADIUS	Remote Authentication Dial-in User Service
RC	Root Certificate
RED	Random Early Detection or Random Early Drop
RegEx	Regular Expression
Regular Expression (RegEx)	‘RegEx’ or ‘regex’ is a way for a user to define how an application should search for a specific pattern in text strings and then what the application should do when a pattern match is found. For example, a regular expression could tell a program to search for all text lines that contain the word "SPAM" and then implement a security filter to block all calls from the offending source.
Remote Authentication Dial-in User Service (RADIUS)	A popular authentication, authorization, and accounting (AAA) protocol for network access or IP mobility applications which can be used in both local and roaming situations.
Rivest, Shamir, & Adleman (RSA)	RSA describes a public key encryption algorithm and certification process to protect user data over networks. The system was designed by three individuals whose last names now designate the process.
Root Certificate (RC)	In cryptography and computer security, a root certificate is an unsigned public key certificate, or a self-signed certificate, and is part of a Public Key Infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard. Normally an X.509 certificate includes a digital signature from a Certificate Authority (CA) which vouches for correctness of the data contained in a certificate. The authenticity of the CA's signature, and whether the CA can be trusted, can be determined by examining its certificate in turn. This chain

	must however end somewhere, and it does so at the root certificate, so called as it is at the root of a tree structure. (A CA can issue multiple certificates, which can be used to issue multiple certificates in turn, thus creating a tree). Root certificates are implicitly trusted. They are included with many software applications. The best known is Web browsers; they are used for SSL/TLS secure connections. However this implies that you trust your browser's publisher to include correct root certificates, and in turn the certificate authorities it trusts and anyone to whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates. This (transitive) trust in a root certificate is merely assumed in the usual case, there being no way in practice to better ground it, but is integral to the X.509 certificate chain model.
RSA	Rivest, Shamir & Adleman
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
Secure Sockets Layer (SSL)	SSL is a commonly-used method for managing the security of a message transmitted via the Internet and is included as part of most browsers and Web server products. Originally developed by Netscape, SSL gained the support of various influential Internet client/server developers and became the de facto standard until evolving into Transport Layer Security (TLS). The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer (where a “socket” is an endpoint in a connection). SSL uses the Rivest, Shamir, and Adleman (RSA) public-and-private key encryption system, which also includes the use of a digital certificate. Avaya SBC supports certificates with 2048-bit or 4096-bit keys. If a Web site is hosted on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.
Security Association (SA)	An SA is the process by which “secret words” or “keys” are exchanged between communicating parties in order to establish a secure connection.

	SA also entails the management, life, and rotation of keys during the communication session.
Server Authentication	The process of authenticating the server's identity by using the server certificate (in TLS).
Session Hijack	A type of network security attack wherein the attacker takes control of a communication session between two end points and masquerades as one of them (see "Man-in-the-Middle Attack").
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SIV	Sender Intention Verification / Validation
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPAM	A common term used to describe the deliberate flooding of Internet addresses or voice mail boxes with multiple copies of the same digital or voice message in an attempt to force it on users who would not otherwise choose to receive it. SPAM can be either malicious or simply annoying, but in either case the cost of sending those messages are for the most part borne by the recipient or the carriers rather than by the sender (SPAMMER).
SPAM-over-Instant Messaging (SPIM)	SPIM is a term used to designate unsolicited bulk messages that target Instant Messaging (IM) services. SPIM is perpetuated by bots (short for "robot", a computer program that runs automatically) that harvest IM screen names off of the Internet and simulate a human user by sending SPAM to the screen names via an IM. The SPIM typically contains a message or link to a Web site that the 'Spimmer' (the individual or organization responsible for sending the SPIM) is trying to market.
SPAM-over-Internet Telephony (SPIT)	SPIT is a term used to designate unsolicited bulk messages broadcast over VoIP to phones connected to the Internet. Although marketers already use voice mail for commercial messages, SPIT makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately. Internet phones are often mapped to telephone numbers, in the interests of computer-telephony integration (CTI) but each has an IP address as well. Malicious users can harvest VoIP addresses or may hack into a computer used to route VoIP calls. Furthermore, because calls routed over IP are much more difficult to trace, the potential for fraud is significantly greater. (See also "SPAM").
Spoof	A prevalent method of deceiving VoIP endpoints to gain access to and manipulate its resources (for example, faking an Internet address so that

	a malicious user looks like a known or otherwise harmless and trusted Internet user).
SRTP	Secure Real-Time Transport Protocol
SRV	Service Record
SSL	Secure Socket Layer
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCP/UDP	Transmission Control Protocol / User Datagram Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToD	Time-of-Day
ToS	Type-of-Service or Terms-of-Service
Transport Layer Security (TLS)	A popular security protocol that ensures privacy between servers (applications) and clients (users) communicating on the IP network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security using some encryption method such as the Data Encryption Standard (DES), but can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. Although TLS is based on Netscape's SSL 3.0 protocol, the two are not interoperable. See “Secure Sockets Layer (SSL)”.
Tunneling	A security method used to ensure that data packets traversing an unsecure public network do so in a secure manner that prevents disruption or tampering.
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

URL	Uniform Resource Locator
Virus	A program that replicates itself by being copied or initiating its copying to another program, operating system, or document. Viruses are transmitted in many ways, such as in attachments to e-mails, as part of downloadable files, or be present on diskettes or CDs. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances or events cause their code to be executed by the unsuspecting host.
VLAN	Virtual LAN
VM	Voice Mail
VoIP	Voice-over-Internet Protocol
VPN	Virtual Private Network
XML	Extensible Markup Language
Zero-Day Attack	A particular type of exploit that takes advantage of a security vulnerability in a network on the same day that the vulnerability itself becomes generally known. Ordinarily, since the vulnerability isn't known in advance, there is oftentimes no way to guard against an exploit or attack until it happens.
Zombie	An IP network element that has been surreptitiously taken over by an attacker, usually without the user's knowledge.

Index

Special Characters

_checklist, edge gateway 639
_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT 625

Numerics

911 calls 182, 184
96x1 phones as remote users limitation 484

A

AAA
  field descriptions 42, 276
AAMS configuration 633
accessing Avaya SBC device
  through SSH 459
accessing port matrix 647
act on statements
  scripting language 568
  statement 568
active users
  field descriptions 436
add
  Domain DoS profile 294
  signaling interface 272, 545
  Topology Hiding header 305
Add Media Forking Profile
  field descriptions 230
Add Media Interface Pop-up Window Field Descriptions 275
add server configuration profile
  field descriptions 319
Add Server Flow
  field descriptions 168
add session flow
  field descriptions 174
Add Subscriber Flow
  field descriptions 164
add URI group
  add URI group criteria 179, 185
  field descriptions 179, 185
add user
  field descriptions 28
add user agent
  field descriptions 271
adding
  adding 132, 133, 135, 136
  Avaya SBC device 48
  custom recording tone 605
  Header Manipulation rule 344
  internal IP in System Manager 486
adding *(continued)*
  interworking profile 331
  media forking profile 230
  media interface 631
  network 349
  network interface 345
  new recording tone 605
  new SIP server profile 318
  new user agent 270
  RADIUS server 36
  regex expression 343
  request header parameters 135
  request parameters 132
  response header parameters 136
  response parameters 133
  routing profile 259
  routing rule to trunk server flow 615
  session flow for a media server 636
  session flow for recording server 606
  SNMP management server 239
  SNMP user account 236
  URI Manipulation rule 343
  URI or domain 329
adding a media attribute in SDP 579
Adding a new media interface 274, 641
Adding a Routing Rule 263
adding a URI
  URI group 178
Adding Media Forking Profile to Session Policy 231
adding network 349
adding network interface 345
Administration
  AAA 659
  User 659
administrative account
  creating 27
  deleting 30
  editing 30
  lockout options 31
  password rules 31
administrative state
  editing 348
administrative users 435
advanced option
  configuration 220
advanced options
  field descriptions 220
alarms
  field descriptions 381
  managing 380
application pane 657
application relay
  IM 504

application relay configuration
RTCP monitoring ... 69
application rule ... 109
counter ... 95, 96
processing ... 95
Application rule ... 105
Application Rule ... 103–106
application rules ... 103
creating ... 513
architecture
standard platform ... 81
audit logs
field descriptions ... 424
viewing ... 424
automatic blacklisting of network source IP ... 283
Avaya Aura SIP Resiliency ... 617
Avaya Binary Floor Control ... 589
Avaya SBC
traps ... 450
Avaya SBC device
adding ... 48
Avaya SBC for Avaya Trunk
configuring ... 541
Avaya support website ... 650

B

back to back H248 proxy
branch SBC ... 643
core SBC ... 643
back-to-back
single Session Manager ... 522
back-to-back-to-back
checklist ... 523
SBC systems ... 556
SBCs ... 554
backup ... 193
frequency ... 194
recommendations ... 194
backup and restore
field descriptions ... 197
banner messages ... 57
basic configuration checklist ... 192
BFCP
configuring ... 589
overview ... 589
blacklist rules
changing ... 74
blacklisting
network source IP ... 283
blocking
subnet ... 284
blocking IP/URI
permanently ... 285
border rule ... 106–108
Border Rule screen
field descriptions ... 107
border rules
configuration ... 106
Branch Survivability ... 543
configuring ... 544
routing profile ... 547
built-in structures ... 572
functions ... 572
regular expressions ... 572
variables and arrays ... 570

C

CA
certificates ... 364
CA certificates
deleting ... 365
viewing ... 365
cadf file
uploading ... 235
call
trace ... 443
call between a remote worker and an internal phone through Avaya SBC ... 458
call between two remote workers through SBC ... 457
call flow
call flow ... 97–99
example ... 97–99
call flow call processing
call flow call processing ... 97
example ... 97
call flow inbound policy invocation
call flow inbound policy invocation ... 98
example ... 98
call flow outbound policy invocation
call flow outbound policy invocation ... 99
example ... 99
call flow route resolution
call flow inbound route resolution ... 98
example ... 98
call flow server flow matching
call flow server flow matching ... 98
example ... 98
call flow splitting
increasing capacity ... 96
call flow transmit to network
call flow transmit to network ... 99
example ... 99
call from remote worker
subscriber flow matching ... 92
call handling
WebRTC ... 592
call preservation ... 612
configuration checklist ... 613
call processing
inbound ... 91
outbound ... 94
SIP ... 88, 91

call reconstruction 617
call server
securing SIP phones 80
securing SIP trunk 78
call server profile
creating 489
call sever
call processing toward network 95
routing 88
call toward server
server flow matching 94
call towards a server
route resolution 93
CDR adjunct
creating 624
field descriptions 624
CDR file
field descriptions 672
CDR measurement 623
certificate
extract 357
certificate authority certificates
deleting 365
viewing 365
certificate file
uploading 359
certificate management 355
certificate revocation list 366
certificate revocation lists
deleting 367
viewing 367
certificates 358
CA 364
deleting 363
installing 358
viewing 363
CES
CA certificate 608
CES CA certificate
extract 608
CES proxy
configuration 610
change password
field descriptions 25
changing
administrative state 348
blacklist rules 74
calling party presentation 580
DNS IP 471
FQDN 471
gateway IP on a single server 467
gateway IP on Avaya SBC 470
gateway IP on secondary EMS 469
hostname 470
management IP 60
management IP on a single server 467
management IP on Avaya SBC 470
changing *(continued)*
management IP on secondary EMS 469
network mask 467
network mask details on Avaya SBC 470
network mask details on secondary EMS 469
network passphrase 470
transaction expire 616
Changing IP address of the primary EMS server on the secondary EMS server 469
changing NTP address on SBC devices 468
changing primary EMS IP on unreachable SBC 468
charging rule 140–143
field descriptions 141
checklist
configuring external media server 633
configuring transcoding 620
establishing end-to-end TLS communications 352
Geographic-redundant deployment 561
media tunneling 630
multiple session manager configuration 551
Presence server configuration 519
SIP trunk configuration 528
classification of requests/responses matching a particular domain policy group at the node 451
clearing
alarms 381
click to call 520
client TLS profile
create 609
clipcs
select 450
clipcs command line interface
clipcs command line interface 448
commands descriptions 448
clipcs console 447
clipcs top commands
instance commands 450
clone
SIP Server Profile 328
cloning
Application Rule 105
border rule 108
charging rule 142
cloning 108, 119, 123, 139, 151, 166, 171, 175, 256
Domain DoS profile 296
interworking profile 342
LDAP server 234
media rule 119
security rule 123
server endpoint flow 171
session flow 175
session policy 151
signaling rule 139
SNI group 377
SNMP trap profle 252
subscriber endpoint flow 166
ToD rule 256

cloning *(continued)*
Topology hiding profile ... 304
Cloning an existing routing profile ... 264
code blocks
statements ... 569
codec prioritization ... 119
configuring ... 621
codec prioritizations
codec prioritizations ... 149
field descriptions ... 149
collect archive field descriptions ... 426
collect logs field descriptions ... 426
collecting
log files ... 425
collection
delete ... 648
edit ... 648
generating PDF ... 648
sharing content ... 648
Command History file ... 450
command line interface
overview ... 459
Command Line Interface ... 23
commands
clipcs console ... 447
instance ... 450
commissioning
Avaya SBC device ... 53
Communication Manager administration required for Remote Worker ... 484
component failure alarm ... 390
concurrent sessions
counter ... 95, 96
config/firmware
files download ... 651
configurable portable snapshot
creating ... 203
configurable portable snapshots
restoring ... 204
configuration
endpoint policy group ... 95
File server ... 652
phone ... 653
configuration checklist
back-to-back ... 555
back-to-back-to-back ... 557
configure
application relay settings ... 554
configuring
application relay ... 518, 643
automatic snapshots ... 196
Avaya SBC for HA deployment using CLI ... 460
Avaya SBC for other trunks ... 542
BFCP ... 589
CES proxy ... 610
click to call ... 520
codec prioritization ... 621
configuring *(continued)*
emergency calls from unregistered endpoints ... 520
endpoint policy group ... 622
FECC ... 591
H248 relay ... 642
High Availability ... 62
inbound signaling rule to send 200 ok response for options request ... 133
media server ... 635
MTCTI messaging ... 189
multi-tenancy ... 502
multi-tenancy configuration ... 502
packet capture ... 443
port bonding ... 58
RADIUS authentication ... 32, 39
recording server ... 600
RTCP monitoring generation support ... 73
server flow for transcoding ... 622
single server deployment using CLI ... 461
SNI group ... 376
UCID ... 603
unregistered endpoints ... 520
X.509 certificate authentication ... 34
configuring application relay
core SBC ... 69
DMZ SBC ... 70
remote Avaya SBC ... 70
RTCP monitoring ... 69, 70
configuring Avaya SBC
real time trunk status ... 416
configuring back to back H248 proxy
branch SBC ... 644
core SBC ... 644
configuring E911 ELIN Gateway ... 170
configuring external media server checklist ... 633
configuring HA Heartbeat Interval
configuring HA Max Retries ... 228
configuring multi-session manager
back-to-back-to-back SBC systems ... 556
back-to-back-to-back SBCs ... 554
configuring Presence server
checklist ... 519
configuring SBC
simultaneous downloads ... 653
console ... 447
content
publishing PDF output ... 648
searching ... 648
sharing ... 648
sort by last updated ... 648
watching for updates ... 648
converting
certificates to PEM format ... 351
counter
application rule ... 95, 96
concurrent sessions ... 95, 96
CPU alarms ... 382

create 491
custom PPM mapping profile 494
standard PPM mapping profile 509
creating
administrative account 27
Application Rule 103
blocklist profile 283
border rule 106
call server flow 539
CDR adjunct 624
charging rule 140
client TLS profile 609
configurable portable snapshot 203
creating 106, 110, 121, 125, 144, 149, 164, 167, 254
CSR 356
endpoint flow 164, 167
external Media Interface toward Trunk Server 538
External Signaling Interface toward Trunk-side Server 536
FGDN groups 613
internal Media Interface toward call server 538
interworking profiles 529
LDAP server 232
media rule 110, 254
policy group 144
Radius profile 625
reverse proxy for multi-tenant 502
reverse proxy policy 498
Routing Profile 532
routing rule for call preservation 615
security rule 121
server endpoint flow 167
Server Profile for Call Server 530
Server Profile for trunk server 531
session flow 174
session policy 149
session policy for media server 635
session policy for Recording Server 604
signaling interface for a phone network 490
signaling rule 125
snapshot for KVM 207
snapshot for VMware 205
SNI group 377
SNMP trap profile 239
subscriber endpoint flow 164
TLS client profile 372
TLS server profile 368, 545, 632
Topology Hiding profile 302, 535
trunk server flow 540
URI group 178
user account 27
Creating
server interworking profile 553
creating and restoring
configurable snapshot using CLI 466
creating routing profile for a trunk server 533
CRL
CRL *(continued)*
installing 366
CRLs
deleting 367
viewing 367
CSR
creating 356
CSRs
externally generated 357
custom PPM mapping profile
field descriptions 497

D

dashboard
about 657
alarms 657
component descriptions 380
dashboard 380
incidents 657
installed devices 657
notes 657
screen 379
DAT file
deleting 476
editing 476
installing 475
data replication is broken 390
data replication pg_xlog usage more than 1 GB 391
database failure alarms 387
debug logs
location 431
debugging
field descriptions 217, 428
decrypting
encrypted files 316
delete
SIP Server Profile 328
Topology Hiding header 306
Topology Hiding profile 305
deleting
a scrubber rules package 301
add a word 378
administrative account 30
application rule 109
Application Rule 106
CA certificates 365
certificate authority certificates 365
certificate revocation lists 367
certificates 363
charging rule 143
CRLs 367
deleting
.... 109, 120, 124, 139, 147, 152, 167, 172, 176, 180, 257
Domain DoS profile 297
existing user agent 272

deleting *(continued)*
Header Manipulation rule ... 345
interfaces ... 348
interworking profile ... 343
LDAP server ... 235
media rule ... 120
policy group ... 147
policy set ... 147
RADIUS server ... 38
secondary EMS ... 467
security rule ... 124
session flow ... 176
session policy ... 152
signaling rule ... 139
snapshot for KVM ... 208
snapshot for KVM deletion ... 208
SNI group ... 378
SNMP trap profile ... 253
SNMP user account ... 239
system snapshot ... 205
TLS client profile ... 375
TLS server profile ... 372
ToD rule ... 257
URI from URI group ... 180
URI group ... 181
URI Manipulation rule ... 344
URI or domain ... 329
user account ... 30
deleting a routing rule ... 264
deleting a snapshot ... 206
deleting an existing routing profile ... 265
deleting an existing signaling interface ... 274
deleting media interface ... 276
deleting regex rules ... 344
deletingserver
deleting
.... 109, 120, 124, 139, 147, 152, 167, 172, 176, 180, 257
flow ... 172
deletingsubscriber
deleting
.... 109, 120, 124, 139, 147, 152, 167, 172, 176, 180, 257
flow ... 167
deploying
geographically dispersed Avaya SBC HA ... 67
designating a snapshot server ... 194
device configuration ... 48
Device Management
field descriptions ... 49
Device Management Overview ... 209
diagnostics
field descriptions ... 434
diagnostics results ... 433
diagram
remote user topology ... 483
direction flags
direction flags *(continued)*
In/Out ... 96
disabling
media tunneling ... 631
network interfaces using CLI ... 465
SNMP traps by severity ... 253
disabling application debug logs ... 430
disabling GUI debug logs ... 431
disk partition space alarms ... 383
display settings
field descriptions ... 657
DMZ services ... 666
DNS SRV ... 330
documentation center ... 648
finding content ... 648
navigation ... 648
documentation portal ... 648
Domain DoS
field descriptions ... 294
domain dos configurations ... 289
Domain DoS profile
rename ... 297
Domain DoS profiles ... 294
domain policies ... 663
Domain Policies ... 77
Unified Communications ... 77
domain policies field descriptions ... 663
DoS
security features ... 290
dos ddos attack type descriptions ... 290
DoS learning
field descriptions ... 298
DoS Protection
editing ... 329
recalculate values ... 329
DoS whitelist ... 329
DoS Whitelist
adding ... 329
deleting ... 329
DoS/DDoS global parameters
field descriptions ... 291
DoS/DDoS settings
editing ... 293
download files
config/firmware ... 651
downloading
log files ... 425
downloading PLDS
license file ... 63
downloading the SBC MIB ... 451
dynamic licensing ... 52

E

EASG
enabling ... 36
Edge gateway ... 637

edit
Topology Hiding header 306
edit wizard
field descriptions 55
editing
administrative account 30
administrative state 348
Application Rule 104
border rule 107
charging rule 141
codec prioritization 119
Domain DoS profile 297
DoS Protection 329
editing . 107, 118, 123, 132, 134, 136, 137, 146, 150, 256
endpoint policy group 146
existing user agent 271
Header Manipulation rule 344
interfaces 349
interworking profile 332
LDAP server 233
media rule 118, 256
network management parameters using CLI 349, 466
policy set 146
RADIUS server 38
request header parameters 136
response header parameters 137
response parameters 134
security rule 123
server endpoint flow 171
session flow 174
session policy 150
signaling rule 132
SIP server profile 318
SIP server profile parameters using CLI 465
SNMP profile 252
SNMP user account 238
subscriber endpoint flow 165
TLS client profile 375
TLS server profile 371
URI group 180
URI Manipulation rule 343
user account 30
editing a routing rule 263
Editing an existing Media Interface 275
Editing an Existing Routing Profile 263
editing an existing signaling interface 273
editing device configuration 214
editing regex rules 343
Emergency call routing for Direct Routing 170
emergency calls 182, 184
emergency calls from unregistered endpoints 520
emergency group 179
EMS software upgrade 63
EMS web interface 655
Administration 659
Backup 659, 660
button descriptions 668
EMS web interface *(continued)*
configuration profiles 661
Dashboard 659, 660
Device Management 659, 660
log in 23
Restore 659, 660
System parameters 661
task pane 658
tool bar 656
enabling
AAMS offloading 634
CDR in an application rule 627
EASG 36
FGDN 614
interfaces 193
media tunneling 631
network interfaces using CLI 465
periodic statistics 628
SIP Resiliency 617
transcoding 620
transrating 620
enabling debug logs 427
enabling GUI debug logs 431
enabling high availability 216
enabling or disabling an installed scrubber rules package 300
endpoint administration
GROUP identifier 651
endpoint flow 164, 167
endpoint flows
managing 163
endpoint policy 563
creating 513
endpoint policy group
configuration 95
configuring 622
editing 146
endpoint policy rules
rules 143
enterprise wide licensing 52
Equinox and Avaya SBC interoperability with SRTP 590
establishing end-to-end TLS communications
checklist 352
extended hostname validation 376
external media interface for a phone network
creating 493
external signaling interface 490
extract certificate 357
extracting
CES CA certificate 608

F

Failover Group Domain Name
enabling 614
Failure reason code mapping 421
far end camera control 591
FECC

FECC *(continued)*
configuring ... 591
FGDN
enabling ... 614
FGDN group
field descriptions ... 614
FGDN groups
creating ... 613
field description
TLS certificates ... 361
field descriptions
active users ... 436
add server configuration profile page ... 319
add snapshot server ... 195
add user ... 28
add user agent ... 271
advanced options ... 220
alarms ... 381
Application Rule ... 103
audit logs ... 424
backup and restore ... 197
CA certificate ... 365
CDR adjunct ... 624
CDR file ... 672
change password ... 25
configuring application relay for RTCP monitoring ... 71
CRL ... 366
custom PPM mapping profile ... 497
debugging ... 217, 428
Device Management ... 49
diagnostics ... 434
display settings ... 657
DoS learning ... 298
DoS/DDoS global parameters ... 291
external media interface for phone network ... 494, 641
FGDN group ... 614
firewall ... 75
incident viewer ... 405
internal media server for Avaya call server ... 494, 641
interworking profile ... 332
lockout ... 31
network management ... 346
new profile ... 373
new server profile screen ... 368
password ... 31
periodic statistics ... 412
Radius profile ... 625
RADIUS server authentication ... 32, 39
reverse proxy ... 177
Reverse Proxy ... 498
scrubber ... 301
Security Rules ... 122
server status ... 417
SigMa ... 583
Signaling Interface ... 492
standard PPM mapping profile ... 511
syslog management ... 267
field descriptions *(continued)*
syslog viewer ... 423
system viewer ... 409
Topology Hiding Profiles ... 303
trace ... 443
TURN Relay ... 597
TURN STUN configuration ... 595
user registrations ... 415
X.509 certificate authentication ... 35
File server
configuration ... 652
filed descriptions
H248 server ... 640
files download
config/firmware ... 651
filtering
registered users ... 414
server flows ... 172
finding content on documentation center ... 648
finding port matrix ... 647
firewall
field descriptions ... 75
firmware/config
files download ... 651
Forward Error Correction
FEC ... 590
From header
Topology Hiding examples ... 309
functions ... 572
built-in ... 572
built-in structures ... 572

G

GDPR
enabling ... 314
GDPR compliance ... 312
Geographic-redundant
non-HA mode ... 559
Geographic-redundant deployment ... 559
HA mode ... 560
geographically dispersed Avaya SBC HA pair
interface connections ... 66
Graphical User Interface (GUI)
browser support ... 22
GROUP identifier
endpoint administration ... 651
groups
uniform resource identifier ... 177
URI ... 177
grub password complexity ... 25
GUI and console alarm list ... 393
GUI password ... 25

H

H248 profile ... 639

H248 Profile field descriptions 640
H248 server 640
HA failovers 60
HA node
HA node 62
status states 62
hard disk failure alarm 386
hardware specifications 449
Header Manipulation rule
adding 344
deleting 345
editing 344
HEADERS variable 570
High Availability
configuring 62
High-Availability pair
geographically dispersed 65
hook points 573
hw_specs_report.txt 449

I

identity engine 176
identity engine server
configuring 176
In/Out
direction flags 96
inbound
call processing 91
policy invocation 92
inbound policy
invocation 87
incident viewer
field descriptions 405
incidents 395, 404
increasing capacity
call flow splitting 96
installation wizard
field descriptions 54
installing 358
Avaya SBC device 53
CA certificate 364
CRL 366
third-party certificates 356
installing rules
scrubber 300
instance
commands 450
interaction
Communication Manager administration required for Remote Worker 484
interface
signaling 272, 545
viewing 348
interfaces
deleting 348
existing signaling interface 274
interfaces *(continued)*
view 274
internal IP
adding 486
internal media interface
avaya call server 493
create internal 493
creating 493
internal signaling interface 491
internal signaling interface toward call server 537
interworking profile
adding 331
cloning 342, 488
deleting 343
editing 332
field descriptions 332
renaming 342
invocation
inbound policy 87
outbound policy 95
outbound policy call processing 88
IP threshold timer 283
IP, gateway, and network mask change 467
Ipcsstatssipcalls 454

K

KVM snapshot creation 207

L

LDAP based call routing 258
LDAP server 232–235
LDAP server profile 232
learned DoS parameters
setting 298
license compliance 436
license file
downloading PLDS 63
limitations
96x1 phones as remote users 484
Remote Worker registration 484
third-party SIP endpoints 484
link failure alarm 386
load balancing 258
locating
SIP servers 89
lockout
field descriptions 31
lockout options 31
log files 422, 425
logging
EMS web interface 23
logging in to EMS 459
login failure alarm 395
logon banner 57
logs 422

M

MAC based LDAP authentication 232
MAC based LDAP authentication field descriptions 233
management IP
changng 60
managing
endpoint flows 163
network options 226
SBC logging level 217
session flows 163
SIP options 225
TLS client profile 372
TLS profile 367
TLS server profiles 368
Managing Avaya SBC security devices 22
managing device-specific settings 272
Managing Port options 227
Managing security features 225
manipulation of P-Asserted-Identity Header 578
matching
server flow 88
subscriber flow 86
media
unachoring 153
unanchor 152
Media Forking
overview 229
media interface
adding 631
media rule 110, 118–120
creating 512
media rules 109
field descriptions 111
Media NAT 111
media server
configuring 635
media server offloading 634
media statistics 623
media tunneling 630
checklist 630
disabling 631
enabling 631
Mediasec 312
memory alarms 382
MIB
OIDs 455
webRTC statistics 454
mobile workspace
topology diagram 483
monitoring 379
licenses 436
RTCP 228
rtcp for remote worker 525
Monitoring & Logging
system 659, 667
Monitoring RTCP
Monitoring RTCP *(continued)*
single Session Manager deployment 519
monitoring tools 437
MTCTI messaging
configuring 189
multi-session manager
web interface 550
multi-tenant CTI 189, 498
multiple recording sessions 602

N

network
adding 349
interface 345
viewing 348
network connectivity overview 317
network interface
adding 345
network interfaces
configuring 345
network management
editing 349
field descriptions 346
network options
manage 226
network teaming 58
network& flows
settings 665
networks
editing 349
new administrator-added alarm 394
new user-added alarm 394
next generation 911 ..... 182, 184

O

OID
system configuration 452
options tab display field descriptions 226
other trunks
configuration 542
other variables 572
out of dialog requests dropped 453
out of dialog responses dropped 453
out of transaction responses dropped 453
outbound
call processing 94
outbound policy
invocation 95
outbound policy call processing
invocation 88
overview 22
basic system configuration 191
command line interface 459
security configuration 289

P

packet capture
configuration ... 443
passthrough ... 347
password
console ... 24
EMS GUI ... 24
field descriptions ... 31
policies ... 23
password hashing mechanisms ... 25
password rules ... 31
performance statistics ... 417
periodic statistics
enabling ... 628
field descriptions ... 412
viewing ... 412
PFX
extract ... 357
phone
configuration ... 653
PKCS#12
extract ... 357
policies
session ... 148
policies and rules
associations ... 83
configuration ... 81
policy group ... 144, 147
policy group summary ... 145
policy invocation
inbound ... 92
route resolution ... 92
policy set ... 146, 147
policy sets ... 147
pooled licensing
using ... 52
port bonding ... 58
port matrix ... 647
port ranges
field descriptions ... 227
portable snapshots
configuring ... 204
PPM mapping profile
custom ... 494
standard ... 509
prerequisites ... 48
Prerequisites ... 475
Presence Server
configuring ... 565
private enterprise OIDs ... 451
process failure alarm ... 387
processing
application rule ... 95
profile
call server ... 489
propagating ... 285
protocol scrubbing ... 299

Q

QoS parameters tab ... 138

R

RADIUS authentication
configuring ... 32, 39
Radius profile ... 626, 627
creating ... 625
field descriptions ... 625
RADIUS server ... 36
field descriptions ... 37
RADIUS server authentication
field descriptions ... 32, 39
real time
server status ... 416
rebooting a device ... 210
reconfiguration command options ... 461
Record Route header
Topology Hiding examples ... 310
recording
multiple sessions ... 602
recording server
configuration ... 600
regenerating self-signed certificates ... 471
Regenerating the rest credentials ... 471, 472
registered users
user registrations ... 414
viewing ... 414
registration processing
SIP ... 86
related documentation ... 645
relay services
field descriptions ... 504
remote access ... 586
Remote Branch Office server ... 546
remote log server
configuring ... 314
remote log server field descriptions ... 315
remote support ... 586
remote worker
checklist ... 487
Session Manager configuration ... 485
Remote Worker registration limitation ... 484
rename
SIP Server Profile ... 328
renaming
Application Rule ... 105
border rule ... 108
charging rule ... 142
Domain DoS profile ... 297
interworking profile ... 342
LDAP server ... 234
media rule ... 119

renaming *(continued)*
renaming ... 108, 119, 123, 139, 151, 256
security rule ... 123
session policy ... 151
signaling rule ... 139
SNI group ... 377
SNMP trap profile ... 252
ToD rule ... 256
Topology Hiding profile ... 304
URI group ... 181
Renaming an Existing Routing Profile ... 265
reordering
policy sets ... 147
reordering ... 147
server endpoint flow ... 172
subscriber endpoint flow ... 167
reordering precedence
reordering precedence ... 175
session flows ... 175
reordering routing rule precedence ... 264
request header parameters ... 135, 136
Request Headers Parameters Tab ... 135
request parameters ... 132
response header parameters ... 136, 137
Response Headers Parameters Tab ... 136
response parameters ... 133, 134
Responses Parameters Tab ... 133
restarting
services ... 76
restarting a device ... 210
Restarting spiritAgent ... 473
restore ... 193
restoring ... 208
automatically ... 202
configurable portable snapshots ... 204
configuration data ... 199
manually ... 202
system snapshot ... 199
restoring a snapshot ... 207
retrieving
a snapshot file ... 201
Reverse Proxy
field descriptions ... 498
reverse proxy policy
creating ... 498
reverse proxy profile
field descriptions ... 177
reverse proxy service
create ... 500
reverse proxy service for file or firmware download
create ... 501
RFC support ... 670
Round Trip Time ... 73
route resolution
call towards a server ... 93
policy invocation ... 92
routing profile ... 87
route resolution *(continued)*
subscriber processing toward remote worker ... 93
routing ... 184
call processing toward network ... 95
toward network ... 88
routing profile
adding ... 259
Branch Survivability ... 547
call server ... 514
fields descriptions ... 186, 260
route resolution ... 87
Routing Profiles ... 257
Routing Rule Management ... 263
RTCP
monitoring relay ... 68
RTCP monitoring
remote worker ... 524
single Session Manager ... 520
RTCP monitoring generation ... 72
RTCP Monitoring Relay
field descriptions ... 68
RTCP Monitoring Report Generation
field descriptions ... 73
RTCP multiplexing ... 110
rules
border ... 106
endpoint policy rules ... 143
media ... 109
security rules ... 120
signaling ... 140
signaling rules ... 124
Time of Day (ToD) rules ... 254
rules and policies
associations ... 83
configuration ... 81
rules and policies configuration checklist ... 85
running
scripts on the CES server ... 609
turntop command ... 593

S

SAL ... 586
SBC
back-to-back-to-back ... 554, 556
SBC OID descriptions ... 451
sbceconfigurator.py ... 461
sbceinfo commands
getapptype ... 447
getemsip ... 447
gethwtype ... 447
getversion ... 447
scenarios
media unanchoring ... 153
screen
dashboard ... 379
script size

script size *(continued)*
SigMa ... 567
scripting language
session statement ... 567
signaling manipulation ... 566
scrubber ... 299
field descriptions ... 301
scrubber actions
configuration ... 301
scrubber rules
installing ... 300
viewing ... 300
SDP capability negotiation ... 109
SDP header
Topology Hiding examples ... 311
SDP variable ... 571
searching for content ... 648
secure CES proxy ... 608
security configuration overview ... 289
Security Feature Control ... 225
security rule ... 121, 123, 124
security rules
rules ... 120
Security Rules
field descriptions ... 122
selecting
log levels ... 266
serial ID ... 637, 640
server endpoint flow ... 167, 171, 172
server flow ... 172
Branch Session Manager ... 547
Core Session Manager ... 548
creating ... 515
matching ... 88
server flow for transcoding
configuring ... 622
server flow matching
call toward server ... 94
server interworking ... 331
server status ... 416
field descriptions ... 417
services
restarting ... 76
session
policies ... 148
session flow ... 174–176
editing ... 174
session flow for a media server
adding ... 636
session flow for recording server
adding ... 606
session flows ... 175
managing ... 163
session manager
Avaya SBC internal and external IP addresses ... 553
configure primary and secondary ... 553
Session Manager
Session Manager *(continued)*
disabling PPM ... 487
session policy ... 149–152
field descriptions ... 149
Session Policy
media forking profile ... 231
session policy for media server
creating ... 635
session statement
scripting language ... 567
statement ... 567
session variables ... 568
setting
learned DoS parameters ... 298
setting EMS time zone ... 64
settings
externally generated CSRs ... 357
SNMP ... 235
sharing content ... 648
showflow
examples ... 445
syntax ... 445
using ... 445
shutting a device down ... 209
SigMa
script size ... 567
Sigma Design Overview ... 584
SigMa Editing the Allow Header ... 581
SigMa Editor
field descriptions ... 583
SigMa Prefix Stripping ... 583
SigMa primer
signaling manipulation ... 566
SigMa Replace From Header For a Set of Users ... 580
SigMa Scripting Examples ... 574
SigMa scripting language
signaling manipulation ... 566
SigMa scripting tutorial ... 578–581, 583
SigMa Scripting Tutorial ... 577
Signaling
QoS parameters tab ... 138
signaling ... 138
signaling interface
field descriptions ... 273
for an Avaya call server ... 491
signaling manipulation
scripting language ... 566
SigMa primer ... 566
SigMa scripting language ... 566
signaling rule ... 125, 132, 139
field descriptions ... 125
signaling rule ... 125
signaling rules ... 140
rules ... 124
simultaneous downloads
configuring SBC ... 653
single sign on ... 176

single sign on *(continued)*
configuring ... 176
SIP
call processing ... 88, 91
SIP message processing
high level ... 86
SIP phones
call server ... 80
SIP registration
processing ... 86
SIP server
DoS configuration ... 289
SIP server configuration
profile management ... 317
SIP server profile
adding new ... 318
editing ... 318
SIP servers
locating ... 89
SIP statistics ... 408
SIP trunk
call server ... 78
SIP trunk configuration
checklist ... 528
SIP trunking overview ... 527
SIPREC
codec prioritization ... 604
configuration ... 599
creating media rule ... 604
SIPREC feature
overview ... 598
snapshot
deleting ... 206
restoring ... 207
system ... 196
snapshot for KVM ... 208
snapshot for KVM restoration ... 208
SNI group ... 377, 378
configuring ... 376
SNMP ... 473
settings ... 235
SNMP management server
adding ... 239
SNMP MIB ... 451
SNMP trap profile
clone ... 252
creating ... 239
delete ... 253
rename ... 252
SNMP traps
disable by severity ... 253
SNMP user account
adding ... 236
deleting ... 239
editing ... 238
SNMP user account field descriptions
field descriptions ... 237
Software management ... 659, 660
software version ... 448
solution
config/firmware files download ... 651
sort documents ... 648
specifying
SigMa Script in Server Configuration ... 584
SRTP failover
considerations ... 590
SRTP support ... 590
standard PPM mapping profile
field descriptions ... 511
statement
session statement ... 567
statements
code blocks ... 569
statistics ... 408
subscriber endpoint flow ... 164–167
subscriber flow ... 167
advanced services ... 516
matching ... 86
subscriber flow matching
call from remote worker ... 92
subscriber processing toward remote worker
route resolution ... 93
support ... 650
swapping
Avaya SBC devices in single server deployment ... 211
swapping Avaya SBC devices ... 211
swapping EMS server in HA pair deployment ... 213
swapping EMS server in single server deployment ... 212
swversion ... 448
syslog management
field descriptions ... 267
Syslog Parameter Management ... 266
syslog viewer
field descriptions ... 423
system alarms ... 380–382
managing ... 380
system incidents ... 404
system information ... 433
system logs ... 422
system monitoring ... 379
system snapshot ... 196
system status information ... 407
system viewer
field descriptions ... 409
system wide single endpoint dos configurations ... 289

T

tagging
VLAN ... 347
tcpdump ... 444
running in CLI ... 445
Telemetry reports ... 419
disabling ... 418

Telemetry reports *(continued)*
enabling ... 418
Telemetry Reports
field descriptions ... 420
Template Wizard ... 474
field descriptions ... 477
using ... 476
verifying ... 481
Tenant configuration ... 286
Tenant Configuration
field descriptions ... 287
tenant configuration profile ... 286–288
third-party certificates
installing ... 356
third-party SIP endpoints limitation ... 484
Time of Day (ToD) rules
rules ... 254
time zone ... 64
tips and tricks
TLS ... 351
TLS
tips and tricks ... 351
TLS client profile
creating ... 372
deleting ... 375
editing ... 375
managing ... 372
TLS management
management ... 665
TLS parameter management ... 351
TLS profile
managing ... 367
TLS server profile
creating ... 368, 545, 632
deleting ... 372
editing ... 371
managing ... 368
To header
topology hiding ... 310
ToD
field descriptions ... 145, 255
policy ... 145
ToD ... 255
ToD rule ... 254, 256, 257
topology diagram
remote worker ... 483
Topology Hiding ... 304
affected headers ... 307
topology hiding examples for request-line header ... 308
Topology Hiding header
adding ... 305
deleting ... 306
editing ... 306
Topology Hiding headers ... 308
Topology Hiding profile
clone ... 304
creating ... 302
Topology Hiding profile *(continued)*
deleting ... 305
Topology Hiding Profiles
field descriptions ... 303
Topology Hiding settings
examples ... 308
trace
call ... 443
field descriptions ... 443
traceSBC ... 437
command line options ... 439
filter options ... 442
log files ... 437
operational modes ... 439
performance benefits ... 438
SIP and PPM logging administration ... 438
usage examples ... 442
user interface ... 440
training ... 649
transaction expire
changing ... 616
transcoding
enabling ... 620
introduction ... 619
transcoding configuration
checklist ... 620
transrating ... 619
trap
description ... 240
troubleshooting ... 432
trunk registration ... 330
trunk server flow ... 540
TURN Relay
field descriptions ... 597
TURN STUN configuration
field descriptions ... 595
turntop
usage ... 593
turntop command
running ... 593

U

UCID ... 138
configuration ... 603
unblocking
IP/URI address ... 285
Unified Communications ... 77
uniform resource identifier
groups ... 177
uninstalling device configuration ... 215
unregistered endpoints ... 520
upgrading system management ... 215
upload
certificate file ... 359
uploading
cadf file ... 235

URI
groups ... 177
URI from URI group ... 180
URI group ... 178, 180
deleting ... 181
renaming ... 181
URI Manipulation rule
adding ... 343
deleting ... 344
editing ... 343
regex rules ... 343
URN mapping ... 182
user account
creating ... 27
deleting ... 30
editing ... 30
user accounts ... 26
user agents ... 270
user deleted alarms ... 395
user privilege change alarm ... 394
user-defined variables ... 573
users ... 435
using
pooled licensing ... 52
showflow ... 445

V

variable ... 570, 571
variables ... 567, 568, 572
variables and arrays
built-in ... 570
built-in structures ... 570
VGA connection ... 459
Via header
Topology Hiding example ... 311
videos ... 650
view
existing signaling interface ... 274
viewing
administrative users ... 435
alarms ... 380
audit logs ... 424
authorized user agents ... 271
CA certificates ... 365
certificate authority certificates ... 365
certificate revocation lists ... 367
certificates ... 363
CRLs ... 367
device configuration ... 214
diagnostics results ... 433
Domain DoS profile ... 296
DoS/DDoS settings ... 290
incidents ... 404
interface ... 348
logs ... 422
network ... 348
viewing *(continued)*
performance statistics ... 417
periodic statistics ... 412
policy group summary ... 145
registered users ... 414
scrubber rules ... 300
server status ... 416
SIP statistics ... 408
statistics ... 408
system alarms ... 380
system incidents ... 404
system logs ... 422
viewing ... 145, 404, 408, 433, 435
Viewing an existing media interface ... 276
viewing EMS time zone ... 64
viewing existing server interworking profiles ... 331
viewing IP URI Blocklist ... 418
Viewing SIP Server profile ... 317
VLAN
use ... 347
VMware
snapshots ... 205

W

watchlist ... 648
web collaboration
configuring ... 564
webRTC
configuring TURN relay service ... 596
configuring TURN/STUN profile ... 594
WebRTC
call handling ... 592
webRTC considerations ... 592
where clause ... 567
whitelisting
Avaya SBC internal IP address ... 486

X

X.509 certificate authentication
configuring ... 34
field descriptions ... 35

Z

Zero Down Time support for AEC deployments ... 587