Administering Avaya Session Border Controller for Enterprise

Release 8.0.x
Issue 4
August 2019

© 2014-2019, Avaya Inc.
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 mediums which may include product information, 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the

software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT 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 MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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 Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 18
Purpose 18
Change history 18
Warranty 19
Chapter 2: Overview 20
Manage Avaya SBCE security devices 20
Graphical User Interface 20
Command Line Interface 21
Logging on to the EMS web interface 21
Passwords 22
Console and SSH passwords complexity 22
EMS GUI password complexity 22
Password policies 23
Chapter 3: Administrative User Accounts 24
Administrative accounts 24
Creating a new administrative account 25
Editing an administrative account 26
Deleting an administrative account 27
Setting administrative account privileges 27
Configuring the RADIUS server 28
Enhanced Access Security Gateway 28
System Administration field descriptions 28
Chapter 4: Device Configuration 31
Prerequisites 31
Adding an Avaya SBCE device 31
Device Management field descriptions 32
Using pooled licensing 33
Commissioning an Avaya SBCE device 34
Installation Wizard field descriptions 35
Edit device field descriptions 37
Changing the management IP from the EMS web interface 38
High Availability failovers 38
Configuring High Availability 39
HA Node Status States 40
Upgrade of the EMS software 41
Obtaining a license file from Avaya PLDS 41
Viewing the EMS server time zone 42
Setting the EMS server time zone 42
Exiting the Avaya SBC Runtime Options screen 43

High-Availability pair geographically dispersed 43
Interface connections for a geographically dispersed Avaya SBCE HA pair 44
Deploying a geographically dispersed Avaya SBCE HA configuration 46
Configuring RTCP monitoring relay 46
RTCP Monitoring Relay field descriptions 47
Application relay configuration for RTCP monitoring 47
Configuring application relay for RTCP monitoring in core Avaya SBCE 48
Configuring application relay for RTCP monitoring in DMZ Avaya SBCE 49
Configuring application relay for RTCP monitoring in remote Avaya SBCE 49
Configuring application relay for RTCP monitoring in core, remote, and DMZ Avaya SBCE field descriptions 50
RTCP monitoring generation support 51
Round Trip Time 51
Configuring RTCP monitoring generation support 52
Adding a new blacklist rule 53
Firewall field descriptions 53
Chapter 5: Domain Policy, Routing, and Message Flow Administration 56
Governing Unified Communications with Domain Policies 56
Unified Communications Policies 56
Example: Call server with SBCE securing SIP trunk 57
Example: Call server with SBCE securing SIP phones 59
Rules and policies configuration 60
Architecture 60
Rule and policy associations 62
Rules and policies checklist 64
SIP message processing 65
SIP registration processing 65
Subscriber flow matching 66
Inbound policy invocation registration processing 66
Route resolution 66
Server flow matching 67
Outbound policy invocation call processing 67
Transmit to network registration processing 67
SIP call processing on Avaya SBCE 68
Inbound call processing 68
Subscriber flow matching for call originated from remote worker 69
Policy invocation and route resolution 69
Inbound policy invocation 69
Route resolution for call towards remote worker 70
Route resolution for a call towards a server 70
SIP servers identification 71
Outbound call processing 73
Server flow matching for a call to a server 73

Outbound policy invocation for registration processing 74
Transmit to network for call processing 74
Application rule processing for endpoint policy group configuration 74
Maximum concurrent sessions per endpoint counter 75
Maximum concurrent sessions counter 75
Rules for call flows 75
In/Out direction flags 75
SIP call flow example 76
Call flow example for call processing 77
Call flow example for server flow matching in calls originated from a server 77
Call flow example for inbound policy invocation 77
Call flow example for route resolution 77
Call flow example for server flow matching in a call towards a server 78
Call flow example for outbound policy invocation 78
Call flow example for transmit to network 78
Call flow example from PSTN trunk to a Call Center Elite user 79
Domain policies management 82
Application rules 83
Border rules 86
Media rules 89
Security rules 96
Signaling rules 100
Charging rules 116
Endpoint policy groups 119
Session policies 123
Manage endpoints and session flows 138
Endpoint flows 138
Session flows 144
Single Sign-On and Identity Engine 147
Configuring Single Sign-On and an Identity Engine server 147
Uniform Resource Identifier groups 148
Creating a new URI group 149
Editing a URI group 151
Deleting a SIP URI from an existing URI group 151
Renaming a URI group 152
Deleting a URI group 152
Chapter 6: System Configuration 154
Basic system configuration overview 154
Basic configuration quick-start checklist 155
Reconfiguring Avaya SBCE 156
Enabling interfaces 157
Backup and restore 157
Designating a Snapshot Server 157

Creating system snapshots 159
Restoration of a system snapshot 160
Retrieving a snapshot file 161
Restoring a snapshot file using Restore by File option 161
Deleting a system snapshot 163
Configuring automatic snapshots 163
Creating a configurable snapshot 166
Restoring portable snapshots 166
Management of deployed Avaya SBCE security devices 167
Shutting down an Avaya SBCE security device 168
Restarting an Avaya SBCE application 168
Rebooting an Avaya SBCE security device 168
Swapping Avaya SBCE devices in HA pair deployment 169
Swapping a Avaya SBCE device in single server deployment 170
Swapping an EMS server in single server deployment 170
Swapping a primary EMS server in HA pair deployment 171
Swapping a secondary EMS server in HA pair deployment 172
Viewing device configuration 173
Editing device configuration 173
Deleting device configuration 174
Upgrading system management 174
Enabling High Availability 175
Managing Avaya SBCE logging level 176
Debugging field descriptions 176
Advanced Options configuration 178
Advanced Options field descriptions 178
Security feature control 182
Managing SIP options 183
Allowing reuse of the same IP 184
Managing port options 184
Monitoring RTCP 186
Configuring HA Heartbeat Interval and Max Retries 186
Global Parameters overview 187
Adding a new RADIUS server 187
Editing an existing RADIUS server 188
Deleting an existing RADIUS server 189
Media Forking overview (Standard Platform only) 189
Adding a Media Forking profile (Standard Platform only) 190
Adding Media Forking Profile to Session Policy (Standard Platform only) 191
MAC-based LDAP authentication 192
LDAP Server Profile 192
Creating a new LDAP server 193
Editing an existing LDAP server 194

Renaming an LDAP server ... 194
Cloning an existing LDAP server ... 195
Deleting an LDAP server ... 195
SNMP settings ... 196
Uploading a cadf file to System Manager ... 196
SNMP v3 ... 197
Creating an SNMP trap profile ... 200
Adding a management server ... 202
Enabling and disabling traps by severity ... 203
Time of Day (ToD) rules ... 204
Creating a new Time of Day rule ... 204
Cloning an existing Time of Day rule ... 205
Editing an existing Time of Day rule ... 206
Renaming an existing Time of Day rule ... 206
Deleting an existing Time of Day rule ... 207
Routing profiles ... 207
LDAP based call routing ... 207
Load balancing ... 208
Creating a new routing profile ... 209
Routing rule management ... 212
Cloning an existing routing profile ... 214
Renaming an existing routing profile ... 215
Deleting an existing routing profile ... 215
Syslog parameter management ... 216
Selecting log levels ... 216
Syslog management field descriptions ... 217
User agents (Advanced Services only) ... 220
Adding a new user agent (Advanced Services only) ... 220
Editing an existing user agent (Advanced Services only) ... 220
Viewing authorized user agents (Advanced Services only) ... 221
Deleting an existing user agent (Advanced Services only) ... 221
Managing device-specific settings ... 221
Adding a new signaling interface ... 222
Editing an existing signaling interface ... 223
Viewing an existing signaling interface ... 223
Deleting an existing signaling interface ... 223
Adding a new media interface ... 224
Editing an existing media interface ... 225
Viewing an existing media interface ... 225
Deleting an existing media interface ... 226
Chapter 7: Security Configuration ... 227
Overview ... 227
System wide single endpoint DoS configurations ... 227

Domain DoS configurations ... 227
SIP server DoS configuration ... 227
DoS Security features ... 228
Viewing DoS/DDoS settings ... 228
Editing DoS/DDoS settings ... 231
Domain DoS profiles ... 232
Adding a new Domain DoS profile ... 232
Viewing a Domain DoS profile ... 234
Cloning an existing Domain DoS profile ... 235
Renaming an existing Domain DoS profile ... 235
Editing an existing Domain DoS profile ... 236
Deleting a Domain DoS profile ... 236
Setting learned DoS parameters ... 237
DoS Learning field descriptions ... 237
Protocol scrubber ... 238
Scrubber package file path ... 238
Viewing scrubber rules ... 239
Installing a scrubber rules package ... 239
Enabling or disabling an installed Scrubber Rules package ... 240
Deleting a Scrubber Rules package ... 240
Configuring scrubber actions ... 240
Creating a new Topology Hiding profile ... 241
Topology Hiding Profiles field descriptions ... 242
Renaming a Topology Hiding profile ... 243
Cloning a Topology Hiding profile ... 244
Deleting a Topology Hiding profile ... 244
Adding a new Topology Hiding header ... 245
Editing a Topology Hiding Header ... 245
Deleting a Topology Hiding header ... 246
Headers affected by Topology Hiding ... 246
Topology Hiding headers ... 247
Topology Hiding settings examples ... 248
Chapter 8: Server and Network Interface configuration ... 253
Overview ... 253
SIP Server Configuration Profile management ... 253
Adding a new SIP Server profile ... 253
Viewing a SIP Server profile ... 261
Editing a SIP Server profile ... 261
Cloning an existing SIP Server profile ... 262
Renaming an existing SIP Server profile ... 262
Deleting an existing SIP Server profile ... 262
DoS Whitelist ... 263
Editing and recalculating the DoS Protection parameters ... 264

Server interworking..... 264
Adding a new Interworking profile..... 264
Viewing existing Server Interworking profiles..... 272
Editing the Server Interworking profile parameters..... 272
Cloning a Interworking profile..... 272
Renaming an existing Interworking profile..... 273
Deleting an Interworking profile..... 273
Adding a new URI Manipulation rule..... 273
Editing an existing URI Manipulation rule..... 274
Deleting an existing URI Manipulation rule..... 274
Adding a new Header Manipulation rule..... 274
Editing a Header Manipulation rule..... 275
Deleting a Header Manipulation rule..... 275
Networks and interfaces management..... 276
Adding a new network interface..... 276
Virtual LAN..... 277
Changing the administrative state of an interface..... 278
Deleting an existing interface..... 278
Viewing an existing interface or network..... 279
Adding a new network..... 279
Editing network management parameters..... 279
Chapter 9: TLS Management..... 281
TLS Parameter Management..... 281
Certificate Management..... 281
Installing third-party certificates..... 282
Creating a certificate signing request..... 282
Settings for externally generated CSRs..... 283
Extracting a certificate and key from a PFX or PKCS#12 keystore..... 283
Certificates..... 284
Installing certificates..... 284
Uploading certificate file..... 285
Viewing certificate details..... 286
Deleting certificates..... 286
TLS Certificates screen field descriptions..... 287
Certificate Authority certificates..... 289
Installing CA certificate..... 289
Viewing Certificate Authority details..... 290
Deleting Certificate Authority certificates..... 290
Install CA Certificate screen field descriptions..... 291
Certificate Revocation Lists..... 291
Installing Certificate Revocation List..... 291
Viewing Certificate Revocation List details..... 292
Deleting Certificate Revocation Lists..... 292

Install CRL screen field descriptions..... 292
TLS Profile Management..... 293
Client Profile Management..... 293
Creating a client profile..... 293
TLS client profile screen field descriptions..... 294
Editing a Client Profile..... 296
Deleting a client profile..... 296
Server Profile Management..... 297
Creating a new TLS server profile..... 297
TLS server profile screen field descriptions..... 298
Editing a server profile..... 300
Deleting a server profile..... 300
Checklist for establishing end-to-end TLS communications..... 301
Considerations for working with TLS..... 304
Converting a certificate to PEM format..... 304
Extended hostname validation..... 305
SNI Group..... 305
Creating a new SNI group..... 306
Renaming an SNI group..... 306
Cloning an existing SNI group..... 307
Deleting an SNI group..... 307
Chapter 10: System Monitoring..... 309
Dashboard..... 309
Dashboard content descriptions..... 309
Manage system alarms..... 310
Viewing current system alarms..... 310
Clearing system alarms..... 311
Viewing system incidents..... 311
Incident Viewer field descriptions..... 312
Viewing system SIP statistics..... 315
Statistics Viewer field descriptions..... 315
Viewing periodic statistics..... 318
Periodic statistics field descriptions..... 319
Real Time SIP Server Status..... 320
Configuring Avaya SBCE for Real Time Trunk status..... 320
Viewing the status of the SIP servers..... 321
Server Status field descriptions..... 321
User registration..... 321
Viewing the list of registered users..... 322
User Registrations field description..... 322
Viewing system logs..... 323
Syslog Viewer field descriptions..... 324
Viewing audit logs..... 325

Audit Logs field descriptions ... 326
Viewing diagnostics results ... 327
Diagnostics field descriptions ... 327
Viewing administrative users ... 328
Active Users field descriptions ... 329
Trace ... 329
Configuring Packet Capture ... 329
Trace field descriptions ... 330
Logs collection ... 331
Collecting and downloading logs ... 331
Collect logs field descriptions ... 332
Collect Archive field descriptions ... 332
Chapter 11: Avaya SBCE CLI commands ... 333
Overview ... 333
Configuring Avaya SBCE for HA deployment using CLI ... 333
Configuring Avaya SBCE for single server deployment using CLI ... 334
traceSBC commands ... 334
sbceinfo commands ... 335
Running clipcs commands ... 336
Instance commands ... 338
Avaya SBCE reconfiguration script options ... 338
Enabling or disabling network interfaces using CLI ... 340
Editing SIP server profile parameters using CLI ... 340
Editing network management parameters using CLI ... 340
Creating and restoring configurable snapshot using CLI ... 341
Changing management IP, gateway and network mask details for a single server deployment ... 341
Changing management IP for an HA deployment ... 341
Changing hostname ... 343
Changing network passphrase ... 344
Regenerating self-signed certificates ... 344
Changing DNS IP and FQDN ... 344
Enabling or disabling network interfaces using CLI ... 344
Accessing Avaya SBCE ... 345
Chapter 12: Configuring Avaya Session Border Controller for Enterprise for Avaya Aura® Remote Worker ... 348
Remote worker overview ... 348
Limitation for registering Remote Workers ... 350
Session Manager configuration for Avaya SBCE ... 350
Remote worker configuration checklist ... 352
Cloning Avaya-ru profile ... 353
Creating an Avaya call server profile ... 353
Creating an external signaling interface for a phone network ... 355

Creating an internal signaling interface for an Avaya call server 356
Add Signaling Interface field descriptions 356
Creating an external media interface for a phone network 357
Creating an internal media interface for an Avaya call server 358
Add Media Interface field descriptions 358
Creating PPM Mapping Profile for Session Manager 359
PPM Mapping Profile field descriptions 360
Creating Reverse Proxy Policy 361
Reverse Proxy Policy field descriptions 361
Creating a reverse proxy service for PPM traffic 362
Creating a reverse proxy service for file or firmware download 363
Creating reverse proxy service for multi-tenant or IPO powered 365
Relay Services field descriptions 366
Creating a media rule 370
Creating application rules 370
Creating an endpoint policy group 371
Creating a routing profile towards Avaya Aura® call server 372
Creating a server flow 373
Creating a subscriber flow 374
Configuring application relay for IM 375
Checklist for configuring Presence server 376
Creating PPM mapping profile for presence server 377
Monitoring RTCP for a single Session Manager deployment 378
Application relay settings for RTCP monitoring using single Session Manager 378
Configuring Avaya SBCE to support emergency calls from unregistered endpoints 379
Checklist for back-to-back configuration with a single Session Manager 380
Checklist for back-to-back-to-back configuration with a single Session Manager 381
Monitoring RTCP for back-to-back-to-back deployment 383
Application relay settings for monitoring RTCP using back-to-back-to-back deployment 384

Chapter 13: Multiple Session Manager support for Avaya SBCE in Remote Worker deployment 385

Multiple Session Manager configuration checklist 386
Configuring the Avaya SBCE IP addresses corresponding to the primary and secondary Session Managers 388
Creating a server interworking profile 388
Configuring application relay settings for multiple Session Manager 389
Multiple Session Manager support with back-to-back Avaya SBCEs 389
Back-to-back configuration checklist 390
Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBCEs 391
Back-to-back-to-back configuration checklist 392
Geographic-redundant deployment 394
Geographic-redundant deployment in the non-HA mode 394
Geographic-redundant deployment in the HA mode 395

Checklist for configuring Geographic-redundant deployment..... 395
Creating PPM Mapping Profile for Session Manager..... 397
Creating an endpoint policy..... 399
Configuring Presence Server..... 400
Configuring PPM settings on Session Manager..... 400
Configuring Avaya SBCE for web collaboration..... 400
Chapter 14: Configuration of Server flows for SIP Trunking..... 402
SIP Trunking overview..... 402
Generic Avaya SBCE SIP trunk configuration checklist..... 403
Creating Interworking Profiles..... 404
Creating Server Profile for Call Server..... 405
Creating Server Profile for Trunk-side server..... 406
Creating Routing Profile for Call Server..... 407
Creating Routing Profile for Trunk Server..... 408
Creating a Topology Hiding profile..... 410
Creating external signaling interface toward Trunk-side server..... 411
Creating Internal Signaling Interface toward Call Server..... 412
Creating External Media Interface toward Trunk Server..... 413
Creating Internal Media Interface toward call server..... 413
Creating call server flow..... 414
Creating trunk server flow..... 415
Configuring Avaya SBCE for SIP Trunk..... 416
Configuring Avaya SBCE for other trunks..... 417
Chapter 15: Signaling Manipulation..... 418
Signaling manipulation..... 418
SigMa scripting language..... 418
SigMa primer..... 419
SigMa Scripting examples..... 426
SigMa Scripting Tutorial..... 429
Signaling Manipulation Scripts field descriptions..... 435
Sigma Design Overview..... 436
Specifying a SigMa script in a server configuration..... 436
Chapter 16: Remote access..... 438
Chapter 17: Video devices interoperability configuration..... 439
Binary Floor Control Protocol..... 439
Administering Binary Floor Control Protocol..... 439
SRTP overview..... 440
Considerations for SRTP after failover..... 440
Forward Error Correction..... 440
Far End Camera Control..... 441
Administering Far End Camera Control..... 441
Chapter 18: WebRTC-enabled call processing..... 442
WebRTC-enabled call handling..... 442

WebRTC considerations ... 442
Turntop ... 443
Configuring the TURN/STUN profile for WebRTC calls in Avaya SBCE ... 443
Configuring the TURN relay service for WebRTC calls in Avaya SBCE ... 445
Chapter 19: Avaya SBCE configuration for SIPREC integration ... 447
Checklist for configuring Avaya SBCE for SIPREC ... 447
Configuring a Recording Server ... 449
Enabling UCID for the signaling rules used on the Session Manager endpoint policy group ... 450
Creating a media rule for the Recording Server ... 451
Creating a new session policy for the Recording Server ... 452
Adding a custom wave file for the recording tone ... 453
Adding a session flow for the Recording Server ... 454
Chapter 20: Secure Client Enablement Services proxy configuration ... 455
Client Enablement Services CA certificate ... 455
Extracting the Client Enablement Services CA certificate ... 455
Creating a client TLS profile ... 456
Configuring CES proxy ... 457
Chapter 21: Avaya SBCE configuration for Call Preservation ... 459
Checklist for configuring Avaya SBCE for Call preservation ... 460
Creating FGDN groups ... 460
FGDN Group field descriptions ... 461
Enabling FGDN for a Session Manager in the FGDN group ... 461
Creating a routing rule for Call preservation ... 462
Adding the routing rule to the trunk server flow ... 462
Changing transaction expiry time in Server Interworking ... 463
Chapter 22: Avaya Aura® SIP Resiliency ... 464
Enabling SIP Resiliency ... 464
Chapter 23: Avaya SBCE configuration for transcoding and transrating ... 466
Checklist for configuring Avaya SBCE for transcoding ... 466
Enabling transcoding and transrating ... 467
Administering codec prioritization ... 467
Configuring endpoint policy group ... 468
Configuring a server flow for transcoding ... 468
Chapter 24: CDR measurement and media statistics ... 470
Creating a CDR adjunct ... 470
CDR adjunct field descriptions ... 471
Creating a Radius profile ... 471
Radius profile field descriptions ... 472
Enabling CDR in an application ... 473
Enabling periodic statistics ... 473
Chapter 25: Media tunneling ... 475
Media tunneling checklist ... 475

Enabling media tunneling..... 476
Disabling media tunneling..... 476
Adding a media interface..... 476
Creating a server profile..... 477
Chapter 26: Avaya SBCE configuration for Avaya Aura® Media Server offboarding..... 478
Checklist for configuring external media server..... 478
Enabling Avaya Aura® Media Server offboarding..... 479
Configuring a media server..... 479
Creating a session policy for a media server..... 480
Adding a session flow..... 481
Chapter 27: Resources..... 482
Documentation..... 482
Finding documents on the Avaya Support website..... 483
Accessing the port matrix document..... 483
Avaya Documentation Portal navigation..... 484
Training..... 485
Viewing Avaya Mentor videos..... 485
Support..... 486
Appendix A: Solution for simultaneous downloads of config and firmware files..... 487
Simultaneous downloads of config/firmware files..... 487
GROUP identifier in endpoint administration..... 487
File server configuration example..... 488
Phone configuration..... 489
Configuring Avaya SBCE..... 489
Appendix B: Configuring Avaya SBCE for interoperability with Avaya Multimedia Messaging..... 491
Appendix C: EMS web interface..... 492
EMS screen elements..... 492
Tool bar field descriptions..... 493
Display settings field descriptions..... 494
Application pane..... 494
Dashboard screen content area..... 494
Task pane..... 495
EMS web interface button descriptions..... 504
Appendix D: CDR file field descriptions..... 506
Glossary..... 513

Chapter 1: Introduction

Purpose

This document contains information about administering and configuring Avaya Session Border Controller for Enterprise (Avaya SBCE).

This document provides information about how to use the Unified Communications Policies features, also referred as Domain Policies, of Avaya SBCE. 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 SBCE.

Change history

Issue	Date	Summary of changes
1	February 2019	Release 8.0 document
2	March 2019	Updated Geographic-redundant deployment topic
3	July 2019	• Removed the option of Next Hop In-Dialog from Creating a routing profile towards Avaya Aura® Call Server topic. • Added a note in Add routing profile field descriptions topic for Next Hop In-Dialog option.
4	August 2019	Updated the document for following Release 8.0.1 changes: • Added CAF-0251 in “Restoration of a system snapshot” section. • Added a new field of Received Server Host in “Relay Services field descriptions” section.

Warranty

Avaya provides a one-year limited warranty on Avaya SBCE hardware and 90 days on Avaya SBCE software. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the support details for Avaya SBCE in the warranty period is available on the Avaya Support website http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Overview

Avaya Session Border Controller for Enterprise (Avaya SBCE) is a UC network security solution. You can administer Avaya SBCE by using the Element Management System (EMS) web interface.

Avaya SBCE supports following redundancy options:

- Stand-alone
- Geo - redundant
- High Availability
- Geo + HA

Manage Avaya SBCE security devices

Avaya SBCE security devices can be monitored and controlled either remotely through Graphical User Interface (GUI) or locally through Command Line Interface (CLI). The GUI access is provided by Ethernet management interface ports that are located on each Avaya SBCE equipment chassis. With Ethernet management interface ports, administrators can have 10 simultaneous log-ons to the EMS web interface. CLI access is provided by the console port or vga port based on the parameter chosen during install or upgrade. The ports are located on the Avaya SBCE equipment chassis. With console ports, administrators can establish direct, physical connections to the devices by using any commonly available terminal device for provisioning, management, troubleshooting, maintenance, and repair. You can gain access to the GUI and CLI interfaces any time when an Avaya SBCE security device is operational. Also, CLI access can be achieved remotely by ssh into the EMS or SBC server using port 222.

Graphical User Interface

Avaya SBCE 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 SBCE device.

Command Line Interface

Command Line Interface (CLI) is a management interface that provides local access to a particular Avaya SBCE 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. CLI is available whenever an Avaya SBCE 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 on 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 of the EMS server.
3. Press `Enter`.

   The system displays the Session Border Controller for Enterprise screen.
4. In the **Username** field, type the user name.
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**.

   The system displays the Dashboard screen.

Passwords

Two types of passwords are associated with Avaya SBCE:

- Console and SSH password
- Element Management System (EMS) GUI password

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 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 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.

Password policies

The root and ipcs passwords are determined and set during product installation.The EMS GUI has a separate password. When you log in for the first time after installation, the system prompts you to create a new password for accessing the EMS GUI. The default user ID and password is `ucsec`.

Password restrictions are enforced on the ucsec and ipcs accounts. The new password must meet the password criteria of minimum 8 characters, including:

- One uppercase letter, one lowercase letter, and one number.
- One special character from the hyphen (-), underscore (_), at sign (@), asterisk (*), and exclamation point (!).You must not use the number sign (#), dollar sign ($), and ampersand (&).

Note:

The customer network administrator determines the Avaya SBCE CLI root and ipcs passwords during the installation procedure. Two installation steps prompt the installer to enter a chosen password.

Chapter 3: Administrative User Accounts

Administrative accounts

You can create the following types of administrative user accounts:

- System Administrator

  The System Administrator user accounts have full read/write permission for the Avaya SBCE security device features, which includes adding, editing, and deleting other administrative accounts.

- Service Administrator

  The Service Administrator user accounts have the same privileges as the System Administrator user accounts. However, Service Administrator user account users cannot add new accounts. Service Administrator user accounts can only view TLS and Firewall settings.

- Auditor

  The Auditor user accounts have read privileges for viewing incidence and statistical logs only.

- Security Administrator

  The Security Administrator user accounts can manage only system users, TLS, and firewall settings.

- Backup Administrator

  The Backup Administrator user accounts can create or restore snapshots.

- Avaya Services Administrator

  The Avaya Services Administrator is a default role for EASG administrators. The privileges are similar to System Administrator accounts.

- FIPS 140-2 Crypto Officer

  The FIPS 140-2 Crypto Officer user accounts can only view and manage TLS settings.

- Avaya Services Maint. and Support

  The Avaya Services Maint. and Support is a default role for ASG support users. The privileges are similar to Auditor accounts.

Use the Administration feature to create, edit, and delete administrative user accounts.

Creating a new administrative 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 **Add User**.

   The EMS server displays the Add User window.
5. Enter the required information in the appropriate fields and click **Finish**.

Result

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

Related links

Add user field descriptions on page 25

Add user field descriptions

Name	Description
User Name	The system name assigned to the owner of this account.
Real Name	The real name of the individual for whom this account is being created.
Contact Information	The contact information, for example, email and phone number of the owner of this account.
Type	The types of users. The options are: • **Local**: A normal, locally authenticated user. • **RADIUS**: A user authenticated through a remote RADIUS server. This option shows only if a RADIUS server is configured and RADIUS is enabled on the **Administration Parameters** tab. • **ASG**: A user authenticated through ASG. You cannot manually choose this option .
Password	The login password being assigned to this account. Clear the **RADIUS User** check box to activate this field.
Confirm Password	A reliability feature to ensure that the correct password has been entered in the previous field. Only activated if in the **Type** field, **RADIUS** user type is not selected. Do not select **RADIUS** user type in the **Type** field to activate this feature.
Force Password Change on Next Login	An option to determine whether the system forces a password change when the user logs in the next time.

Table continues…

Name	Description
Role	The level of administrative access to be granted to this account. The options are: • **System Administrator**: Get full read/write permission for the Avaya SBCE security device features, which includes adding, editing, and deleting other administrative accounts. • **Service Administrator**: Can only view TLS and Firewall settings and cannot add new accounts. • **Auditor**: Get read privileges for viewing incidence and statistical logs only. • **Security Administrator**: Can manage only system users, TLS, and firewall settings. • **FIPS 140–2 Crypto Officer**: Can only view and manage TLS settings. • **Backup Administrator**: Can create or restore snapshots. The default value in the **Role** field is **System Administrator**. You can change this value to add users with different roles.
Status	The options are: • **Normal** • **Disabled** • **Locked** You cannot change the status of the user to Locked. The EMS server displays the status of a user as Locked only when the user has been locked out after unsuccessful login attempts. **Note:** Disabling a user account or changing the role of a user account disconnects all clients connected to that user account.

Editing an administrative 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 **Edit** for a user account.
   a. In the Edit User window, edit information in the required fields.
   b. Click **Finish**.

Related links

Add user field descriptions on page 25

Deleting an administrative 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**.

Setting administrative account privileges

About this task

Use this procedure to configure administration parameters for the following user accounts:

- Administrator
- Manager
- Supervisor

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 **Settings** tab, enter the required information.
5. Click **Save**.

Result

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

Related links

System Administration field descriptions on page 28

Configuring the RADIUS server

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** > **AAA**.
4. On the **RADIUS** tab, select the **RADIUS Server** check box to enable the already configured RADIUS server profile.
5. Click **Save**.

Enhanced Access Security Gateway

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 SBCE 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 SBCE 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 .

System Administration field descriptions

Name	Description
Users tab	
User Name	The system name assigned to the owner of this account.
Real Name	The real name of the individual for whom this account is being created.
Contact Information	The contact information, for example, email and phone number of the owner of this account.

Table continues…

Name	Description
Type	The user type. The options are: • **Local**: A normal, locally authenticated user. • **RADIUS**: A user authenticated through a remote RADIUS server. This option is displayed only if a RADIUS server is configured and RADIUS is enabled on the **Administration Parameters** tab. • **ASG**: A user authenticated through ASG. You cannot select this option manually.
Role	The level of administrative access available for this account. The options are: • **System Administrator**: The highest level of system access with full read and write permissions for all screens and features. With this role, you can create and delete new user accounts. • **Service Administrator**: With this role, you can create other logins, modify or assign roles, install licenses, and install PKI certificate and keys. • **Security Administrator** • **FIPS 140–2 Crypto Officer** • **Auditor**: This role provides read only access to the system. You cannot run any commands. • **Backup Administrator**: With this role, you can perform backup and restores.
Settings Tab	
Local Account Password Expiration (days)	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 (days)	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.
RADIUS Tab	
Radius Server	A check box indicating whether RADIUS user accounts must be authenticated. If selected, RADIUS user accounts are authenticated by the RADIUS server selected from the corresponding drop-down menu. If cleared, RADIUS user accounts are not authenticated.
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.
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.
EASG Tab	
Enable	Displays if EASG is currently disabled.
Disable	Displays when EASG is currently enabled.

Chapter 4: Device Configuration

Prerequisites

To ensure successful device configuration, you must first ensure that Avaya SBCE is installed and functional. For more information, see *Deploying Avaya Session Border Controller*.

Adding an Avaya SBCE device

About this task

Use the following procedure to add one or more Avaya SBCE devices.

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. On the Add Device page, enter the **Host Name** and the **Management IP** address of the Avaya SBCE devices.

   Note:

   Ensure that the host names of the devices are unique.
5. **(Optional)** If the device you add must support high availability, select the **High Availability** check box and enter details in the following fields:
   - **Host Name for second Node**
   - **Management IP for second Node**
6. Click **Finish**.

Result

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

Device Management field descriptions

Devices tab

Name	Description
Device Name	The name of the EMS or Avaya SBCE device.
Management IP	The management IP address of the device.
Version	The version of Avaya SBCE.
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.

Licensing tab

Name	Description
Use Local WebLM Server	An option to use a local WebLM server. Virtualized EMSes cannot run on a local WebLM server.
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	A value that determines the reserved or unreserved status of licenses according to usage. If there is a need to acquire more licenses, Avaya SBCE uses the fetch count to determine how many licenses must be acquired. Similarly, if usage decreases, Avaya SBCE reducing the number of licenses matching the fetch count. This value cannot be 0.

Table continues…

Name	Description
Low Watermark	The percentage of free licenses available with Avaya SBCE for a feature. If the number of licenses available decreases below the Low Watermark, Avaya SBCE requests for more licenses. The low watermark cannot be more than 50%. For example, Avaya SBCE might have 500 licenses reserved, with 20% Low Watermark, and Fetch Count 50. In this case, Avaya SBCE monitors when the number of free licenses reduces to less than 20% of 50, that is 10. At the 491st acquired request, Avaya SBCE requests more licenses with a fetch count.
High Watermark	The percentage of free licenses available with Avaya SBCE for a feature, exceeding which Avaya SBCE releases the licenses.If the number of licenses available increases beyond the High Watermark, Avaya SBCE releases the excess licenses. The high watermark cannot be less than 50%. For example, Avaya SBCE has 500 licenses reserved, with 40% High Watermark, and Fetch Count 50. Avaya SBCE monitors when the license usage increases to more than 40% and releases licenses equal to the fetch count, that is 50. Therefore, if free licenses increase to more than 200, that is, 40% of 500, Avaya SBCE releases 50 licenses.

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.

Using pooled licensing

Before you begin

Install a license in WebLM for the pooled licensing feature.

About this task

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with

multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.
3. Click the **Licensing** tab.
4. 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.
5. Click **Save**.

Commissioning an Avaya SBCE device

About this task

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

You can identify the Avaya SBCE 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 SBCE 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, complete the required fields.

   For more information , see Installation Wizard field descriptions.
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 Avaya SBCE.
11. Provide an appliance name for the Avaya SBCE 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.

Installation Wizard field descriptions

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

Name	Description
Device Configuration	
Appliance Name	A descriptive name assigned to the Avaya SBCE security device being provisioned. This name is subsequently used as the device host name.
High Availability	A check box indicating that the Avaya SBCE 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.

Table continues…

Name	Description
Secondary	The IP address of the secondary DNS server.
License Allocation	
Standard Sessions	The number of standard sessions for the device.
Advanced Sessions	The number of advanced sessions for the device.
Scopia Video Sessions	The number of Scopia video sessions for the device.
CES Sessions	The number of Client Enablement Services (CES) proxy sessions for the device.
Transcoding Sessions	The number of transcoding sessions for the device.
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 SBCE device.
Interface	The physical interface of the Avaya SBCE 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 for Enterprise*.
Network Configuration	
IP	The IP address of the Avaya SBCE device that is being configured.
Public IP	The IP address used by the Avaya SBCE 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 SBCE 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

Edit device field descriptions on page 37

Edit device field descriptions

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

Name	Description
General Settings	
Appliance Name	A descriptive name assigned to the Avaya SBCE 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 SBCE 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 SBCE 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 SBCE device.
Netmask	The subnet mask of the Avaya SBCE device.
Gateway	The default gateway address.
IPv4 Network Settings	
Management IP	Management IP address of the Avaya SBCE device.
Network Prefix and Subnet Mask	The subnet mask of the Avaya SBCE device.
Gateway	The default gateway address.
Dynamic License Settings	
Standard Sessions	The number of standard sessions for the device.
Advanced Sessions	The number of advanced sessions for the device.
Scopia Video Sessions	The number of Scopia video sessions for the device.
CES Sessions	The number of Client Enablement Services (CES) proxy sessions for the device.
Transcoding Sessions	The number of transcoding sessions for the device.

Table continues…

Name	Description
CLID	A five-digit number indicating the centralized licensing ID.
Encryption	The encryption field. The default value is **Yes**.

Related links

Installation Wizard field descriptions on page 35

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 SBCE 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 SBCE connected to the EMS.

High Availability failovers

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

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

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE 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 SBCE, with a router or L3 switch. If you do not put the Avaya SBCE 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 SBCE.

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

Peer node unavailable: If a peer node is unavailable, the currently active or running Avaya SBCE becomes the primary Avaya SBCE. The active Avaya SBCE 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 SBCE compares its active links with the number of active links for the peer Avaya SBCE. When the primary SBCE detects that the secondary SBCE has more active links, the secondary Avaya SBCE takes over as the new primary Avaya SBCE. Failovers are not initiated for M1 and M2 link failures.

Note:

Before Avaya SBCE Release 6.3, inbound and outbound physical ports or single wire modes were configured for Avaya SBCE. If any physical link failed in these modes, Avaya SBCE failed over because the system cannot serve calls with a single link or when links are unavailable.

Avaya SBCE 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 SBCE is down, but the secondary Avaya SBCE also has the same number of links active, failover is not required.

Avaya SBCE 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 SBCE 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.

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 SBCE security functionality is provided continuously, regardless of any hardware or software failures. High availability requires a minimum of two Avaya SBCE 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. In the navigation pane, click **Device Management**.
3. On the Device Management page, click **Add**.
4. In the **Host 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 **Host Name for second Node** field, type the name of the device to which the Avaya SBCE 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 SBCE device on page 31

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 SBCE is active and handling call traffic.
Secondary	Avaya SBCE is inactive and in stand-by mode.
Down	The Primary SBC detects that Avaya SBCE 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 SBCE is going through the initialization procedure.
HAElection	Avaya SBCE is determining whether to go into active or standby mode.
Synchronizing	Avaya SBCE is replicating data from the other SBC.
Unconfigured	Avaya SBCE is configured as an HA device but not yet received the configuration from EMS.
Unknown	EMS does not recognize the HA status Avaya SBCE 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 for Enterprise*.

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 SBCE. 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 SBCE 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 only when you want 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 SBCE/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 SBCE (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 for Enterprise*.

Viewing 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 pound sign (#) prompt, type `ipcs-options` .

   The CLI displays the Avaya SBC Runtime Options screen.
4. Scroll to view the TimeZone.
5. Click **Select**, and press `Enter`.

   The current time zone screen is displayed. If not, the application displays a pop-up window with a message.

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 `ipcs-options`.

   The CLI displays the Avaya SBCE Runtime Options screen.
4. Scroll to **Configure TimeZone**.
5. Click **Select**, and press `Enter`.

   The CLI displays the time zone screen.
6. Scroll down and select the correct time zone from the alphabetical list.
7. Click the **Skip** tab, and press `Enter` to accept the default GMT time zone.
8. Click **Select** and press `Enter`.

   The CLI saves the new time zone setting.

Exiting the Avaya SBC Runtime Options screen

Procedure

1. On the Runtime Options screen, click **Select**, and press **Enter**.

   The system displays the previous screen.

2. Select **Done**, and press **Enter**.

   The system displays the pound sign (#) prompt.

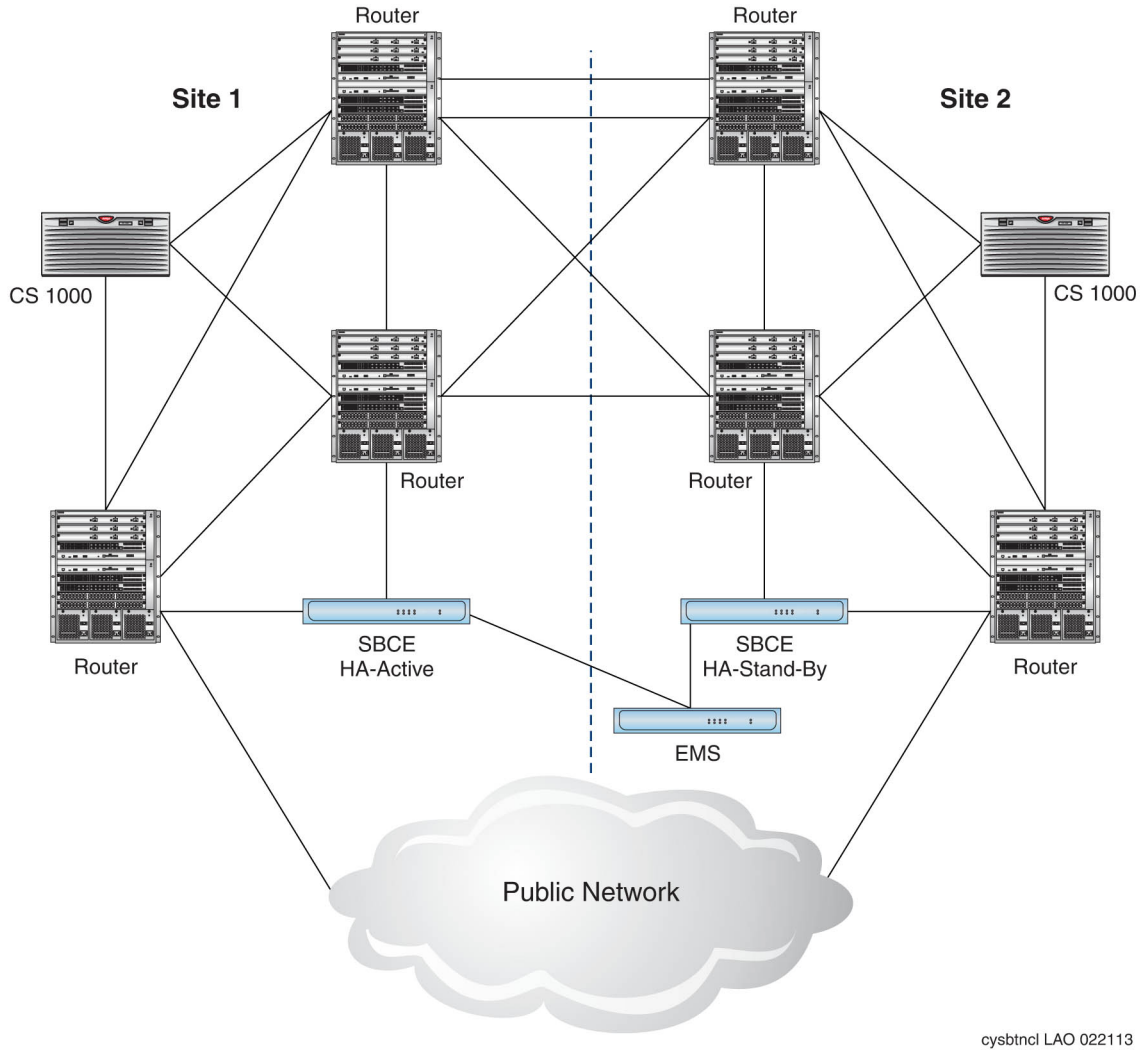
High-Availability pair geographically dispersed

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

One Avaya SBCE 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 SBCE to maintain real-time network information. If the HA Primary Avaya SBCE fails, the HA Secondary Avaya SBCE 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 SBCE device models in the HA implementation , except the Portwell Cad Avaya SBCE .

Example



Interface connections for a geographically dispersed Avaya SBCE HA pair

The following interface connections are required before deploying a geographically dispersed Avaya SBCE HA pair.

Interface	Description
EMS	

Table continues…

Interface	Description
M1 interface or management IP	EMS uses this IP to: • Communicate with the Avaya SBCE devices. • Send the database to the Avaya SBCE devices. • Check the status of the Avaya SBCE devices. • Communicate with the NTP and DNS. **Note:** M1 interface does not support IPv6 address.
Avaya SBCE	
M1 interface or management IP	Avaya SBCE 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 SBCE M1 IP is not on the same subnet as EMS M1 IP, the Avaya SBCE 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 SBCE devices. This interface does not require an IP.

In an HA pair deployment, Avaya SBCE instances use a Keep alive mechanism to check call processing module availability for the other Avaya SBCE. Keep alive interval is the duration between two keep alive requests. Maximum retries is the number of keep alive requests sent before declaring that other Avaya SBCE instance's call processing module is unavailable. You can change this value on the EMS web interface from **Network & Flows** > **Advanced Options** > **HA pairs**.

Important:

The A1 and B1 IP addresses are shared between the two Avaya SBCE devices. These IPs must be capable of routing and being handled at both sites. The IPs are swapped between the Avaya SBCE 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 SBCE interface that will now handle the IPs that were being handled by the new Secondary Avaya SBCE.

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

Deploying a geographically dispersed Avaya SBCE HA configuration

Procedure

1. Install each Avaya SBCE 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. **Host Name**
   b. **Management IP**
   c. **High Availability**
   d. **Host 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 SBCE 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 in Avaya SBCE updates RTCP packets with appropriate End Point IP and Hop Information.

Note:

RTCP monitoring feature has been renamed to RTCP monitoring relay from Release 7.2.1 and later.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE and Core Phones. RTCP MON traffic is received on Core SBCE-1 public IP-A and is sent out to the prognosis server using Core SBCE-1 private IP-A.
- Relay 2: For traffic coming from Media Gateway. RTCP MON traffic is received on core SBCE-1 private IP-A and is sent out to the prognosis server using Core SBCE-1 private IP-B.

46xx settings file configuration for RTCP monitoring

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

- SET RTCPCONT 1
- SET RTCPMON 192.168.11.105 {SBCE 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 SBCE internal signaling IP address on the System Parameter ip-options page.

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

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

Therefore, you must configure application relay RTCP monitoring in:

- Core Avaya SBCE
- Remote Avaya SBCE
- Remote user deployment

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

Configuring application relay for RTCP monitoring in core Avaya SBCE

About this task

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

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 SBCE Relay IP address / Core SBCE Private IP-A**.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE

About this task

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

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 SBCE Relay IP address / Core SBCE Private IP-A** .

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE

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 SBCE Relay IP address / DMZ SBCE Private IP-A**

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE.
Remote IP/FQDN	• Prognosis server IP address for configuring application relay for RTCP monitoring in core and DMZ Avaya SBCE. • Remote SBCE Relay IP address for configuring application relay for RTCP monitoring in remote Avaya SBCE.
Remote Port	The port number of the server IP. Remote port for configuring application relay for RTCP monitoring in core, DMZ and, remote Avaya SBCE is 5005.
Remote Transport	The transport protocol for contacting the server IP. Select **UDP** for RTCP monitoring in core, DMZ and, remote Avaya SBCE 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.
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 SBCE is 5005.
Connect IP	The IP address for communicating with the prognosis server. • Type the remote Avaya SBCE internal signaling IP for configuring application relay for RTCP monitoring in remote.Avaya SBCE. • Click the network name, and select the interface that prognosis can reach for configuring application relay for RTCP monitoring in core and DMZ.Avaya SBCE.

Table continues…

Name	Description
Listen Transport	The transport protocol used for communication between the endpoint and interface at Avaya SBCE. Select **UDP** for RTCP monitoring in core, DMZ and, remote Avaya SBCE 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 SBCE. • **Hop-by-Hop Traceroute** for configuring application relay for RTCP monitoring in DMZ Avaya SBCE.

RTCP monitoring generation support

This feature is applicable only for SIP trunks.

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

Avaya SBCE calculates Round Trip Time (RTT) based on the RTCP streams coming from a SIP trunk or from a enterprise network.

Avaya SBCE 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 RTT.

Avaya SBCE itself generates RTCP streams and calculates RTT to calculate the quality metrics. Avaya SBCE also calculates the lost packets based on the media statistics components.

Related links

Round Trip Time on page 51

Configuring RTCP monitoring generation support on page 52

Round Trip Time

Round Trip Time (RTT) or Round Trip Delay Time (RTD) 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 RTT by using the following formulae:

RTT = (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 RTD that is not provided by the network.

Related links

RTCP monitoring generation support on page 51

Configuring RTCP monitoring generation support

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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**.

Related links

RTCP monitoring generation support on page 51
RTCP Monitoring Report Generation field descriptions on page 52

RTCP Monitoring Report Generation field descriptions

Name	Description
RTCP Monitoring Report Generation	Specifies whether RTCP monitoring report generation is enabled.
SBCE Interface IP	Specifies the source IP address of Avaya SBCE for communication between Avaya SBCE and the monitoring tool. **Note:** The IP address must be the IPv4 address.
SBCE Interface Port	Specifies the source port number of Avaya SBCE for communication between Avaya SBCE 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.

Table continues…

Name	Description
Monitoring Frequency based on RTCP Report	Specifies the number of RTCP packets received from a SIP trunk after which Avaya SBCE generates the RTCP monitoring report.
Monitoring interval in absence of RTCP Report	Specifies the interval (in seconds) between two consecutive RTCP monitoring reports.

Related links

Configuring RTCP monitoring generation support on page 52

Adding a new blacklist rule

About this task

You can change the blacklist rules to prevent Avaya SBCE from accepting data from specific IP addresses. Similarly, you can set up whitelist rules to always allow data from specific IP addresses. From the firewall settings, you can also change the number of connections initiated per second for a particular type of service and prevent DoS attacks.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 by using the IP addresses and ports that you specified. Avaya SBCE blocks any data received from the source IP address and any data sent to the destination address specified in the blacklist rule.

Related links

Firewall field descriptions on page 53

Firewall field descriptions

Blacklist tab

Name	Description
Name	The name of the blacklist rule.

Table continues…

Name	Description
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** • **HTPPS** • **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 53

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 SBCE 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 SBCE 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:

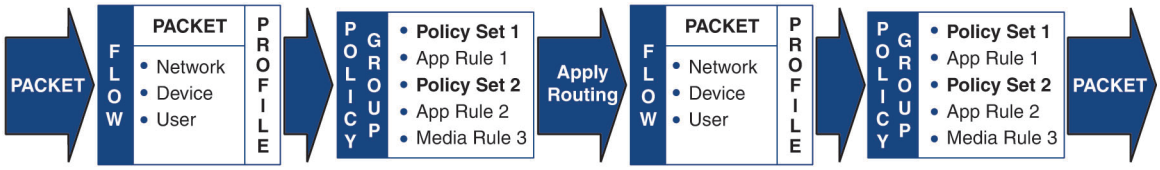
- Subscriber Flows: Identify SIP phones and users.
- Server Flows: Identify SIP servers

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 SBCE:

Example



cysbpolp LAO 021413

Example: Call server with SBCE 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 SBCE Flow.
  - between Trunk Server and Avaya SBCE 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 SBCE receives the packet.
2. Avaya SBCE determines Flow.
3. Call Server to Avaya SBCE Flow points to Call Server Policy Group. Avaya SBCE applies the policy and routes the packet to the determined destination.

4. Trunk Server to Avaya SBCE REVERSE Flow points to Trunk Server Policy Group. Avaya SBCE applies the policy.
5. Packet is sent to Trunk Server.

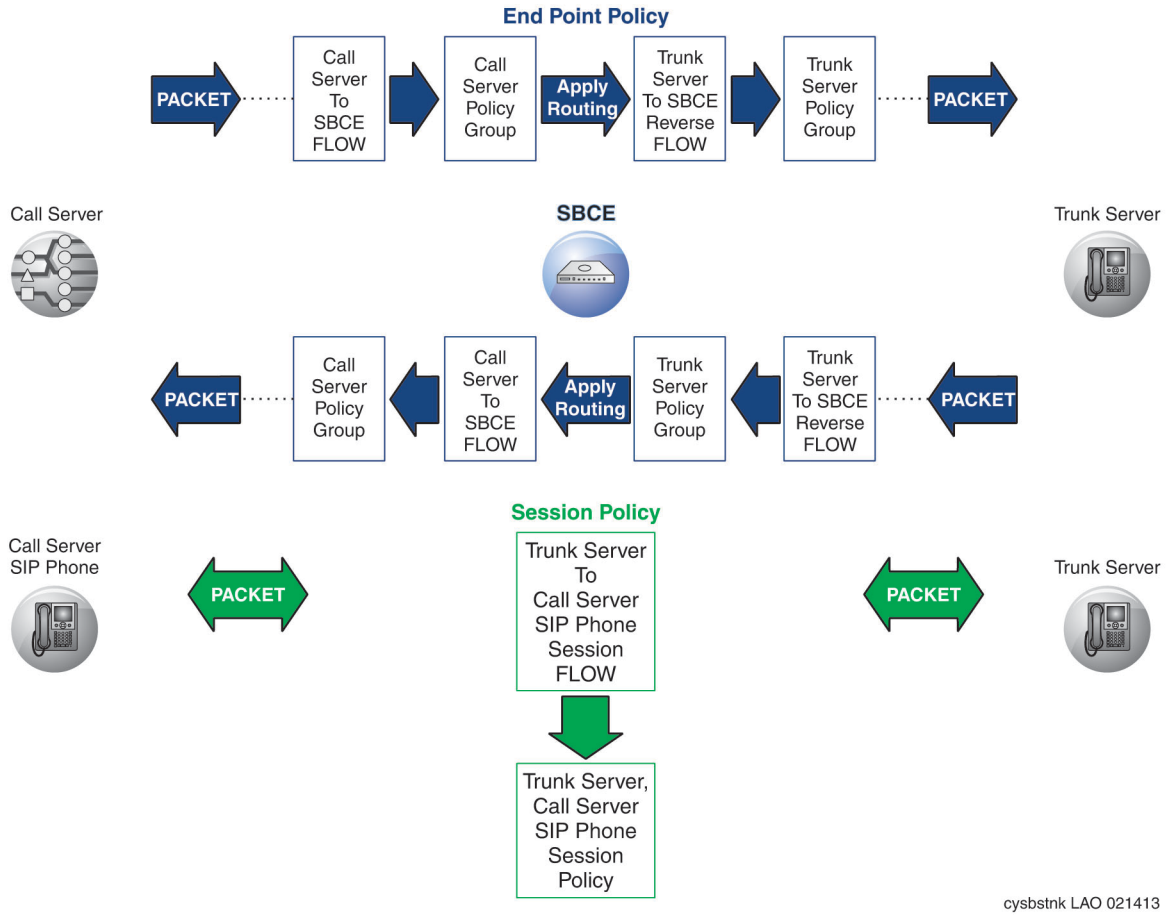
Call coming from Trunk Server

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

Session Policy

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

Example



Example: Call server with SBCE 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 SBCE Flow.
  - between SIP Phone and Avaya SBCE 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 SBCE receives the packet.
2. Avaya SBCE determines Flow.
3. Call Server to Avaya SBCE Flow points to Call Server Policy Group. Avaya SBCE applies the policy and routes the packet to the determined destination.
4. SIP Phone to Avaya SBCE REVERSE Flow points to SIP Phone Policy Group. Avaya SBCE applies the policy.
5. Packet is sent to the SIP phone.

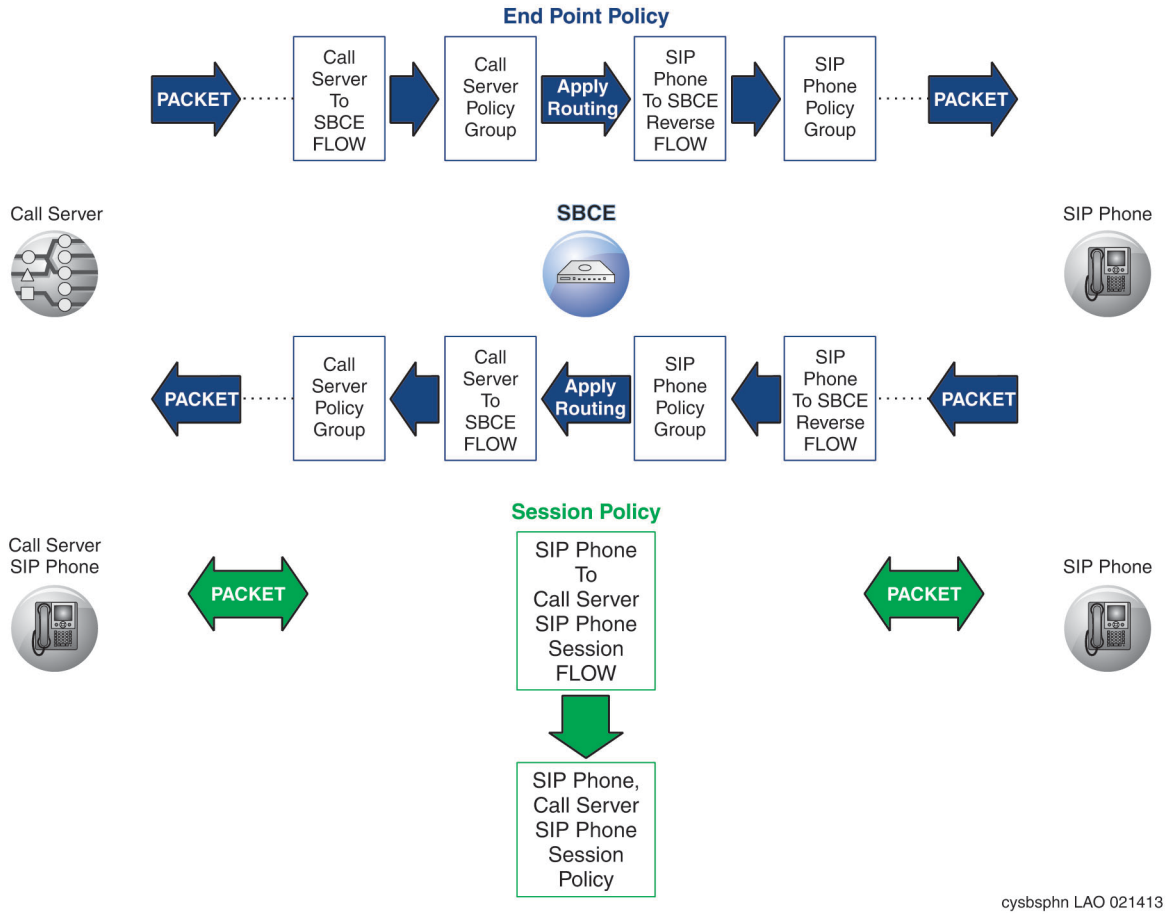
Call coming from SIP Phone

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

Session Policy

1. Avaya SBCE receives the packet.
2. Avaya SBCE determines Flow.
3. SIP Phone to Call Server SIP Phone Session Flow points to SIP Phone or Call Server SIP Phone Session Policy. Avaya SBCE 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 SBCE architecture uses a standard platform and a micro platform. The standard platform example is a single Avaya SBCE 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 SBCE 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

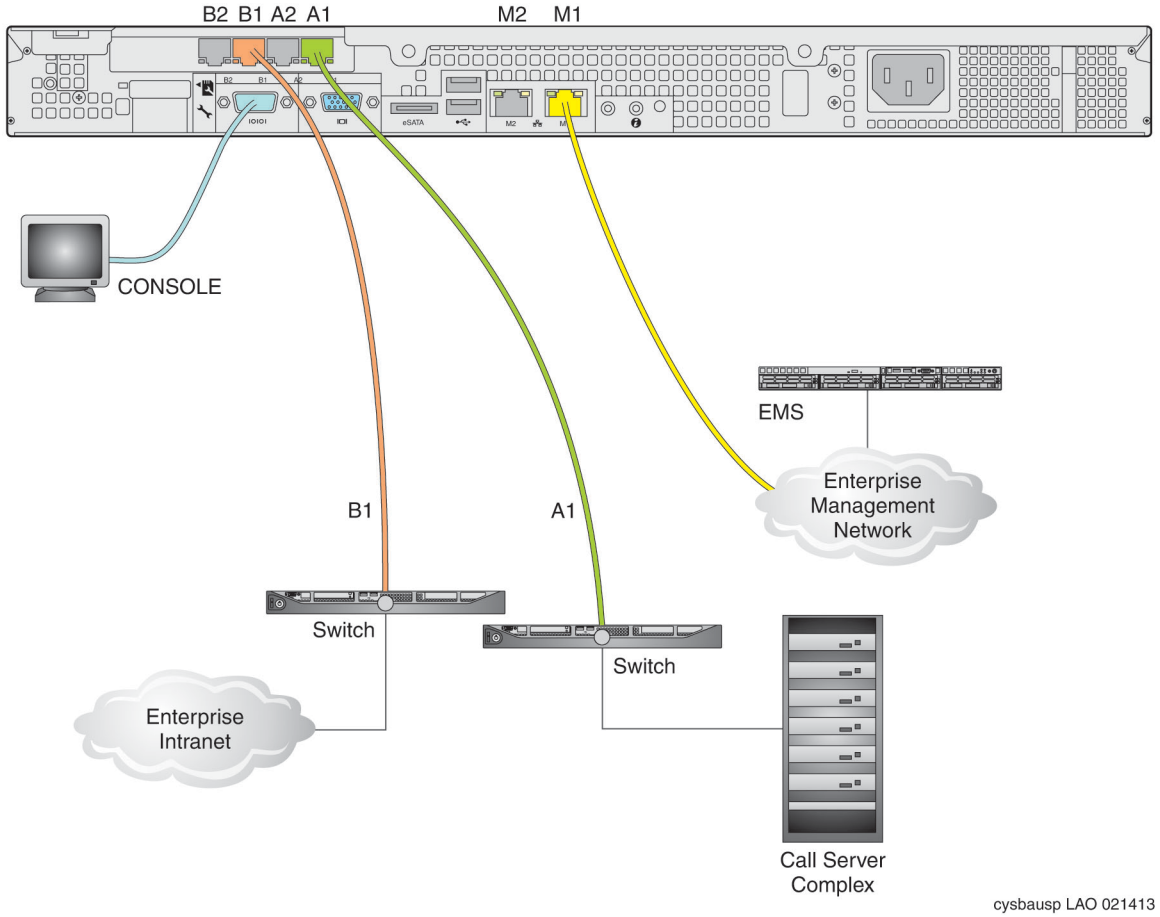


Figure 1: Avaya SBCE architecture using a standard platform

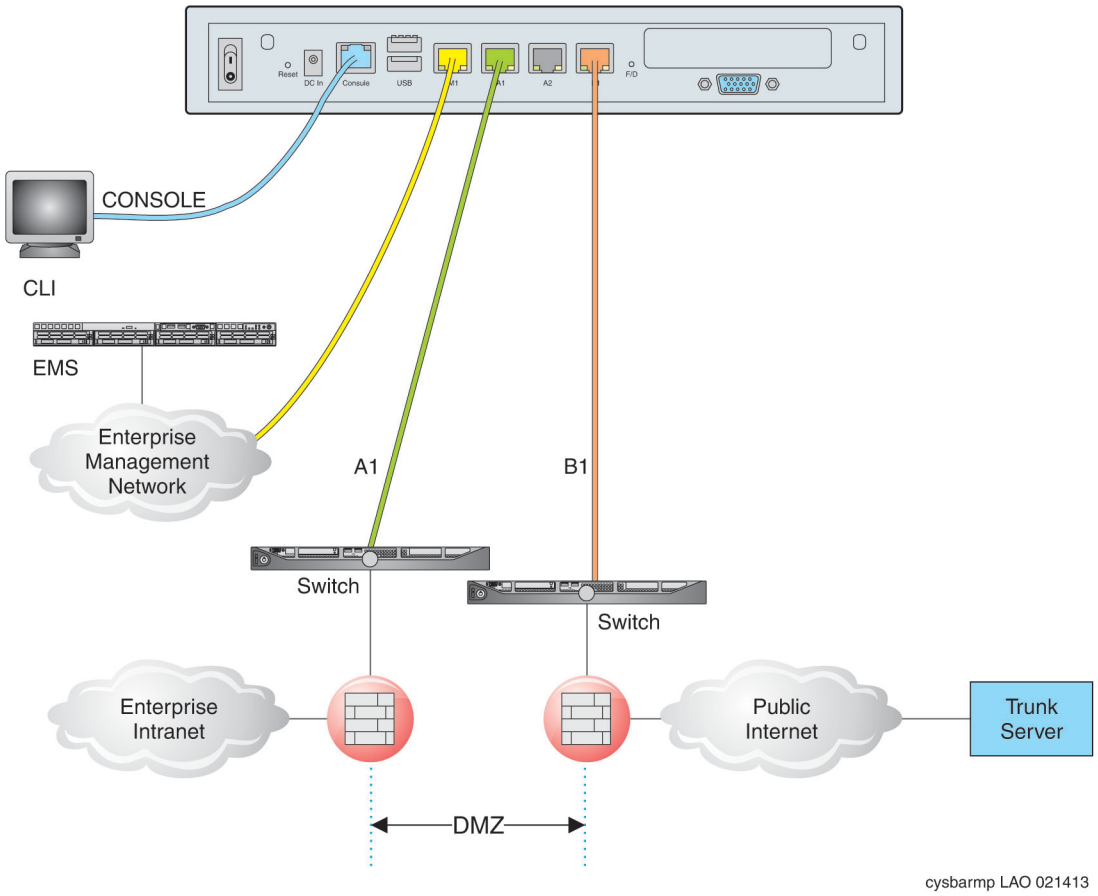


Figure 2: Avaya SBCE architecture using a micro platform

Rule and policy associations

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

Example

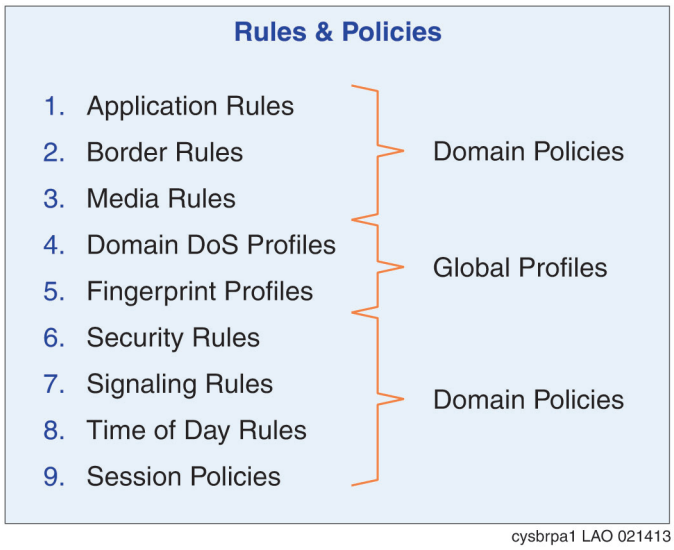


Figure 3: List of rules with the policies

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:

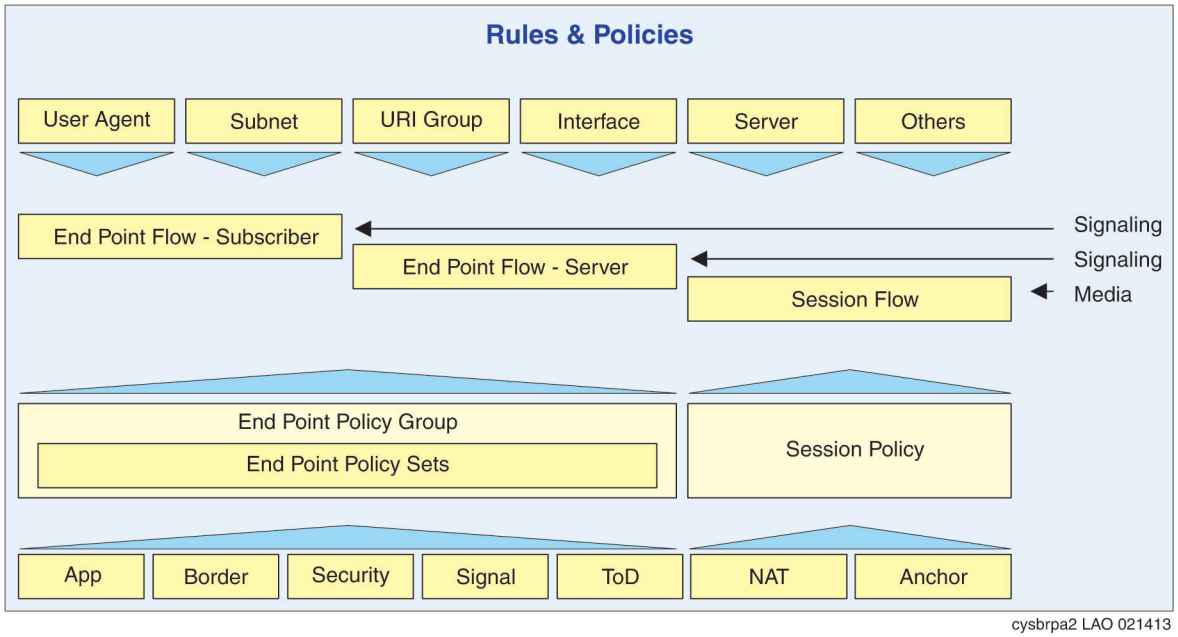


Figure 4: Types of signaling and media flows with the policies and policy groups and sets

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

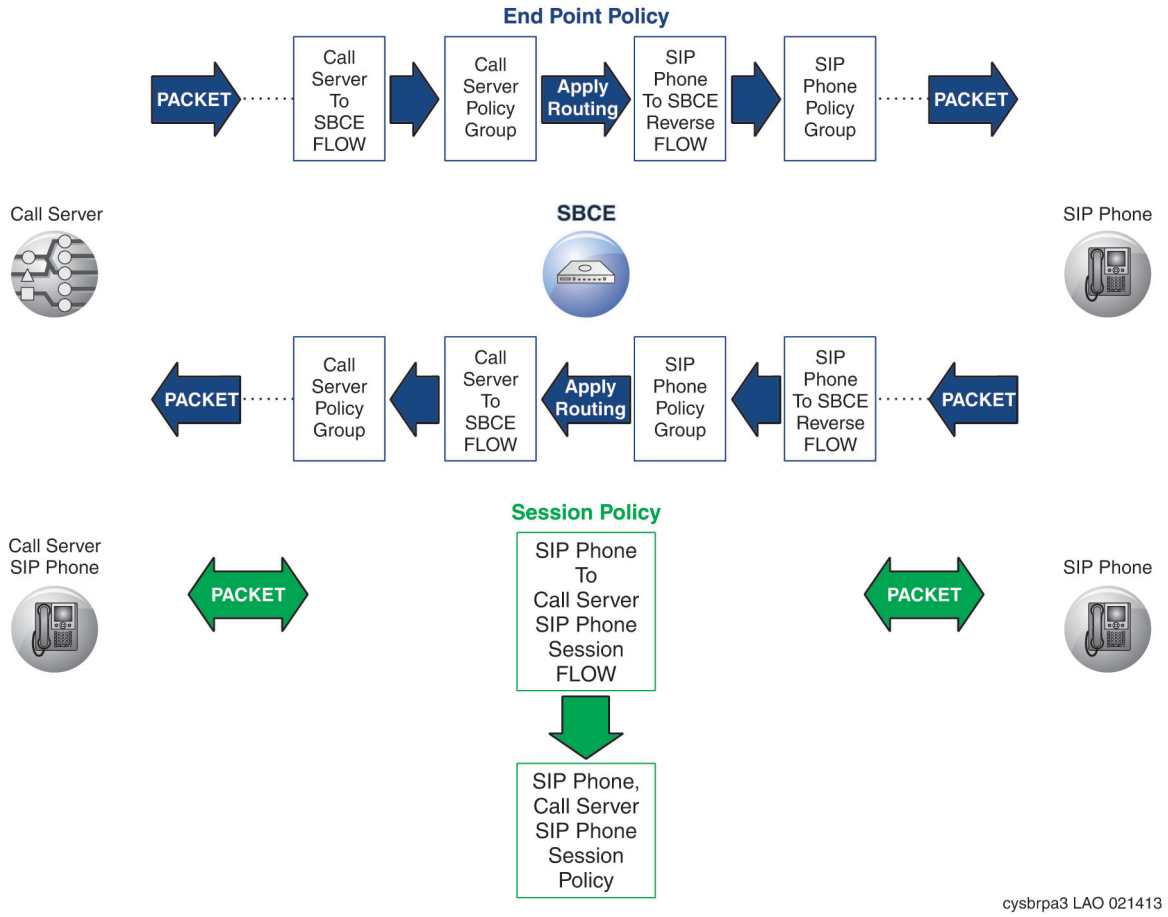


Figure 5: Session and subscriber flows with the policies

Rules and policies checklist

No.	Task	Reference	Notes
1	Configure application rules.	Creating a new application rule on page 83	
2	Configure border rules.	Creating a new border rule on page 86	
3	Define media rules.	Creating a new media rule on page 89	
4	Define domain DoS rules.	Adding a New Domain DoS Profile on page 232	
5	Create security rules.	Creating a new security rule on page 97	

Table continues…

No.	Task	Reference	Notes
6	Define signaling rules.	Creating a new signaling rule on page 100	Block Option Request Headers with 403 Forbidden.
7	Create charging rules	Creating a new charging rule on page 116	
8	Set time-of-day rules.	Creating a new ToD rule on page 204	
9	Create a policy group.	Creating a new policy group on page 119	

SIP message processing

SIP messaging involves the following processes:

- SIP registration processing
- SIP call processing on Avaya SBCE
- 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 SBCE 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

SIP servers identification on page 71

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 SBCE, 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 SBCE

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

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.

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 SBCE 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

Policy invocation and route resolution on page 69

Server flow matching for a call to a server on page 73

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

Policy invocation and route resolution on page 69

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

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.

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 SBCE 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 SBCE.

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 SBCE 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.

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 SIP 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.

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 SBCE 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

Application Policy Enforcer applies the application rules. Application rules regulate the number of audio, video, and Instant Messaging sessions that are allowed for each endpoint, remote worker, trunk server, or a call server. Each application rule contains the following two counters for every media type and In/Out direction flags for the media type:

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

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 SBCE, 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 SBCE, 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 SBCE 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 SBCE 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 SBCE.

Trunk User —> ostn-cm —> pstn-asm —> SBCE —> 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 SBCE for routing the calls from PSTN trunk to the CCE server, see Provisioning for PSTN trunk Aura Session Manager on page 79.

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 SBCE 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 – 10.32.3.1:5060

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 SBCE 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 SBCE 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 SBCE.

Trunk User —> ostn-cm —> pstn-asm —> SBCE —> 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
TCP Connection Type	SUBID
TLS Connection Type	SUBID

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

Table continues…

Field	Value
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

Table continues…

Field	Value
Advanced	
Enable Grooming	Enabled
Interworking Profile	avaya-ru (Default profile)
TLS Client Profile	Avaya-SBC-Client
TCP Connection Type	SUBID
TLS Connection Type	SUBID

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
Signaling	default-low
Time of Day	default-low

Domain policies management

The management of domain policies includes the following topics:

- Application rules
- Border rules
- Media rules
- Security Rules

- Signaling Rules
- Charging Rules
- End-Point policy groups
- Session Policies

Application rules

Application rules define the type of SBC-based Unified Communications (UC) applications Avaya SBCE 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. In the navigation pane, click **SBCE**.
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 .
In	Check box indicating that this application rule applies to the audio and video traffic entering the enterprise network.

Table continues…

Name	Description
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.
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.
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 SBCE sends an INVITE for connecting the call. Connect: Stores data in the CDR file from the time Avaya SBCE 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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, select **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 SBCE 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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 comprising the selected border Rule set.

4. In the application pane, click the border rule that you want 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.

Result

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 SBCE must handle media packets that adhere to the set parameters.

Creating a new Media Rule

About this task

Use the following procedure to create a new Media Rule.

Caution:

Avaya provides a default Media 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. In the navigation pane, click **SBCE**.
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. 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. Enter the appropriate values, and click **Finish**.

Result

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 126

Media Rules field descriptions

Encryption tab

Name	Description
Audio Media Encryption and Video Media 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 have the option of encrypting RTCP signaling. The system will keep 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 for Format #1.
Preferred Format #3	The third most preferred encryption method for media traffic. Available selections are the same as those for Format #1.
Encrypted RTCP	Indicates whether RTCP will use encryption. **Note:** This check box is active for selection if at least one of the three preferred encryption formats include SRTP.
MKI	MKI is 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 lifetime expires.
Lifetime	Specifies the time interval after which session keys would be generated. These keys are not passed in signaling. Session keys are based on MKI. Currently, Avaya SBCE does not support 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
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.
Preferred Codecs	Names of audio codecs that you want specifically matched in a particular order. These are optional fields that must 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 at the same time. Then, click **>** to move the codecs to the **Selected** column. You can change the order of the codecs in the **Selected** column by clicking **^** or **v**. The **P-Time** column lists the available packetization times. When you select a codec and a p-time, and then 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 will apply transrating at the selected p-time for the preferred codecs.
Video 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 When Needed	This field is unavailable for Video Codecs. Avaya SBCE does not support transcoding for video codecs.
Transrating	This field is unavailable for Video Codecs. Avaya SBCE does not support transrating for video codecs.

Table continues…

Name	Description
Preferred Codecs	Names of video codecs that you want specifically matched in a particular order. These are optional fields that must 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 at the same time. Then, click **>** to move the codecs to the **Selected** column. You can change the order of the codecs in the **Selected** column by clicking **^** or **v**. The **P-Time** column lists the available packetization times. When you select a codec and a p-time, and then 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 will apply transrating at the selected p-time for the preferred codecs.

Advanced tab

Name	Description
Silencing Enabled	Check box to enable the **Media Silencing** feature.
Media Silencing	Indicates whether Avaya SBCE detects media packets from both legs of a call within the set time period. If no media packets are detected, Avaya SBCE sends an incident report to the Syslog and the call is disconnected.
Timeout	Indicates the time 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 SBCE sends an incident report to the Syslog or the call is terminated.
BFCP Enabled	Indicates whether Binary Floor Control protocol 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 facilitate giving 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 of the token. Avaya SBCE can support one BFCP channel for multiple video content channels.
FECC Enabled	Indicates whether Far End Camera Control is enabled. It provides mixed encryption support for audio, main video, and Far End Camera Control (FECC). In the media path using a RTP payload type sends control signaling to control the far end camera. The FECC channel facilitates in setting up the signaling for the media path, and control signals are send on this path using RTP payload type of a particular codec type (H.224)
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 both IPv4 and IPv6 hosts.
Local Preference	Specifies the order of preference for the Alternate Network Address Types IPv4 and Dual Stack.
Use Remote Preference	Specifies that the remote party must be given ANAT preference to answer the offer in the 200 OK response, irrespective of the ANAT preference configured on Avaya SBCE.

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 only 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 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 **Audio** and **Video** fields: • EF • AF11 • AF12 • AF13 • AF21 • AF22 • AF23 • AF31 • AF32 • AF33 • AF41 • AF42 • AF43 • Other...

SDP capability negotiation

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

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

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

Editing an existing Media Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. After making the appropriate edits, click **Finish**.

Result

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. In the left navigation pane, click **Domain Policies** > **Media Rules**.
3. In the Application pane, select the media rule whose codec prioritization parameters you want to edit.
4. Click the **Codec Prioritization** tab.
5. In the lower-center section of the page, click **Edit**.

   The system displays the codec prioritization window.

6. Enter the required information in the appropriate fields, and click **Edit**.

   The Content pane displays the edited parameters when you select the session policy.

Cloning an existing Media Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 comprising the selected media rule set.

4. In the application pane, select the name of the media rule that you want 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, and click **Finish**.

Result

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

Renaming an existing media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, select **SBCE**.
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 comprising the selected media rule set.
4. In the application pane, select the name of the media 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 media rule, and click **Finish**.

Result

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

Deleting an existing media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 comprising the selected media rule set.
4. In the application pane, select the name of the media rule that you want 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

Result

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 SBCE from the Scrubber feature of Global Parameters. For more information, see and Protocol Scrubber on page 238 and Installing a scrubber rules Package on page 239.

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. In the navigation pane, click **SBCE**.
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 SBCE 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 as with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 as with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 as with administrator credentials.
2. In the navigation pane, select **SBCE**.
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 as with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE, 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. In the navigation pane, click **SBCE**.
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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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 SBCE 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 SBCE 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	
Enabled	Indicates whether the Signaling Quality-of-Service (QoS) feature is enabled.

Table continues…

Name	Description
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.
Node ID	A unique two-byte network node identifier that is assigned to the Avaya SBCE 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. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE can handle OPTIONS request from Session Manager.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE.

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. In the navigation pane, click **SBCE**.
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 EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, select **SBCE**.
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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE. If the URI pattern of the Refer-To header matches with the URI patterns administered and defined by Avaya SBCE, then Avaya SBCE 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 SBCE 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 SBCE adds the existing P-Charging-Vector for that session again.

Creating a new charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

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**

Editing an existing charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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**.

Cloning an existing charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

Renaming a charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

Deleting a charging rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

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 SBCE 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 SBCE security product exhaustively inspects traffic. The Avaya SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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 SBCE 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.

Table continues…

Name	Description
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. • 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 52

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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 SBCE security product handles media packets matching these criteria.

Avaya SBCE uses session policies for:

- Media unanchoring
- Media forking
- SIP recording
- Codec prioritization
- Prefered codecs determination
- Delayed SDP handling

  If the INVITE message comes with no SDP, the SDP will be added by using the codecs configured in the session policy.

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.

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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, type a name for the new session policy, and click **Next**.

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

Result

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

Session Policy field descriptions

Name	Description
Media Anchoring	Enables or disables media anchoring. The system enables the **Media Forking Profile** and **Recording Server** fields only when you select the **Media Anchoring** field.
Media Forking Profile	Specifies a media forking profile.
Converged Conferencing	Do not enable this field.
Recording Server	Indicates whether the server is a recording server. The system enables the **Recording Type** and **Play Recording Tone** fields if you select the **Recording Server** field.
Recording Type	Specifies the type of media recording. The options are: • Full Time • Selective
Play Recording Tone	Indicates whether a recording tone will be played when the recording session begins. The recording tone is a short duration wave file that supports the G729 and PCMU codecs.
Call Termination on Recording Failure	Specifies whether Avaya SBCE must terminate the recording session when the Recording Servers do not respond. This feature works only for SIPREC trunking scenarios and not for SIPREC remote worker scenarios.
Routing profile	Specifies a routing profile for the recording server.
Video Recording	Enables or disables video recording. The system enables the **Video Recording** only when you select the **Recording Server** field.
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.

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 SBCE supports media unanchoring for all non-hairpin calls, including trunk to enterprise, enterprise to trunk, remote to enterprise, and enterprise to remote. Avaya SBCE supports media unanchoring for audio, video, and multimedia calls.

Unanchoring media for existing session policies

Before you begin

Configure a session policy profile, and then use the profile to create a session flow.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.
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**.

Note:

- If you clear the media anchoring check box, media forking profile becomes unavailable. If you want to use the media forking feature, Avaya SBCE cannot unanchor the media.
- In a deployment, if a network has a remote Avaya SBCE deployed before the core Avaya SBCE deployment and a subnet user is behind a NAT device, you can unanchor media for the core Avaya SBCE.

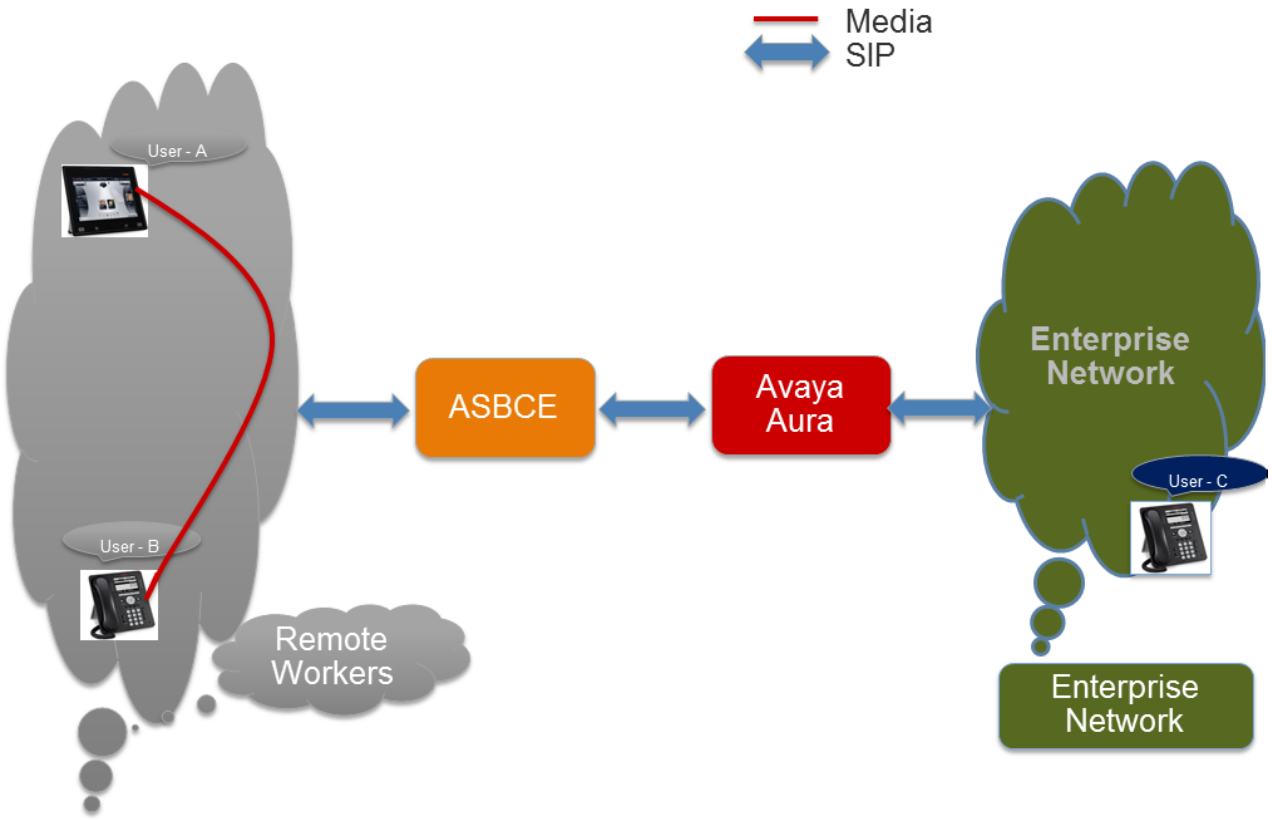
Media unanchoring scenarios

Avaya SBCE can release media when:

- Both endpoints or ends of the call pass through the same Avaya SBCE
- Both end points can negotiate with the same media format, SRTP or RTP

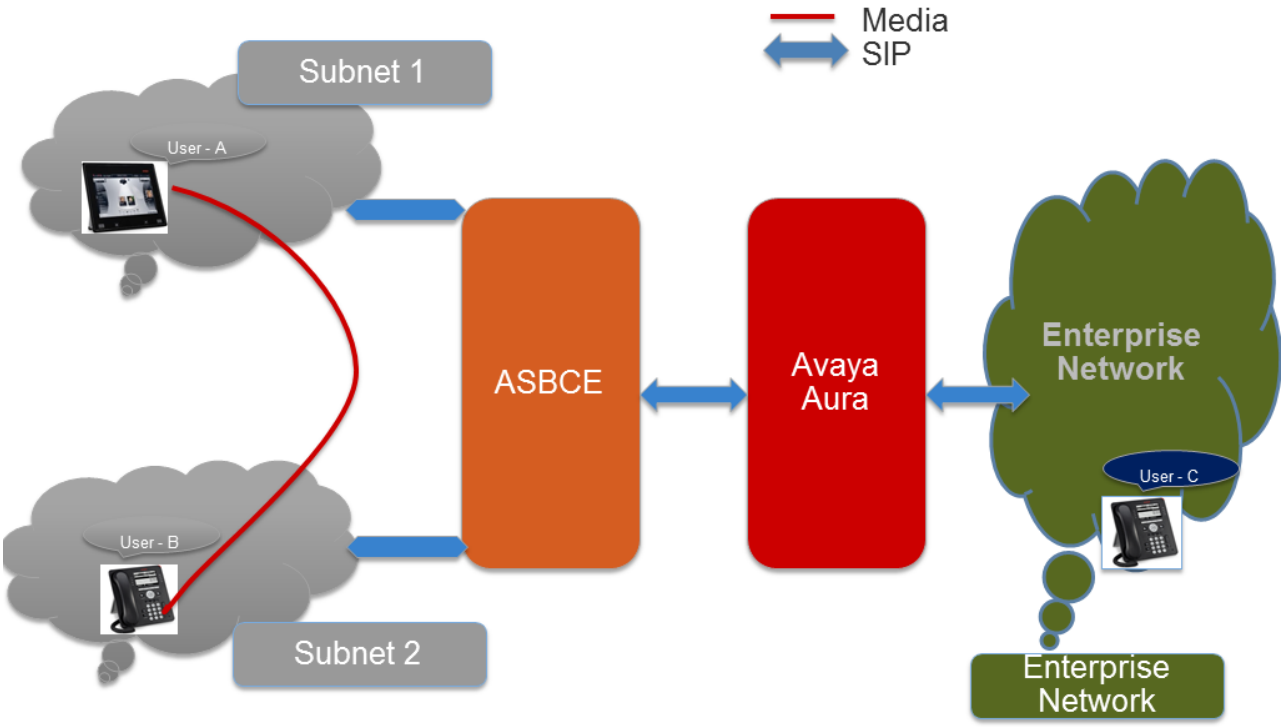
This section covers a few scenarios in which Media unanchoring can be used.

Remote workers in the same subnet



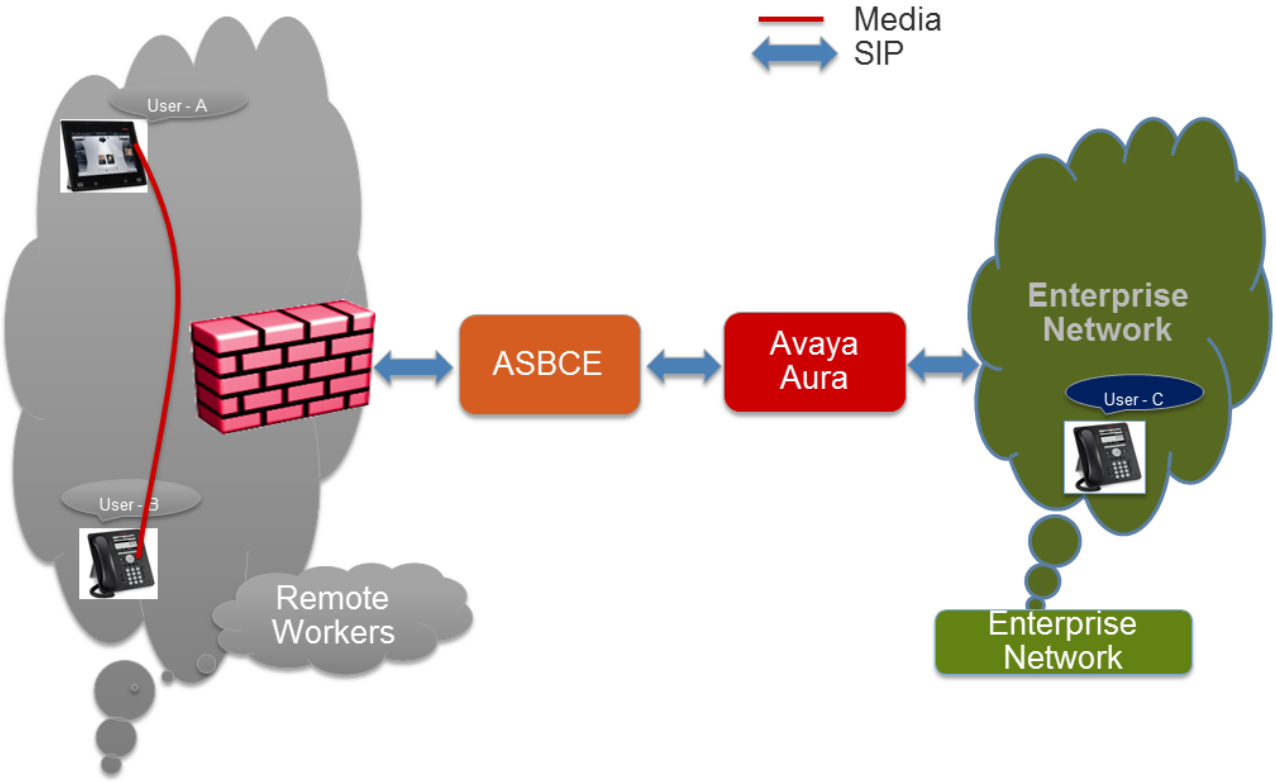
As the endpoints are in the same subnet, the Avaya SBCE can be configured to flow the media directly between the endpoints.

Remote workers in two different subnets



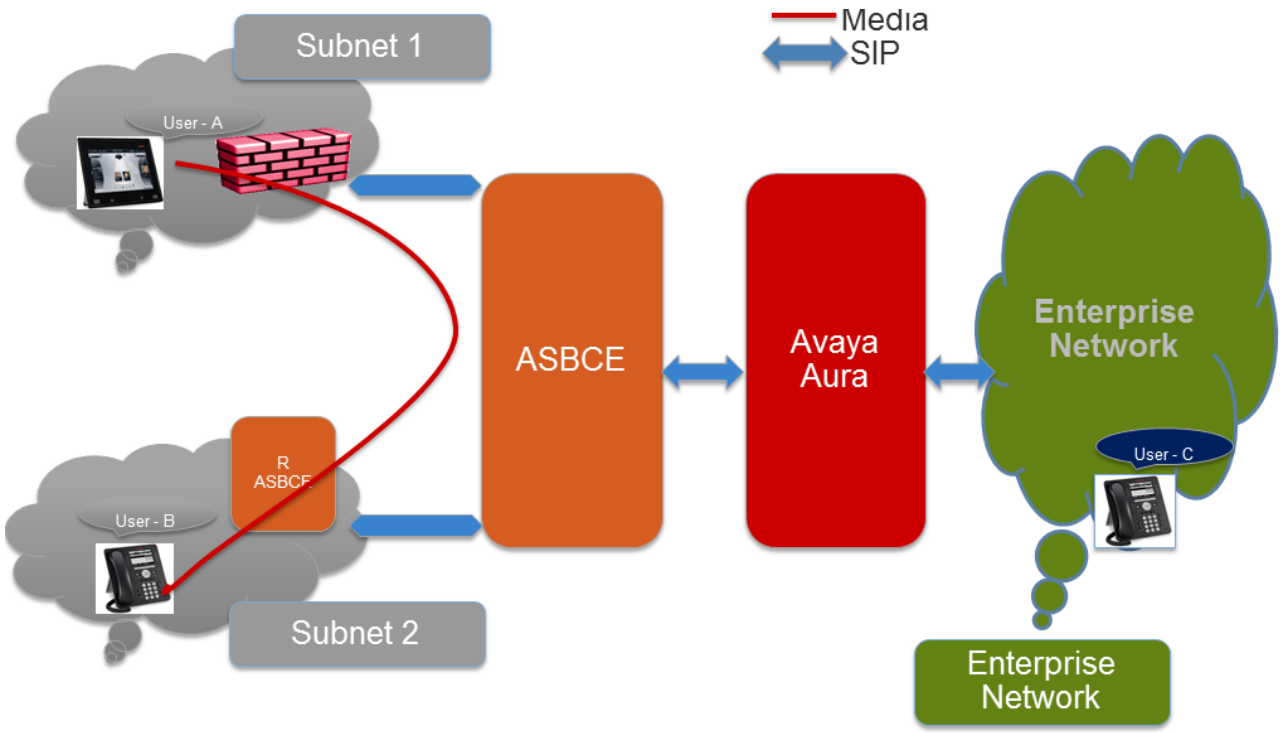
Avaya SBCE can be configured to release the media between two different subnets. The subnets must be reachable to flow the media.

Remote workers behind the same NAT



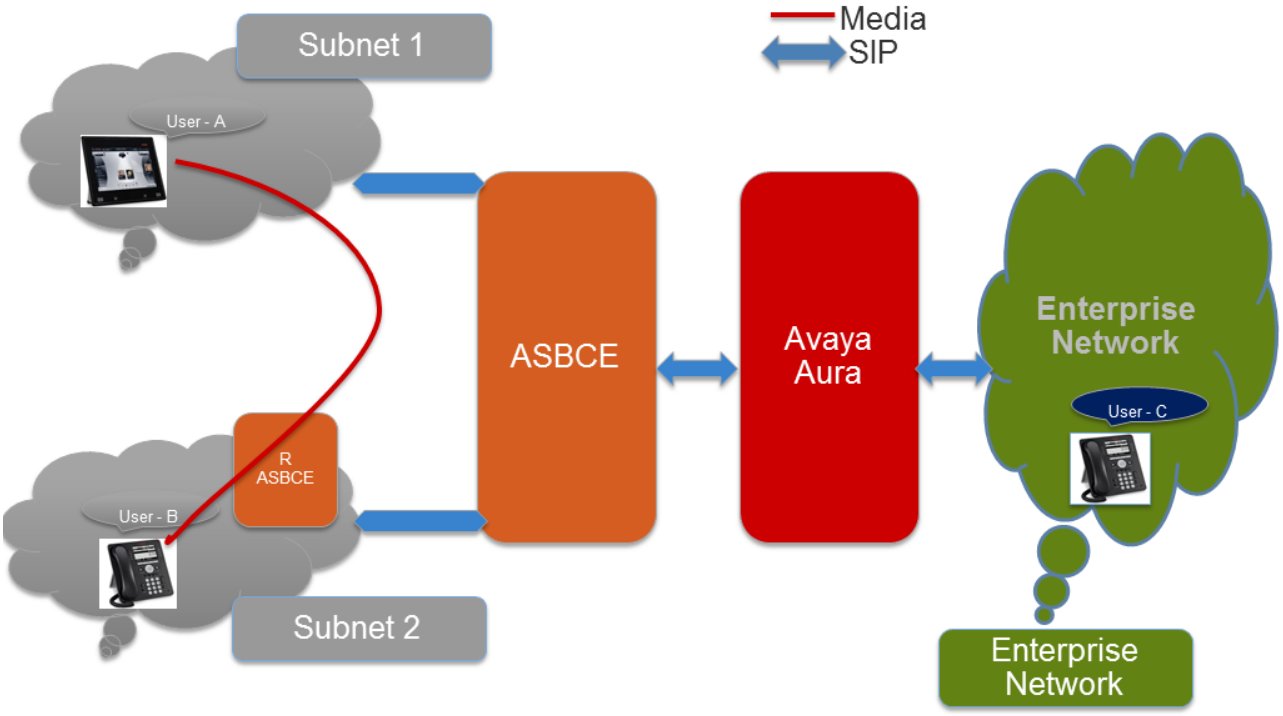
When Avaya SBCE detects that both remote workers in the call are behind the same NAT device, Avaya SBCE can enable media flow directly between the remote workers.

Remote branch office with Avaya SBCE



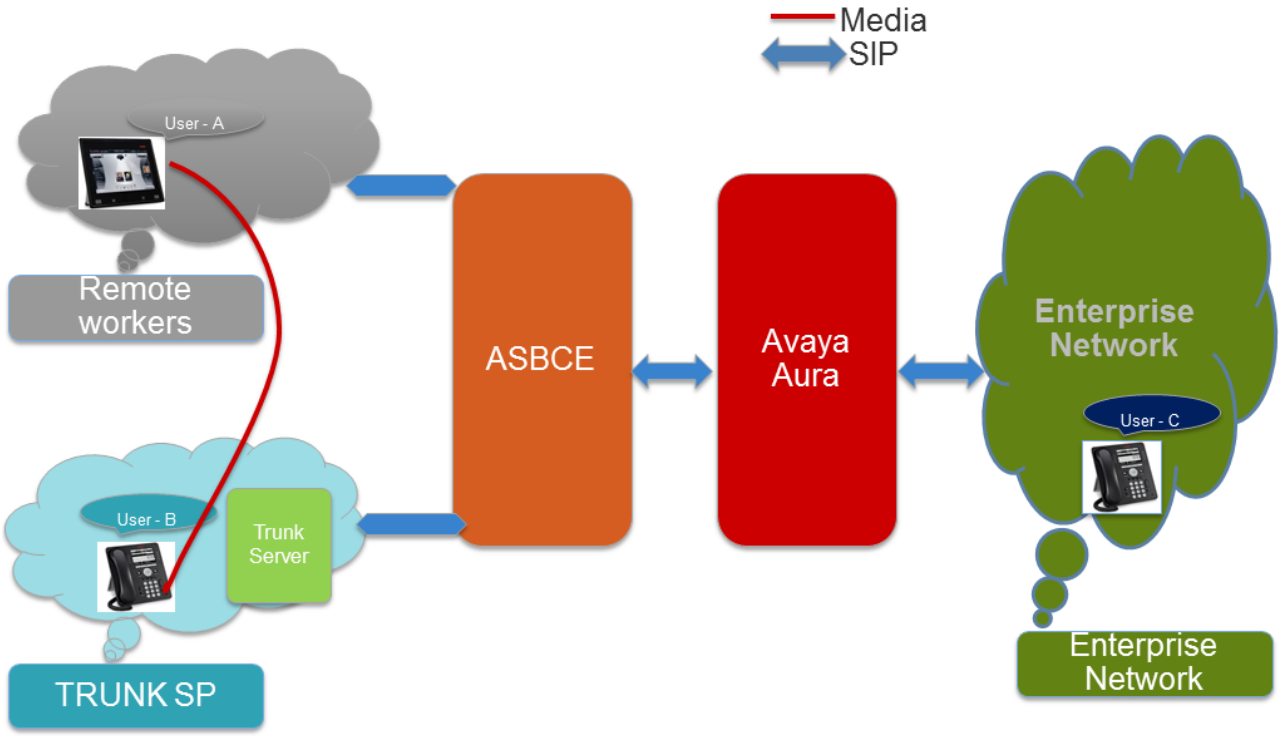
In this scenario, the endpoints belong to two different subnets. However, one of the endpoints is behind a NAT device, and the other subnet has remote Avaya SBCE. The Core Avaya SBCE can be configured to release the calls between these subnets by using the remote Avaya SBCE. To release the media from core Avaya SBCE, enable the **has remote sbc** flag during Session Flow configuration.

Remote branch office with Avaya SBCE



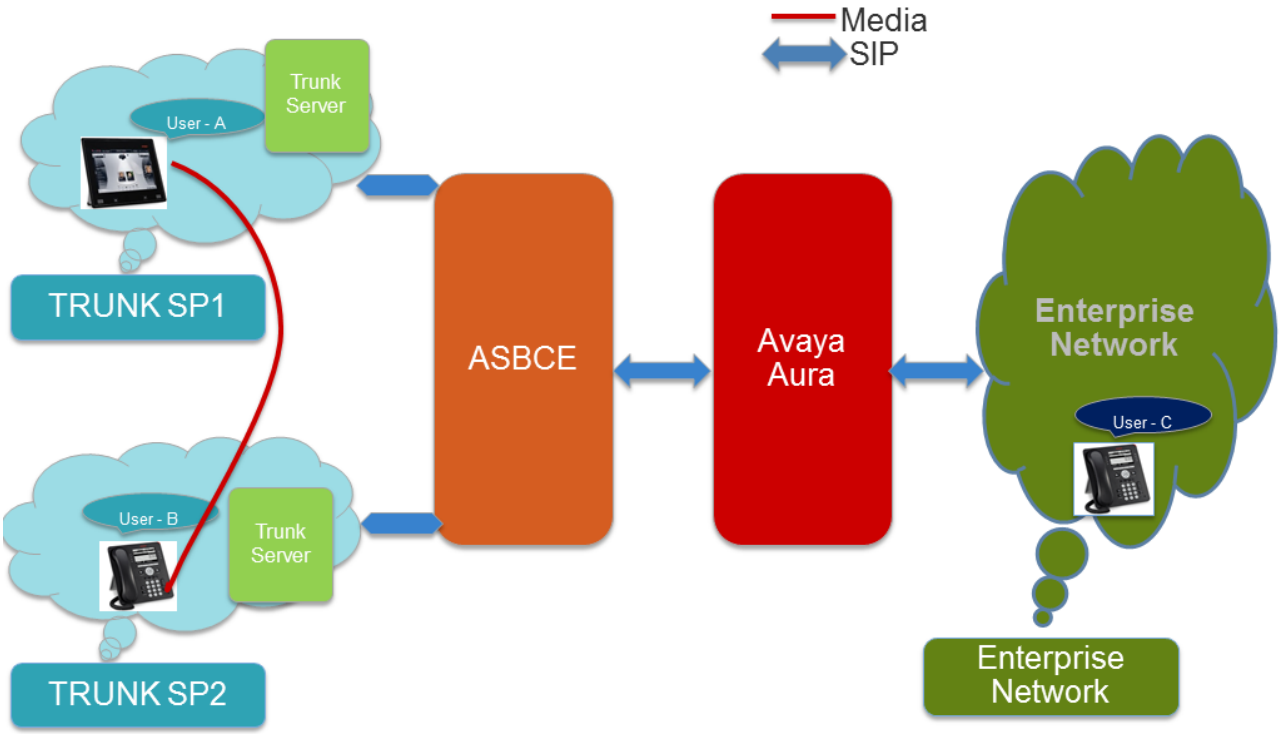
In this scenario, the endpoints belong to two different subnets, and one of the subnets has remote Avaya SBCE. The Core Avaya SBCE can be configured to release the calls between these subnets.

Calls between remote workers and Trunk users with same Avaya SBCE



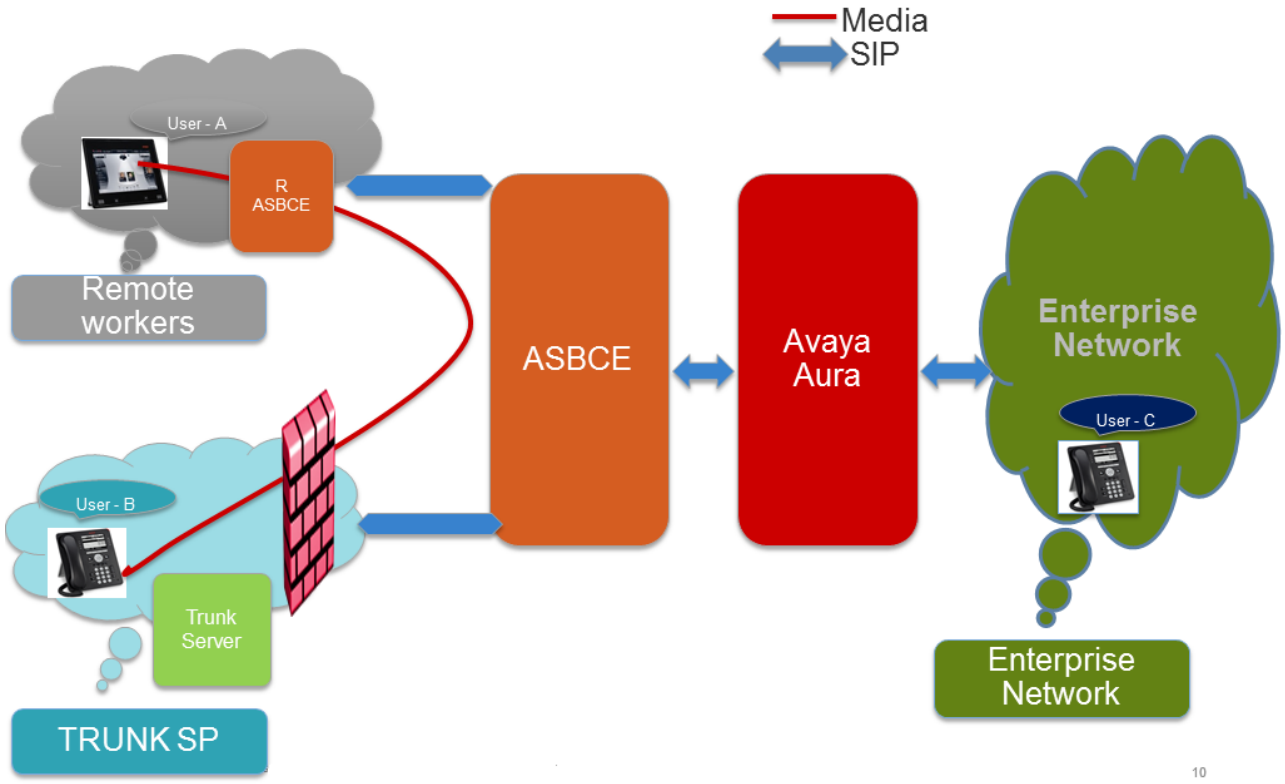
In this scenario, a call is established between remote worker from one subnet to the trunk subnet user. As these endpoints pass through the same Avaya SBCE, the Avaya SBCE device can be configured to release media between these endpoints. Both subnets must be reachable.

Calls between two trunks with the same Avaya SBCE



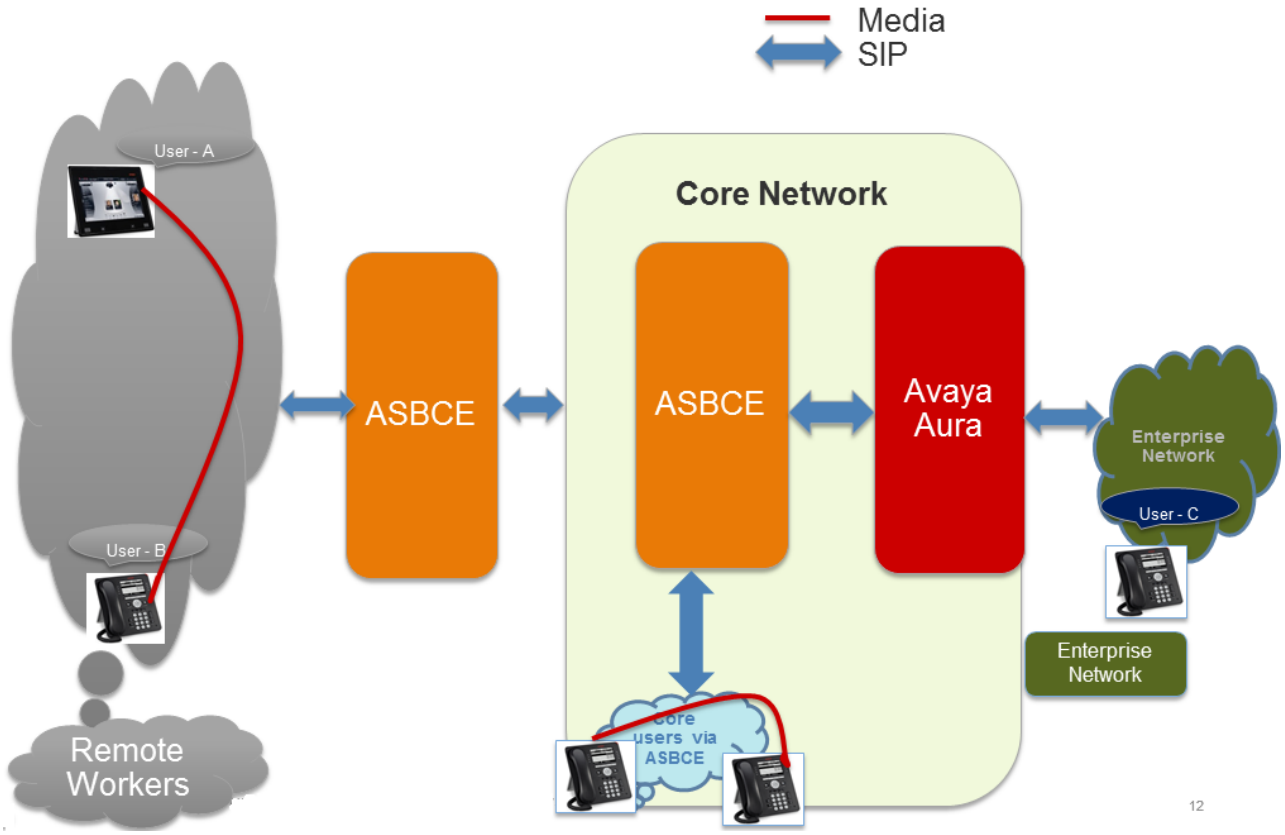
In this scenario, a call is established between two different trunk subnet users. As the endpoints pass through the same Avaya SBCE, the Avaya SBCE device can be configured to release media between these endpoints. Both subnets must be reachable.

Trunk behind firewall and Remote branch office with Avaya SBCE



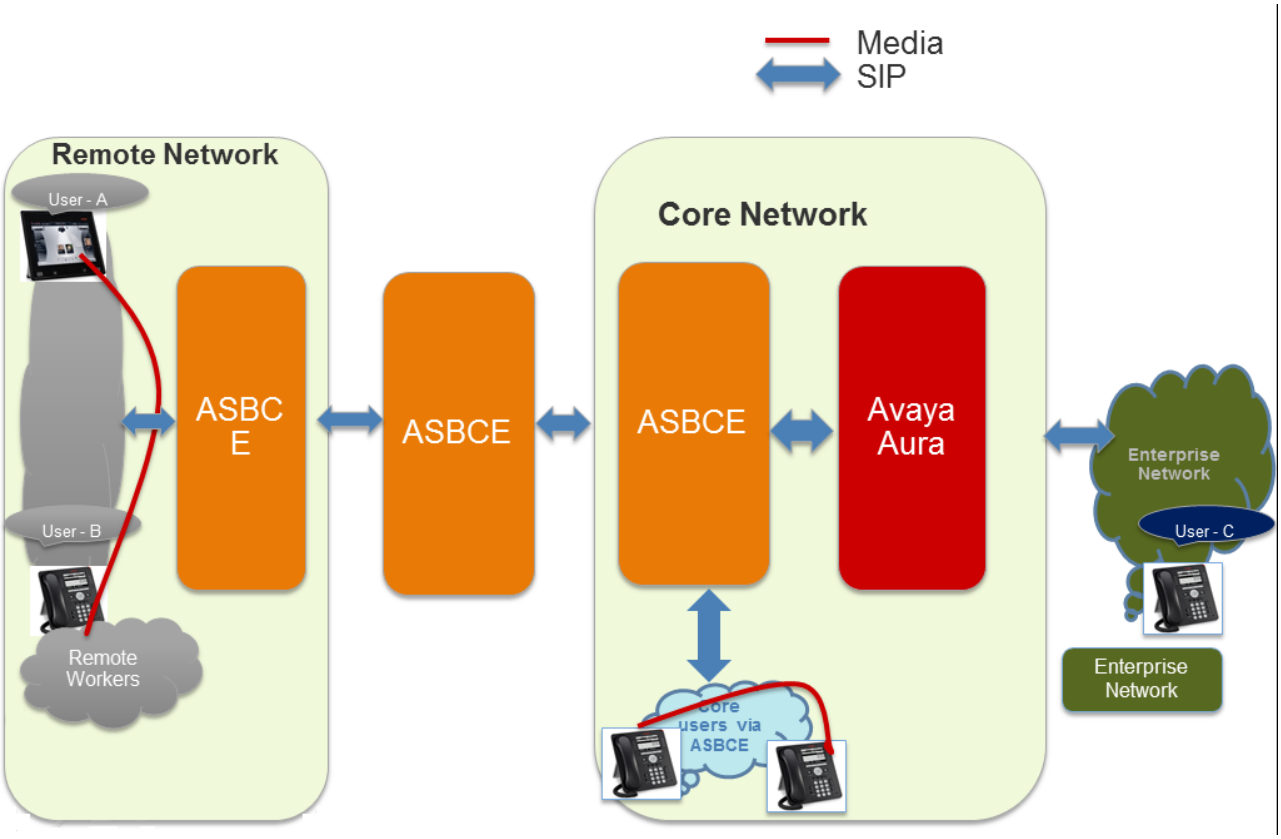
In this scenario, one subnet belongs to the trunk connected to Avaya SBCE, and the other subnet has a remote worker connected to Avaya SBCE with remote Avaya SBCE. The core Avaya SBCE can be configured to release calls between these subnets, by using the remote Avaya SBCE. To release the media from core Avaya SBCE, enable the **has remote sbc** flag during Session Flow configuration.

Back-to-back Avaya SBCE deployment



In this scenario, core and DMZ Avaya SBCE devices can be configured to release the media between the endpoints. For more information, see the section for back-to-back Avaya SBCE deployment.

Back-to-back-to-back Avaya SBCE deployment



In this scenario Remote, DMZ, and core Avaya SBCE devices can be configured to release the media between the endpoints. For more information, see the section for back-to-back-to-back Avaya SBCE deployment.

Editing an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. Edit the required fields, and click **Finish**.

Result

The Content area displays the edited media forking parameters when you click the media tab of the session policy.

Cloning an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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**.

Result

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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**.

Result

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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.

Result

The application pane no longer displays the deleted session policy.

Manage endpoints 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 flows

The following sections contain the procedures to create, clone, view, edit, and delete Endpoint Flows.

New endpoint flow creation

Endpoint Flows are of two types: Subscriber and Server. Subscriber Endpoint 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. Server End-Point Flows refer to the IP call servers that connect to SIP trunk services.

Creating a subscriber flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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.

Creating a server flow

About this task

Use the following procedure to manually create a server endpoint flow.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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.

Endpoint flow field descriptions

Add Subscriber Flow Profile field descriptions

Name	Description
Criteria	
Flow Name	A field in which you can enter a name for the Subscriber Flow profile.

Table continues…

Name	Description
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.
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.

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.
Topology Hiding Profile	A drop-down menu from which you select the Topology Hiding Profile to be used for this Server End Point Flow.

Table continues…

Name	Description
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	Selecting **Link Monitoring from Peer** enables Avaya SBCE to send a 200 OK response for a match of the SIP OPTIONS request with a server flow. If you clear **Link Monitoring from Peer** check box, then OPTIONS request will be relayed to the destination server.

Cloning an existing endpoint flow

Additional Endpoint Flows can be added to the Avaya SBCE security repertoire. You can add Endpoint Flows by cloning existing Subscriber Endpoint Flows and Server Endpoint Flows and editing the desired parameters to create new flow policies. The following sections contain the procedures necessary to clone existing Endpoint Flows.

Note:

An endpoint flow cannot be cloned from one Avaya SBCE security device and applied to another Avaya SBCE security device. A clone can only be assigned to the same Avaya SBCE security device from which the original flow came.

Cloning an existing subscriber endpoint flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

Cloning an existing server endpoint flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.

   Separate tabs displays 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 end-point 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.

Editing existing endpoint flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 or 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.

   The Edit Flow screen for Subscriber Flows has two pages. While editing Subscriber Flows, you must complete the fields on the first page and click **Next** to edit fields on the second page.

7. Click **Finish**.

Reordering the precedence of endpoint flows

Procedure

1. Log in to the EMS web interface with administrator credentials..
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Click the **Subscriber Flows** tab or 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 End-Point Flows in the new order of precedence.

Deleting an existing endpoint flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **End Point Flows**.
4. Select the **Subscriber Flows** tab or 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.

Session flows

The following sections contain the procedures necessary to create, clone, view, edit, and delete session flows.

Creating a new session flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The content area displays currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flow screen.
5. Enter the requested information in the appropriate fields, and click **Finish**.

Result

The Content Area displays the new session flow.

Add 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 SBCE. 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 SBCE system is deployed before core Avaya SBCE deployment and any of the subnet users are behind a NAT device. In this deployment core, Avaya SBCE unanchors the media.

Cloning an existing session flow

About this task

You can add session flows to the Avaya SBCE 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 SBCE security device and applied to another Avaya SBCE security device. A clone can only be assigned to the same Avaya SBCE security device from which the original flow came.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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.

Editing existing session flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE security device.
4. Locate the Session flow that you want to edit, and click **Edit**.

   The EMS server displays the Edit Flow screen.
5. Edit the required fields and click **Finish**.

Result

The EMS server updates, saves the edited session flow. The Content Area displays the edited session flow.

Reordering the precedence of session flows

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The content area displays the session flows currently defined for that Avaya SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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 SBCE external address.

Configuring Single Sign-On and an Identity Engine server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. Enter the appropriate values and click **Finish**.

Result

The content pane displays the newly created reverse proxy profile.

Reverse Proxy Profile field descriptions

Name	Description
Service Name	Indicates the name of the reverse proxy profile.
Listen IP	Indicates the IP address of an external Avaya SBCE
Listen Port	Indicates the port number that remote workers use for SSO service. For HTTPS the default value is 443 and for HTTP default value is 80.
Listen Protocol	Protocol that remote workers use for the SSO service.
Listen TLS Profile	Indicates the already configured TLS profiles. **Listen TLS Profile** field is accessible if you select HTTPS in **Listen Protocol** field.
Listen Domain	Indicates the domain name which remote workers use for the SSO service.
Connect IP	Indicates the IP address that Avaya SBCE uses for communicating with IDE server.
Server Protocol	Indicates the protocol for IDE server. **Note:** For security reasons, you must use HTTPS.
Server TLS Profile	Indicate the already configured server profiles.
Rewrite URL	Check box to enable **URL Replace** for the profile.
Load Balancing Algorithm	Indicates the load balancing algorithm for the reverse proxy profile.
PPM Mapping Profile	Indicates the already configured PPM mapping profile.
Reverse Proxy Policy Profile	Indicates the number of requests permitted per second.
Whitelisted IPs	Indicates 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.

Creating a new URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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**.

Result

The content pane displays the new URI group.

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 126

Adding an additional URI to an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 126

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.

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 SBCE 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 183.

Related links

Managing SIP options on page 183

Editing a URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE.**
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 126

Chapter 6: System Configuration

Basic system configuration overview

With the Avaya SBCE EMS web interface, you can configure and manage the following system-related security features of the Avaya SBCE security products deployed in an enterprise VoIP network:

- Back up/Restore system information.
- Manage Avaya SBCE security devices.
  - Provision installed Avaya SBCE security devices.
  - Establish secure shell sessions.
  - Shutdown and reboot individual SBCE devices.
  - Restart Avaya SBCE applications.
  - View, edit, and delete Avaya SBCE 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 SBCE architecture
- Basic configuration quick-start steps checklists
  - Reconfigure Avaya SBCE.
  - 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 quick-start checklist

Task	Description
Reconfigure (if required)	See Reconfiguring Avaya SBCE on page 156.
Enable Interfaces	See Enabling interfaces on page 157.
Configure URI Groups	See Creating a new URI group on page 149.
Configure Routing Profiles	See Creating a new routing profile on page 209.

Table continues…

Task	Description
Interworking Profiles	See Adding a new Server Interworking Profile on page 264.
Add Servers (Call/Trunk)	See Creating an Avaya call server profile (advanced services only) on page 353 and Adding a new SIP Server profile on page 253.
TLS Certificates	See Creating a Certificate Signing Request on page 282 and Installing certificates on page 284.
TLS Profiles	See Creating a new TLS server profile on page 297.
Domain Policy Group	See Creating a new policy group on page 119.
Signaling Interface	See Adding a new signaling interface on page 222.
Media Interface	See Adding a new Media Interface on page 224.
Subscriber Flow	See Creating a new subscriber end-point flow on page 139.
Server Flow	See Creating a new server endpoint flow on page 139.
Session Flow	See Creating a new session flow on page 145 and Creating a new session policy on page 124.

Reconfiguring Avaya SBCE

About this task

You must not configure the management interfaces, for example, M1 and M2, and media interfaces, for example, A1, A2, B1, and B2, on the same subnet. Standard platform interfaces are M1, M2, A1, A2, B1, and B2.

Portwell platform interfaces are M1, A1, A2, and B1.

Note:

Before you begin

To avoid possible routing problems, ensure that the data interfaces and maintenance interfaces are configured on different subnets when configuring:

- The data interfaces A1/A2 and B1/B2 on the Installation Wizard screen.
- 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 for Enterprise*.

Procedure

1. To uninstall the Avaya SBCE device from a web interface, navigate to **Device management** > **Devices** and click **Uninstall**.
2. Start a secure shell (SSH) connection to the SBCE using the ipcs account.
3. Go to the `/usr/local/ipcs/icu/pylib` directory.

4. Run the **`sbceconfigurator.py configure --with-default`** command to configure Avaya SBCE with default values.
5. Reprovision Avaya SBCE in the web interface.

Enabling interfaces

Procedure

1. Log in to the EMS web interface with administrator credentials
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Network Management**.
4. Click the **Interfaces** tab and enable the required interfaces.

Backup and restore

The Backup and restore feature provides ability to create and restore snapshots of EMS and configured SBCEs.

The backup information is stored to a user-defined location either on the local EMS server or on a configured remote server. The location should be secure and physically separate from the Avaya SBCE equipment chassis for later retrieval or restoration.

Note:

- For EMS, you can take a configuration backup manually and restore as needed, or you can configure snapshots automatically.
- For SBCE, you can only take backup manually.
- You can backup and restore only the functional SBCE devices.
- You can download the snapshot by using the download link provided in the **Snapshot** tab.

Designating a Snapshot Server

About this task

Configuration data snapshots contain information such as (identity?) certificates and (security?) keys, which can be misused to gain unauthorized access to Avaya SBCE.

You can only restore a snapshot to the same Avaya SBCE 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 SBCE product version does not match, the restore operation will fail and the system settings will revert to the earlier state.

Before you begin

Ensure that:

- The selected storage directory on the designated remote server is accessible only to authorized users.
- 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 159

Add 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 SBCE configuration data.

Table continues…

Name	Description
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.
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.

Creating system snapshots

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for creating snapshot for the EMS server or **SBCE** for device specific snapshot configuration.
3. In the navigation pane, click **Backup/Restore**.
4. On the Backup/Restore page, click the **Snapshots** tab.
5. Select the designated snapshot server.
6. Click **Create Snapshot**.

   The EMS server displays the Create Snapshot window.
7. Enter a name for the snapshot, and click **Create**.

Result

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.

Restoration of a system snapshot

You can restore Avaya SBCE configuration data snapshot on EMS manually or configure automatic restoration of the snapshots..

Manual

The manual method of restoring configuration snapshots is a two-step process. The snapshot is first retrieved from the snapshot server and then uploaded to the EMS for restoration. To restore EMS to a previous snapshot configuration, you must:

- Retrieve a snapshot. See Retrieving a snapshot file on page 161
- Restore a snapshot. See Restoring a snapshot file using Restore by File option on page 161

Automatic

The automatic method is a process that restores EMS to the previous configuration without further intervention. See “Restoring a snapshot file”.

Caution:

During both methods, EMS goes into the offline mode when the files are being transferred and the device is being reconfigured.

Avaya SBCE detection or mitigation features are unavailable for the entire duration of the restore procedure, making the EMS and Avaya SBCE single server deployment vulnerable to intrusions and attacks.

Restoration procedures must be completed only during times of relative EMS server inactivity or during scheduled periods of maintenance.

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 virtualized environment:

Server	NICs	Hardware category
CAD 0230	6	110
Dell R320	6	310
Dell R630	6	310
HP DL360 G8	6	311
HP DL360 G9	6	311
VMWare SBCE	6	110
Nutanix	6	110
Avaya Converged Platform 100 series server with profile 3	6	310
Avaya Converged Platform 100 series server with profile 5	6	310
Portwell CAF-0251	4	110

Related links

Retrieving a snapshot file on page 161
Restoring a snapshot file using Restore by File option on page 161
Restoring a snapshot file on page 162

Retrieving a snapshot file

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for retrieving snapshot for the EMS server or **SBCE** 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 using Restore by File option

About this task

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.

Use the following procedure to upload the snapshot from your local workstation to the EMS server and reconfigure the EMS.

Before you begin

Retrieve a snapshot file.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for restoring a snapshot for the EMS server or **SBCE** 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 by File window, click **Chose 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 EMS server successfully restores a snapshot, in an HA configuration, both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The EMS server takes several minutes to reboot after backup configuration.

Restoring a snapshot file

Before you begin

Create a system snapshot.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for restoring a snapshot for the complete EMS server or **SBCE** 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 SBCE 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 SBCE goes offline and reconfigures the snapshot file.

Note:

After the system successfully restores a snapshot, in an HA configuration both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The system takes several minutes to reboot after backup configuration.

Related links

Retrieving a snapshot file on page 161
Restoring a snapshot file using Restore by File option on page 161

Deleting a system snapshot

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS** for deleting the snapshot for the complete EMS server or **SBCE** 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.

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**.

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_03-20-2017_15-32-25_8.0.x.0-12-13295.bak. Avaya SBCE 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 SBCE configuration data.

Table continues…

Name	Description
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.
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.

Creating a configurable snapshot

Before you begin

Ensure that Avaya SBCE 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**.

Result

The EMS server creates a portable snapshot in `/usr/local/ipcs/snapshots/configurable_snapshot/`.

Restoring portable snapshots

About this task

You can restore snapshots from an HA system to separate Avaya SBCE instances and vice versa.

Before you begin

Ensure that the Avaya SBCE instance on which you are restoring the snapshot and the Avaya SBCE instance from which the snapshot was taken:

- Have the same number of interfaces.

- Are of the same version.

Ensure that the Avaya SBCE instance on which the snapshot is being restored is in a Commissioned state.

Important:

The EMS server restore affects services on Avaya SBCE 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.

Management of deployed Avaya SBCE security devices

In addition to configuring newly installed Avaya SBCE 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 SBCE security devices.
- Restart Avaya SBCE applications.
- Swap Avaya SBCE devices.
- View, edit, and delete Avaya SBCE device configurations.

Shutting down an Avaya SBCE 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 SBCE 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 SBCE 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 SBCE 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 SBCE 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 SBCE 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 Avaya SBCE devices in HA pair deployment

About this task

Use this procedure to swap an Avaya SBCE device in an HA pair deployment.

Before you begin

Ensure that one of the Avaya SBCE devices in the HA pair is non-functional.

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 SBCE with different IP address.

   For more information, see *Deploying Avaya Session Border Controller for Enterprise*.
5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
   c. Clear the HA check box.
6. When the state of the newly added Avaya SBCE device becomes Registered, click **Swap Device**.
7. Select the IP address of the new device added in the **Device to Replace** field.
8. Click **Finish.**

   The EMS server does not display the old Avaya SBCE device in the **Devices** tab.

Swapping a Avaya SBCE device in single server deployment

About this task

Use this procedure to swap an Avaya SBCE device in single server deployment.

Before you begin

Ensure that you have created and saved the backup file of a functional Avaya SBCE device.

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 SBCE with a different IP address. For more information, see *Deploying Avaya Session Border Controller for Enterprise*.
5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
   c. Clear the HA check box.
6. When the state of the newly added Avaya SBCE device becomes Registered, click **Swap Device**.
7. Select the backup file of the new device added in the **Device to Replace** field.

   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 SBCE device in the **Devices** tab.

Swapping an EMS server in single server deployment

About this task

Use this procedure to swap an EMS server in single server deployment

Before you begin

Ensure 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 SBCE device installed on the system.
5. Select the backup file of the new device.

   Important:

   The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.
6. Run the following command to change the EMS IP address on the installed Avaya SBCEs:

   ```
   sbceconfigurator.py change-ems-ip <old_ems_ip> <new_ems_ip>
   ```

   Note:

   The IP addresses of the old and the new EMS must be different.
7. Reboot all the connected EMS servers.

Related links

Swapping a primary EMS server in HA pair deployment on page 171
Swapping a secondary EMS server in HA pair deployment on page 172
Restarting an Avaya SBCE application on page 168

Swapping a primary EMS server in HA pair deployment

About this task

Use this procedure to swap the primary EMS server in HA pair deployment.

Before you begin

Ensure that the primary EMS server is non functional.

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 SBCE device installed on the system.

5. Provide the IP address for the secondary EMS server.
6. Run the following command to change the EMS IP address on the installed Avaya SBCEs:

```
sbceconfigurator.py change-ems-ip <old_ems_ip> <new_ems_ip>
```

Note:

The IP addresses of the old and the new EMS must be different.

7. Reboot all the connected EMS servers.

Related links

Swapping an EMS server in single server deployment on page 170
Swapping a secondary EMS server in HA pair deployment on page 172
Restarting an Avaya SBCE application on page 168

Swapping a secondary EMS server in HA pair deployment

About this task

Use this procedure to swap the secondary EMS server in HA pair deployment.

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 for Enterprise*.
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 single server deployment on page 170
Swapping a primary EMS server in HA pair deployment on page 171
Restarting an Avaya SBCE application on page 168

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 SBCE 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 SBCE 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 SBCE configuration file.

Deleting device configuration

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 Avaya SBCE security device that you want to uninstall.

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

Result

The EMS server removes the Avaya SBCE 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 SBCE 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 SBCE 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	Specifies the process for which you want to enable logs. This field displays processes such as: • LogServer • OAMPSERVER • SYSMON • SSYNDI • TURNCONTROLLER
Subsystem	Specifies the subsystem 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
IH	Creates detailed logs generated by a GUI IH client. IH handles statistics retrieval from the application.
SOAP	Creates detailed logs generated by a GUI SOAP client. SOAP handles communication with EMS and Avaya SBCE Communication Manager servers, for example, restart application, reboot device, and uninstall device.
EMS-CM Relay	Creates detailed logs generated by SOAP relay module. This module handles communication relay between EMS Communication Manager and Avaya SBCE Communication Manager. For example, for device registration and configuration retrieval.
Shell Commands	Creates detailed logs when you start any external process.
File Uploads	Creates detailed logs for user file uploads, for example, upgrade packages, scrubber packages, and certificates.
Licensing	Creates detailed logs generated by a GUI WebLM client.
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

Third-Party Logs

Name	Description
Nginx	Controls log levels for nginx. The options are: • Info • Notice • Warn • Error • Crit • Alert • Emerg
Transcoding	Controls log levels for transcoding. The options are: • None • All

Advanced Options configuration

With the **Advanced Options** feature, you can:

- Enable or disable Avaya SBCE security features.
- Configure SIP signaling message options.
- Designate signaling and media port ranges.
- Configure RTCP monitoring.
- Configure load monitoring.
- Configure HA keepalive timer.

Advanced Options field descriptions

Periodic Statistics tab

Name	Description
Collect Periodic Statistics	Specifies whether collecting periodic statistics must be enabled.

Table continues…

Name	Description
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
Single Source DoS Protection	Enables the Single Source DoS Protection feature.
Phone Dos/DDoS Protection	Enables the Phone DoS/DDoS Protection feature.
Call Walking Protection	Enables the Call Walking Protection feature.
Stealth DoS/DDoS Protection	Enables the Stealth DoS/DDos Protection feature.
Transcoding	Enables the media transcoding feature.
AMS Offloading	Enables the AMS offloading feature.
Transrating	Enables the transrating feature.
Media Tunneling	Enables the media tunneling 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 SBCE supports SRTP over SIP towards the SIP trunks or call servers. Avaya SBCE 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 SBCE 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.

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 SBCE from a Trunk Server or Call Server.

Name	Description
Signaling Port Range	Used by Avaya SBCE to start connections for outgoing SIP requests from Avaya SBCE towards a SIP Server (Call Server or Trunk Server). The direction of these ports is away from Avaya SBCE.
Config Proxy Internal Signaling Port Range	Used by Avaya SBCE to start connections from Avaya SBCE 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 SBCE.
Listen Port Range	Used in PORTID Mode. See *Managing SIP Server Configurations*. Avaya SBCE 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 SBCE.
HTTP Port Range	Used by Tinyproxy to start connections for Avaya SBCE 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 SBCE.

RTCP Monitoring

Name	Description
RTCP Monitoring	Enables or disables RTCP monitoring.

Table continues…

Name	Description
Node Type	Specifies the type of Avaya SBCE configuration for the node. The options are: • **Core** • **DMZ** • **Remote**
Relay IP	Specifies the relay IP address. **Note:** • For CORE Avaya SBCE configuration, in the **Relay IP** field, click **Core SBC Internal IP1**. • Core Avaya SBCE 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
SBCE Interface IP	Specifies the source IP address of Avaya SBCE for communication between Avaya SBCE and the monitoring tool. **Note:** The IP address must be the IPv4 address.
SBCE Interface Port	Specifies the source port number of Avaya SBCE for communication between Avaya SBCE 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 SBCE 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 SBCE to keep track of the status of other Avaya SBCE in HA pair. The default keep alive interval is 500 milliseconds. The time range is 300 to 1500 milliseconds.
Max Retries	The maximum number of attempts for which Avaya SBCE must try to reach the HA pair.

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 Scopia management entity does load balancing towards the internal side. All http requests sent for dialing out use the internal load balancer logicto identify the appropriate Avaya SBCE. • **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.
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 SBCE security features.

The security features enable or disable settings defined here apply specifically to each Avaya SBCE device that is currently selected in the Application Pane. These settings only enable or disable one or more security features for the selected Avaya SBCE device.

The actual thresholds for each one of these security features are globally defined for all Avaya SBCE devices within the network by selecting: **Configuration Profiles** > **Domain DoS**.

See DoS Security Features on page 228.

Managing security features

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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. In the navigation pane, click **SBCE**.
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.

Table continues…

Name	Description
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. SBCE 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 SBCE supports the use of the same IP for more than one data interface. Use the following configuration to assign non-unique addresses to Avaya SBCE data interfaces.

Warning:

Do not use the same IP for different Avaya SBCE devices in the same network.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE from a Trunk Server or Call Server.

Name	Description
Signaling Port Range	(Direction = Away from Avaya SBCE) This port range is used by Avaya SBCE to start connections for outgoing SIP requests from Avaya SBCE towards a SIP Server (Call Server or Trunk Server).
Config Proxy Internal Signaling Port Range	(Direction = Away from Avaya SBCE) This port range is used by Avaya SBCE to start connections from Avaya SBCE toward Configuration Servers. For example, configuration servers of the following types: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP.
Listen Port Range	(Direction = Toward Avaya SBCE) This port range is used in PORTID Mode, see *Managing SIP Server Configurations*. Avaya SBCE 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.

Table continues…

Name	Description
HTTP Port Range	(Direction = Away from Avaya SBCE) This port range is used by Tinyproxy to start connections for Avaya SBCE 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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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**.

Global Parameters overview

With Global Parameters, you can manage Syslog and RADIUS parameters and provision authorized user agents (endpoints).

Adding a new RADIUS server

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** > **AAA**.
4. Click **Add**.

   The EMS server displays the Add Server screen.
5. Enter the requested information in the appropriate fields.
6. Click **Finish**.

Result

The EMS server displays the new RADIUS server in the content area.

Add 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 .

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 SBCE to maintain the current session upon receipt of the SESSION EXPIRE message. Clear the check box for Avaya SBCE to end the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method that the Avaya SBCE 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 SBCE 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 SBCE 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.

Editing an existing RADIUS server

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** > **AAA**.
4. Click **Edit**.

   The EMS server displays the Edit Server pop-up window.
5. Edit the required fields and click **Finish**.

Result

The EMS server updates and saves the RADIUS server configuration.

Deleting an existing RADIUS server

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** > **AAA**.
4. Click **Delete** corresponding to the RADIUS server that you want to delete.

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

Result

The EMS server deletes the selected RADIUS server.

Media Forking overview (Standard Platform only)

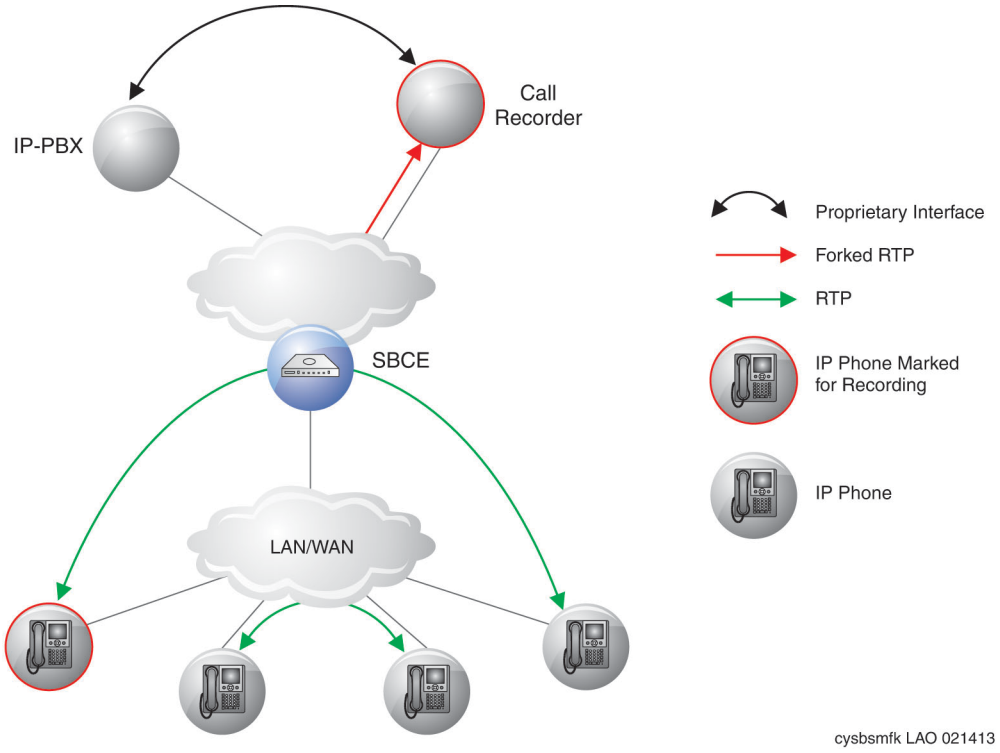
The Media Forking feature allows the Avaya SBCE device to fork media packets according to a designated Media Forking Profile. This solution addresses problems faced by call recorders deployed for quality assurance and compliance.

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 SBCE 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 SBCE device in the picture, the spanning of all ports is not required, as the Avaya SBCE 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. In the navigation pane, click **SBCE**.
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.
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. In the navigation pane, click **SBCE**.
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 SBCE supports LDAP version 3.

With this feature, Avaya SBCE:

- 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 SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE must wait for a response from the LDAP server.
Caching	The check box to enable caching.

Table continues…

Name	Description
Cache Size	The maximum number of entries that Avaya SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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.

SNMP settings

About this task

Provisioning SNMP parameters (v3) includes granting certain users access to the SNMP information. Use the following procedure to create the access accounts.

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. In the navigation pane, click **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 user access.

Uploading a cadf file to System Manager

About this task

To see Avaya SBCE alarms on System Manager, you must upload the Avaya SBCE common alarms definition file (cadf) to System Manager.

Procedure

1. Locate the cadf jar file for Avaya SBCE, `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.

SNMP v3

Adding SNMP v3 access

About this task

Use the following procedure to configure user access for SNMP v3 information.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **SNMP**.
3. In the content pane, click **SNMP v3** tab.
4. Click **Add**.

   The EMS server displays the Add User pop-up window.
5. Enter the requested information into the appropriate fields.
6. Click **Finish**.

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*.

Result

The content area displays the new SNMP v3 account.

SNMP field descriptions

Add User screen- 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.

Table continues…

Name	Description
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.
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 existing SNMP v3 account

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **SNMP**.
3. In the content pane, click **SNMP v3** tab.
4. Click **Edit**.

   The EMS server displays the Edit User pop-up window.
5. Edit the required fields and click **Finish**.

Result

The content area displays the edited SNMP v3 account.

Deleting an existing SNMP v3 account

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **SNMP**.
3. In the content pane, click **SNMP v3** tab.
4. Click **Delete** corresponding to the SNMP v3 account that you want to delete.

   The EMS server displays a confirmation pop-up window
5. Click **OK** to confirm the deletion of the SNMP user.

Result

The content pane no longer displays the deleted SNMP v3 user.

Creating an SNMP trap profile

About this task

With SNMP trap profiles, you can select the traps that Avaya SBCE must send to the Serviceability Agent.

You can create and use new SNMP trap profiles for SNMP v3 users. The EMS server uses the default trap profile for SNMP v1 and v2 users.

Procedure

1. Log in to the EMS server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **SNMP Traps**.

   The EMS server 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**.

Result

The EMS server 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.

Trap descriptions

Trap name	Description	Level
ipcsScpFailure	Secure copy failed for log files	Critical
ipcsCopyFailure	Copy action failed for log files	Critical
ipcsCPUUsage	CPU usage exceeded a set threshold	Critical: CPU utilization is 100% Major: CPU utilization is over 95%
ipcsMemoryUsage	Memory usage exceeded a set threshold	Critical: Memory utilization is 100%
ipcsDiskUsage	Disk usage exceeded a set threshold	Critical: Disk usage is over 90% Major: Disk usage is over 80% Minor: Disk usage is over 70%
ipcsDiskFailure	Hard disk failed	Critical
ipcsNetworkFailure	Network failed	Critical
ipcsProcessFail	Process in use failed	Critical
ipcsDatabaseFail	Database failed	Critical

Table continues…

Trap name	Description	Level
ipcsHAFailure	High Availability failed	Critical : Primary server is down Informational: Secondary server is coming to Primary server
ipcsHAHeartBeatFailure	Heartbeat from secondary HA server failed	Critical
ipcsRSAFailure	RSA algorithm failed	Critical
ipcsIncidenceNotification	Notification for incidence occurring in Avaya SBCE	No severity level is defined for this alarm.

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 server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **SNMP Traps**.

   The EMS server 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 server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **SNMP Traps**.

   The EMS server 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 server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **SNMP Traps**.

   The EMS server 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 server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **SNMP Traps**.

   The EMS server 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.

Adding a management server

Procedure

1. Log in to the EMS server with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Monitoring & Logging** > **SNMP**.

4. Click the **Management Servers** tab.
5. Click **Add**.

   The EMS server 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**.

Enabling and disabling traps by severity

About this task

Avaya SBCE supports severity-based enabling and disabling of traps only for traps generated by Avaya SBCE. You cannot disable system-generated traps.

Procedure

1. Log in to the EMS server with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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.

Table continues…

Name	Description
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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.
7.

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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 in conjunction with other types of domain policies. Routing profiles identify a particular call flow and thereby 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 because 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 SBCE uses that user data to route incoming calls from a SIP trunk within the enterprise network.
- On receiving SIP INVITE from SIP trunk, Avaya SBCE initiates an LDAP query towards LDAP server.
- On receiving the query response from LDAP server, Avaya SBCE selects next hop based on the configured routing profiles.

The communication of Avaya SBCE 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 SBCE 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 SBCE 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 SBCE uses the Heartbeat feature configured on the server entity. Avaya SBCE 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 SBCE 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 SBCE fails to route messages using resolved routing entry, then Avaya SBCE uses the next routing entry from the routing profile.

Creating a new routing profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, **SBCE**.
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.

Add 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 SBCE 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 SBCE 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 SBCE 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
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.

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. In the navigation pane, **SBCE**.
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. In the navigation pane, **SBCE**.
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. In the navigation pane, **SBCE**.
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. In the navigation pane, click **SBCE**.
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

About this task

Use the following procedure to make an exact copy or clone of an existing Routing profile.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, **SBCE**.
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 that 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. In the navigation pane, **SBCE**.
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 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. In the navigation pane, **SBCE**.
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 that you want to delete.
5. Click **Delete**.

   The EMS server displays the delete confirmation pop-up window.
6. Click **OK** to confirm the deletion of the routing profile.

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. In the navigation pane, click **SBCE** to select the security device for which you want to configure log-level information
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 • Trace • Security • Protocol • Registrations • Audit
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.
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.

Table continues…

Name	Description
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.
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.
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 SBCE 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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation page, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. Enter the requested information in the appropriate fields.

   Note:

   Port configuration is optional. However, if the user has a data firewall then the user must synchronize the ports configured in the Avaya SBCE with the ports in the data firewall. If the user has no data firewall, no action is required.
6. Click **Finish**.

Result

The EMS server displays the new configuration in the Signaling Interface screen.

Add 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 SBCE used by SIP signaling messages traversing the network.
TCP Port	The port that the Avaya SBCE security device processes for TCP packets.
UDP Port	The port that the Avaya SBCE security device processes for UDP packets.
TLS Port	The port that the Avaya SBCE 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 SBCE security device. This check box must be enabled only on the Internal Side Interface of Avaya SBCE, that is, towards call server. You must enable the Avaya SBCE TLS port before enabling this check box.
Shared Control Port	The port that the Avaya SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
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. Edit the required fields, and click **Finish**.

Result

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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, **SBCE**.
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 SBCE to which media packets are sent.
Port Range	The range of ports on the Avaya SBCE 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**.

Table continues…

Name	Description
Buffer Size	The maximum size of video frames that Avaya SBCE stores on its network buffer. For example, if the **Buffer size** is set to 400 KB, then Avaya SBCE 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 SBCE 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. In the navigation pane, **SBCE**.
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. In the navigation pane, **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface parameters.

Deleting an existing media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.

   The EMS server displays the Media Interface parameters.
4. In the content pane, click **Delete** corresponding to the Media 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 media interface.

Chapter 7: Security Configuration

Overview

From the EMS web interface, you can view various security-related features of Avaya SBCE 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

Related links

Creating a new Topology Hiding profile on page 241

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 228.

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:

The threshold settings for each DoS/DDoS attack protection security features defined here apply globally to all SBCE 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 SBCE 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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 228

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 SBCE.

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 SBCE.

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 SBCE.

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 SBCE.

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 the administrator credentials.

2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

Table continues…

Name	Description
Max Concurrent Sessions	Maximum number of concurrent sessions
Number of Remote Users	Number of remote users for the DoS profile
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.

Table continues…

Name	Description
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 SBCE. • **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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 232

Deleting a Domain DoS profile

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 inn to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. Select the Avaya SBCE 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 SBCE 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 237

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.
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 237

Protocol scrubber

Protocol Scrubbing is an Avaya SBCE feature that utilizes a highly sophisticated statistical mechanism to check incoming SIP signaling messages for various types of protocol-specific events and anomalies. Protocol scrubbing verifies certain message characteristics, such as proper message formatting, message sequence, field length, and content, against editable templates that are received from Avaya. Typically, messages that violate the security rules dictated by the scrubber templates are dropped. Messages that violate syntax rules are repaired by being re-written, truncated, rejected, or dropped, depending upon the processing rules imposed by the templates.

Note:

Protocol Scrubbing rule templates are prepared by Avaya and can only be minimally edited by the user.

With the Protocol Scrubbing feature for SIP, you can:

- Install a scrubber rules package.
- Enable or disable the scrubber rules contained in the package.
- Delete the package from the system.
- View a list of all currently installed scrubber rules.

Note:

VIPER signatures are similar to Scrubber Packages, and are created by the VIPER team, and then packaged and released by the engineering team after testing.

See Security Rules on page 96.

Scrubber package file path

The latest Scrubber packages are present in the following directory in the EMS: `/usr/local/scrubber`. The old Scrubber package must be removed, and the new package must be installed. See Deleting an Existing Scrubber Rules Package on page 240 and Installing a scrubber rules Package on page 239 respectively.

Viewing scrubber rules

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 installed scrubber rules and templates.

Installing a scrubber rules package

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 containing the chosen scrubber package.
7. Select the scrubber package.
8. Click **Install**.

   The EMS server loads and enables the selected scrubber package and lists the package in the **Packages** tab.

   Note:

   You must enable Scrubber in the Security Rules of Domain Policies before it takes effect. Once you enable the Scrubber in the Security Rules of Domain Policies, a list of packages will be required for the Security Rule.

Related links

Security rules on page 96

Enabling or disabling an installed Scrubber Rules package

Before you begin

Ensure that the Scrubber Rules package is installed and enabled.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **System Parameters** > **Scrubber**.
4. Click the **Packages** tab.
5. In the content area , click the **Toggle** button corresponding to the scrubber package that you want to enable or disable.

Result

The selected scrubber package is enabled or disabled.

Deleting a Scrubber Rules package

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 the administrator credentials.
2. In the navigation pane, click **SBCE**.

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
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.

Creating a new Topology Hiding profile

About this task

Topology Hiding modifies the domain portion of SIP headers. For example, 1234@avaya.com can become 1234@135.122.18.7. Though changing the headers can obscure 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.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 **Add**.

   The EMS server displays the Topology Hiding Profile screen.
5. Enter the required information in the appropriate fields and click **Finish**.

Result

The EMS server saves the data and displays the new profile in the application pane.

Related links

Protocol scrubber on page 238

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**

Table continues…

Name	Description
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.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 247 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 248, descriptions are provided for all possible combinations of selections in the **Header**, **Criteria**, and **Replace Action** fields.

Avaya SBCE ignores the Topology Hiding setting for the Refer-To header if:

- The Refer-To has an embedded Replaces header.
- Avaya SBCE has an existing SIP INVITE dialog for the Replaces header.

In this scenario, Avaya SBCE uses the contact of the replacing dialog to rewrite the Refer-To URI.

Related links

Topology Hiding headers on page 247
Topology Hiding settings examples on page 248

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		

Table continues…

Main Header names	Headers affected by Main Header	Header affecting this header
Refer To		To
Diversion		
SDP Headers		
Origin Header		

Related links

Headers affected by Topology Hiding on page 246

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.

Related links

Headers affected by Topology Hiding on page 246
Topology Hiding examples for Request-Line Header on page 248
Topology Hiding examples for From header on page 249
Topology Hiding examples for To header on page 250
Topology Hiding examples for Record-Route header on page 251
Topology Hiding examples for Via header on page 251
Topology Hiding examples for SDP header on page 251

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

Related links

Topology Hiding settings examples on page 248

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

Related links

Topology Hiding settings examples on page 248

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

Related links

Topology Hiding settings examples on page 248

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

Related links

Topology Hiding settings examples on page 248

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 SBCE 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.

Related links

Topology Hiding settings examples on page 248

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

Related links

Topology Hiding settings examples on page 248

Chapter 8: Server and Network Interface configuration

Overview

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.

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 SBCE 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.

Adding a new SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 page, enter the requested information in the appropriate fields, and click **Next**.

7. On the Edit SIP Server Profile - Authentication page, enter the requested information in the appropriate fields and click **Next**.
8. On the Edit SIP Server Profile - Heartbeat page, enter the requested information in the appropriate fields and click **Next**.
9. On the Edit SIP Server Profile - Registration page, enter the requested information in the appropriate fields and click **Next**.

   Note:

   The EMS server does not display the Edit SIP Server Profile - Heartbeat tab and Edit SIP Server Profile - Registration tab 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 page, enter the requested information in the appropriate fields.
12. Click **Finish** to save the changes.

Add Server Configuration profile field descriptions

General tab

Name	Description
Profile Name	The name of the server profile.
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 SBCE. • **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 SBCE first looks for custom host names configured in the TLS profile. If the custom host name is blank, Avaya SBCE then looks for the SIP Domain specified in the server configuration.

Table continues…

Name	Description
DNS Query Type	The DNS query type that Avaya SBCE 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. This is the default query type for migrated customers in Release 7.2.1 and earlier. • **SRV**: Used when Avaya SBCE sends the SRV type query to the DNS server. 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 SBCE 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 SBCE does not support AAAA-query for FQDN. • You can select **DNS Query Type** for **Server Type** as **Trunk Server** only.
TLS Client Profile	The TLS Client profile to be used for the SIP server. The **TLS Client Profile** option is available for **DNS Query Type** as **NAPTR** only.
IP Addresses/FQDNs	The IP address or Fully Qualified Domain Name (FQDN) of the SIP server. You can add multiple IPs and 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 SBCE.
Verify TLS Common Name	The option for specifying whether the TLS common name must be verified during the TLS handshake. The EMS server displays this field only when the **Server Type** is **Remote Branch Office**.

Table continues…

Name	Description
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 SBCE 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 unavailable 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**.

Authentication tab

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 inactivated.
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 tab

Name	Description
Enable Heartbeat	Indicates whether a synchronization signal (heartbeat) is established between the Avaya SBCE 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.
Method	Specifies the method by which the heartbeat is maintained. The options are: • **OPTIONS** • **PING**
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 tab

Name	Description
Register with All Servers	To send a REGISTER message to all servers. • For the **DNS Query Type** as None/A, Avaya SBCE 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 SBCE 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. If the highest priority server is non-functional on DNS TTL expiry, SBCE 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 SBCE sends a REGISTER message to servers.
From URI	Specifies the source of the REGISTER message.
To URI	Specifies the destination of the REGISTER message.

Advanced tab

Name	Description
Enable DoS Protection	Indicates whether DoS protection is enabled for the SIP server. 1. 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. 2. 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.
Connection Type	Specifies the manner in which the connection is established. The options are: • **SUBID** • **PORTID** • **MAPPING**

Table continues…

Name	Description
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 SBCE provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBCE 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 SBCE uses to route SIP traffic through an alternate Session Manager when a Session Manager is unreachable.
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.

DoS Whitelist tab

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.
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.

Table continues…

Name	Description
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 SBCE. • **Whitelist**: The call is not blocked if the call originator exists in the **Whitelist**.

Note:

Registration tab and **Heartbeat** tab are not available for **Server type** as **Remote Branch Office**.

Viewing a SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The application pane displays the list of available server profiles.

Editing a SIP Server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 and click **Finish**.

Cloning an existing SIP Server profile

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.

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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE.**
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**.

Server interworking

With the Server Interworking in Configuration Profiles, you can set certain parameters to make Avaya SBCE function in an enterprise VoIP network using different implementation of the SIP protocol.

Adding a new Interworking profile

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles screen, click **Add**.

The EMS server displays the Interworking Profile page.

5. In the **Profile Name** field, type a name for the new interworking profile, and click **Next**.
6. On the Interworking Profile page, type the requested information in the appropriate fields for the **General** tab.
7. Click **Next**.
8. On the Interworking Profile - SIP Timers page, type the requested information in the appropriate fields for the **Timers** tab.
9. Click **Next**.
10. On the Interworking Profile page, type the requested information in the appropriate fields for the **Privacy** tab.
11. Click **Next**.
12. On the Interworking Profile page, type the requested information in the appropriate fields for the **Advanced** tab.
13. Click **Finish** to save the settings.

Add Interworking Profile field descriptions

General tab

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**
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**

Table continues…

Name	Description
183 Handling	Determines how 183 Session Progress messages are handled. The options are: • **None** • **SDP** • **No SDP**
Refer Handling	Indicates whether Avaya SBCE 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 SBCE through the enterprise call server. Avaya SBCE 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**
URI Group	Indicates the URI group that is required for REFER handing. **Note:** SBCE enables the **URI Group** field only when you select the **Refer Handling** checkbox.
Send Hold	Indicates whether Avaya SBCE 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:** SBCE enables the **Send Hold** check box only when you select the **Refer Handling** check box.
Delayed Offer	Indicates whether Avaya SBCE sends an INVITE message to the transferee without SDP. If you select **Delayed Offer**, Avaya SBCE gets the complete capabilities of the transferee as an SDP Offer message. SBCE enables the **Delayed Offer** check box only when you select the **Refer Handling** check box.
3xx Handling	Indicates whether the Avaya SBCE security device will handle the *3xx Redirection Response* messages.
Diversion Header Support	Indicates whether the Avaya SBCE 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 SBCE security device processes delayed SDP packets.

Table continues…

Name	Description
Re-Invite Handling	Indicates whether re-invite handling is enabled for Avaya SBCE. If a trunk or call server does not want in-dialog **RE-INVITES**, then enable re-invite . Precondition: **RE-INVITE SDP** must be the same as the previous INVITE transaction SDP. For example, consider a trunk server that has Re-Invite Handling enabled. When the first **INVITE** with SDP goes to the trunk server, Avaya SBCE stores this message. When the next **INVITE** goes to the trunk server, then Avaya SBCE tries to match the current **INVITE SDP** with the stored SDP. If both SDPs are same, then Avaya SBCE stops **INVITE** and responds . However, if a second INVITE comes without any SDP change, while adding extra SDP parameters to Hold or Resume, then Avaya SBCE handles **RE-INVITE**.
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 SBCE 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 SBCE security device. supports the T.38 FAX Relay standard.
URI Scheme	Indicates the URI scheme that the Avaya SBCE security device will use. The options are: • **SIP** • **TEL** • **ANY**
Via Header Format	Indicates the header format used by the Avaya SBCE security device. The options: • **RFC3261** • **RFC2543**

Timers tab

Name	Description
SIP Timer	
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.

Table continues…

Name	Description
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 tab

Name	Description
Privacy	
Privacy Enabled	Indicates whether privacy is used between the Avaya SBCE 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 SBCE 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 SBCE 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 SBCE uses the P-Preferred-ID during private sessions.
Privacy Header	Specifies the Privacy Header to be used during privacy sessions.

URI Manipulation tab

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 SBCE 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 SBCE 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 tab

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.

Advanced tab

Name	Description
Record Routes	Directs the Avaya SBCE security device to record route information. The options are: • **None**: Avaya SBCE does not add any record route. However, to remove all record routes, enable Topology Hiding (TH) with record route auto. • **Single Side**: Avaya SBCE adds only one record route. If Avaya SBCE receives a 200 OK message, Avaya SBCE passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed. • **Both Sides**: Avaya SBCE adds two record routes. If Avaya SBCE receives a 200 OK message, Avaya SBCE 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 (Both Sides)**: Avaya SBCE adds two record routes, but not to the in-dialog message. If Avaya SBCE receives a 200 OK message, Avaya SBCE 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 SBCE adds one record route, but not to the in-dialog message. If Avaya SBCE receives a 200 OK message, Avaya SBCE passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed.

Table continues…

Name	Description
Include Endpoint IP for Context Lookup	Directs the Avaya SBCE security device to use endpoint IP while looking for Avaya SBCE internal SIP context.
Extensions	Directs the Avaya SBCE security device to use functionality specific to different environments. The available options are: • **Avaya** • **Nortel** • **Lync** • **Cisco**
Diversion Manipulation	Directs the Avaya SBCE security device to copy SIP Diversion header from 3xx messages to Sip Request messages while 3xx handling is enabled on Avaya SBCE 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 SBCE 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 SBCE security device to use far-end firewall functionality.
Route Response on Via Port	Directs the Avaya SBCE security device to use SIP Via header port to route response.
Relay INVITE Replace for SIPREC	Check box to enable **Relay INVITE Replace for SIPREC**.
MOBX Re-INVITE Handling	Check box to enable **MOBX Re-INVITE Handling**.
DTMF	
DTMF Support	Indicates the type of DTMF support. The options are: • **None** • **SIP NOTIFY** • **RFC 2833 Relay and SIP Notify** • **SIP INFO** • **RFC 2833 Relay and SIP Info** • **Inband**

Viewing existing Server Interworking profiles

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profile page with the list of available interworking profiles in the application pane.

Editing the Server Interworking profile parameters

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles page, click the tab, for example, **General**, **Timers**, or **Advanced** to edit the parameters.

   The EMS server displays the parameters for that tab.
5. Click **Edit**.

   The EMS server displays the corresponding Editing Profile page.
6. Edit the required parameters, and click **Finish**.

Cloning a Interworking profile

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 new URI Manipulation rule

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profiles page.
4. Click **URI Manipulation** tab.
5. Click **Add**.
6. On the Add Rule page, type the requested information in the appropriate fields.

7. Click **Finish**.

Editing an existing URI Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. Edit the required regex parameters, and click **Finish**.

Deleting an existing URI Manipulation rule

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 new Header Manipulation rule

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profiles page.

4. Click **Header Manipulation** tab.
5. Click **Add**.
6. On the Add Rule page, type the requested information in the appropriate fields.
7. Click **Finish**.

Editing a Header Manipulation rule

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The EMS server displays the Interworking Profiles page.
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. Edit the required parameters, and click **Finish**.

Deleting a Header Manipulation rule

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE routing protocols, thus requiring an intimate knowledge of the VoIP network topology to be effective.

When you install an Avaya SBCE 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 SBCE device, see *Installing an Avaya SBCE device*. The network-specific information populates various **Network Management** tabs. To optimize the device performance and network efficiency, you can change the information.

Adding a new network interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.
Dhcp	Status of the DHCP feature for the interface: enabled or disabled.

Add VLAN

Name	Description
Name	Provide the interface name or VLAN interface name.

Table continues…

Name	Description
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.

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 SBCE on a VLAN use a physical link connected to a physical interface.

The second step is to configure all networks to which Avaya SBCE connects. Each network to which Avaya SBCE 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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

Changing the administrative state of an interface

Procedure

1. Log in to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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 using the administrator credentials.
2. In the navigation pane, click **SBCE**.
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

TLS Parameter Management

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 SBCE security products utilize TLS primarily to facilitate secure communications with remote users.

Avaya SBCE 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 SBCE 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” and “TLS profile management”.

Certificate Management

Use certificate management function of Avaya SBCE to manage all certificates used in TLS handshakes.

Note:

All certificates, certificate authorities, and certificate revocation lists uploaded to the EMS must be valid PEM-encoded X.509 certificates. Certificates not in this format can be converted using a proper SSL tool, such as the publicly available OpenSSL tool at https://www.openssl.org/. For tips and tricks about working with certificates using OpenSSL, see “Tips and tricks for working with TLS”.

Certificate Signing Requests

The GUI of EMS includes a basic built-in tool to generate a CSR, specifically for use on EMS.

Generating a CSR using the built-in tool that is provided in Avaya SBCE generates a CSR that is compatible with Avaya SBCE. However, using this built-in tool to generate a CSR is not mandatory.

Related links

Installing third-party certificates on page 282

Installing third-party certificates

About this task

Use this procedure to change the TLS certificate presented to the user when logging in to the management GUI.

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 key must be equal to greater than 2048-bit.

Procedure

1. Copy the PEM-encoded certificate and associated private key to the EMS server.
2. To encrypt the RSA private key, type `enc_key` *`path_to_key_file private_key_passphrase`*.

   path_to_key_file is the path where the private key file is stored, and *private_key_passphrase* is the passphrase for the key. If the private key does not have a passphrase, use `""` as the *private_key_passphrase*.
3. Navigate to the directory where you saved the copy of the certificate and private key.
4. 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.

Related links

Certificate Management on page 281

Creating a certificate signing request

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 screen field descriptions on page 287

Settings for externally generated CSRs

If you want to generate your own CSR for use with the Avaya SBCE, the following settings are recommended:

- Private Key Strength: 2048-bit or greater
- 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 SBCE.
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.

Certificates

An X.509 public key certificate is used to identify the Avaya SBCE 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.

Installing certificates

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 SBCE 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 SBCE EMS web interface.
7. If you generate CSR using the Avaya SBCE 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 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, reencode 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 SBCE. 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 SBCE.

    For an HA pair, the certificate and key are uploaded to the primary device and synchronized to the secondary device.

    Important:

    From Release 8.0 and later, EMS server synchronizes and installs certificate on multi-server and single server deployment automatically.

Related links

TLS Certificates screen field descriptions on page 287

Viewing certificate details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen.
4. Locate the Avaya SBCE 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. In the navigation pane, click **SBCE**.

3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen.

4. Locate the Avaya SBCE 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.

TLS Certificates screen 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.
Allow Weak/Certificate Key	An option to permit usage of a weak private keys. This option bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
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 SBCE. 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.

Table continues…

Name	Description
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. You cannot provide wildcard (*) characters 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 4096) 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.
Subject Alt Name	An optional text field that can be used to further identify this certificate. You can provide multiple comma-separated entries in this field. You can make maximum of 10 **Subject Alt Name** entries. You cannot provide wildcard (*) characters in this field. Avaya SBCE supports DNS hostname, IP address and SIP domain name as the valid entries for **Subject Alt Name** field. Avaya SBCE does not support SIP URI as a valid value for the **Subject Alt Name** field.
Passphrase	The password used when encrypting the private key.
Confirm Passphrase	A verification field for the Passphrase.
Contact Name	The name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.
Contact E-mail	The e-mail address of the contact.

Certificate Authority certificates

A Certificate Authority certificate, or CA certificate, is used to verify that a party is trusted by Avaya SBCE. Avaya SBCE accepts both CA root certificates and intermediary CA certificates.

Installing CA certificate

Procedure

1. Log in to the EMS web interface with administrator credentials
2. In the navigation pane, click **SBCE**.

3. In the navigation pane, click **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 screen field descriptions on page 287

Viewing Certificate Authority details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.
4. Locate the Avaya SBCE certificate authority certificate that you want to view and click **View**.

   The EMS server displays the View CA Certificate window.
5. After viewing the certificate authority certificate information, click the Cancel icon.

Deleting Certificate Authority certificates

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.

   The EMS server displays the Certificates screen in the Content Area.
4. Locate the Avaya SBCE certificate authority (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**.

Result

The EMS server displays the Certificates screen with the deleted CA certificate.

Install CA Certificate screen 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. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.
Certificate File	The location of the certificate on your system. Click **Browse** to locate the file.

Certificate Revocation Lists

A Certificate Revocation List, or CRL, is used to revoke certificates that have been issued by a CA that Avaya SBCE trusts. CRL is the only way to revoke an invalid certificate. CRLs list information embedded in certificates, and CA certificates are ignored.

Installing Certificate Revocation List

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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**.

Viewing Certificate Revocation List details

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.
4. Locate the Avaya SBCE certificate revocation list that you want to view, and click **View**.
5. After viewing the certificate revocation list information, click the Cancel icon.

Deleting Certificate Revocation Lists

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Certificates**.
4. Locate the Avaya SBCE certificate revocation list that you want to delete, and click **Delete**.
5. Click **OK** to delete the selected certificate revocation list.

Result

The EMS server displays the Certificates screen with the deleted CRL.

Install CRL screen 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.

TLS Profile Management

The basis of the Avaya SBCE 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.

Client Profile Management

A Client Profile is used where the Avaya SBCE 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.

Creating a client profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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.

Result

The EMS server installs and displays the new TLS client profile.

Related links

TLS client profile screen field descriptions on page 294

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. The options are: • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** 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**.

Related links

Creating a client profile on page 293

Editing a Client Profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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 294

Deleting a client profile

About this task

Use the following procedure to delete an existing TLS client profile.

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. In the navigation pane, click **SBCE**.
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**.

Result

The EMS server deletes the TLS client profile.

Server Profile Management

A Server Profile is used where Avaya SBCE 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.

Creating a new TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click **Add**.

   The EMS server displays the New Profile window.
5. Enter the requested information into the appropriate fields.
6. Click **Finish**.

Result

The EMS server creates, installs and lists the TLS server profile in the application pane.

Related links

TLS server profile screen field descriptions on page 298

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.
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 SBCE 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 SBCE 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 SBCE 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 SBCE 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. The options are: • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** 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.
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.

Table continues…

Field	Description
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 (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**.

Related links

Creating a new TLS server profile on page 297

Editing a server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. Edit the desired fields and click **Finish**.

   To go to the previous field values and close this screen, click the Cancel icon.

Deleting a server profile

About this task

Use the following procedure to delete an existing TLS server profile.

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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**.

Result

The EMS server deletes the TLS server profile.

Checklist for establishing end-to-end TLS communications

Prerequisites

To establish end-to-end TLS communication, it is assumed that:

- Avaya SBCE 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 SM and CM 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 SBCE can identify and communicate with all external entities.	

Table continues…

No.	Task	Description	✔
2	Generate a certificate signing request.	A CSR must be generated for Avaya SBCE for signing by the CA. The signed certificate is used to identify the Avaya SBCE. For more information, see Creating a certificate signing request on page 282.	
3	Install the third-party certificate.	After the CA signs the CSR, upload the signed CSR to Avaya SBCE. For more information, see Installing certificates on page 284.	
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 SBCE 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 297.	

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 SBCE 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 293.	
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 SBCE. **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 223.	

Table continues…

No.	Task	Description	✔
7	Update the subscriber flow.	To enable the Avaya SBCE 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 existing endpoint flows on page 143.	
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 SBCE 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 261.	

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.

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 SBCE 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`.

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 SBCE must support TLS Server Name Indication (SNI).

Note:

Avaya SBCE provides server default certificate for backward compatibility for clients that do not support SNI.

SNI Group

An SNI group is a collection of TLS profiles. The functionality of SNI group depends on Avaya SBCE, if it is acting as a client or as a server during the communication.

Avaya SBCE as a server

When client sends a handshake packet to the Avaya SBCE server, then depending on the **Server Profiles** option in **TLS Management** > **Server Profiles**, Avaya SBCE 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 SBCE server accepts handshake packet and allows the communication.

Avaya SBCE as a client

For enabling SNI from the Avaya SBCE client, enable **Extended Hostname Verification** from **TLS Management** > **Client Profiles** and provide the **Server Hostname**. Avaya SBCE 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 SBCE 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 SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **SNI Group**.

   The application pane displays the existing SNI group.
4. Click **Add**.

   Avaya SBCE displays the first SNI Group window.
5. In the **Rule Name** field, type a name for the new SNI Group, and click **Next**.

   Avaya SBCEdisplays 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. In the navigation pane, click **SBCE**.
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 SBCEdisplays 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. In the navigation pane, click **SBCE**.
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 SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE displays the delete confirmation window.
6. Click **OK**.

Result

The application pane no longer displays the deleted SNI group.

Chapter 10: System Monitoring

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 SBCE security devices.
- Avaya SBCE 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.
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 SBCE security devices currently deployed throughout the network.
Incidents (past 24 hours)	A list of current incidents reported by Avaya SBCE security devices to the EMS web interface.

Table continues…

Name	Description
Active Alarms (past 24 hours)	A list of current alarms reported by Avaya SBCE 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.

Manage system 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 SBCE device for which you want to view the alarms.

   The Alarms section displays all the currently active alarms for the selected Avaya SBCE 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.

Table continues…

Name	Description
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 SBCE 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**.

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.

Viewing system 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** toolbar, click **SIP Statistics**.

   Warning:

   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**

Statistics Viewer field descriptions

SIP Summary tab

Name	Description
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.

Table continues…

Name	Description
Active Calls	The number of active SIP calls.
Active SRTP Calls	The number of active calls using media as SRTP.
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.

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.

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.

Table continues…

Name	Description
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.

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 Scopia® video session licenses that are reserved.
Scopia Video Sessions In-Use	The number of Avaya Scopia® video session licenses that are currently in use.
CES Sessions Reserved	The number of CES session licenses that are reserved.
CES Sessions In-Use	The number of CES 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.

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** toolbar, click **Periodic Statistics**.
3. To view the statistics, click one of the following tabs:
   - **Summary**
   - **Subscriber Flow**
   - **Server Flow**
   - **Policy Group**
   - **To URI**
   - **From URI**

Periodic statistics field descriptions

Name	Description
Total Registrations	The number of active SIP registration requests received.
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 SBCE because of policy violation.
Calls Rejected by SBC	The number of SIP calls rejected by Avaya SBCE.
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 SBCE.
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 SBCE.
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 SBCE detected any inactivity.
Media Relinquished Calls	The number of media relinquished calls.
Shared Control Calls	The number of shared control calls.

Table continues…

Name	Description
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.

Real Time SIP Server Status

Avaya SBCE Release 6.3 onwards, 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. You can use the **Server Status** option of the **Status** toolbar to view the status of the connection. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

For the servers to show up in the Status window, you must configure server heartbeat in Server Configuration.

Configuring Avaya SBCE for Real Time Trunk status

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Services** > **SIP Servers**.
4. Click the **Heartbeat** tab.
5. Select the **Enable Heartbeat** check box.

   This option enables the heartbeat. After enabling the heartbeat, configure the server flow for this server.
6. In the navigation pane, click **Network & Flows** > **Endpoint flows** > **Server flows**.

   For more information about creating server flows, see Creating Flow toward Call Server on page 414.

   Note:

   In a high availability failover scenario, the EMS server displays the actual status of the server after 5–10 seconds.

   If the server address used is FQDN, the FQDN must be successfully resolved by the Avaya SBCE to display the server status.

Viewing the status of the SIP servers

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** toolbar, click **Server Status**.

   The EMS server displays the Status screen.

   The EMS server displays server information, such as Server Profile, FQDN, IP address, Transport, Port, Heartbeat Status (UP/DOWN/UNKNOWN), Registration Status (REGISTERED/NOT REGISTERED/UNKNOWN) and Time when the status field was last updated.

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.
Registration Status	The registration status of the server.
TimeStamp	The date and time when the server status was updated.

Note:

- When **Heartbeat** is enabled and **Registration** is disabled on the Server Configuration page, then **Registration Status** displays the status as UNKNOWN.
- When **Heartbeat** is disabled and **Registration** is enabled on the Server Configuration page, then **Heartbeat Status** displays the status as UNKNOWN.

User registration

You can view the list of users that are registered through Avaya SBCE 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** toolbar, click **User**.

   The EMS server displays the list of registered users.
3. 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 SBCE 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.

User Registrations field description

The User Registrations screen displays the list of endpoints registered through Avaya SBCE 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 of Registration	The time when the user registration status was last updated.

When the endpoint tries to register to Avaya SBCE, each call server uses the following information:

Name	Description
SBC device	The Avaya SBCE device that receives the REGISTER message.

Table continues…

Name	Description
Session Manager address	The address of the call server with the primary or secondary status.
Registration state	The registration status of the endpoint.

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 SBCE 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**

Table continues…

Name	Description
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.

Viewing diagnostics results

About this task

The Diagnostics screen provides a variety of tools to aid in troubleshooting Avaya SBCE operation. Available tools include a full diagnostic test suite, and individual tabs to monitor certain functional aspects of Avaya SBCE, such as TCP and TLS activity.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Diagnostics**.

   The EMS server displays the Diagnostics 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 EMS server 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 SBCE to EMS.
Ping: EMS to SBC	Sends a ping request from EMS to Avaya SBCE.
SBC Link Check: A1	Checks the Avaya SBCE A1 interface. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2

Table continues…

Name	Description
Ping SBC [A1] to Gateway	Sends a ping request from the Avaya SBCE A1 interface to the Gateway. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2
Ping SBC [A1] to Primary DNS	Sends a ping request from the Avaya SBCE 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 SBCE 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.

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.

Trace

With the Trace function, you can trace an individual packet or group of packets comprising a call through Avaya SBCE. The information shows how the call traversed the Avaya SBCE-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. In the navigation pane, click **SBCE**.
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.
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.

Logs collection

Using log collection feature you can:

- Collect and download logs from a web interface for investigating and troubleshooting an issue.
- Sort the collected logs by **File Name**, **File Size**, and **Last Modified**.
- Sort the collected logs in ascending and descending order.
- Delete the logs that you do not require.

Collecting and downloading logs

About this task

Use this procedure to collect and download logs from a web interface for investigating and troubleshooting an issue.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Monitoring & Logging** > **Logs Collection**.
4. In the application pane, click the type of device for which you want to collect logs.
5. In the content area, click the **Collect Logs** tab and do the following:
   a. Select the type of logs that you want to collect.
   b. Click **Collect Logs** to collect the selected logs.

   The EMS server saves the collected logs in **Log Archive**.
6. In the content area, do the following:
   a. Click **Log Archive**.
   b. Select the log file that you want to download.

      The EMS server saves the log file on your computer.

Collect logs field descriptions

Name	Description
All Logs	Specifies database and application 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	Specifies the database dump logs.
Application logs	Specifies SSYNDI logs.
GUI logs	Specifies the web interface and jsp logs. **Note:** The **GUI logs** option is available for EMS only.
Upgrade Logs	Specifies upgrade related logs.
Crash Dumps	Specifies heap dumps.
From Date & Time	Specifies the **From Date & Time** after which any log file modified or generated will be collected.
To Date & Time	Specifies the **To Date & Time** before which any log file modified or generated will be collected. **Note:** Logs generated and modified between **From Date & Time** and **To Date & Time** time range will be collected.

Collect Archive field descriptions

Name	Description
File Name	The file name of the collected logs.
File Size	The size of the collected logs in bytes.
Last Modified	The date and time when the collected logs were last modified.

Button	Description
Delete	Deletes the selected log.

Chapter 11: Avaya SBCE CLI commands

Overview

The Command Line Interface (CLI) provides a high-speed serial management interface for local or remote access to the Avaya SBCE security device. With the CLI, you can access Avaya SBCE 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.

Note:

If any firewall is present between EMS and Avaya SBCE, port 222 must be open bidirectionally.

The CLI for Avaya SBCE interface, hereafter referred to as clipcs, is available when Avaya SBCE is running. Security is provided through a combination of account login and user access privileges.

Configuring Avaya SBCE for HA deployment using CLI

Before you begin

- EMS server must be functional and in the same network with Avaya SBCE.
- Both Avaya SBCEs in the HA pair must be installed and functional.

Procedure

1. Log in to the primary Avaya SBCE device.
2. Edit `cli_sbce_config.sample` file located at `usr/local/ipcs/etc` by removing # sign and modifying the respective parameters.
3. Rename the `cli_sbce_config.sample` file to `cli_sbce_config`.

   Primary and secondary Avaya SBCEs are added to the EMS server in commissioned state.

   Note:

   You should not change any configurations at secondary Avaya SBCE when you are configuring Avaya SBCE for HA deployment using CLI.
4. Check `cli_sbce_config` file for successful configuration of Avaya SBCE.

If configuration is successful, `cli_sbce_config` will be renamed to `cli_sbce_config.commissioned` file.

Configuring Avaya SBCE for single server deployment using CLI

Before you begin

- Install Avaya SBCE.
- EMS server must be functional and in the same network with Avaya SBCE.

Procedure

1. Log in to the Avaya SBCE device.
2. Edit `cli_sbce_config.sample` file located at `/usr/local/ipcs/etc` by removing # sign and modifying the respective parameters.
3. Rename the `cli_sbce_config.sample` file to `/usr/local/ipcs/etc/cli_sbce_config`.

   Avaya SBCE is in commissioned state.
4. Check `cli_sbce_config` file for successful configuration of Avaya SBCE.

   If configuration is successful, `cli_sbce_config` will be renamed to `cli_sbce_config.commissioned` file.

traceSBC commands

Use **`traceSBC`** to start the traceSBC tool from the command line interface. For command line help, use the –h parameter.

Syntax

```
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.

Examples

To start a new capture, run 'traceSBC' without arguments and then press `s`: **`traceSBC`**

To filter SIP messages from/to 1.1.1.1 and 2.2.2.2: **`traceSBC -i`** *"1.1.1.1|2.2.2.2"*

To analyze a previously captured SSYNDI file named my_sbc.log: **`traceSBC my_sbc.log`**. 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, go to **Monitoring & Logging** > **Debugging**. Select the SBCE device and then click the **SSYNDI debug logs**checkbox.

sbceinfo commands

Use the **`sbceinfo`** command options to obtain system version, application type, and hardware details.

Syntax

```
sbceinfo [options]
```

Where options are:

getversion	Displays Avaya SBCE version information.
gethwtype	Displays Avaya SBCE hardware information.
getemsip	Displays the EMS IP address.
getapptype	Displays the application type running on the server.

Running clipcs commands

About this task

The **clipcs** commands are used to display basic information about Avaya SBCE 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.

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 SBCE systemwide commands can be executed. The Instance mode is the next level of administrative control that provides direct access to a particular Avaya SBCE 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 (#), type `clipcs` and press `Enter`.

   The system displays the Avaya SBCE 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. On the `SBC#` prompt, type `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 SBCE nodes. In the Instance mode, this command displays the detailed operational status of the node being accessed.
select	Selects a particular Avaya SBCE node for access and activates the Instance mode.

Running the show flow command

About this task

The **show flow** command for the Avaya SBCE is used for troubleshooting network problems in active sessions, where media is unidirectional or is not received.

Procedure

1. On the root level prompt (#), type **clipcs** .

   The system starts the Avaya SBCE console.

2. On the `SBC#` prompt, type `help`.

   The system displays the list of available **clipcs** commands.

3. On the root level prompt (#), type **show flow** *static* or `show flow <dynamic> <(ip addr) || (ip_addr:port)] [RTP/RTCP/SRTP/SRTCP].`

   The system displays the media relay information for the active session phone IP.

   Note:

   If you specify a port number in the command line, the protocol entry at the end of the command line is not valid.

Instance commands

Instance commands are also referred to as **top** commands. These commands are used to display detailed information about a specific Avaya SBCE node in the network and EMS node with multiple Avaya SBCE 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 SBCE node or communicate with the selected EMS or Avaya SBCE 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 SBCE node. The display is automatically refreshed every 5 seconds.

Avaya SBCE reconfiguration script options

Table 14: sbceconfigurator.py command options

#	Command	Description	Usage
1	**change-ip-gw-mask**	Changes the management IP address, gateway, and subnet mask.	**sbceconfigurator.py change-ip-gw-mask** <*MGMT_IP*> <*GW_IP*> <*NW_MASK*>
2	**change-ems-ip**	1. Changes the primary or active EMS IP address on the secondary or standby EMS. 2. Changes the secondary or standby EMS IP address on the primary or active EMS and all the Avaya SBCE servers connected to EMS. 3. Changes the primary or active EMS IP address on the connected Avaya SBCE 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*

Table continues…

#	Command	Description	Usage
3	**change-hostname**	Changes host name.	**sbceconfigurator.py change-hostname** *HOSTNAME*
4	**change-ntp-ip**	Changes NTP IP address.	**sbceconfigurator.py change-ntp-ip** *NTP IP*
5	**change-dns-ip-fqdn**	Changes DNS IP address.	**sbceconfigurator.py change-dns-ip-fqdn** *DNS IP*
6	**change-nw-passphrase**	Changes network passphrase.	**sbceconfigurator.py change-nw-passphrase** *passphrase*
7	**change-ssl-certs**	Generates self-signed certificate for EMS and single servers.	**sbceconfigurator.py change-ssl-certs** *first, last name Org.unit Org.Name City State 2-digit-country_code*
8	**change-sbce-ip**	Changes the Avaya SBCE IP address on the EMS database. Sequence to execute this command: 1. Change Management IP address, gateway, mask on theAvaya SBCE server by using the command **change-ip-gw-mask** 2. Run the **change-sbce-ip** command on EMS CLI to notify the EMS about the Avaya SBCE IP change.	**sbceconfigurator.py change-sbce-ip** *sbce-old-ip sbce-new-ip*
9	**factory-reset** (For SBC only)	Use the following procedure to reset Avaya SBCE to the factory default state: 1. To uninstall the Avaya SBCE 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. 3. 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**

Enabling or disabling network interfaces using CLI

Procedure

1. Log in to the Avaya SBCE 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>
```

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 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 SBCE servers connected to EMS are reachable. If any Avaya SBCE server is unreachable, exits or proceeds with changing the EMS IP address on the

reachable Avaya SBCE 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 SBCEs.

Change in management IP requires a change in the NTP address configuration on all Avaya SBCE servers connected to EMS.

Note:

All Avaya SBCE servers must have the changed EMS IP address.

Changing primary EMS IP on unreachable Avaya SBCE

About this task

Use this procedure only when Avaya SBCE 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 NTP address on Avaya SBCE devices

About this task

Changing management IP of EMS requires a change in the NTP address configuration on all the Avaya SBCE servers connected to EMS. For the proper functionality of OpenVPN, ensure that the date and time on the Avaya SBCE servers match the date and time on the EMS server. The recommended procedure is to configure the EMS IP as the NTP IP address of the Avaya SBCE devices.

Procedure

1. Log on to the Avaya SBCE device as a super user.
2. Type `sbceconfigurator.py change-ntp-ip` *`NTP-IP`*, where *NTP-IP* is the new NTP IP address.

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 SBCE server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBCE restarts indicating a successful completion of the management IP change. After changing the management IP, the primary EMS and Avaya SBCE devices must be notified about the new Avaya SBCE IP address of the secondary EMS.
3. Log on to the primary EMS and Avaya SBCE 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 SBCE device.

Changing management IP, gateway IP, and network mask details on Avaya SBCE

Procedure

1. Log on to the Avaya SBCE server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBCE restarts indicating successful completion of the management IP change. After changing the management IP, the EMS must be notified about the new Avaya SBCE 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 SBCE in the EMS database.

Changing hostname

Procedure

1. Log in to the Avaya SBCE 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 SBCE.

Changing network passphrase

About this task

Network passphrase is important for EMS-Avaya SBCE authentication. If you change the network password for an Avaya SBCE, ensure that you change the passphrase on all systems connected to the Avaya SBCE.

Procedure

1. Log in to the Avaya SBCE 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 SBCE's where the command is executed.

Regenerating self-signed certificates

Procedure

1. Log in to the EMS CLI using administrative privileges.
2. Run the following command: **`sbceconfigurator.py change-ssl-certs`**.

Changing DNS IP and FQDN

Procedure

1. Log in to the Avaya SBCE CLI using administrative privileges.
2. Type `sbceconfigurator.py change-dns—ip—fqdn` *`DNS IP FQDN`*.

   The EMS server changes the DNS IP and FQDN.

Enabling or disabling network interfaces using CLI

Procedure

1. Log in to the Avaya SBCE 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>
```

Accessing Avaya SBCE

Logging in to EMS through VGA connection for non-Portwell servers

Before you begin

Connect the monitor to EMS through a VGA cable. Connect a keyboard to EMS.

Procedure

1. Press `Enter` to establish a communications connection.

   The system prompts you to enter the username and password.
2. Enter your username and password, and press `Enter`.

Accessing Avaya SBCE device.through SSH

Before you begin

Ensure that you install a SSH application, such as PuTTY, on your system.

About this task

Use this procedure to establish a secure connection to the Avaya SBCE device.

Procedure

1. Start PuTTY.

   The system displays the PuTTY Configuration window.
2. In the **Host Name (or IP Address)** field, type the IP address of the Avaya SBCE device.

   Through SSH, you can access only EMS or M1 interface for Avaya SBCE.
3. In the **Port** field, type the port of the Avaya SBCE device.

   The port is 222.
4. In the **Connection type** field, click SSH.
5. Click **Open**.

   The EMS server establishes the session and displays the Command Line prompt.
6. On Command Line Interface, log in as ipcs.
7. In the **Password** field, type the password and press `Enter`.

   TheAvaya SBCE device displays the dollar ($) prompt.
8. To go to the root level or super user privileges, type `sudo su` and press `Enter`.

   The EMS server displays the super user command line prompt (#).

Connecting directly to a Avaya SBCE device

About this task

You can access the clipcs command line interface locally by connecting to an Avaya SBCE chassis with any SSH client.

Procedure

1. Physically connect your terminal device to the console port on the front of the Avaya SBCE equipment chassis.
2. Establish a communications session with the command shell.
3. Log in to the command shell.

Connecting a terminal device to the SBCE equipment chassis

About this task

Use the following procedure to physically connect a communications device to the Avaya SBCE equipment chassis.

Procedure

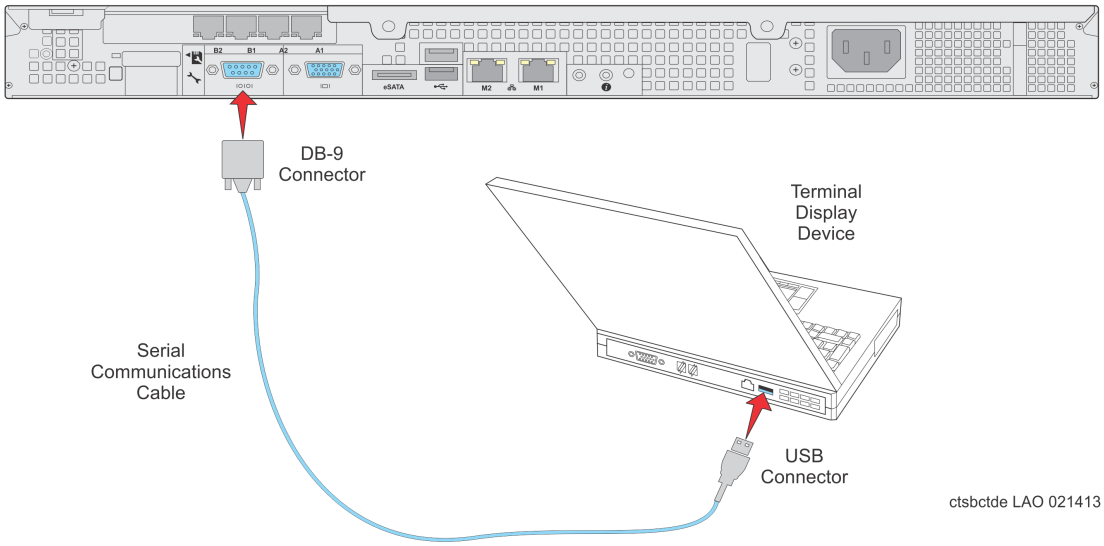
1. Find the Console port on the Avaya SBCE equipment chassis or, for the Element Management System (EMS), the UART (serial COM) port.

   For Amax EMS hardware the console (serial COM) port is disabled. Therefore, for Amax hardware, use a CRT/LED terminal and keyboard instead.

   The UART port for the EMS is located on the back panel of the equipment chassis. The Console port for the Avaya SBCE equipment chassis is located on the front panel. For more information, see *Deploying Avaya Session Border Controller for Enterprise*.
2. Connect an RJ45-terminated serial communications cable or a DB-9 cable depending on the chassis model.

   Use the following example to connect the terminal device to the Console or UART port.

Example



Establishing a communications session

About this task

Use the following procedure to establish a communications session with the Avaya SBCE command shell.

Procedure

Configure the communications parameters of your terminal program, and press `Enter`.

Use the settings in the Console port communications settings table.

The system displays a prompt for your user name and password.

Console port communications settings

To establish a communications session with the Avaya SBCE command shell, enter the following settings in your terminal program.

Parameter	Value
Baud Rate	19200
Parity	None
Data Bits	8
Stop Bits	1
Connection Setting	Use Com1 for serial connection. If you are using a USB serial adapter, the Com port is different than 1. Use Device Manager to find out the correct port.

Chapter 12: Configuring Avaya Session Border Controller for Enterprise for Avaya Aura® Remote Worker

Remote worker overview

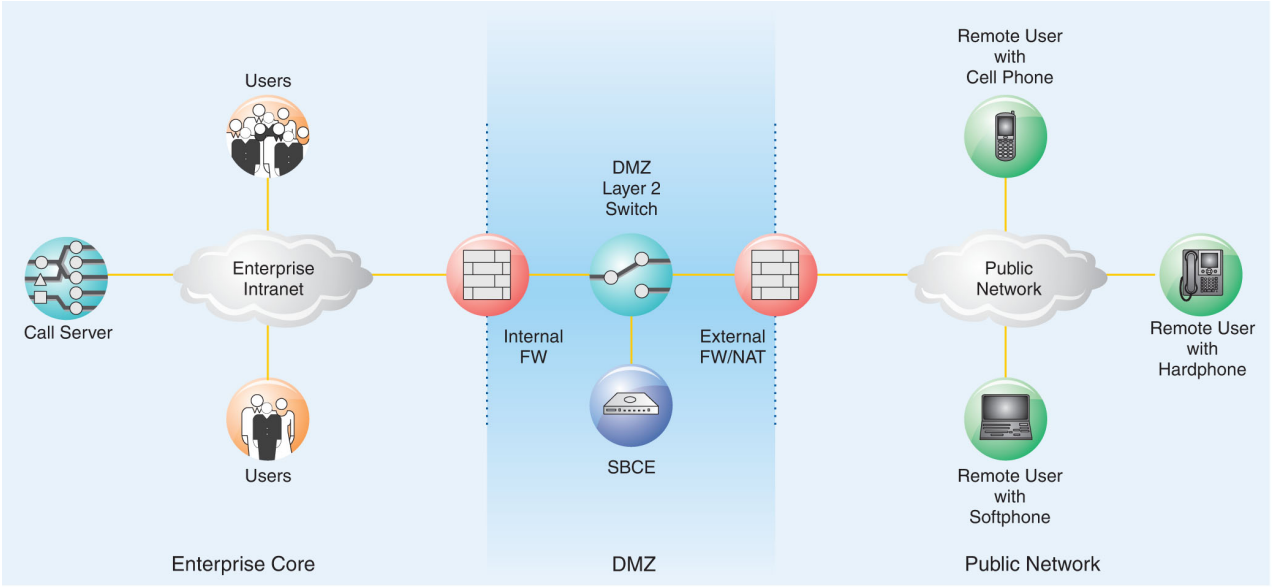
Avaya SBCE delivers security to a SIP-based enterprise network. This chapter describes how to configure Avaya SBCE for Avaya Aura® remote worker.

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 SBCE 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 SBCE internal IP.
- Configure Media or Signaling QoS on Avaya SBCE. Enable SIP Video specifically on Avaya SBCE, 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 SBCE, take a packet capture or run the **`traceSBC`** command to determine whether the issue is with Avaya SBCE. If further debugging is required, enable debug logs and get the appropriate logs. For troubleshooting, see Viewing current system incidents on page 311 and Viewing current system alarms on page 310.
- Review the Avaya SBCE, Avaya Aura® Session Manager, and endpoint release notes for fixes, limitations, and workarounds.

Limitation for registering Remote Workers

While sending a 301 Moved Permanently response from Session Manager, Avaya SBCE 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 SBCE 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 SBCE on the A1 interface. Then, Avaya SBCE 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 SBCE. However, Avaya SBCE 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 SBCE 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 SBCE 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 SBCE does not officially support registration of third-party SIP endpoints at this stage.

Session Manager configuration for Avaya SBCE

Configure Session Manager to whitelist internal IP of SBC and to disable PPM rate limiting.

Whitelisting Avaya SBCE 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 SBCE 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**.

Adding the internal IP of Avaya SBCE 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 SBCE.
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.

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**.

Remote worker configuration checklist

No.	Task	Link	✔
1.	Create an Avaya call server profile.	Creating an Avaya call server profile (advanced services only) on page 353	
2.	Create an external signaling interface for the phone network.	Creating an external signaling interface toward phone network on page 355	
3.	Create an internal signaling interface for the Avaya call server.	Creating an internal signaling interface toward Avaya call server on page 356	
4.	Create an external media interface for the phone network.	Creating an external media interface toward phone network on page 357	
5.	Create an internal media interface for the Avaya call server.	Creating an internal media interface toward Avaya call server on page 358	
6.	Create a PPM Mapping profile.	Creating PPM Mapping Profile on page 359	
7.	Creating a reverse proxy service for PPM traffic.	Creating a reverse proxy service for PPM traffic on page 362	
8.	Configure reverse proxy service for downloading file or firmware.	Creating reverse proxy service for file or firmware download on page 363	
9.	Create a media rule.	Creating a media rule on page 370	
10.	Create a server flow.	Creating server flow on page 373	

Table continues…

No.	Task	Link	✔
11.	Configure application rules for concurrent sessions per endpoint and maximum concurrent sessions.	Creating application rules on page 370	
12.	Create an endpoint policy.	Creating an endpoint policy on page 371	
13.	Create a routing profile to the Avaya call server.	Creating a routing profile to Avaya call server on page 372	
14.	Create a subscriber flow.	Creating a subscriber flow on page 374.	
15.	If you are setting up an Avaya Scopia®remote worker, administer BFCP and FECC.	Administering Binary Floor Control Protocol on page 439	
16	Add a URI group for emergency numbers.	Creating a new URI group on page 149	
17	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 183	

Cloning Avaya-ru profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.

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 Avaya-ru profile on page 353

Creating an external signaling interface for a phone network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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

Add signaling interface field descriptions on page 222

Creating an internal signaling interface for an Avaya call server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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

Add signaling interface field descriptions on page 222

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.

Table continues…

Name	Description
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 SBCE 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 SBCE.

Creating an external media interface for a phone network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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 SBCE displays the new external and internal media interfaces.

Related links

Add Media Interface field descriptions on page 358

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.

Table continues…

Name	Description
Port Range	Starting and ending port range numbers. The port range is from 35000 through 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 358

Creating PPM Mapping Profile for Session Manager

About this task

You must create a mapping profile for each group of remote workers, who have the same pair of Session Managers as the primary Session Manager and the secondary Session Manager.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **DMZ Services** > **PPM Mapping**.
4. On the Mapping Profiles page, click **Add**.
5. In the **Profile Name** field, type the profile name.
6. Click **Next**.
7. In the **Server Type** field, click Session Manager.
8. In the **SIP Server Profile** field do one of the following:
   - Click the server configuration for Session Manager.
   - Select the **Custom** check box, enter appropriate values in the **Server Address/Port**, **Server Transport**, **Mapped IP/Port**, and **Mapped Transport** fields, and click **Finish**.

     The EMS server displays the **Server Address/Port**, **Server Transport**, **Mapped IP/Port**, and **Mapped Transport** fields only when you select the **Custom** check box next to the **SIP Server Profile** or **SBC Device** fields.

     You must use this option to specify a server address, port, and transport that is different from the values configured in the server configuration profiles. For example, for a multiple Avaya SBCE deployment, where the Avaya SBCE servers are controlled by more than one EMS, use the **Server Address/Port** field to specify the IP of the EMS that controls an Avaya SBCE.

     If you select the **Custom** check box, skip the remaining steps in this procedure.

9. In the **Server Address** field, click the IP address.
10. In the **SBC Device** field, do one of the following:
    - In the **Signaling Interface** field, select a corresponding external signaling interface of Avaya SBCE.

      In the **Mapped Transport** field, click the transport port, for example, **TLS (5061)**.
    - Select the **Custom** check box, enter appropriate values in the, **Mapped IP/Port**, and **Mapped Transport** fields.
11. To add the PPM profile to the selected Session Manager, click **Finish**.

Related links

PPM Mapping Profile field descriptions on page 360

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
Server Address	The IP address or FQDN of the server.
SBC Device	Session Manager name of the Avaya SBCE device.
Signaling Interface	The signaling interface used for the profile.
Server Configuration	The server configuration profile that is used with the PPM mapping profile. This field is available only when you select the Session Manager **Server Type**.
Server Address	The address and port of Session Manager. This field is available only when you select the Session Manager **Server Type**.
Mapped Transport	The transport protocol used for the mapping profile. This field is available only when you select the Session Manager **Server Type**.
Custom	A check box to enable a custom server address, transport, mapped IP and transport that are different from the values configured in the server configuration profile.

Table continues…

Name	Description
Server Transport	The transport protocol used for the server. This field is available only when you select the **Custom** check box.
Mapped IP/Port	The mapped IP or FQDN and the corresponding port. This field is available only when you select the **Custom** check box.

Related links

Creating PPM Mapping Profile for Session Manager on page 359

Creating Reverse Proxy Policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **Reverse Proxy Policy**.
4. On the Reverse Proxy Policy page, provide data in the required fields.
5. Click **Finish**.

Related links

Reverse Proxy Policy field descriptions on page 361
Creating a reverse proxy service for PPM traffic on page 362
Creating a reverse proxy service for file or firmware download on page 363
Creating reverse proxy service for multi-tenant or IPO powered on page 365
Relay Services field descriptions on page 366

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.
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.

Table continues…

Name	Description
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. 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.

Related links

Creating Reverse Proxy Policy on page 361

Creating a reverse proxy service for PPM traffic

About this task

Use the following procedure for each Avaya SBCE.

Procedure

1. Log in to the EMS.web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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, do the following:
   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 SBCE 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 SBCE 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.

Related links

Creating Reverse Proxy Policy on page 361

Creating a reverse proxy 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 SBCE 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. In the navigation pane, click **SBCE**.

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, do the following:
   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 SBCE 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 SBCE 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**.

Related links

Creating Reverse Proxy Policy on page 361

Creating reverse proxy service for multi-tenant or IPO powered

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. In the navigation pane, click **SBCE**.
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, do the following:
   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 SBCE 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 SBCE and Avaya Equinox® works as follows:

      - Without "Any" option in **Received server host**: Avaya SBCE 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 SBCE 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 Reverse Proxy Policy on page 361

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	

Table continues…

Field	Description
Remote IP/FQDN	Specify the server IP address or FQDN as follows: • For RTCP (Core Avaya SBCE): Monitoring Server IP address. • For IM (DMZ Avaya SBCE): Core Avaya SBCE external IP address. • For Avaya SBCE at remote site: DMZ Avaya SBCE external/public IP.
Remote Port	Specify the port as follows: • For RTCP (Core Avaya SBCE): RTCP monitoring port. • For IM (DMZ Avaya SBCE 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 SBCE): Core Avaya SBCE external IP address. • For RTCP (DMZ Avaya SBCE): DMZ Avaya SBCE external IP address. • For IM (DMZ Avaya SBCE) and Avaya SBCE at remote site: Remote Avaya SBCE external IP address.
Listen Port	Specify the port as follows: • For RTCP (Core Avaya SBCE): RTCP monitoring port. • For IM (DMZ Avaya SBCE and remote site): 5222.
Connect IP	Specify the network name and IP address as follows: • For RTCP (Core Avaya SBCE): Core Avaya SBCE internal IP1 address. • For RTCP (DMZ Avaya SBCE): DMZ Avaya SBCE internal IP address. • For IM (DMZ Avaya SBCE) and Avaya SBCE at remote site: Remote Avaya SBCE internal IP address.
Listen Transport	Specify the listen protocol. The options are: TCP, UDP, and TLS.

Table continues…

Field	Description
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 SBCE): End-to-end Rewrite, Hop-By-Hop Traceroute, and Bridging. • For RTCP (DMZ Avaya SBCE): Hop-By-Hop Traceroute. • For RTCP (Remote Avaya SBCE): 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.
Listen IP	External Avaya SBCE 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 SBCE 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 SBCE server.
Connect IP	Network name and IP address that Avaya SBCE uses to communicate with file servers.

Table continues…

Name	Description
Load Balancing Algorithm	Algorithm used for load balancing for the reverse proxy. Available options include: • Round-Robin • IP Hashing • Least # of Connections
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.
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 SBCE 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 SBCE 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 IPO powered)

Name	Description
Service Name	XMPP profile name.
Listen IP	External Avaya SBCE IP address and network name. **Note:** Use a different IP address for SIP signaling and media.

Table continues…

Name	Description
Listen Port	80 for HTTP. 443 for HTTPS.
Remote FQDN/IP	FQDN or IP address that Avaya SBCE 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 SBCE uses to relay XMPP messages.

Related links

Creating Reverse Proxy Policy on page 361

Creating a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 new Media Rule on page 89

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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
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. 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. In the following **URI Group**, **User Agent**, **Source Subnet**, **Via Host**, and **Contact Host** fields, leave the default values.
   - Depending on customer requirements, modify these fields.
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. In the Profile section, in the **Source** field, click **Subscriber**.
11. In the **Media Interface** field, select the corresponding media interface towards the endpoint.

    For example, the name of the interface can be Med_Intf_Ext_to_Phone_Net.
12. 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.
13. In the **Routing Profile** field, click the name of the routing profile that points toward the Avaya call server, for example, Route_to_Avaya_Server.
14. If you require TLS transport, in the **TLS Client Profile** field, select an appropriate TLS profile.
15. In the **File Transfer Profile** field, leave the default value: None.
16. Select **Phone Interworking Profile** as **avaya-ru**.

17. In the **Presence Server Address** field, type the Presence server address.

    In Release 6.3.1, 6.3.2, 6.3.3, 7.0 and 7.1, Avaya SBCE does not rewrite the Presence Subscription URI if Remote Workers use FQDN instead of the external Avaya SBCE 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 Equinox® 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 SBCE is not resolvable in the enterprise network.

18. **(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 Equinox® 3.0.

19. Click **Finish**.

Related links

Adding a new user agent (Advanced Services only) on page 220
Add URI Group field descriptions on page 150
User agents (Advanced Services only) on page 220

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 Equinox® for all platforms: Release 3.0.

     Avaya Equinox® 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

No.	Task	Description	Reference	✔
1	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 374	

Table continues…

No.	Task	Description	Reference	✔
2	Create PPM Mapping Profile for Presence server.	In future releases, the following endpoints will support Presence server configuration by using PPM Mapping Profile: • Avaya one-X® Communicator for Windows: Release 6.2 FP6 • Avaya one-X® Communicator for all other platforms: Release 3.0 • 96x1 phones: Release 6.5 • Avaya Equinox® for all platforms: Release 3.0	Creating PPM mapping profile for presence server on page 377	
3	Create reverse proxy service for PPM traffic.	Reverse proxy configuration is done after creating a PPM mapping profile.	Creating a reverse proxy service for PPM traffic on page 362	

Creating PPM mapping profile for presence server

About this task

PPM mapping profile for Presence Server must be part of the same PPM Mapping profile as the profile created for Session Manager. Use this procedure to create PPM mapping profile for presence server.

Note:

Currently, most endpoints do not support the presence server configuration through a PPM mapping profile. Until endpoints support this configuration, go to **Network & Flows** > **End Point Flows**, and add the presence server IP address in the **Presence Server Address** field.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **DMZ Services** > **PPM Mapping**.

   The system displays the Mapping Profiles page.
4. In the **Server Type** field, click **Presence**.
5. In the **Server Address** field, type the IP address or FQDN of the presence server.

   The Server address you enter must match with the SIP entity IP address or FQDN configured in System Manager for Presence

6. In the **SBC Device** field, click the Avaya SBCE device.
7. Click **Finish**.

Next steps

Configure a reverse proxy service for PPM traffic.

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. In the navigation pane, click **SBCE**.
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 SBCE.

   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 SBCE for RTCP traffic received from DMZ Avaya SBCE 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 SBCE and core phones

RTCP traffic received on Core Avaya SBCE external IP Address is sent out to a monitoring server using Core Avaya SBCE 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 SBCE 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 366

Configuring Avaya SBCE to support emergency calls from unregistered endpoints

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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`.
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.
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 SBCE 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 SBCE.
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 SBCE.
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 SBCE.	Remote worker configuration checklist on page 352.		
2.	Configure DMZ Avaya SBCE.	Remote worker configuration checklist on page 352.		
2a.	Configure the server interworking profile.	Creating Interworking Profiles on page 404	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**.	

Table continues…

No.	Task	Reference	Notes	✔
2b.	Configure the server.	Creating an Avaya call server profile on page 353.	Ensure that the server configuration points to corresponding external IP address of core Avaya SBCE. **Note:** Select the server interworking profile created in Step 2a.	
2c.	Configure the subscriber flow.	Creating a subscriber flow on page 374.		
2d.	Creating a reverse proxy service for file or firmware download.	Creating reverse proxy service for file or firmware download on page 363.		
2e.	Configure application relay settings for IM.	Application relay settings for IM on page 366.		

Checklist for back-to-back-to-back configuration with a single Session Manager

No	Task	Reference	Notes	✔
1.	Configure core Avaya SBCE.	Remote worker configuration checklist on page 352.		
2.	Configure DMZ Avaya SBCE.	Remote worker configuration checklist on page 352.		
2a.	Configure the server interworking profile.	Creating Interworking Profiles on page 404.	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.	

Table continues…

No	Task	Reference	Notes	✔
2b.	Configure the server.	Creating an Avaya call server profile on page 353.	Ensure that the server configuration points to the corresponding external IP address of core SBCE. **Note:** Select the server interworking profile created in Step 2a.	
2c.	Configure the subscriber flow.	Creating a subscriber flow. on page 374		
2d.	Configure reverse proxy for file download.	Creating reverse proxy service for file or firmware download. on page 363		
2e.	Configure application relay settings for IM.	Configuring application relay for IM. on page 375		
3.	Configure remote Avaya SBCE.			
3a.	Do not configure public IP address in the **Network Management** feature.			
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.	

Table continues…

No	Task	Reference	Notes	✔
3c.	Configure server.		When the Avaya SBCE 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 SBCE 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 366		

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. In the navigation pane, click **SBCE**.
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 SBCE configuration, click **DMZ**.
   - For CORE Avaya SBCE configuration, click **Core**.
   - For remote Avaya SBCE configuration, click **Remote**.

7. In the **Relay IP** field, click **None**.

   For Core Avaya SBCE configuration, in the **Relay IP** field, click the IP address of the core Avaya SBCE Internal IP1.

   Note:

   Core Avaya SBCE Internal IP1 address is the address used to send RTCP traffic received from DMZ Avaya SBCE and core phones towards a monitoring server.

8. For Core Avaya SBCE 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 SBCE 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 SBCE).

Configure two application relays for the Core Avaya SBCE as follows:

Relay 1 : For RTCP traffic coming from DMZ Avaya SBCE and core phones

RTCP traffic is received on Core Avaya SBCE external IP address and is sent out to a monitoring server using Core Avaya SBCE 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 SBCE internal IP2 address.

Note:

If there are multiple Core Avaya SBCE, repeat the RTCP configuration steps on each Avaya SBCE.

For more information about application relay settings, see the Application relay field descriptions section.

Related links

Relay Services field descriptions on page 366

Chapter 13: Multiple Session Manager support for Avaya SBCE in Remote Worker deployment

After Avaya SBCE installation, Avaya SBCE is ready for configuration and is available for administration through the web console.

Avaya SBCE 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 SBCE corresponding to the primary and secondary Session Manager.

Note:

Avaya SBCE 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 SBCE in a multiple Session Manager environment.

Note:

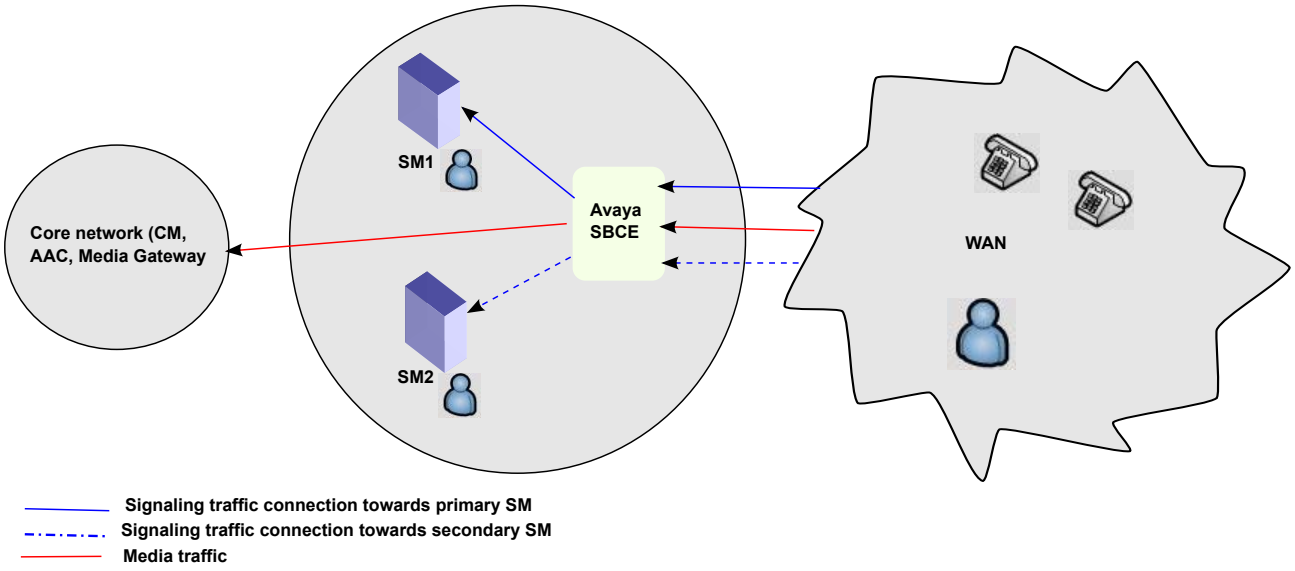
In the following sections:

- The IP address on Avaya SBCE towards the internet is referred to as an external address.
- The IP address on Avaya SBCE towards the core network or call server is referred to as an internal address.

Single Avaya SBCE connected to two Session Managers

In the following scenario, the phones in the network maintain two socket connections to Avaya SBCE, at two different IP addresses hosted by Avaya SBCE:

- One socket for traffic to primary Session Manager 1
- Second socket for traffic to secondary Session Manager 2



Multiple Session Manager configuration checklist

No	Task	Notes	Reference
1.	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 388.
2.	Create two external signaling interfaces and two internal signaling interfaces.		Creating an external signaling interface toward phone network on page 355. Creating an internal signaling interface toward Avaya call server on page 356.
3.	Create two external media interfaces and two internal media interfaces.		Creating an external media interface toward phone network on page 357. Creating internal media interface toward Avaya call server on page 358.
4.	Create a media rule.		Creating a media rule on page 370.
5.	Create a server interworking profile.		Creating a server interworking profile on page 388.

Table continues…

No	Task	Notes	Reference
6.	Ensure that voice sessions are set as per the user license in the application rules and enable video.		Creating application rules on page 370.
7.	Create an endpoint policy.		Creating an endpoint policy on page 371.
8.	Create two server profiles, one for the primary and another for the secondary Session Manager.	Ensure that you enable heartbeat so that Avaya SBCE 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 353.
9.	Create a reverse proxy for file download.		Creating a reverse proxy service for file or firmware download on page 363.
10.	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 SBCE 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 372.
11.	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 374.
12.	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 139.
13.	Configure an application relay for IM.		Configuring application relay for IM on page 375.

Note:

For more information about remote worker configuration, see Remote worker configuration checklist on page 352.

Configuring the Avaya SBCE IP addresses corresponding to the primary and secondary Session Managers

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   Avaya SBCE 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 SBCE system.
8. Click **Finish**.

Creating a server interworking profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.

   Avaya SBCE displays the Interworking Profiles page.
4. Select the **avaya-ru** profile, and click **Clone**.

   Avaya SBCE 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. In the navigation pane, click **SBCE**.
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*.

Related links

Creating a reverse proxy service for file or firmware download on page 363
Configuring application relay for IM on page 375
Topology Hiding settings examples on page 248

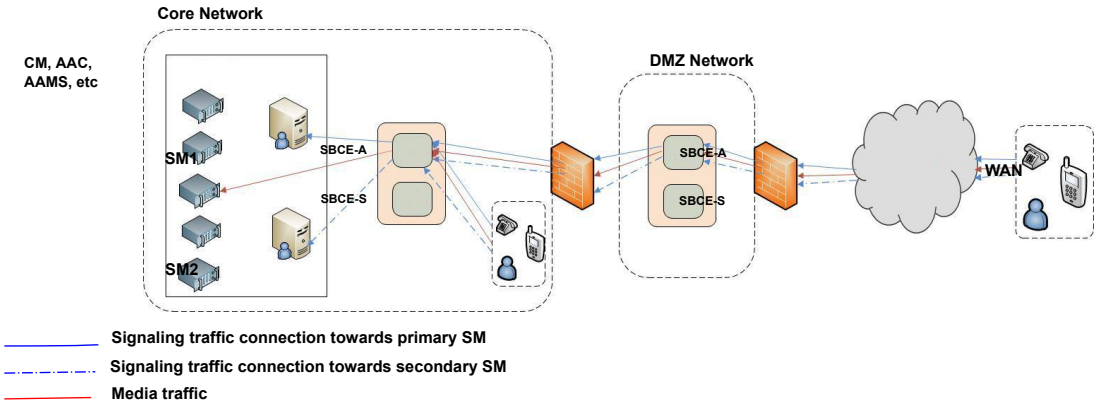
Multiple Session Manager support with back-to-back Avaya SBCEs

Avaya SBCEs are deployed back-to-back in a multiple Session Manager remote worker solution. In the solution, one Avaya SBCE is deployed in the DMZ network and another Avaya SBCE in the CORE network.

You can manage both Avaya SBCEs 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 SBCE deployment.

In the following diagram, the core and DMZ Avaya SBCEs have been deployed in HA mode.



Back-to-back configuration checklist

In the following table, the first task refers to the configuration of Avaya SBCE in the Core network. The rest of the tasks refer to the configuration of Avaya SBCE in the DMZ network.

For more information, see *Multiple Session Manager configuration checklist*.

Note:

Remote workers must register to IP address of Avaya SBCE in DMZ.

No.	Task	Notes	✔
1.	Configure Avaya SBCE in the Core network.	Use the multiple Session Manager configuration checklist.	
2.	Configure Avaya SBCE 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 SBCE 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 SBCE in remote location and Avaya SBCE 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 SBCE. **Note:** Repeat this step for each Core Avaya SBCE that you deploy. Do not configure server configuration for Presence server. Ensure that you enable heartbeat so that Avaya SBCE 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 service for file or firmware download on page 363.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Configuring application relay for IM on page 375.	

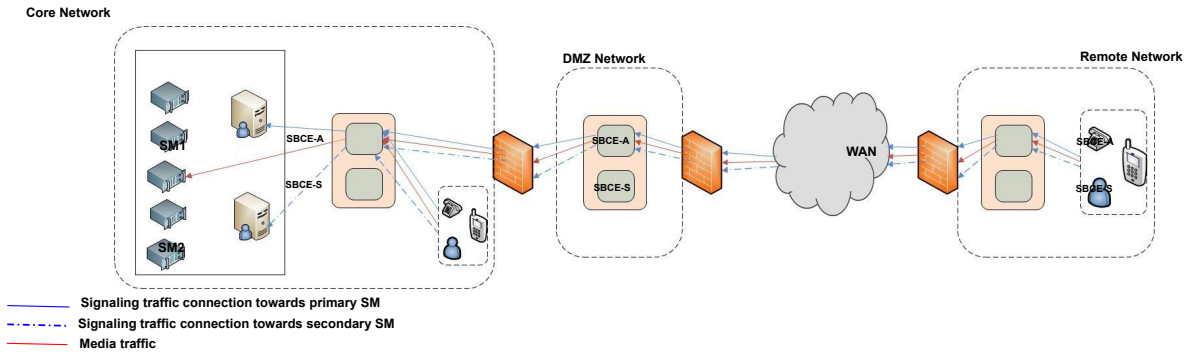
Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBCEs

Avaya SBCEs are deployed at three levels in a multi-Session Manager remote worker solution. In this solution, one Avaya SBCE is deployed in the DMZ network, one or more Avaya SBCEs are deployed in the CORE network, and another Avaya SBCE is deployed in the remote site.

There is no restriction on the number of EMS web consoles used to manage the Avaya SBCE. The only requirement is to manage all core Avaya SBCEs using a single EMS web console.

Note:

Ensure network reachability between EMS and the Avaya SBCE that it manages.



Back-to-back-to-back configuration checklist

No.	Task	Details	✔
1.	Configure core Avaya SBCE.	Use the multi-Session Manager checklist in the previous section. **Important:** Task 1 refers to configuring Core Avaya SBCE. However, the other tasks given below, that is 2, 2a, 2b, 2c, 2d, and 2e refer to configuration of Avaya SBCE in DMZ network and 3, 3a, 3b, 3c, 3d, 3e, and 3f refer to configuration of SBC in remote network	
2.	Configure Avaya SBCE in the DMZ network.	For more information about configuring Avaya SBCE in DMZ, see the previous section. If there are no remote workers configured to get the service from DMZ Avaya SBCE directly, the **Enable heartbeat** field in the **Server Configuration** feature corresponds to Core Avaya SBCE 1 and Core Avaya SBCE 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 SBCE in remote location and Avaya SBCE 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 SBCE. **Note:** Repeat this step for each Core Avaya SBCE that is deployed. Ensure that you enable heartbeat so that Avaya SBCE 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 service for file or firmware download on page 363.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Relay Services field descriptions on page 366.	
3.	Configure the remote Avaya SBCE.		
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 SBCE 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 SBCE in DMZ.	
3d.	Configure default topology profile.		
3e.	Configure a reverse proxy for file download.	See Creating a reverse proxy service for file or firmware download on page 363.	

Table continues…

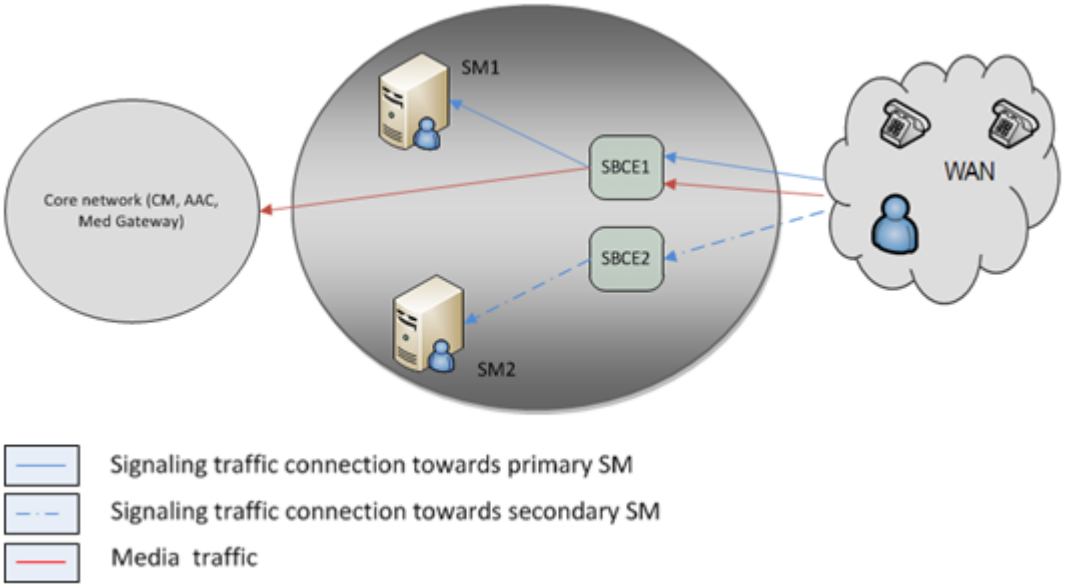
No.	Task	Details	✔
3f.	Configure an application relay to support IM for remote workers.	See Configuring application relay for IM on page 375.	

Geographic-redundant deployment

In a Geographic-redundant deployment, you can deploy two different Avaya SBCE devices in two different data centers. You can deploy the devices as individual Avaya SBCE devices or devices managed by their own EMS. You can deploy these Avaya SBCE 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.

Geographic-redundant deployment in the non-HA mode

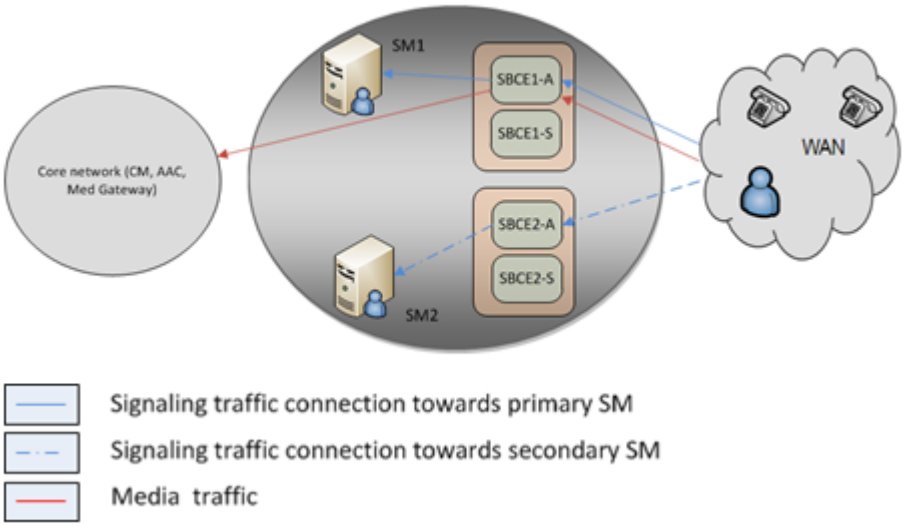
In the following diagram, SBCE1 and SBCE2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBCE1 corresponding to the primary Session Manager, SM1. The second connection with SBCE2 corresponds to the secondary Session Manager, SM2.



Geographic-redundant deployment in the HA mode

In the following diagram, SBCE1 and SBCE2 are two different physical devices that are deployed in an HA mode in different data centers. The endpoints have one connection with SBCE1-A, that is Active SBCE corresponding to the primary Session Manager, SM1. The second connection is with SBCE2-A, Active SBCE corresponding to the secondary Session Manager, SM2.

During an SBCE1-A fail over, SBCE1-S, which is the standby Avaya SBCE, handles the media of the active calls. During an SBCE2-A fail over, SBCE2-S, which is the standby Avaya SBCE, handles the media of the active calls.



Checklist for configuring Geographic-redundant deployment

Use the following checklist to configure the Geographic-redundant Avaya SBCE deployment.

Note:

All Avaya SBCE devices in a Geographic-redundant Avaya SBCE deployment must be controlled by the same external EMS.

In the following checklist:

- The IP address on Avaya SBCE towards the internet is referred to as external address.
- The IP address on Avaya SBCE 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.

No.	Task	Reference	Notes	✔
1	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 388		
2	Create two external signaling interfaces.	Creating an external signaling interface toward phone network on page 355		
3	Create two internal signaling interfaces.	Creating an internal signaling interface toward Avaya call server on page 356		
4	Create two external media interfaces.	Creating an external media interface toward phone network on page 357		
5	Create two internal media interfaces.	Creating internal media interface toward Avaya call server on page 358		
6	Create a server interworking profile.	Creating a server interworking profile on page 388		
7	Create two server profiles, one for the primary and another for the secondary Session Manager.	Creating an Avaya call server profile on page 353		
8	Create PPM Mapping Profiles for each group of remote workers that has the same pair of Session Managers as primary and secondary Session Manager.	Creating PPM Mapping Profile on page 397		
9	Configure reverse proxy service for downloading file or firmware.	Creating reverse proxy service for file or firmware download on page 363		
10	Create an endpoint policy.	Creating an endpoint policy on page 399		
11	Create two routing policies for SM1 and SM2.	Creating a routing profile to Avaya call server on page 372		

Table continues…

No.	Task	Reference	Notes	✔
12	Create two subscriber endpoint flows corresponding to the primary and secondary Session Managers.	Creating a subscriber flow on page 374.	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.	
13	Create two server flows corresponding to the primary and secondary Session Managers..	Creating a new server endpoint flow on page 139		
14	Create application rules.	Creating application rules on page 370	Ensure that voice sessions are set as per the user license in the application rules and enable video.	
15	Configure application relay for IM.	Configuring application relay for IM on page 375		
16	Create a reverse proxy service for PPM traffic.	Creating a reverse proxy service for PPM traffic on page 362		
17	Configure web collaboration.	Configuring Avaya SBCE for web collaboration on page 400		
18	Configure PPM Settings on Session Manager.	Configuring PPM settings on Session Manager on page 400		
19	If Session Manager Firewall is enabled, add the SBCE Internal IP in the Whitelist.	—		
20	Configure Presence Services.	Configuring Presence Server on page 400		

Creating PPM Mapping Profile for Session Manager

About this task

You must create a mapping profile for each group of remote workers, who have the same pair of Session Managers as the primary Session Manager and the secondary Session Manager.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **PPM Services** > **Mapping Profiles**.
3. On the Mapping Profiles page, click **Add**.
4. In the **Profile Name** field, type the profile name.
5. Click **Next**.
6. In the **Server Type** field, click Session Manager.
7. In the **Server Configuration** field do one of the following:
   - Click the server configuration for Session Manager.
   - Select the **Custom** check box, enter appropriate values in the **Server Address/Port**, **Server Transport**, **Mapped IP/Port**, and **Mapped Transport** fields, and click **Finish**.

     The system displays the **Server Address/Port**, **Server Transport**, **Mapped IP/Port**, and **Mapped Transport** fields only when you select the **Custom** check box next to the **Server Configuration** or **SBC Device** fields.

     You must use this option to specify a server address, port, and transport that is different from the values configured in the server configuration profiles. For example, for a multiple Avaya SBCE deployment, where the Avaya SBCE servers are controlled by more than one EMS, use the **Server Address/Port** field to specify the IP of the EMS that controls an Avaya SBCE.

     If you select the **Custom** check box, skip the remaining steps in this procedure.
8. In the **Server Address** field, click the IP address.
9. In the **SBC Device** field, click the Avaya SBCE device.
10. In the **Signaling Interface** field, select a corresponding external signaling interface of Avaya SBCE.
11. In the **Mapped Transport** field, click the transport port, for example, **TLS (5061)**.
12. To add the PPM profile to the selected Session Manager, click **Finish**.
13. Perform the following steps for deployments with Avaya Aura Release 6.2 or later:
    a. On the Mapping Profiles page, click **Add**.
    b. In the **Profile Name** field, type the profile name.
    c. Click **Next**.
    d. In the **Server Type** field, click **Presence Server**.
    e. In the **Server Address** field, type the Presence server IP address or FQDN.
    f. In the **SBC Device** field, click the Avaya SBCE device.
    g. In the **Signaling Interface** field, select a corresponding external signaling interface of Avaya SBCE.

h. In the **Mapped Transport** field, click the transport port, for example, **TLS (5061)**.

i. In the **Server Configuration** field, map the Presence server IP address to Avaya SBCE device.

j. To add the PPM profile to the selected Session Manager, click **Finish**.

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 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**.

Configuring PPM settings on Session Manager

Procedure

1. Log into the System Manager web interface.
2. Navigate to **Elements** > **Session Manager** > **Session Manager Administration**.
3. Select and edit the Session Manager instance that interfaces with Avaya SBCE for remote operations.
4. Clear the **Limited PPM Client Connection** and the **PPM Packet Rate Limiting** check boxes.
5. Click **Commit**.

Configuring Avaya SBCE 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 **SBCE** 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 SBCE 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 SBCE 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 Adresses** field, type the web collaboration server address and port.

4. For windows flare, additional configuration of application relay is needed on Avaya SBCE:
   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 SBCE 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 SBCE IP address.
   l. In the **Listen Transport** field, click **TCP**.
   m. Click **Finish**.

Chapter 14: Configuration of Server flows for SIP Trunking

SIP Trunking overview

With the SIP Trunking feature of Avaya SBCE 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 SBCE, 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 SBCE 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 SBCE device for processing. See Figure 6: Avaya SBCE deployed in the enterprise DMZ on page 403. If the signaling traffic is encrypted, the Avaya SBCE device decrypts all TLS encrypted traffic and looks for anomalous behavior. Then, Avaya SBCE forwards the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

Example

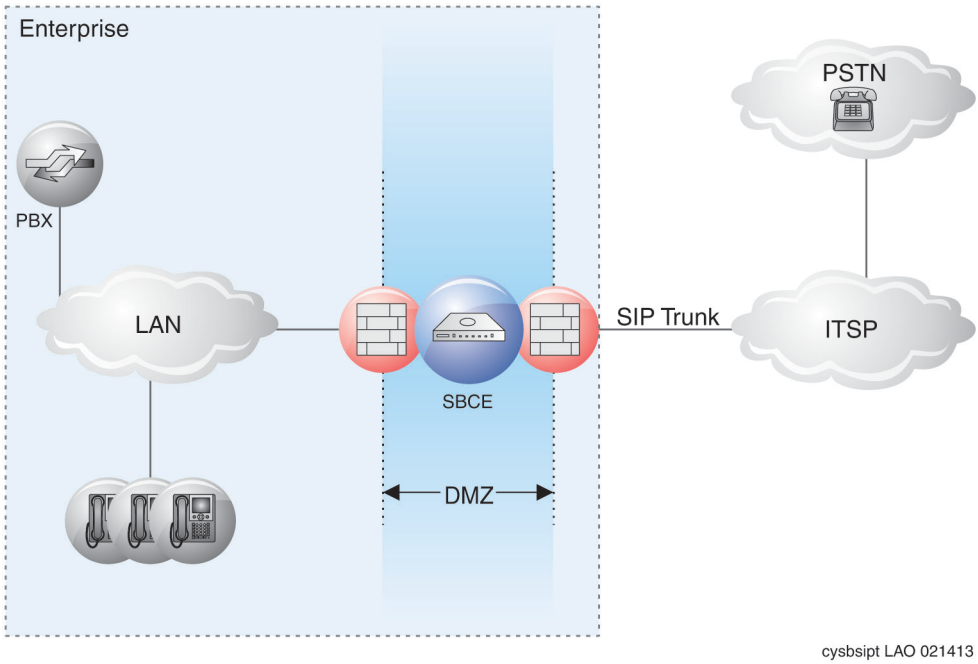


Figure 6: Avaya SBCE deployed in the enterprise DMZ

Generic Avaya SBCE SIP trunk configuration checklist

Use this checklist while configuring a generic Avaya SBCE 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 sever Application Notes.

No.	Task	Reference	✔
1	Create interworking profiles.	Creating Interworking Profiles on page 404.	
2	Create server profiles for call server and trunk server.	Creating Server Profile for Call Server on page 405 and Creating Server Profile for Trunk Server on page 406.	
3	Create routing profile for call server and trunk server.	Creating Routing Profile for Call Server on page 407 and Creating Routing Profile for Call Server on page 407.	
4	Create Topology Hiding Profile.	Creating a Topology Hiding profile on page 410	

Table continues…

No.	Task	Reference	✔
5	Create signaling interfaces.	Creating External Signaling Interface toward Trunk Server on page 411 and Creating Internal Signaling Interface Toward Call Server on page 412.	
6	Create media interfaces.	Creating External Media Interface toward Trunk Server on page 413 and Creating Internal Media Interface Toward Call Server on page 413.	
7	Create server flows.	Creating Flow toward Call Server on page 414 and Creating Flow toward Trunk Server on page 415.	
8	Perform server-specific configuration for SIP trunking.	Configuring SBCE for Avaya Trunk on page 416..	

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. In the navigation pane, click **SBCE**.
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 the Configuring Avaya SBCE for SIP trunk and Configuring Avaya SBCE for other trunks sections.

Related links

Configuring Avaya SBCE for SIP Trunk on page 416
Adding a new Interworking profile on page 264

Creating Server Profile for Call Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.
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 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. In the navigation pane, click **SBCE**.
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 Routing Profile for 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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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 407.
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 SBCE can failover from one trunking server to the next. The ways in which Avaya SBCE 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 SBCE 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 navigation pane, click **SBCE**.

3. 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.
4. In the Application pane, click the default profile.
5. In the Content pane, click **Clone**.

   The system displays the Clone Profile window.
6. 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.
7. To modify the cloned profile, in the left navigation pane, click the cloned profile.
8. In Content pane, click **Edit**.
9. After you have modified the values, click **Finish** to save, submit, and exit.

Related links

Topology Hiding settings examples on page 248

Creating external signaling interface toward Trunk-side server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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. In the navigation pane, click **SBCE**.
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.

Related links

Add signaling interface field descriptions on page 222

Creating External Media Interface toward Trunk Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.

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. In the navigation pane, click **SBCE**.
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 trunk server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the left navigation pane, click **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. In the **URI Group**, **Transport**, and **Remote Subnet** fields, leave the default (*) values.

   Depending on customer requirements, modify these fields.
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 **File Transfer Profile** field, leave the default value: None.
12. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
13. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.
14. 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.

15. Click **Finish**.

Related links

User agents (Advanced Services only) on page 220
Add URI Group field descriptions on page 150

Configuring Avaya SBCE 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. In the navigation pane, click **SBCE**.
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 SBCE 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.

Related links

Adding a new Interworking profile on page 264

Chapter 15: Signaling Manipulation

Signaling manipulation

This section provides an overview of Avaya SIP signaling header manipulation feature for the Avaya SBCE 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 developed by Avaya to define any SIP message manipulation that will be performed by Avaya SBCE.
- Packet Path and Hook Points: The packet path where a message transverses through the Avaya SBCE stack and the hook points within the path where actions defined in a SigMa script can be acted upon.
- Avaya SBCE GUI SigMa Editor: Access to the SigMa Editor for creating SIP signaling manipulation scripts that is provided through the standard Avaya SBCE 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 SBCE. Using this language, one can write a script and tie it to a given flow through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given hook point. For more information, see *Hook Points*.

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.

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 419.
- 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 SBCE	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.

Built-In Variables and Arrays

For lists of built-in variables and arrays, with their valid forms, descriptions, and illustrations, see the following.

HEADERS Variable on page 422

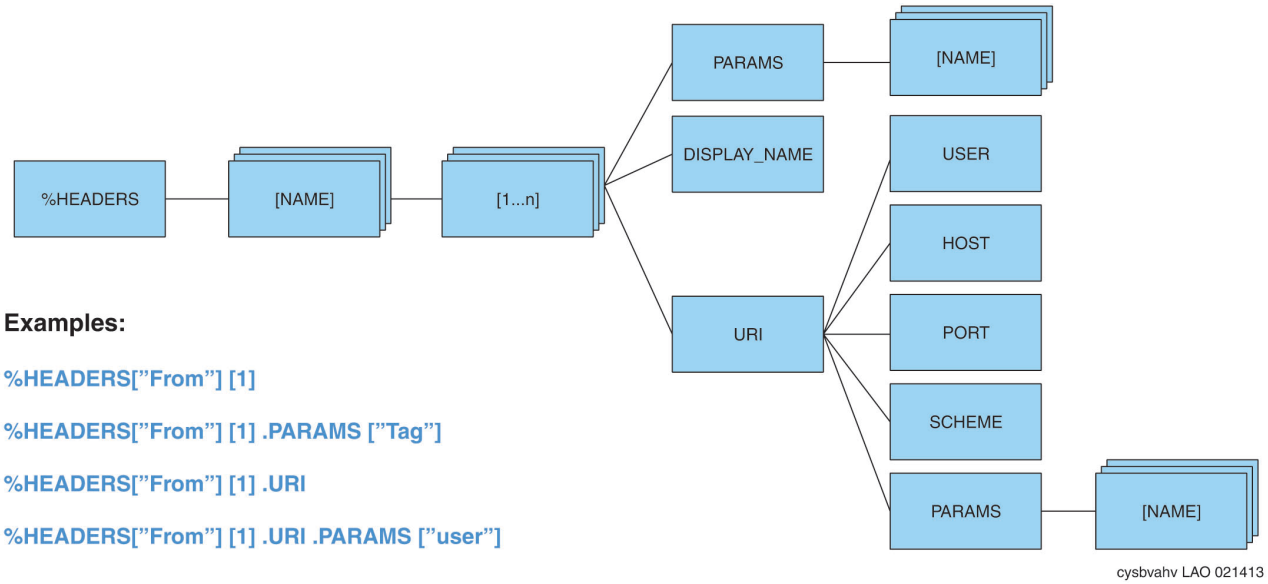
SDP Variable on page 423

Other Variables on page 424

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”]

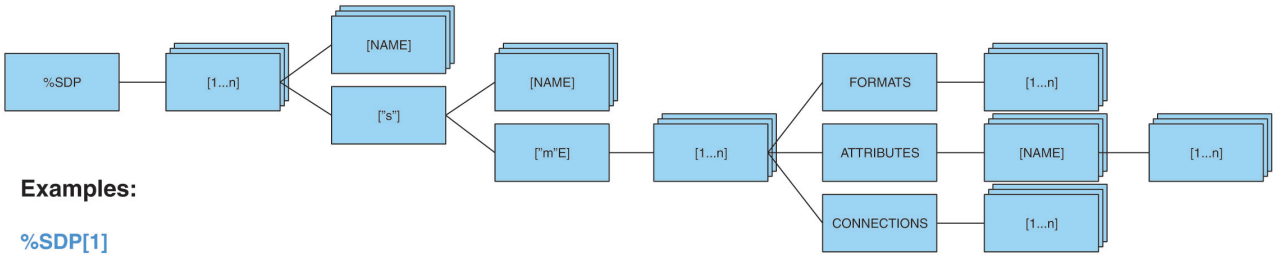
%HEADERS[”From”] [1] .URI

%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 nth 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).

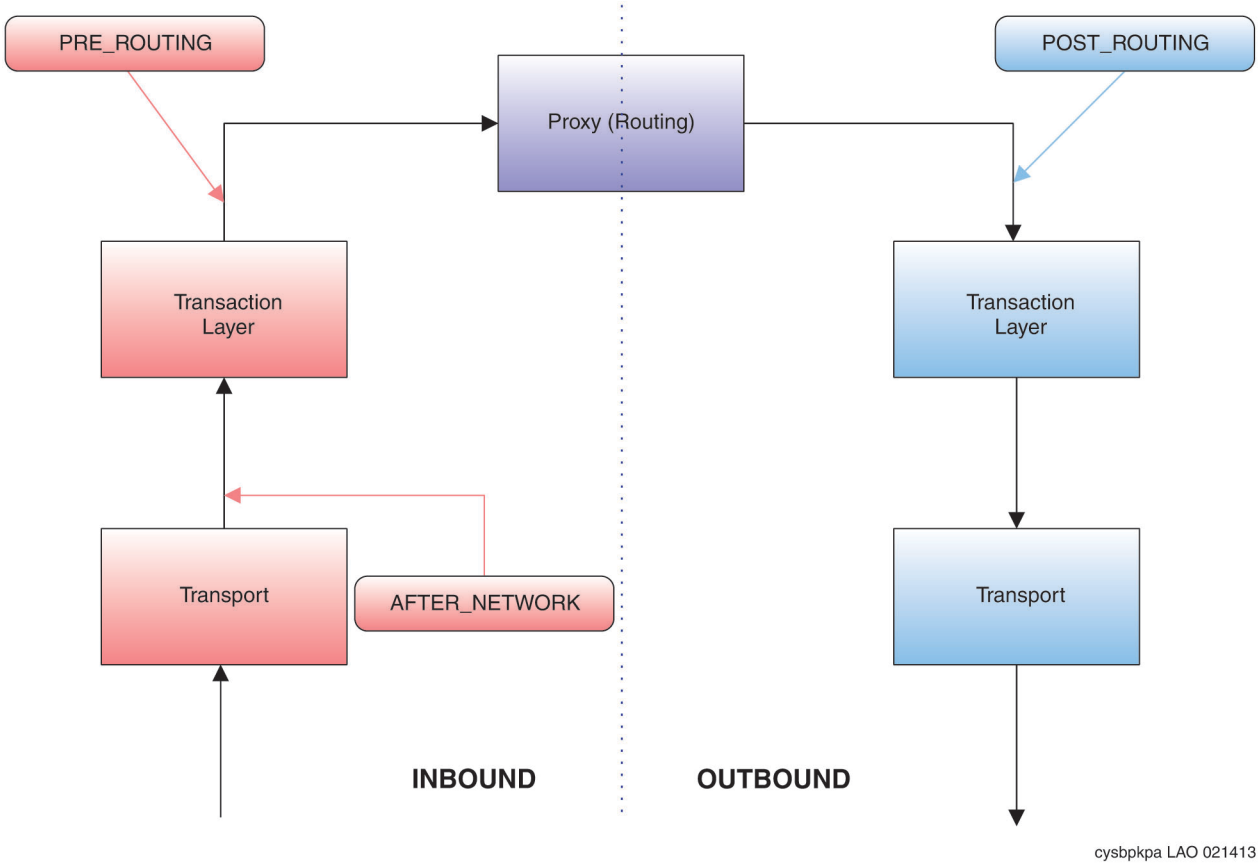
Hook points

Several hook points are illustrated in the figure and table.

Hook points are points within the Avaya SBCE 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 SBCE 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 SBCE.

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.

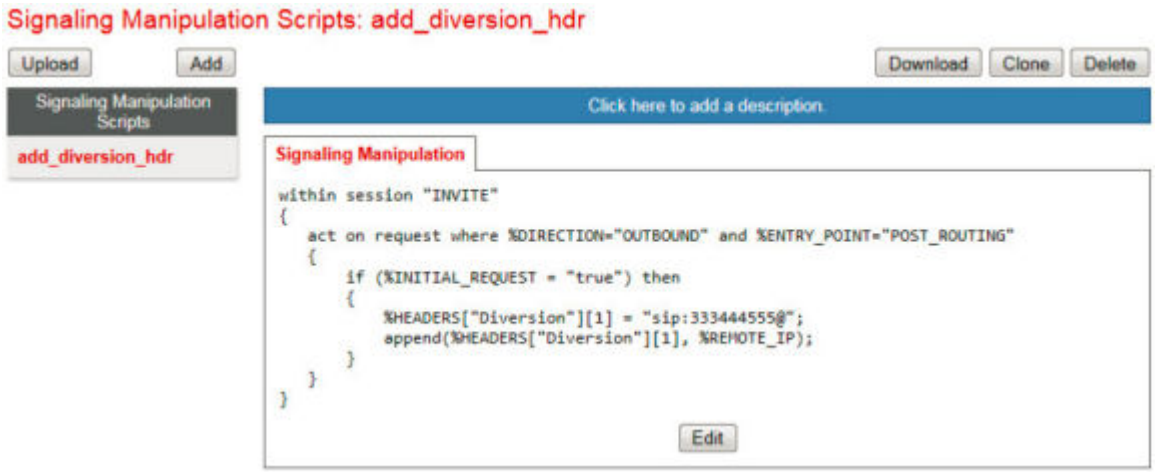
Signaling Manipulation Scripts field descriptions

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. In the navigation pane, click **SBCE**.
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 16: Remote access

Secure Access Link

Use Secure Access Link (SAL) for remote access to Avaya SBCE systems in non-IP Office environments. Register Avaya SBCE for remote access with the customer SAL. For information about configuring SAL, see *Implementing Secure Access Link Gateway*.

SSL VPN

When sold with IP Office, use remote access to SSL VPN into IP Office and then use Avaya SBCE. Register and configure Avaya SBCE and IP Office. For more information, see the job aid titled *ASBCE GRT Registration and Remote Connectivity via IP Office SSL/VPN NAPT*, which is available on http://support.avaya.com.

For information about configuring Avaya SBCE, and for remote worker and trunk configuration, see *Administering Avaya Session Border Controller for Enterprise*.

Chapter 17: Video devices interoperability configuration

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 Scopia® 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.

Administering Binary Floor Control Protocol

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 SBCE 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 SBCE.

Avaya SBCE does not use Master Key Index (MKI) and encrypted RTCP for Avaya Scopia® interoperability. Avaya SBCE negotiates the SDP session by using unencrypted RTCP.

Note:

Avaya SBCE 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 Equinox® 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 SBCE supports FECC Offer and Answer in SDP. Avaya SBCE 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 SBCE 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 SBCE 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 SBCE applies encryption according to SDP Capability Negotiation and SDES by Avaya SBCE policy.

Administering Far End Camera Control

About this task

When you enable the FECC feature, Avaya SBCE Release 6.3 supports SRTP policy settings for the FECC media application line.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 18: WebRTC-enabled call processing

WebRTC-enabled call handling

Avaya SBCE 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 SBCE in DMZ. In this scenario, Avaya SBCE, 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 SBCE 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 SBCE.

A WebRTC-enabled browser supports symmetric NAT and multiple IP addresses.

Avaya SBCE 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 Snap-in 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 SBCE 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 SBCE 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

Running the turntop command

Procedure

1. Log in to the Avaya SBCE 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`.

Configuring the TURN/STUN profile for WebRTC calls in Avaya SBCE

Before you begin

In the navigation pane, click **Device Management** and verify the following details:

- The Avaya SBCE name and the management IP address.
- The Element Management System (EMS) name and the management IP address.
- The **Status** column of Avaya SBCE EMS displaying `Commissioned`.

About this task

Use this procedure to verify that the Avaya SBCE 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service**.

   The Application pane lists the registered Avaya SBCE 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 SBCE security devices.
4. From the application pane, select the Avaya SBCE 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 SBCE 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.

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.

Table continues…

Name	Description
Media Relay Port Range	Port range for the media relay. This range must not overlap with the port ranges used by Avaya SBCE 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.
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**.

Configuring the TURN relay service for WebRTC calls in Avaya SBCE

Before you begin

In the navigation pane, click **Device Management** and verify that the Device Management page displays the following details:

- The Avaya SBCE name and the management IP address

- The Element Management System (EMS) name and the management IP address
- The **Status** column of Avaya SBCE 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 SBCE 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service**.

   The Application pane lists the registered Avaya SBCE 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 SBCE security devices.
4. From the application pane, select the Avaya SBCE 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 SBCE 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.

Add TURN Relay field descriptions

Name	Description
Listen IP	Listen IP of TURN server.
Media Relay IP	Media relay IP of TURN server.
Service FQDN	TURN server listen FQDN
TURN/STUN Profile	Displays the TURN/STUN profiles

Chapter 19: Avaya SBCE configuration for SIPREC integration

Avaya SBCE supports a SIPREC-based solution to enable recording media sessions between Avaya SBCE and a SIP Recording Server.

Avaya SBCE supports SIPREC for remote worker and SIP trunking. The SIPREC configuration for remote worker and SIP trunking are the same, except for differences in server flow configuration towards the recorder.

Avaya SBCE supports SIPREC with transcoding when the main call is transcoded. Avaya SBCE does not support transcoding to the Recorder in this release. You must ensure that G729AB or G711 is configured on both sides of the media rules, although transcoding can happen with different codecs.

This section only shows the steps for SIPREC recording configuration. Before adding configurations for SIPREC recording, you must configure SIP trunking on Avaya SBCE.

SIPREC requires one standard and one advanced license for every recorded call. To make a call that is recorded, you must have two standard and one advanced license.

In addition to the WebRTC audio and video recording, from Release 8.0.1 and later, you can record audio and video using SIP Recording feature for:

- SIP trunk calls
- SIP calls between remote worker

Video recording supports IPv6, IPv4, and ANAT addressing on the SIPREC interface. For the successful video recording, the calling and called party must be configured with H264 codec.

Checklist for configuring Avaya SBCE for SIPREC

No.	Task	Reference	✔
1	Configure a Recording Server.	Configuring a Recording Server on page 449	

Table continues…

No.	Task	Reference	✔
2	Create a routing profile for the Recording Server.	Creating a new routing profile on page 209	
3	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 450	
4	Assign the recording type and routing profile in Session Policies.	Creating a new session policy for the Recording Server on page 452	
5	Create an application rule for the Recording Server.	Creating a new Application Rule on page 83	
6	Create a media rule with appropriate codec prioritization for the Recording Server. **Note:** For SRTP calls, ensure interworking is enabled. Avaya SBCE 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 451	
7	Create an endpoint policy group for the Recording Server.	Creating a new endpoint policy group on page 119	
8	Ensure that you provision enough RTC 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.		
9	Create a session policy for the Recording Server.	Creating a new session policy for the Recording Server on page 452	

Table continues…

No.	Task	Reference	✔
10	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 454	
11	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 SBCE interface towards recorder is set as the signaling interface for the server flow.	Creating a server flow on page 139	

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. In the **Server Type** field, click **Recording Server**.
7. In the **IP Address/FQDN** field, type the IP address of the Recording Server.
8. In the **Port** field, type the port number.
9. In the **Transport** field, click a transport protocol.
10. Click **Next**.
11. On the Add Server Configuration — Heartbeat page, type the requested information in the appropriate fields.

    Enable heartbeat for load balancing solutions.
12. Click **Next**.

    The system displays the Add Server Configuration — Advanced page.
13. 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.
14. Ensure that the **Enable Grooming** check box is selected.

    For a recording server, the system selects the **Enable Grooming** field by default. Do not clear the **Enable Grooming** check box.
15. **(Optional)** If the Transport type is TLS, select the appropriate TLS client profile.
16. Click **Finish**.

Next steps

Configure routing profile.

Related links

Creating a new routing profile on page 209

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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Domain Policies** > **Signaling Rules**.
4. Click the Signaling Rule that the Avaya SBCE 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 SBCE 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

About this task

If you enable video, ensure that the stations are not monitored on Communication Manager or by any third party server. Attempting to use station monitoring when video is enabled results in unexpected results such as no media or one-way media.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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.

   WFO 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 either on 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. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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, 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** check box.
7. Select the **Recording Server** check box.
8. In the **Recording Type** field, select the type of recording required.

   The available options are Full Time and Selective.
9. **(Optional)** To play a tone to indicate that the call is being recorded, select the **Play Recording Tone** check box.

   The default recording tone is the `CALL_CONNECTING` wave file. If required, you can replace the default tone with a new, short duration wave file.
10. **(Optional)** To configure Avaya SBCE to terminate the session when Recording Servers do not respond, select the **Call Termination on Recording Failure** check box.
11. In the **Routing Profile** field, click the routing profile that Avaya SBCE must use for the Recording Server.

12. Select the **Video Recording** field to start the video recording. **Video Recording** field is available from Release 8.0.1 and later. By default, **Video Recording** is disabled.
13. Click **Finish**.

Next steps

- Create a session flow and associate the session policy with the session flow.
- Create a server flow for each Recording Server.

Related links

Creating a server flow on page 139
Adding a session flow for the Recording Server on page 454
Session Policy field descriptions on page 125

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 SBCE 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 SBCE 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 SBCE server starts.

Adding a session flow for the Recording Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The content area displays currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flow 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 SBCE 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 SBCE.
9. In the **Session Policy** field, select the session policy that you created for the Recording Server.
10. Click **Finish**.

Chapter 20: 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 SBCE provides a secure proxy that must be deployed in the enterprise DMZ. Avaya SBCE 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 SBCE.

For more information, see the Installing certificates section.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the left navigation pane, click **TLS Management** > **Client Profiles**.
4. Click **Add**.

   The system displays the New profile screen.
5. In the **Profile Name** field, type `AvayaCESClient`.

6. In the **Certificate** field, click a certificate.
7. In the **Peer Verification** field, click **Required**.
8. In the **Peer Certificate Authorities** field, click a certificate.
9. In the **Verification Depth** field, type `1`.
10. In the **Renegotiation Time** field, type `0`.
11. In the **Renegotiation Byte Count** field, type `0`.
12. In the **Ciphers** field, click **Default**.
13. 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 Equinox® for all platforms: Release 3.0.

     Avaya Equinox® 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 SBCE 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 SBCE internal IP address.

    Avaya SBCE 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 21: Avaya SBCE configuration for Call Preservation

This section describes the configuration in Avaya SBCE to use the Call Preservation feature.

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 only for SIP Routing Element (SRE) flows.

For 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 SBCE, use enhanced SIP timing and recovery techniques to provide signaling path continuity during Session Manager failure. When Avaya SBCE detects that a Session Manager is unreachable, Avaya SBCE routes the SIP traffic through the alternate Session Manager by using the Failover Group Domain Name (FGDN) in the Session Manager Via and Record-route headers. 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 SBCE will support following features of Call Preservation from Release 8.0:

- Multiple Device Access (MDA)
- Call Bridging
- Call Transfer

  Note:

  Call Transfer feature to preserve the call transactions during flight will not work.
- Ad-hoc conference hosted by Communication Manager
- Ad-hoc conference hosted by conference server
- Call Pickup
- Conference call hosted on the conference server

Checklist for configuring Avaya SBCE for Call preservation

No.	Task	Reference	✔
1	Create an FGDN group and add FGDNs administered in Session Manager.	Creating FGDN groups on page 460	
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 460	
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 462	
4	Add the routing rule to the trunk server flow.	Creating a routing rule for Call preservation on page 462	
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 462	
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 Avaya Aura® for the Session Manager Call preservation feature.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Configuration Profiles** > **FGDN Groups**.
4. Do one of the following:
   - To add a new FGDN group, click **Add** above 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 the domain names 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. In the navigation pane, click **SBCE**.
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, in the **TCP Failover Port** and the **TLS Failover Port** fields, type appropriate port numbers.
11. Click **Finish**.

Related links

Add Server Configuration profile field descriptions on page 254

Creating a routing rule for Call preservation

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, **SBCE**.
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

Add routing profile field descriptions on page 210

Adding the routing rule to the trunk server flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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

Endpoint flow field descriptions on page 139

Changing transaction expiry time in Server Interworking

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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

Add Interworking Profile field descriptions on page 265

Chapter 22: 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 SBCE 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 SBCE does not require SIP Resiliency or call reconstruction for HA failovers. You can deploy Avaya SBCE 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 SBCE when the server flows are configured with URI groups. To avoid this, Avaya SBCE must be able to configure URI groups with or without “+” sign as a prefix.

Related links

Enabling SIP Resiliency on page 464

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**.

Related links

Avaya Aura SIP Resiliency on page 464

Chapter 23: Avaya SBCE configuration for transcoding and transrating

Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBCE 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 lesser number of packets and packet overhead because packetization period is increased. For example, the packetization period (ptime) is 40 ms on WAN and 10 ms on internal enterprise network on for the same codec. For this example, transcoding is not required, but transrating is required because packetization period for the same codec is different between inbound and outbound streams.

This section describes the configuration in Avaya SBCE to support transcoding and transrating.

Checklist for configuring Avaya SBCE for transcoding

No.	Task	Description	✔
1	Enable the transcoding and tranrating features.	Enabling transcoding and transrating on page 467	
2	Administer codec prioritization.	Administering codec prioritization on page 467	
3	Add the media rule, which has transcoding enabled, to an endpoint policy group.	Configuring endpoint policy group on page 468	
4	Add the endpoint policy group to a server flow.	Configuring a server flow for transcoding on page 468	

Enabling transcoding and transrating

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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**.

Administering codec prioritization

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **SBCE**.
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. In the navigation pane, click **Network & Flows** > **End Point Flows**.
3. Click the device for which you want to change the trunk server flow.
4. Click the **Server Flow** tab.
5. In the row corresponding to the server flow that you want to change, click **Edit**.

6. In the **End Point Policy Group** field, click the endpoint policy group with the transcode-enabled media rule.
7. Click **Finish**.

Chapter 24: 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 SBCE saves the CDR records on the local hard drive. Avaya SBCE periodically sends data to the CDR adjunct using SFTP. You can configure the frequency when Avaya SBCE 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 SBCE to SFTP. In this case, CDR adjunct and Avaya SBCE validate each other based on a shared username and password.

  Avaya SBCE 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 60 GB, `/archive/cdr/` can use up to 30 GB. Avaya SBCE raises a CDR alarm if `/archive/cdr/` uses more than 21 GB space.

  Avaya SBCE begins purging CDR when `/archive/cdr/` usage crosses the 80% threshold. For example, if `/archive/cdr/` usage crosses the 24 GB threshold, Avaya SBCE 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 SBCE.

Creating a CDR adjunct

Procedure

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

2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Monitoring & Logging** > **CDR Adjunct**.
4. Configure the following fields:
   - 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 SBCE must store the CDR files.
   - In the **Update Interval** field, click the interval at which Avaya SBCE pushes data to the CDR adjunct.
5. Click **Save** to save the changes.

CDR adjunct field descriptions

Name	Description
Address	The address of the SFTP server.
Username	The user name.for the SFTP server.
Password	The password to gain access to 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 SBCE stores CDR files.
Update Interval	The interval at which Avaya SBCE sends data to the CDR adjunct.

Creating a Radius profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Services** > **RADIUS**.
4. On the Radius Profile page, click **Add**.
5. In the **Rule Name** field, type the name of the Radius profile, and click **Next**.
6. In the **Server Address & Port** field, type the Radius server address and port in the following format:

IP_address:*port*

7. In the **Alternate Server Address & Port** field, type the Radius server address and port in the following format:

   IP_address:*port*

8. In the **Shared Secret** and **Confirm Shared Secret** fields, type the shared password for Avaya SBCE and the Radius server.
9. In the **Number of Retries** field, type the number of times that Avaya SBCE must try to connect to the Radius server.
10. In the **Retry Timeout** field, type the time interval for which Avaya SBCE must wait for a response from the Radius server.
11. In the **Connect Port** field, type the port number of the Avaya SBCE client port to send the Radius request messages.
12. In the **Health Check Interval** field, type the time interval for sending a health check signal to the Radius server when the Radius server is down.
13. Click **Finish**.

Radius profile field descriptions

Name	Description
Rule name	The Radius profile name.
Server Address & Port	The Radius server address.
Alternate Server Address & Port	The Radius server address to reach when the primary server is down.
Shared Secret	The shared password for Avaya SBCE and Radius server.
Confirm Shared Secret	The field to confirm the shared password for Avaya SBCE and Radius server.
Number of Retries	The number of attempts that Avaya SBCE must try to connect to the Radius server.
Retry Timeout	The time interval for which Avaya SBCE must wait for a response from the Radius server.
Connect Port	The Avaya SBCE 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.

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. In the navigation pane, click **SBCE**.
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.
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 SBCE receives an ACK for the INVITE.
9. Click **Finish**.

Related links

Application Rule screen field descriptions on page 83

Enabling periodic statistics

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 25: Media tunneling

The media tunneling feature provides uniform client messaging and signaling from team engagement and customer engagement client SDKs.

Avaya SBCE 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 SBCE 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 SBCE, 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.

Media tunneling checklist

No.	Task	Notes	✔
1	Enable converged conferencing.	See Enabling media tunneling on page 476.	
2	Add a media interface.	See Adding a media interface on page 476.	
3	Create a server profile.	See Creating a server profile on page 477.	

Enabling media tunneling

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. Select the **Media Tunneling** check box in **Network & Flows** > **Advanced Options** > **Feature Control** tab to enable the Media Tunneling feature.
4. Click **Finish**.

Disabling media tunneling

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. Clear the **Media Tunneling** check box in **Network & Flows** > **Advanced Options** > **Feature Control** tab to disable the Media Tunneling feature.
4. Click **Finish**.

Adding a media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, **SBCE**.
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**.
6. Click **Add**.
7. In the **Name** field, type a descriptive name for the media interface.
8. In the **IP address** field, select an IP address.
9. In the **Port Range** field, type the port range.

10. 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.

11. Click **Finish**.

Creating a server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.

   The EMS server displays the Server Profiles screen.
4. Click **Add**.

   The EMS server displays the New Profile window.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select a certificate.
7. In the **Peer Verification** field, click **Optional**.
8. In the **Peer Certificate Authorities** field, do not select a CA certificate.
9. Click **Finish**.

Chapter 26: Avaya SBCE configuration for Avaya Aura® Media Server offboarding

Avaya SBCE supports an external Avaya Aura® Media Server that supports both transrating and transcoding. Avaya SBCE 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, in the routing profile choose **Round Robin** or **Load Factor** in the **Load Balancing** field.

Checklist for configuring external media server

No.	Task	Reference	✔
1	Enable Avaya Aura® Media Server offboarding.	Enabling Avaya Aura Media Server offboarding on page 479	
2	Configure a Media Server.	Configuring a media server on page 479	
3	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**.	Creating a new routing profile on page 209	
4	Assign the media type and routing profile in Session Policies.	Creating a session policy for a media server on page 480	
5	Create an application rule for the Media Server.	Creating a new Application Rule on page 83	
6	Create an endpoint policy group for the Media Server.	Creating a new endpoint policy group on page 119	

Table continues…

No.	Task	Reference	✔
7	Create a session policy for a Media Server.	Creating a session policy for a media server on page 480	
8	Create a session flow for the Media Server.	Adding a session flow on page 481	
9	Create 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 139	

Enabling Avaya Aura® Media Server offboarding

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the left navigation pane, click **Network & Flows** > **Advanced Options**.
4. Click the **Feature Control** tab.
5. Select the **AMS_OFFLOADING** check box.
6. Click **Save**.

Configuring a media server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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. In the **Server Type** field, click **Media Server**.

7. In the **IP Address/ FQDN** field, type the IP address of the media server.
8. In the **Port** field, type `7150`.

   Avaya SBCE supports only TCP transport protocol for media servers.
9. Click **Next**.
10. On the Add Server Configuration Profile — Authentication, and Add Server Configuration Profile — Heartbeat screens, type the requested information in the appropriate fields, and click **Next**.
11. On the Add Server Configuration Profile — Advanced screen, type the requested information in the appropriate fields.
12. Click **Finish**.

Next steps

Configure a routing profile.

Creating a session policy for a media server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **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, 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 session flow and associate the session policy with the session flow.
- Create a server flow for each media server.

Adding a session flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
3. In the navigation pane, click **Network & Flows** > **Session Flows**.

   The content area displays currently defined session flows.
4. Click **Add**.

   The EMS server displays the Add Flow 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 SBCE.
8. In the **Session Policy** field, select the session policy that you created for the media server.
9. Click **Finish**.

Next steps

1. Create a media and signaling interface.
2. Create a server flow for every media server.
3. In the server flow, assign the media interface, signaling interface, and endpoint flow created for Avaya Aura® Media Server.

Chapter 27: 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 for Enterprise Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBCE.	Sales engineers, solution architects, and implementation engineers
Avaya Converged Platform Overview and Specification	Describes the key features of Avaya Converged Platform	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation and administration		
Installing the Dell PowerEdge R630 Server	Hardware installation and preliminary configuration.	Implementation engineers
Installing the HP ProLiant DL360 G9 Server	Hardware installation and preliminary configuration.	Implementation engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 8.0.x.	Implementation engineers
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Procedure to deploy Avaya SBCE on VMware.	Implementation engineers
Installing the Avaya Converged Platform 110 Series	Describes how to install Avaya Converged Platform 110 Series.	Sales and deployment engineers, solution architects, and support personnel
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		

Table continues…

Title	Description	Audience
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures for Avaya SBCE.	Implementation engineers and Sales engineers
Maintaining and Troubleshooting the Dell PowerEdge R630 Server	Troubleshooting and maintenance procedures for the Dell PowerEdge R630 Server.	Implementation engineers and Sales engineers
Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server	Troubleshooting and maintenance procedures for the HP ProLiant DL360 G9 Server.	Implementation engineers and Sales engineers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**

- **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.

7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

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
2060W	What is new for Avaya Session Border Controller for Enterprise
2066W	Administering the Avaya Session Border Controller for Enterprise
2080C	Implementing and Supporting Avaya Session Border Controller — Platform Independent
2080T	Avaya Session Border Controller for Enterprise Platform Independent and Support Test
2080V	Implementing and Supporting Avaya Session Border Controller — Platform Independent
26160W	Avaya Session Border Controller for Enterprise Fundamentals
7008T	Avaya Session Border Controller for Midmarket Solutions Implementation and Support Test
7008W	Avaya Session Border Controller for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

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.

Procedure

- 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 **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **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 key word or key words 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 the topic. 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 SBCE, Endpoint.
Requirements:	Required two external IP addresses on Avaya SBCE. Endpoint must be able to reach both the external interfaces of Avaya SBCE.

This solution is an alternate solution to support the simultaneous downloads of configuration and firmware files from different endpoints through Avaya SBCE. In this case, Avaya SBCE does not rewrite the content of the configuration file. The file server must serve the configuration file with Avaya SBCE content by using GROUPS in configuration file. Avaya SBCE requires two IP addresses, one for downloading configuration/firmware files and another interface used for PPM and SIP signaling. Avaya SBCE 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 SBCEs. This feature enables the maintaining of a single configuration file, for the entire enterprise, with individual Avaya SBCE 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 SBCE, 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 SBCE external IP address used for config/firmware files download.

Configuring Avaya SBCE

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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBCE**.
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 SBCE 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 222
Creating a reverse proxy service for file or firmware download on page 363

Appendix B: Configuring Avaya SBCE for interoperability with Avaya Multimedia Messaging

About this task

The timeout value set for Avaya Multimedia Messaging and Avaya SBCE are different. Therefore, when users log in to Avaya Equinox® through Avaya SBCE, they lose service periodically. To support long polling used in Avaya Multimedia Messaging, you must run a script that sets the timeout value.

Procedure

1. Download the patch file `sbc700-nginx-20150708.tar` from PLDS.
2. Type `mkdir /archive/cespatchdir`.

   The system creates a temporary directory in `/archive`.
3. Type `cd /archive/cespatchdir`.
4. Type `tar xf sbc700-nginx-20150708.tar`.
5. Type `./sbce-patch.sh -i sbc700-nginx-20150708.tar.bz2`.

   The system installs the patch.
6. Type `./sbce-patch.sh -l`.
7. Verify that the patch has been installed.

Appendix C: EMS web interface

The EMS web interface is a fully integrated, web-accessible operations and administration platform for Avaya SBCE UC security products. GUI centralizes and simplifies the provisioning, administration, control, and monitoring of Avaya SBCE.

The EMS web interface contains a Postgres database to store configuration and subscriber information, which is updated by each of the deployed Avaya SBCE 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 492

EMS screen elements

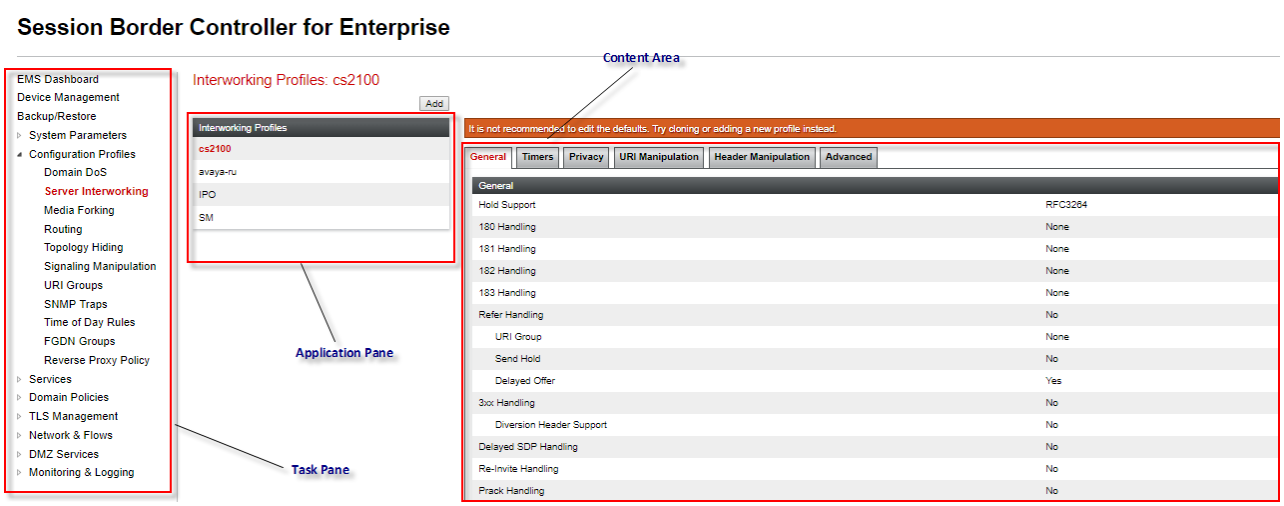
Use the EMS web interface for the administration and configuration of the Avaya SBCE security system.

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 492
[Tool bar field descriptions](#) on page 493
[Display settings field descriptions](#) on page 494
[Application pane](#) on page 494
[Dashboard screen content area](#) on page 494
[EMS web interface button descriptions](#) on page 504

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 492

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 492

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 492

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 SBCE security devices, Avaya SBCE 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.

Table continues…

Name	Description
Installed Devices	Displays a list of all the Avaya SBCE security devices which are installed and provisioned in the enterprise VoIP network
Alarms	Displays a streaming feed which displays currently active system alarms, parsed according to the Avaya SBCE 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 SBCE 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 SBCE 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 492

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.

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.

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 SBCE system configuration. You can also restore the system files through this screen.

Device Management

Use this screen to view, install, configure, shut down, or restart the Avaya SBCE security devices. You can also restart the EMS and SBCE devices from the Device Management screen.

This screen displays the **Devices**, **Updates**, **Licensing** and **Key Bundles** tabs.

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 SBCE 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 SBCE 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.
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.

Table continues…

Name	Description
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: Security : • ipcsScpFailure: Secure copy failed for log files • ipcsCopyFailure: Copy action failed for log files 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 SBCE **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.

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.
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 SBCE. 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 SBCE 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.

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 SBCE 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 SBCE 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
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**

Table continues…

Name	Description
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 SBCE 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 SBCE, 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 SBCE security device. The **Networks** tab allows you to enable or disable Avaya SBCE 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).

Table continues…

Name	Description
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 SBCE. 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.

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 for Enterprise*.
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.

Table continues…

Name	Description
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.
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 SBCE security device.

Table continues…

Name	Description
Shutdown Device	Shuts down the associated Avaya SBCE security device. **Warning:** Before you shut down the Avaya SBCE device, ensure that someone is available on site to turn on the Avaya SBCE device after shutting down.
Restart Application	Restarts an SBCE application.
View Configuration	Displays the configuration of the associated Avaya SBCE security device.
Install Device	Installs the associated Avaya SBCE 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 SBCE 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 492

Appendix D: CDR file field descriptions

Name	Description	Field size in bytes
Ipcs Id	The unique ID that identifies Avaya SBCE.	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
PAI Domain	The 32 last characters of the host part of the P-Asserted-Identity header.	32
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 SBCE 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 SBCE.	10
Server Flow	The first 10 characters of the SIP Server or Subscriber Flow administered on the Avaya SBCE.	10
Session Policy	The first 10 characters of the session flow administered on the Avaya SBCE.	10
Routing Profile	The first 10 characters of the Routing profile administered on the Avaya SBCE.	10
Alternate routes attempted	The number of times Avaya SBCE performs alternate routing.	4
Redirected to domain	The last 32 characters of the host part of the Contact header when Avaya SBCE 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 SBCE 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 SBCE. DO NOT use the slash	8
Connect time	The timestamp of ACK to Initial INVITE ingressing or egressing from Avaya SBCE.	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 SBCE, 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	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 SBCE. • 14: Unsuccessful call. Server failure on remote site. • 15: Unsuccessful call. Server failure at Avaya SBCE • 16: Unsuccessful call. Any other failure at remote site. • 17: Unsuccessful call. Any other failure at Avaya SBCE. • 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 SBCE failover happened during call.	1
Latency Progress	Latency in 100 Trying for Avaya SBCE timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Alert	Latency in 180 or 183 for Avaya SBCE timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Connect	Latency in 200 OK for Avaya SBCE timestamp from INVITE. Applicable to UAC and UAS.	4
Latency Ack	Latency in ACK for Avaya SBCE timestamp from 200 OK. Applicable to UAC and UAS	4
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
SSRC	The SSRC of the RTP data packet source.	4
Lost Pkt	The number of lost packets in the sequence interval.	4

Table continues…

Name	Description	Field size in bytes
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

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 SBCE feature that allows two SBCE 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 SBCE 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
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
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
SBCE	Session Border Controller for Enterprise
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. 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

A

AAMS configuration 478
accessing Avaya SBCE device
  through SSH 345
accessing port matrix 483
active users
  field descriptions 329
act on statements
  scripting language 420
  statement 420
add
  Domain DoS profile 232
  signaling interface 222
  subscriber flow 139
  Topology Hiding header 245
adding
  adding 108, 109, 111, 112
  custom recording tone 453
  Header Manipulation rule 274
  internal IP in System Manager 351
  interworking profile 264
  management server 202
  media forking profile 190
  media interface 476
  network 279
  network interface 276
  new recording tone 453
  new SIP Server profile 253
  new user agent 220
  regex expression 273
  request header parameters 111
  request parameters 108
  response header parameters 112
  response parameters 109
  routing rule to trunk server flow 462
  session flow 481
  session flow for recording server 454
  URI Manipulation rule 273
  URI or domain 263
adding a media attribute in SDP 431
Adding a new media interface 224
Adding a New RADIUS Server 187
Adding a Routing Rule 212
adding a URI
  URI group 149
Adding Media Forking Profile to Session Policy 191
adding network 279
adding network interface 276
adding SNMP v3 Access 197
add interworking profile general
  field descriptions 265
Add Media Forking Profile
Add Media Forking Profile *(continued)*
  field descriptions 190
Add Media Interface Pop-up Window Field Descriptions 224
Add RADIUS Server
  field descriptions 187
add routing profile
  fields descriptions 210
add Server Configuration profile
  field descriptions 254
add session flow
  field descriptions 145
Add SNMP v3 community
  field descriptions 197
add URI group
  add URI group criteria 150
  field descriptions 150
add user
  field descriptions 25
add user agent
  field descriptions 220
administering
  BFCP 439
  codec prioritization 467
  FECC 441
Administration
  AAA 496
  User 496
administrative account
  editing 26
  setting privileges 27
administrative accounts
  creating 25
administrative state
  editing 278
administrative users 328
advanced option
  configuration 178
advanced options
  field descriptions 178
alarms
  field descriptions 310
  managing 310
application pane 494
application relay
  IM 366
application relay configuration
  RTCP monitoring 47
application rule 88
  counter 75
  processing 74
Application rule 85
Application Rule 83–85
application rules 83

application rules *(continued)*
creating 370
architecture
standard platform 60
audit logs
field descriptions 326
viewing 325
Avaya Aura SIP Resiliency 464
Avaya SBCE
reconfiguring 156
Avaya SBCE device
adding 31
Avaya SBCE for Avaya Trunk
configuration 416
Avaya SBCE for interoperability with Avaya multimedia messaging 491
Avaya SBCE SIP trunk configuration
checklist 403
Avaya support website 486

B

back-to-back
single Session Manager 380
back-to-back-to-back
checklist 381
SBCEs 389, 391
backup 157
backup and restore
field descriptions 164
basic configuration checklist 155
BFCP
overview 439
BFCP administration 439
blacklist rules
changing 53
border rule 86–88
border rules
configuration 86
Border Rule screen
field descriptions 87
built-in structures 424
functions 424
regular expressions 424
variables and arrays 422

C

CA
certificates 289
CA certificates
deleting 290
viewing 290
cadf file
uploading 196
call
trace 329
call flow
call flow 76–79
example 76–79
call flow call processing
call flow call processing 77
example 77
call flow inbound policy invocation
call flow inbound policy invocation 77
example 77
call flow outbound policy invocation
call flow outbound policy invocation 78
example 78
call flow route resolution
call flow inbound route resolution 77
example 77
call flow server flow matching
call flow server flow matching 77, 78
example 77, 78
call flow splitting
increasing capacity 75
call flow transmit to network
call flow transmit to network 78
example 78
call from remote worker
subscriber flow matching 69
call handling
WebRTC 442
call preservation 459
configuration checklist 460
call processing
inbound 68
outbound 73
SIP 68
call reconstruction 464
call server
securing SIP phones 59
securing SIP trunk 57
call server profile
creating 353
call sever
call processing toward network 74
routing 67
call towards a server
route resolution 70
call toward server
server flow matching 73
CDR adjunct
creating 470
field descriptions 471
CDR file
field descriptions 506
CDR measurement 470
certificate
extract 283
certificate authority certificates
deleting 290
viewing 290

certificate file
uploading ... 285
certificate management ... 281
certificate revocation list ... 291
certificate revocation lists
deleting ... 292
viewing ... 292
certificates ... 284
CA ... 289
deleting ... 286
installing ... 284
viewing ... 286
CES
CA certificate ... 455
CES CA certificate
extract ... 455
CES proxy
configuration ... 457
change password
field descriptions ... 22
changing
administrative state ... 278
blacklist rules ... 53
calling party presentation ... 432
DNS IP ... 344
FQDN ... 344
gateway IP on a single server ... 341
gateway IP on Avaya SBCE ... 343
gateway IP on secondary EMS ... 343
hostname ... 343
management IP ... 38
management IP on a single server ... 341
management IP on Avaya SBCE ... 343
management IP on secondary EMS ... 343
network mask ... 341
network mask details on Avaya SBCE ... 343
network mask details on secondary EMS ... 343
network passphrase ... 344
transaction expire ... 463
Changing IP address of the primary EMS server on the secondary EMS server ... 342
changing NTP address on Avaya SBCE devices ... 342
changing primary EMS IP on unreachable SBCE ... 342
charging rule ... 116–118
field descriptions ... 117
checklist
configuring external media server ... 478
configuring transcoding ... 466
establishing end-to-end TLS communications ... 301
Geographic-redundant deployment ... 395
media tunneling ... 475
multiple session manager configuration ... 386
Presence server configuration ... 376
clearing
alarms ... 311
Client Profile
management ... 293
client TLS profile
create ... 456
clipcs
select ... 338
clipcs command line interface
clipcs command line interface ... 337
commands descriptions ... 337
clipcs console ... 336
clipcs console commands ... 337
clipcs top commands
instance commands ... 338
clone
SIP Server Profile ... 262
cloning
Application Rule ... 85
border rule ... 88
charging rule ... 117
cloning ... 88, 95, 99, 115, 137, 142, 143, 145, 205
Domain DoS profile ... 235
endpoint flow ... 142
interworking profile ... 272
LDAP server ... 195
media rule ... 95
security rule ... 99
server endpoint flow ... 143
session flow ... 145
session policy ... 137
signaling rule ... 115
SNI group ... 307
SNMP trap profle ... 201
subscriber endpoint flow ... 142
ToD rule ... 205
Topology hiding profile ... 244
Cloning an existing routing profile ... 214
code blocks
statements ... 421
codec prioritization ... 95
administering ... 467
codec prioritizations
codec prioritizations ... 125
field descriptions ... 125
collect archive field descriptions ... 332
collecting
logs ... 331
collection
delete ... 484
edit name ... 484
generating PDF ... 484
sharing content ... 484
collect logs field descriptions ... 332
command line interface
overview ... 333
Command Line Interface ... 21
commands
clipcs console ... 336
instance ... 338
commissioning

commissioning *(continued)*
Avaya SBCE device 34
communications session
establish 347
communications settings
terminal program 347
concurrent sessions
counter 75
config/firmware
files download 487
configurable snapshot
creating 166
configuration
endpoint policy group 74
File server 488
phone 489
configuration checklist
back-to-back 390
back-to-back-to-back 392
configure
application relay settings 389
configuring 491
application relay 375
automatic snapshots 163
Avaya SBCE for HA deployment using CLI 333
Avaya SBCE for other trunks 417
CES proxy 457
emergency calls from unregistered endpoints 379
endpoint policy group 468
High Availability 39
inbound signaling rule to send 200 ok response for options request 109
media server 479
multi tenancy 365
multi tenancy configuration 365
packet capture 329
RADIUS server 28
recording server 449
RTCP monitoring generation support 52
server flow for transcoding 468
single server deployment using CLI 334
UCID 450
configuring application relay
core SBCE 48
DMZ SBCE 49
remote Avaya SBCE 49
RTCP monitoring 48, 49
configuring Avaya SBCE
real time trunk status 320
configuring external media server checklist 478
configuring HA Heartbeat Interval
configuring HA Max Retries 186
configuring multi-session manager
back-to-back-to-back SBCEs 389, 391
configuring Presence server
checklist 376
configuring SBCE
configuring SBCE *(continued)*
simultaneous downloads 489
connecting terminal device 346
connecting to
Avaya SBCE device 346
connection to SBC
terminal device 346
console 336
content
publishing PDF output 484
searching 484
sharing 484
watching for updates 484
converting
certificates to PEM format 304
counter
application rule 75
concurrent sessions 75
create 356
creating
Application Rule 83
border rule 86
call server flow 414
CDR adjunct 470
certificate signing request 282
charging rule 116
client profile 293
client TLS profile 456
configurable snapshot 166
creating 86, 89, 97, 100, 119, 124, 139, 204
endpoint flow 138, 139
external Media Interface toward Trunk Server 413
External Signaling Interface toward Trunk-side Server 411
FGDN groups 460
internal Media Interface toward call server 413
interworking profiles 404
LDAP server 193
media rule 89, 204
new TLS server profile 297
policy group 119
PPM mapping profile for presence server 377
Radius profile 471
reverse proxy for multi tenant 365
Reverse Proxy Policy 361
Routing Profile 407
routing rule for call preservation 462
security rule 97
server endpoint flow 139
server profile 477
Server Profile for Call Server 405
Server Profile for trunk server 406
session flow 145
session policy 124
session policy for media server 480
session policy for Recording Server 452
signaling interface for a phone network 355

creating *(continued)*
signaling rule ... 100
SNI group ... 306
SNMP trap profile ... 200
subscriber endpoint flow ... 139
Topology Hiding profile ... 241, 410
trunk server flow ... 415
URI group ... 149
Creating
server interworking profile ... 388
creating and restoring
configurable snapshot using CLI ... 341
creating a new routing profile ... 209
creating routing profile for a trunk server ... 408
CRLs
deleting ... 292
viewing ... 292
CSRs
externally generated ... 283

D

dashboard
about ... 494
alarms ... 494
component descriptions ... 309
dashboard ... 309
incidents ... 494
installed devices ... 494
notes ... 494
screen ... 309
DB-9 connector
connecting terminal device ... 346
debugging
field descriptions ... 176
delete
SIP Server Profile ... 262
Topology Hiding header ... 246
Topology Hiding profile ... 244
deleting
add a word ... 307
administrative account ... 27
application rule ... 88
Application Rule ... 85
a scrubber rules package ... 240
CA certificates ... 290
certificate authority certificates ... 290
certificate revocation lists ... 292
certificates ... 286
charging rule ... 118
client profile ... 296
CRLs ... 292
deleting ... 88, 96, 100, 115, 123, 137, 144, 147, 151, 207
Domain DoS profile ... 236
end-point flow ... 144
existing user agent ... 221
Header Manipulation rule ... 275
deleting *(continued)*
interfaces ... 278
interworking profile ... 273
LDAP server ... 195
media rule ... 96
policy group ... 123
policy set ... 123
security rule ... 100
server profile ... 300
session flow ... 147
session policy ... 137
signaling rule ... 115
SNI group ... 307
SNMP trap profile ... 202
system snapshot ... 163
ToD rule ... 207
URI from URI group ... 151
URI group ... 152
URI Manipulation rule ... 274
URI or domain ... 263
deleting an existing media interface ... 226
Deleting an Existing RADIUS Server ... 189
deleting an existing routing profile ... 215
deleting an existing signaling interface ... 223
Deleting an existing SNMP v3 Account ... 199
deleting a routing rule ... 213
deleting regex rules ... 274
deploying
geographically dispersed Avaya SBCE HA ... 46
designating a snapshot server ... 157
device configuration ... 31
Device Management
field descriptions ... 32
Device Management Overview ... 167
diagnostics
field descriptions ... 327
diagnostics results ... 327
diagram
remote user topology ... 348
direction flags
In/Out ... 75
disabling
media tunneling ... 476
network interfaces using CLI ... 340, 344
SNMP traps by severity ... 203
display settings
field descriptions ... 494
DMZ services ... 498
documentation portal ... 484
finding content ... 484
navigation ... 484
document changes ... 18
Domain DoS
field descriptions ... 232
domain dos configurations ... 227
Domain DoS profile
rename ... 235

Domain DoS profiles 232
domain policies 499
management 82
Domain Policies 56
Unified Communications 56
domain policies field descriptions 500
DoS
security features 228
DoS/DDoS global parameters
field descriptions 229
DoS/DDoS settings
editing 231
dos ddos attack type descriptions 228
DoS learning
field descriptions 237
DoS Protection
editing 264
recalculate values 264
DoS whitelist 263
DoS Whitelist
adding 263
deleting 263
download files
config/firmware 487
downloading PLDS
license file 41
dynamic licensing 33

E

edit
Topology Hiding header 245
editing
administrative state 278
Application Rule 84
border rule 87
charging rule 117
Client Profile 296
codec prioritization 95
Domain DoS profile 236
DoS Protection 264
editing 87, 94, 99, 108, 110, 112, 113, 121, 136, 206
endpoint policy group 122
existing user agent 220
Header Manipulation rule 275
interfaces 279
interworking profile 272
LDAP server 194
media rule 94, 206
network management parameters using CLI 280, 340
policy set 121
request header parameters 112
response header parameters 113
response parameters 110
security rule 99
server endpoint flow 143, 144
server profile 300
editing *(continued)*
session policy 136
signaling rule 108
SIP server profile 261
SIP server profile parameters using CLI 340
SNMP profile 201
subscriber endpoint flow 143, 144
URI group 151
URI Manipulation rule 274
Editing an existing Media Interface 225
Editing an Existing RADIUS Server 188
Editing an Existing Routing Profile 212
editing an existing signaling interface 223
editing an existing SNMP v3 Account 199
editing a routing rule 213
editing device configuration 173
editing regex rules 274
editng
editing 146
session flow 146
edit wizard
field descriptions 37
emergency group 150
EMS software upgrade 41
EMS web interface 492
Administration 496
Backup 496
button descriptions 504
configuration profiles 497
Dashboard 496
Device Management 496
log in 21
Restore 496
System parameters 496
task pane 495
tool bar 493
enabling
AAMS offboarding 479
CDR in an application rule 473
FGDN 461
interfaces 157
media tunneling 476
network interfaces using CLI 340, 344
periodic statistics 473
SIP Resiliency 464
transcoding 467
transrating 467
enabling high availability 175
enabling or disabling an installed scrubber rules package 240
endpoint
flows 138
endpoint administration
GROUP identifier 487
endpoint flow 139, 144
cloning 142
creating 138
endpoint flows

endpoint flows *(continued)*
managing ... 138
endpoint policy ... 399
creating ... 371
endpoint policy group
configuration ... 74
configuring ... 468
editing ... 122
endpoint policy rules
rules ... 119
enterprise wide licensing ... 33
establishing end-to-end TLS communications
checklist ... 301
exiting the runtime options screen ... 43
extended hostname validation ... 305
external media interface for a phone network
creating ... 357
external signaling interface ... 355
extract certificate ... 283
extracting
CES CA certificate ... 455

F

Failover Group Domain Name
enabling ... 461
far end camera control ... 441
FECC
administration ... 441
FGDN
enabling ... 461
FGDN group
field descriptions ... 461
FGDN groups
creating ... 460
field description
TLS Certificates screen ... 287
field descriptions
active users ... 329
add interworking profile general ... 265
add Server Configuration profile page ... 254
add snapshot server ... 158
add user ... 25
add user agent ... 220
advanced options ... 178
alarms ... 310
Application Rule ... 83
audit logs ... 326
backup and restore ... 164
CDR adjunct ... 471
CDR file ... 506
change password ... 22
configuring application relay for RTCP monitoring ... 50
debugging ... 176
Device Management ... 32
diagnostics ... 327
display settings ... 494
field descriptions *(continued)*
DoS/DDoS global parameters ... 229
DoS learning ... 237
external media interface for phone network ... 358
FGDN group ... 461
firewall ... 53
incident viewer ... 312
install CA certificate ... 291
install CRL ... 292
internal media server for Avaya call server ... 358
network management ... 276
new profile ... 294
new server profile screen ... 298
periodic statistics ... 319
PPM Mapping Profile ... 360
Radius profile ... 472
reverse proxy ... 148
Reverse Proxy ... 361
scrubber ... 241
Security Rules ... 98
server status ... 321
SigMa ... 435
Signaling Interface ... 356
subscriber flow profile ... 139
syslog management ... 217
syslog viewer ... 324
system administration screen ... 28
system viewer ... 315
Topology Hiding Profiles ... 242
trace ... 330
TURN Relay ... 446
TURN STUN configuration ... 444
user registrations ... 322
files download
config/firmware ... 487
File server
configuration ... 488
finding content on documentation portal ... 484
finding port matrix ... 483
firewall
field descriptions ... 53
firmware/config
files download ... 487
flows
endpoint ... 138
session ... 144
Forward Error Correction
FEC ... 440
From header
Topology Hiding examples ... 249
functions ... 424
built-in ... 424
built-in structures ... 424

G

geographically dispersed Avaya SBCE HA pair

geographically dispersed Avaya SBCE HA pair *(continued)*
interface connections 44
Geographic-redundant
non-HA mode 394
Geographic-redundant deployment 394
HA mode 395
Global Parameters
vverview 187
Graphical User Interface (GUI)
browser support 20
GROUP identifier
endpoint administration 487
groups
uniform resource identifier 148
URI 148

H

HA failovers 38
HA node
HA node 40
status states 40
hardware warranty 19
Header Manipulation rule
adding 274
deleting 275
editing 275
HEADERS variable 422
High Availability
configuring 39
High-Availability pair
geographically dispersed 43
hook points 425

I

identity engine 147
identity engine server
configuring 147
In/Out
direction flags 75
inbound
call processing 68
policy invocation 69
inbound policy
invocation 66
incidents 311
incident viewer
field descriptions 312
increasing capacity
call flow splitting 75
installation wizard
field descriptions 35
installing 284
Avaya SBCE device 34
CA certificate 289
Certificate Revocation List 291
installing *(continued)*
third-party certificates 282
installing rules
scrubber 239
instance
commands 338
interface
signaling 222
viewing 279
interfaces
deleting 278
existing signaling interface 223
view 223
internal IP
adding 351
internal media interface
avaya call server 358
create internal 358
creating 358
internal signaling interface 356
internal signaling interface toward call server 412
interworking profile
adding 264
cloning 272, 353
deleting 273
editing 272
renaming 273
invocation
inbound policy 66
outbound policy 74
outbound policy call processing 67
IP, gateway, and network mask change 341

L

LDAP based call routing 207
LDAP server 193–195
LDAP server profile 192
learned DoS parameters
setting 237
license file
downloading PLDS 41
load balancing 208
locating
SIP servers 71
logging
EMS web interface 21
logging in to EMS 345
logs 323
collection 331

M

MAC based LDAP authentication 192
MAC based LDAP authentication field descriptions 193
making a system snapshot 159
management IP

management IP *(continued)*
changng 38
managing
domain policies 82
network options 184
SBCE logging level 176
server profiles 297
session flows 138
SIP options 183
Managing Avaya SBCE security devices 20
managing device-specific settings 221
Managing Port options 184
Managing security features 183
manipulation of P-Asserted-Identity Header 430
matching
server flow 67
subscriber flow 66
media
unachoring 126
unanchor 125
media and video
field descriptions 90
Media NAT 90
Media Forking
overview 189
media interface
adding 476
media rule 89, 94–96
creating 370
media rules
rules 89
media server
configuring 479
media server offboarding 479
media statistics 470
media tunneling 475
checklist 475
disabling 476
enabling 476
mobile workspace
topology diagram 348
monitoring
RTCP 186
rtcp for remote worker 384
Monitoring & Logging
system 503
Monitoring RTCP
single Session Manager deployment 378
multi-session manager
web interface 385
My Docs 484

N

network
adding 279
interface 276
network *(continued)*
viewing 279
network& flows
settings 502
network connectivity overview 253
network interface
adding 276
network interfaces
configuring 276
network management
editing 279
field descriptions 276
network options
manage 184
networks
editing 279

O

options tab display field descriptions 183
other trunks
configuration 417
other variables 424
outbound
call processing 73
outbound policy
invocation 74
outbound policy call processing
invocation 67
overview 20
basic system configuration 154
command line interface 333

P

packet capture
configuration 329
password
console 22
EMS GUI 22
policies 23
passwords 22
periodic statistics
enabling 473
field descriptions 319
viewing 318
PFX
extract 283
phone
configuration 489
PKCS#12
extract 283
policies
session 123
policies and rules
associations 62
configuration 60

policy group 119, 123
policy group summary 121
policy invocation
inbound 69
route resolution 69
policy set 121, 123
policy sets 122
pooled licensing
using 33
portable snapshots
configuring 166
restoring 166
port matrix 483
port ranges
field descriptions 185
PPM Mapping Profile
create 359, 397
field descriptions 360
PPM settings
configuring 400
prerequisites 31
Presence Server
configuring 400
processing
application rule 74
profile
call server 353
protocol scrubbing 238

Q

QoS parameters tab 114

R

Radius profile
creating 471
field descriptions 472
RADIUS server
configuring 28
real time
SIP Server Status 320
rebooting a device 168
recording server
configuration 449
Record Route header
Topology Hiding examples 251
regenerating self-signed certificates 344
registered users
user registrations 321
viewing 322
registration processing
SIP 65
related documentation 482
remote access 438
remote support 438
remote worker
remote worker *(continued)*
checklist 352
Session Manager configuration 350
Remote Worker registration
limitation 350
rename
SIP Server Profile 262
renaming
Application Rule 85
border rule 88
charging rule 118
Domain DoS profile 235
interworking profile 273
LDAP server 194
media rule 96
renaming 88, 96, 99, 115, 137, 206
security rule 99
session policy 137
signaling rule 115
SNI group 306
SNMP trap profile 202
ToD rule 206
Topology Hiding profile 243
URI group 152
Renaming an Existing Routing Profile 215
reordering
policy sets 122
reordering 122
reordering precedence
reordering precedence 146
session flows 146
reordering routing rule precedence 214
request header parameters 111, 112
Request Headers Parameters Tab 111
request parameters 108
response header parameters 112, 113
Response Headers Parameters Tab 112
response parameters 109, 110
Responses Parameters Tab 109
restarting a device 168
restoration of a system snapshot 160
restoration of configuration data 160
restore 157
restoring
portable snapshots 166
restoring a snapshot file 162
restoring a snapshot file manually 161
retrieving
a snapshot file 161
Reverse Proxy
field descriptions 361
reverse proxy profile
field descriptions 148
reverse proxy service
create 362
reverse proxy service for file or firmware download
create 363

Round Trip Time 51
route resolution
call towards a server 70
policy invocation 69
routing profile 66
subscriber processing toward remote worker 70
routing
call processing toward network 74
toward network 67
routing profile
call server 372
route resolution 66
Routing Profiles 207
Routing Rule Management 212
RTCP
monitoring relay 46
RTCP monitoring
remote worker 383
single Session Manager 378
RTCP monitoring generation 51
RTCP Monitoring Relay
field descriptions 47
RTCP Monitoring Report Generation
field descriptions 52
rules
border 86
endpoint policy rules 119
media rules 89
security rules 96
signaling 116
signaling rules 100
Time of Day (ToD) rules 204
rules and policies
associations 62
configuration 60
rules and policies configuration checklist 64
running
scripts on the CES server 456
turntop command 443

S

SAL 438
SBCE
back-to-back-to-back 389, 391
sbceinfo commands
getapptype 335
getemsip 335
gethwtype 335
getversion 335
SBCE reconfiguration command options 338
scenarios
media unanchoring 126
Scopia and Avaya SBCE interoperability with SRTP 440
screen
dashboard 309
scripting language
scripting language *(continued)*
session statement 419
signaling manipulation 418
scrubber 238
field descriptions 241
scrubber actions
configuration 240
scrubber rules
installing 239
viewing 239
SDP capability negotiation 94
SDP header
Topology Hiding examples 251
SDP variable 423
searching for content 484
secure CES proxy 455
security configuration overview 227
Security Feature Control 182
security rule 97, 99, 100
security rules
rules 96
Security Rules
field descriptions 98
selecting
log levels 216
server endpoint flow 139, 143, 144
server flow
creating 373
matching 67
server flow for transcoding
configuring 468
server flow matching
call toward server 73
server interworking 264
server profile
creating 477
management 297
server status
field descriptions 321
session
accessing clipcs remotely 347
flows 144
policies 123
session flow 145–147
adding 481
session flow for recording server
adding 454
session flows 146
session manager
Avaya SBCE internal and external IP addresses 388
configure primary and secondary 388
Session Manager
disabling PPM 352
session policy 124, 136, 137
field descriptions 125
Session Policy
media forking profile 191

session policy for media server
creating ... 480
session statement
scripting language ... 419
statement ... 419
session variables ... 420
setting
learned DoS parameters ... 237
setting EMS time zone ... 42
settings
externally generated CSRs ... 283
sharing content ... 484
show flow dynamic ... 337
shutting a device down ... 168
Sigma Design Overview ... 436
SigMa Editing the Allow Header ... 433
SigMa Editor
field descriptions ... 435
SigMa Prefix Stripping ... 435
SigMa primer
signaling manipulation ... 419
SigMa Replace From Header For a Set of Users ... 432
SigMa Scripting Examples ... 426
SigMa scripting language
signaling manipulation ... 418
SigMa scripting tutorial ... 430–433, 435
SigMa Scripting Tutorial ... 429
Signaling
QoS parameters tab ... 114
signaling ... 114
signaling interface
field descriptions ... 222
for an Avaya call server ... 356
signaling manipulation
scripting language ... 418
SigMa primer ... 419
SigMa scripting language ... 418
signaling rule ... 100, 108, 115
field descriptions ... 101
signaling rule ... 101
signaling rules ... 116
rules ... 100
simultaneous downloads
configuring SBCE ... 489
single sign on ... 147
configuring ... 147
SIP
call processing ... 68
SIP message processing
high level ... 65
SIP phones
call server ... 59
SIPREC
codec prioritization ... 451
configuration ... 447
creating media rule ... 451
SIPREC feature
SIPREC feature *(continued)*
overview ... 447
SIP registration
processing ... 65
SIP server
DoS configuration ... 227
SIP Server Configuration
profile management ... 253
SIP server profile
editing ... 261
SIP Server profile
adding new ... 253
SIP servers
locating ... 71
SIP trunk
call server ... 57
SIP trunking overview ... 402
SNI group ... 305–307
SNMP Settings ... 196
SNMP trap profile
clone ... 201
create ... 200
delete ... 202
rename ... 202
SNMP traps
disable by severity ... 203
software warranty ... 19
solution
config/firmware files download ... 487
specifying
SigMa Script in Server Configuration ... 436
SRTP failover
considerations ... 440
SRTP support ... 440
statement
session statement ... 419
statements
code blocks ... 421
statistics ... 315
subscriber endpoint flow ... 139, 142–144
subscriber flow
advanced services ... 374
matching ... 66
subscriber flow matching
call from remote worker ... 69
subscriber processing toward remote worker
route resolution ... 70
support ... 486
support under warranty ... 19
swapping
Avaya SBCE devices in single server deployment ... 170
swapping Avaya SBCE devices ... 169
swapping EMS server in HA pair deployment ... 171, 172
swapping EMS server in single server deployment ... 170
syslog management
field descriptions ... 217
Syslog Parameter Management ... 216

syslog viewer
field descriptions 324
system administration screen
field descriptions 28
system alarms 310, 311
managing 310
system incidents 311
system logs 323
system statistics 315
system viewer
field descriptions 315
system wide single endpoint dos configurations 227

T

tagging
VLAN 278
terminal device 346
third-party certificates
installing 282
Time of Day (ToD) rules
rules 204
time zone 42
tips and tricks
TLS 304
TLS
tips and tricks 304
TLS management
management 501
TLS Parameter Management 281
tls profile management 293
ToD
field descriptions 120, 204
policy 120
ToD 204
ToD rule 204–207
To header
topology hiding 250
topology diagram
remote worker 348
Topology Hiding 243
affected headers 246
topology hiding examples for request-line header 248
Topology Hiding header
adding 245
deleting 246
editing 245
Topology Hiding headers 247
Topology Hiding profile
clone 244
create 241
deleting 244
Topology Hiding Profiles
field descriptions 242
Topology Hiding settings
examples 248
trace
trace *(continued)*
call 329
field descriptions 330
traceSBC command
usage 334
training 485
transaction expire
changing 463
transcoding
enabling 467
introduction 466
transcoding configuration
checklist 466
trap
description 200
TURN Relay
field descriptions 446
TURN STUN configuration
field descriptions 444
turntop
usage 443
turntop command
running 443

U

UCID 114
configuration 450
Unified Communications 56
uniform resource identifier
groups 148
uninstalling device configuration 174
upgrading system management 174
upload
certificate file 285
uploading
cadf file 196
URI
groups 148
URI from URI group 151
URI group 149, 151
deleting 152
renaming 152
URI Manipulation rule
adding 273
deleting 274
editing 274
regex rules 274
user accounts
administrator account 24
user agents 220
user-defined variables 425
using
pooled licensing 33

V

variable 422, 423
variables 419, 420, 424
variables and arrays
built-in 422
built-in structures 422
VGA connection 345
Via header
Topology Hiding example 251
videos 485
view
existing signaling interface 223
viewing
administrative users 328
alarms 310
audit logs 325
authorized user agents 221
CA certificates 290
certificate authority certificates 290
certificate revocation lists 292
certificates 286
CRLs 292
device configuration 173
diagnostics results 327
Domain DoS profile 234
DoS/DDoS settings 228
incidents 311
interface 279
logs 323
network 279
periodic statistics 318
policy group summary 121
registered users 322
scrubber rules 239
statistics 315
status of the SIP servers 321
system alarms 310
system incidents 311
system logs 323
system statistics 315
viewing 121, 311, 315, 327, 328
Viewing an existing media interface 225
viewing EMS time zone 42
viewing existing server interworking profiles 272
Viewing SIP Server profile 261
VLAN
use 277

W

warranty 19
watch list 484
web collaboration
configuring 400
webRTC
configuring TURN/STUN profile 443
webRTC *(continued)*
configuring TURN relay service 445
WebRTC
call handling 442
webRTC considerations 442
where clause 419
whitelisting
Avaya SBCE internal IP address 351