Administering Avaya Session Border Controller for Enterprise

Release 7.1
Issue 4
September 2017

© 2014-2017, 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. 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 Designated Processor that hosts 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. 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. Note that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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).

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.

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.

Contents

Chapter 1: Introduction 16
Purpose 16
Change history 16
Warranty 16
Chapter 2: Overview 18
Manage Avaya SBCE security devices 18
Graphical User Interface 18
EMS web interface 19
Command Line Interface 31
Logging on to the EMS web interface 31
Passwords 31
Console and SSH passwords complexity 32
EMS GUI password complexity 32
Password policies 32
Chapter 3: Administrative User Accounts 34
Administrative accounts 34
Creating a new administrative account 35
Add user field descriptions 35
Editing an administrative account 36
Deleting an administrative account 36
Setting administrative account privileges 37
Administration field descriptions 37
Avaya Access Secure Gateway 40
Installing an ASG authentication file 40
Chapter 4: Device Configuration 41
Prerequisites 41
Adding an Avaya SBCE device 41
System Management field descriptions 42
Commissioning an Avaya SBCE device 43
Installation Wizard field descriptions 44
Changing the management IP from the EMS web interface 46
High Availability failovers 47
Configuring High Availability 48
HA Node Status States 49
Upgrade of the EMS software 50
Obtaining a license file from Avaya PLDS 50
Viewing the EMS server time zone 51
Setting the EMS server time zone 51
Exiting the Avaya SBC Runtime Options screen 52

High-Availability pair geographically dispersed 52
Interface connections for a geographically dispersed Avaya SBCE HA pair 53
Deploying a geographically dispersed Avaya SBCE HA configuration 55
Configuring RTCP monitoring 56
RTCP Monitoring field descriptions 56
Application relay configuration for RTCP monitoring 56
Configuring Application Relay for RTCP monitoring in core Avaya SBCE 57
Configuring Application Relay for RTCP monitoring in remote Avaya SBCE 58
Changing blacklist rules 59
Firewall field descriptions 60
Chapter 5: Domain Policy, Routing, and Message Flow Administration 62
Governing Unified Communications with Domain Policies 62
Unified Communications Policies 62
Example: Call server with SBCE securing SIP trunk 63
Example: Call server with SBCE securing SIP phones 65
Rules and policies configuration 66
Architecture 67
Rule and policy associations 68
Rules and policies checklist 70
SIP message processing 71
SIP registration processing 71
Subscriber flow matching 71
Inbound policy invocation registration processing 72
Route resolution 72
Server flow matching 72
Outbound policy invocation call processing 73
Transmit to network registration processing 73
SIP call processing on Avaya SBCE 73
Inbound call processing 73
Subscriber flow matching for call originated from remote worker 74
Policy invocation and route resolution 75
Inbound policy invocation 75
Route resolution for call towards remote worker 75
Route resolution for a call towards a server 76
SIP servers identification 76
Outbound call processing 78
Server flow matching for a call to a server 79
Outbound policy invocation for registration processing 79
Transmit to network for call processing 79
Application rule processing for endpoint policy group configuration 80
Maximum concurrent sessions per endpoint counter 80
Maximum concurrent sessions counter 80
Rules for call flows 80

In/Out direction flags ... 80
SIP call flow example ... 81
Call flow example for call processing ... 82
Call flow example for server flow matching in calls originated from a server ... 82
Call flow example for inbound policy invocation ... 82
Call flow example for route resolution ... 83
Call flow example for server flow matching in a call towards a server ... 83
Call flow example for outbound policy invocation ... 83
Call flow example for transmit to network ... 84
Call flow example from PSTN trunk to a Call Center Elite user ... 84
Domain policies management ... 88
Application rules ... 88
Security rules ... 102
Signaling rules ... 108
Endpoint policy groups ... 122
Session policies ... 126
Manage endpoints and session flows ... 140
Endpoint flows ... 141
Cloning an existing endpoint flow ... 145
Editing existing endpoint flows ... 146
Reordering the precedence of endpoint flows ... 147
Deleting an existing endpoint flow ... 147
Session flows ... 147
Single Sign-On and Identity Engine ... 150
Configuring Single Sign-On and an Identity Engine server ... 150
Uniform Resource Identifier groups ... 151
Creating a new URI group ... 151
Adding an additional URI to an existing URI group ... 153
Editing an existing URI group ... 154
Deleting a SIP URI from an existing URI group ... 154
Renaming an existing URI group ... 155
Deleting an existing URI group ... 155
Chapter 6: System Configuration ... 157
Basic system configuration overview ... 157
Basic configuration quick-start checklist ... 158
Reconfiguring Avaya SBCE ... 159
Enabling interfaces ... 160
Backup / Restore system information ... 160
Designating a Snapshot Server ... 160
Making system snapshots ... 161
Restoration of a system snapshot ... 162
Retrieving a snapshot file ... 163
Restoring a snapshot file manually ... 163

Deleting a system snapshot..... 165
Configuring automatic snapshots..... 165
Management of deployed Avaya SBCE security devices..... 167
Shutting down an Avaya SBCE security device..... 167
Restarting an Avaya SBCE application..... 168
Viewing device configuration..... 169
Editing device configuration..... 169
Deleting device configuration..... 169
Upgrading system management..... 170
Enabling High Availability..... 170
Managing Avaya SBCE logging level..... 171
Debugging field descriptions..... 171
Advanced Options configuration..... 173
Viewing a CDR file..... 174
Security feature control..... 177
Managing SIP options..... 178
Allowing reuse of the same IP..... 179
Managing port options..... 179
Monitoring RTCP..... 180
Configuring HA Heartbeat Interval and Max Retries..... 181
Global Parameters overview..... 181
Adding a new RADIUS server..... 182
Editing an existing RADIUS server profile..... 183
Deleting an existing RADIUS server profile..... 184
Media Forking overview (Standard Platform only)..... 184
Adding a Media Forking profile (Standard Platform only)..... 185
Adding Media Forking Profile to Session Policy (Standard Platform only)..... 186
SNMP settings..... 187
Uploading a cadf file to System Manager..... 187
Adding a new SNMP v1/v2 community..... 188
Adding SNMP v3 access..... 192
Creating an SNMP trap profile..... 193
Adding a management server..... 195
Enabling and disabling traps by severity..... 196
Time of Day (ToD) rules..... 196
Creating a new Time of Day rule..... 197
Cloning an existing Time of Day rule..... 198
Editing an existing Time of Day rule..... 199
Renaming an existing Time of Day rule..... 199
Deleting an existing Time of Day rule..... 200
Routing profiles..... 200
Load balancing..... 200
Creating a new routing profile..... 201

Routing rule management 204
Cloning an existing routing profile 206
Renaming an existing routing profile 206
Deleting an existing routing profile 207
Syslog parameter management 207
Selecting log levels 207
Syslog management field descriptions 208
User agents (Advanced Services only) 211
Adding a new user agent (Advanced Services only) 211
Editing an existing user agent (Advanced Services only) 212
Viewing authorized user agents (Advanced Services only) 212
Deleting an existing user agent (Advanced Services only) 212
Managing device-specific settings 212
Adding a new signaling interface 213
Editing an existing signaling interface 214
Viewing an existing signaling interface 214
Deleting an existing signaling interface 214
Viewing an existing media interface 215
Adding a new media interface 215
Editing an existing media interface 216
Deleting an existing media interface 216
Chapter 7: Security Configuration 217
Overview 217
System wide single endpoint DoS configurations 217
Domain DoS configurations 217
SIP server DoS configuration 217
DoS Security features 218
Viewing DoS/DDoS settings 218
Editing DoS/DDoS settings 219
Domain DoS profiles 222
Viewing a Domain DoS profile 222
Adding a new Domain DoS profile 222
Cloning an existing Domain DoS profile 223
Renaming an existing Domain DoS profile 223
Editing an existing Domain DoS profile 223
Deleting a Domain DoS profile 225
Setting learned DoS parameters 225
DoS Learning field descriptions 226
Protocol scrubber 226
Scrubber package file path 227
Viewing scrubber rules 227
Installing a scrubber rules package 227
Configuring scrubber actions 228

Enabling or disabling an installed Scrubber Rules package ... 229
Deleting a Scrubber Rules package ... 229
Creating a new Topology Hiding profile ... 230
Topology Hiding Profiles field descriptions ... 231
Adding a new Topology Hiding header ... 232
Editing a Topology Hiding Header ... 233
Cloning a Topology Hiding profile ... 234
Renaming a Topology Hiding profile ... 234
Headers affected by Topology Hiding ... 235
Chapter 8: Server and Network Interface configuration ... 240
Overview ... 240
SIP Server Configuration Profile management ... 240
Adding a new SIP Server profile ... 240
Viewing a SIP Server profile ... 247
Editing a SIP Server profile ... 247
DoS Whitelist ... 248
Editing and recalculating the DoS Protection parameters ... 248
Cloning an existing SIP Server profile ... 249
Renaming an existing SIP Server profile ... 249
Deleting an existing SIP Server profile ... 250
Server interworking ... 250
Adding a new Interworking profile ... 250
Viewing existing Server Interworking profiles ... 255
Editing the Server Interworking profile parameters ... 256
Adding a new URI Manipulation rule ... 256
Editing an existing URI Manipulation rule ... 257
Deleting an existing URI Manipulation rule ... 257
Adding a new Header Manipulation rule ... 257
Editing a Header Manipulation rule ... 258
Deleting a Header Manipulation rule ... 258
Cloning a Interworking profile ... 258
Renaming an existing Interworking profile ... 259
Deleting an Interworking profile ... 259
Networks and interfaces management ... 259
Adding a new network interface ... 260
Virtual LAN ... 261
Changing the administrative state of an interface ... 262
Deleting an existing interface ... 262
Viewing an existing interface or network ... 262
Adding a new network ... 263
Editing network management parameters ... 263
Chapter 9: TLS Management ... 264
TLS Parameter Management ... 264

Certificate Management 264
Installing third-party certificates 265
Creating a Certificate Signing Request 265
Recommended settings for externally generated CSRs 266
Extracting a certificate and key from a PFX or PKCS#12 keystore 266
Certificates 267
Installing certificates 267
Uploading certificate file 267
Synchronizing and installing certificate in a multi-server deployment 269
Installing certificate on a single server Avaya SBCE 270
Viewing certificate details 271
Deleting certificates 271
TLS Certificates screen field descriptions 272
Certificate Authority certificates 273
Installing CA certificate 274
Viewing Certificate Authority details 274
Deleting Certificate Authority certificates 274
Install CA Certificate screen field descriptions 275
Certificate Revocation Lists 275
Installing Certificate Revocation List Option 275
Viewing Certificate Revocation List details 275
Deleting Certificate Revocation Lists 276
Install CRL screen field descriptions 276
TLS Profile Management 276
Client Profile Management 276
Creating a client profile 277
TLS client profile screen field descriptions 277
Editing a Client Profile 279
Deleting a client profile 279
Server Profile Management 280
Creating a new TLS server profile 280
TLS server profile screen field descriptions 280
Editing a server profile 282
Deleting a server profile 283
Checklist for establishing end-to-end TLS communications 283
Considerations for working with TLS 286
Converting a certificate to PEM format 286
Chapter 10: System Monitoring 288
Dashboard 288
Dashboard content descriptions 288
Manage system alarms 289
Viewing current system alarms 289
Clearing system alarms 290

Viewing system incidents 290
Incident Viewer field descriptions 291
Viewing system SIP statistics 293
Statistics Viewer field descriptions 293
Real Time SIP Server Status 296
Configuring Avaya SBCE for Real Time Trunk status 296
Viewing the status of the SIP servers 297
Server Status field descriptions 297
User registration 297
Viewing the list of registered users 297
User Registrations field description 298
Viewing system logs 299
Syslog Viewer field descriptions 299
Viewing audit logs 301
Audit Logs field descriptions 302
Viewing diagnostics results 302
Diagnostics field descriptions 303
Viewing administrative users 303
Active Users field descriptions 304
Trace 304
Configuring Packet Capture 304
Trace field descriptions 306
Chapter 11: Avaya SBCE CLI commands 308
Overview 308
Root-level console commands 308
Accessing Avaya SBCE 316
Avaya SBCE reconfiguration script options 319
Changing the management IP from the EMS web interface 320
Changing management IP, gateway and network mask details for a single server deployment 321
Changing management IP for an HA deployment 321
Changing hostname 324
Changing network passphrase 324
Regenerating self-signed certificates 324
Changing DNS IP and FQDN 324
Chapter 12: Configuring Avaya Session Border Controller for Enterprise for Avaya Aura® Remote Worker 325
Remote worker overview 325
Limitation for registering Remote Workers 326
Session Manager configuration for Avaya SBCE 327
Remote worker configuration checklist 329
Cloning Avaya-ru profile 330
Creating an Avaya call server profile 330

Creating an external signaling interface for a phone network..... 332
Creating an internal signaling interface for an Avaya call server..... 333
Creating an external media interface for a phone network..... 334
Creating an internal media interface for an Avaya call server..... 334
Creating PPM Mapping Profile for Session Manager..... 335
PPM Mapping Profile field descriptions..... 336
Adding a reverse proxy policy..... 336
Add reverse proxy policy field descriptions..... 337
Creating a reverse proxy service for PPM traffic..... 338
Creating a reverse proxy service for file or firmware download..... 339
Relay Services field descriptions..... 341
Creating a media rule..... 344
Creating application rules..... 344
Creating an endpoint policy group..... 345
Creating a routing profile towards Avaya Aura® call server..... 346
Creating a server flow..... 347
Creating a subscriber flow..... 348
Configuring application relay for IM..... 349
Checklist for configuring Presence server..... 350
Creating PPM mapping profile for presence server..... 350
Monitoring RTCP for a single Session Manager deployment..... 351
Application relay settings for RTCP monitoring using single Session Manager..... 352
Configuring Avaya SBCE to support emergency calls from unregistered endpoints..... 352
Checklist for back-to-back configuration with a single Session Manager..... 354
Checklist for back-to-back-to-back configuration with a single Session Manager..... 355
Monitoring RTCP for back-to-back-to-back deployment..... 356
Application relay settings for monitoring RTCP using back-to-back-to-back deployment..... 357
Chapter 13: Multiple Session Manager support for Avaya SBCE in Remote Worker deployment..... 358
Multiple Session Manager configuration checklist..... 359
Configuring the Avaya SBCE internal and external IP addresses corresponding to the primary and secondary Session Managers..... 361
Creating a server interworking profile..... 361
Configuring application relay settings for multiple Session Manager..... 362
Multiple Session Manager support with back-to-back Avaya SBCEs..... 362
Back-to-back configuration checklist..... 363
Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBCEs..... 364
Back-to-back-to-back configuration checklist..... 365
Multiple Avaya SBCE deployment 366
Multiple Avaya SBCE deployment in the non-HA mode..... 366
Multiple Avaya SBCE deployment in the HA mode..... 367
Multiple Avaya SBCE deployment checklist..... 368
Chapter 14: Configuration of Server flows for SIP Trunking..... 371

SIP Trunking overview 371
Generic Avaya SBCE SIP trunk configuration checklist 372
Creating Routing Profile for Call Server 373
Creating a Topology Hiding profile 374
Creating Interworking Profiles 375
Creating Server Profile for Call Server 375
Creating Server Profile for Trunk-side server 377
Creating external signaling interface toward Trunk-side server 378
Creating Internal Signaling Interface toward Call Server 379
Creating External Media Interface toward Trunk Server 380
Creating Internal Media Interface toward call server 380
Creating call server flow 381
Creating trunk server flow 381
Configuring Avaya SBCE for SIP Trunk 382
Configuring Avaya SBCE for other trunks 383
Chapter 15: Signaling Manipulation 384
Signaling manipulation 384
SigMa scripting language 384
SigMa primer 385
SigMa Scripting examples 392
SigMa Scripting Tutorial 395
Signaling Manipulation Scripts field descriptions 401
Sigma Design Overview 402
Specifying a SigMa script in a server configuration 402
Chapter 16: Remote access 404
Chapter 17: Video devices interoperability configuration 405
Binary Floor Control Protocol 405
Administering Binary Floor Control Protocol 405
SRTP overview 406
Considerations for SRTP after failover 406
Forward Error Correction 406
Far End Camera Control 407
Administering Far End Camera Control 407
Chapter 18: WebRTC-enabled call processing 408
WebRTC-enabled call handling 408
WebRTC considerations 408
Turntop 408
Configuring TURN/STUN relay service for WebRTC calls in Avaya SBCE 409
Chapter 19: Avaya SBCE configuration for SIPREC integration 413
Checklist for configuring Avaya SBCE for SIPREC 413
Configuring a Recording Server 415
Enabling UCID for the signaling rules used on the Session Manager endpoint policy group 416
Creating a media rule for the Recording Server 417

Creating a new session policy for the Recording Server 417
Adding a custom wave file for the recording tone 418
Adding a session flow for the Recording Server 419
Chapter 20: Secure Client Enablement Services proxy configuration 421
Client Enablement Services CA certificate 421
Extracting the Client Enablement Services CA certificate 421
Creating a client TLS profile 422
Configuring CES proxy 423
Chapter 21: Avaya SBCE configuration for Call Preservation 425
Checklist for configuring Avaya SBCE for Call preservation 425
Creating FGDN groups 426
FGDN Group field descriptions 426
Enabling FGDN for a Session Manager in the FGDN group 427
Creating a routing rule for Call preservation 427
Adding the routing rule to the trunk server flow 428
Changing transaction expiry time in Server Interworking 428
Chapter 22: Avaya SBCE configuration for transcoding 430
Checklist for configuring Avaya SBCE for transcoding 430
Enabling the transcoding feature 430
Administering codec prioritization 431
Configuring endpoint policy group 431
Configuring a server flow for transcoding 432
Chapter 23: Resources 433
Documentation 433
Finding documents on the Avaya Support website 433
Training 434
Viewing Avaya Mentor videos 434
Support 435
Using the Avaya InSite Knowledge Base 435
Appendix A: Solution for simultaneous downloads of config and firmware files 437
Simultaneous downloads of config/firmware files 437
GROUP identifier in endpoint administration 437
File server configuration example 438
Phone configuration 439
Configuring Avaya SBCE 439
Appendix B: Configuring Avaya SBCE for interoperability with Avaya Multimedia Messaging 441
Glossary 442

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	Changes
1	June 2016	Initial release
2	February 2017	Updates for Avaya SBCE 7.1 Service Pack 1: • Added configuration steps for reverse proxy policy. • Updated Avaya SBCE user roles.
3	May 2017	Added steps for adding the internal IP of Avaya SBCE in System Manager for remote worker configuration.
4	September 2017	Added note in topology hiding profiles field descriptions topic

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 has two hardware platform versions: the standard platform and the Portwell platform. The standard platform provides identical capabilities to those available in the Portwell platform. In addition, the standard platform provides High-Availability (HA) support for both media and signaling, and Media Forking. HA and Media Forking are available only in the standard platform.

Based on product licensing, Avaya SBCE has the following licensed versions:

- Advanced Services (Advanced Licensing): All services including Remote Worker and SIP Trunking.
- Basic Services (Standard Licensing): SIP Trunking only.

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 38.0/ 38.0 ESR or later
- Microsoft Internet Explorer 9.0 or later

- Microsoft Edge 13.0 or later
- Google Chrome 47.0 and later
- Apple Safari (4) 7.0 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.

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

EMS screen elements

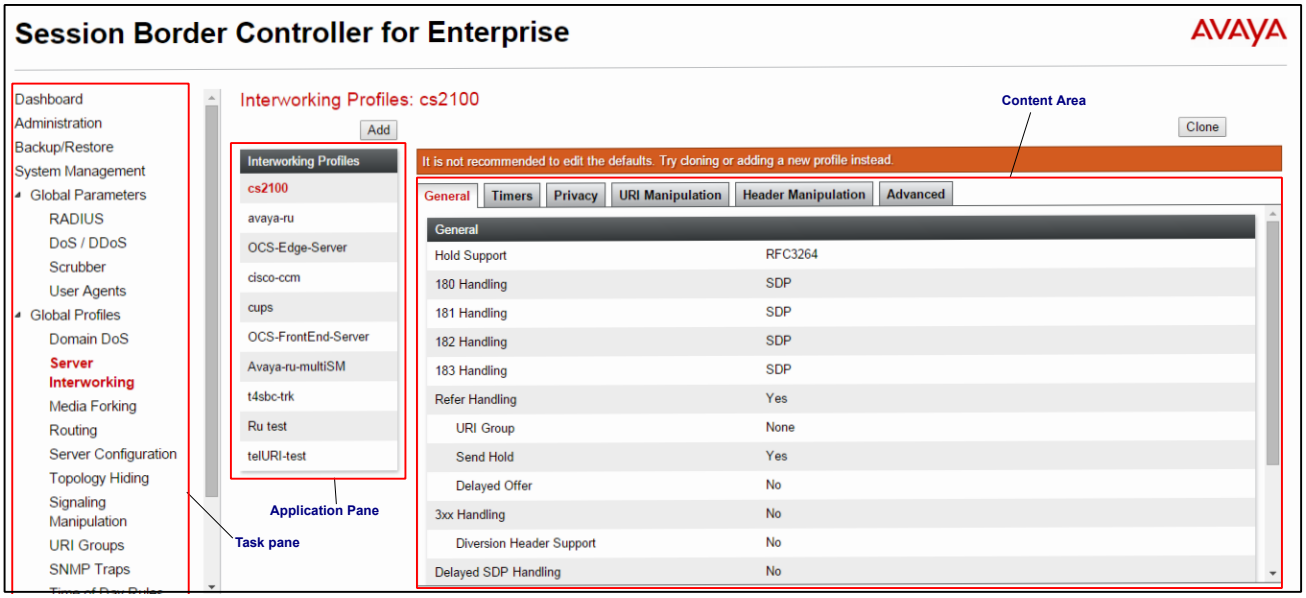
Use the EMS web interface for the administration and configuration of the Avaya SBCE security system.

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



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.

Display settings field descriptions

Name	Description
Menu Style	Selects the display style for the navigation menu. The options are: • Tree

Table continues…

Name	Description
	• Dropdown
Signaling Manipulation Syntax Highlighting	Specifies whether the system highlights the Signaling Manipulation syntax.

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.

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.
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.

Table continues…

Name	Description
	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.

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**
- **Administration Parameters**
- **ASG Configuration**

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.

System Management

Use this screen to view, install, configure, shut down, or restart the Avaya SBCE security devices. You can also restart the EMS from the System Management screen.

This screen displays the **Devices**, **Updates**, **SSL VPN**, and **Licensing** tabs.

Global parameters

Global parameters field descriptions

Name	Description
RADIUS	Displays the **Radius** screen. Use this screen to configure the following RADIUS server parameters: • **Name** • **Primary Address** • **Secondary Address** • **Retry Timeout** • **Max Retry** • **Protocol** • **Server Mode** • **Authentication Protocol** • **Ignore Session Expire** • **Accounting Server**
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.

Global profiles

Global 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.
Routing	Displays the Routing Profile screen. Using this screen, you can manage the parameters related to routing SIP signaling messages to configured routing profiles.
Server Configuration	Displays the Server Configuration screen. This screen contains the following tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. By using these tabs, you can

Table continues…

Name	Description
	configure and manage various SIP call server-specific parameters, such as TCP and UDP port assignments, and heartbeat signaling parameters for configured servers. **Note:** DoS White List and DoS Protection are activated only after selecting the **Enable DoS Protection** check box under the **Advanced** tab.
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.
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

Table continues…

Name	Description
	• 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.

PPM Services

Use this screen to create mapping profiles for each group of remote users. This screen contains the **Mapping Profile** tab.

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 which activate the security features of the Avaya SBCE security device to aggregate, monitor, control, and normalize call flows.

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 per 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 the 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 using the corresponding buttons in the application pane and content area. For a media rule, the system displays parameters related to Media Encryption, Codec Prioritization, Media Silencing, Media BFCP, Media FECC, ANAT, and transcoding.

Table continues…

Name	Description
Security rules	Displays a list of security rules in the application pane. You can add, view, edit, clone, or delete media rules using the corresponding buttons in the application pane and content area. For a security rule, the system displays the following options: **Compliance**, **Scrubber**, and **Domain DoS**. To view or change these values, select the tab corresponding to the parameter.
Signaling rules	Displays a list of signaling rules in the application pane. You can add, view, edit, clone, or delete signaling rules using the corresponding buttons in the application pane and content area. For a signaling rule, the system displays the following options: **General**, **Requests**, **Responses**, **Request Headers**, **Response Headers**, **Signaling QoS**, and **UCID**. To view or change these values, select the tab corresponding to the parameter.
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 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 as identified by the following rules: **Application**, **Border**, **Media**, **Security**, and **Signaling**.
Session Policies	Displays the **Media** tab. Use this tab to control how Avaya SBCE processes the media streams. Session Policies can be added, viewed, edited, cloned, or deleted 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.

Device specific settings

With the Device Specific Settings feature, 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.

Device Specific Settings 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).
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.
DMZ Services	
Relay Services	Enables Web conferencing for Mobile Workspace Users. Displays **Application Relay** , and **Reverse Proxy** tabs. **Application Relay** enables PSOM NAT traversal.

Table continues…

Name	Description
Firewall	Contains **Blacklist**, **Whitelist**, **Services**, and **Source Rate Limiting** tabs. • Blacklist: Provides options to prevent receiving packets from an external source IP or network. Entries included in the Blacklist take priority over entries in the Whitelist. Therefore, ensure that entries to be Whitelisted must not be added to the Blacklist. • Whitelist: Provides options for allowing all packets from an external source IP • Service Feature: Provides an option to allow or block PING for an Avaya 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. On this page, you can configure the following parameters for a TURN/STUN server to facilitate NAT traversal: • Listen Port: Use Port 3478. • Media Relay Port Range: Enter port range used for SRTP and STUN packets exchanged between the browser and Avaya Media Server. This range must not overlap port ranges used by the Avaya SBCE for other protocols such as SIP. • Alternate Server 1: Alternate turn server address to which load on the Avaya SBCE is redirected after the load factor threshold is exceeded. The load factor on a Turn server address is configured with a load factor threshold. When the load factor threshold is exceeded, the load is redirected to an alternate Turn server address on the same Avaya SBCE or a different Avaya SBCE, when the Turn server addresses on the same Avaya SBCE reaches the load factor threshold. • Authentication: If you select **Authentication**, enter the Avaya Media Server Username and Password. Then enter the Realm used in TURN authentication. Often, the Realm matches the SIP domain used in the Avaya Aura® system. • Fingerprint: Enable Fingerprint. • UDP and UDP Relay are enabled by default. Currently, TLS and DTLS are not supported and are unavailable by default.
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 v1/v2**: User profile for SNMP v1/v2. For new installations of Avaya SBCE 7.1, SNMP v1/v2 configuration is unavailable. From Release 7.1, vulnerable SNMP v1/v2 profile configuration has been removed to improve security. For Avaya SBCE instances that upgrade from an older release, options to configure SNMP v1/v2 profiles are still available. • **SNMP v3**: User profile for SNMP v3 users. • **Management Servers**: IP addresses of the servers managing SNMP traps

Table continues…

Name	Description
	• **Trap Severity Settings**: Options to enable or disable traps for a device by severity. Traps can have one of the following severities: Critical, Minor, Major, and Informational.
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.
Advanced Options	Contains **CDR Listing**, **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.
Troubleshooting	Troubleshooting is a subfolder function in **Device Specific Settings**.

Troubleshooting

The Troubleshooting Feature provides options that are useful for troubleshooting problems.

Troubleshooting field descriptions

Name	Description
Debugging	Displays the debugging screen for EMS and devices. This screen contains **Subsystem Logs**, **GUI Logs**, and **Third-Party Logs** tabs. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller 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.
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: **Global Profiles** > **Server Configuration** > **Advanced** > .

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.

Table continues…

Name	Description
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.
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.

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 fulfill the following norms:

- 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

- At the first start up of the Avaya SBCE, the user gets immediate access to the Avaya SBCE system from the console.
- When the user configures the console, the user must provide the root and ipcs account passwords.

- The root and ipcs passwords are determined and set during product installation.
- All the above policy statements apply to the EMS system as well.
- The EMS GUI has a separate password.
- The EMS GUI default password is *ucsec* for the account *ucsec*.

  When you log in for the first time, the system prompts you to create a new password.

Note:

The Console Admin login ID and password are determined by the customer network administrator during the installation procedure. Two installation steps prompt the installer to enter a chosen login and password.

The EMS GUI Admin login ID and password are assigned by Avaya when the Avaya SBCE security is initially configured prior to shipment.

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 **Administration**.
3. On the Administration page, in the Users tab, click **Add User**.
   a. In the Add User window, enter information in the appropriate fields.

      The default value in the **Permissions** field is **Admin**. You can change this value to add users with different permissions.

   b. Click **Finish**.

      In the Users tab, the system displays a new administrative account.

Related links

Add user field descriptions on page 35

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 valid user types 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. This option cannot be selected manually.
Password	The login password being assigned to this account. Only activated if the **RADIUS User** check box is unchecked.
Confirm Password	A reliability feature to ensure that the correct password has been entered in the previous field. Only activated if the **RADIUS User** check box is cleared.
Permission	The level of administrative access to be granted to this account. • Admin: Highest level of system access having full read/write permissions for all screens and features. Can create and delete new user accounts.

Table continues…

Name	Description
	• Manager: Read/write access for all screens and functions, with the exception of being unable to create new user accounts. • Supervisor: Only read access to certain incidence and statistical logs.
Status	The options are Normal, Disabled, and Locked. You cannot change the status of the user to Locked. The system displays the status for a user as Locked only when the user has been locked out after unsuccessful login attempts. **Note:** Disabling a user account or changing the permissions of a user account will disconnect all clients connected to that user account.

Editing an administrative account

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Administration**.
3. On the Administration page, in the **Users** tab, click **Edit** for a user account.
   a. In the Edit User window, edit information for the appropriate fields.
   b. Click **Finish**.

Related links

Add user field descriptions on page 35

Deleting an administrative account

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Administration**.
3. On the **Users** tab, click **Delete** corresponding to the admin user account you want to delete.

   The system displays a confirmation window.
4. 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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Administration**.
3. On the Administration page, click the **Administration Parameters** tab.
4. On the **Administration Parameters** tab, perform the following:
   a. Enter the information in the appropriate fields.
   b. Click **Save**.

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

Related links

Administration field descriptions on page 37

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.
Type	The valid user types 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.

Table continues…

Name	Description
	• ASG: A user authenticated through ASG. This option cannot be selected manually.
Role	The level of administrative access available for this account. • Admin: Highest level of system access having full read/write permissions for all screens and features. Can create and delete new user accounts. • Manager: Read/write access for all screens and functions, with the exception of being unable to create new user accounts. • Supervisor: Only read access to certain incidence and statistical logs.
Administration Parameters tab	
Local Account Password Expiration (days)	A check box indicating whether or not the password assigned to this user account will expire after the number of days indicated in the corresponding field. If selected, the assigned password will expire after the indicated number of days. If cleared, the password assigned to this user account can be used indefinitely.
Local Account Password Expiration Notification (days)	A check box indicating whether the system should display a notification to the user at the time of log in 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.
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.
Failed Attempts Before Lockout	A check box indicating whether or not the user account is locked out after the number of login attempts indicated in the corresponding field.
Lockout Threshold	A check box 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.

Table continues…

Name	Description
	After the lockout duration passes, the next user attempt to log in to a locked account resets the account state to normal.
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.
Reject Previously Used Passwords	The number of previously used passwords that cannot be used.
ASG Configuration tab	
Device	The device on which the action is performed.
Action	The actions that can be performed: Installed, Force Installed, Enabled, Disabled, Uninstalled.
Status	The status of the action: Successful or Unsuccessful.
Timestamp	The time when the last action was performed.
Reason for failure	The failure messages if the action failed.
ASG Configuration button descriptions	
Upload	Upload an ASG authentication file.
Delete	Delete the current ASG authentication file. Use this button to remove all GUI users created by that ASG, disable all ASG users from logging in via SSH, and remove the authentication file from the system.
Enable	Displayed if ASG is currently disabled.
Disable	Displayed when ASG is currently enabled.
Synchronize	If ASG is enabled on EMS, then ASG will be enabled on the SBCs. Conversely, if ASG is disabled on EMS then ASG will be disabled on all Avaya SBCE ars. **Note:** Use this setting only in multiple Avaya SBCE server deployments.

Avaya Access Secure Gateway

The Avaya Access Secure Gateway (ASG) system is a key element in protecting passwords and preventing unauthorized use of maintenance and administration login. On Avaya Enterprise Communications System (ECS) products, Avaya services personnel use all passwords for a single access attempt only. After each login, a new password must be used. ASG 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.

Installing an ASG authentication file

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Administration**.
3. On the Administration page, click **ASG Configuration**.
4. To install an ASG authentication file, click **Upload**.

   The system displays the Install ASG Authentication File page.
5. In the **Authentication File** field, click **Browse** and select an authentication file from your local system.
6. To overwrite the authentication file, select the **Force Overwrite** check box.
7. Click **Load Authentication File**.

Chapter 4: Device Configuration

Prerequisites

To ensure successful operation of this semi-automated feature, you must first ensure that the Avaya SBCE security device 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **System Management**.
3. On the System 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.
6. **(Optional)** To support high availability, enter relevant details in the **Host Name for second Node**, **Management IP for second Node**, and **Signaling HA** fields.
7. Click **Finish**.

   On the System Management page, the system displays a device list with the status of the newly added device as **Registered**.

Related links

System Management field descriptions on page 42

System 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. • Install: For decommissioned devices. • Commissioned: For devices that have been 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.

SSL VPN tab

Name	Description
Status	The current status of the VPN.
Tunnel details	Information about the VPN tunnel.
Enable	An option to enable the SSL VPN.
Account Name	The name of the account.
Account Password	The password for the account. You can leave this field blank to keep the existing password.
Confirm Password	The password repeated for confirmation.
Server Address	The address of the server.
Server Port	The port for the server.
Server Transport	The transport protocol.
Connect IP	The IP address used for the VPN.
Heartbeat Interval	The interval in seconds after which a synchronization signal (heartbeat) is sent from Avaya SBCE to the VPN server.
Retries	The number of retries for sending the heartbeat.
Reconnect Interval	The number of seconds after which an attempt to reconnect must be made.

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

Add Device screen

Name	Description
Host Name	The name of the device that you want to add.
Management IP	The management IP address of the device.
High Availability	An option to indicate that the device is part of a High Availability (HA) pair.
Host Name for second Node	The name of the device that the device must switch to during failure.
Management IP for second Node	The management IP address of the failover device.
Signaling HA	An option to indicate whether HA is required for signaling. When you select this option, the system maintains a copy of the signaling information on the standby device so that all signaling states can be restored upon switchover.

Related links

Adding an Avaya SBCE device on page 41

Commissioning an Avaya SBCE device

Before you begin

Install a license file.

About this task

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

Note:

The Avaya SBCE security devices that are physically installed onto the network and available for commissioning are identified 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**. Each commissioned device has only the **View** option available.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **System Management**.
3. On the System 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 System Management page, the system displays a device list with the status of the newly added device as **Registered**.
6. On the same System Management page, click **Install**.
7. In the Installation Wizard window, complete the required fields.

   For information about Installation Wizard field descriptions, see Installation Wizard field descriptions.
8. Click **Finish**.

   On the System Management page, the system 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 system displays the Installation Wizard.
10. Provide an appliance name for the Avaya SBCE security device being commissioned and complete the deployment settings, such as high availability.
11. Click **Finish**.

    The system 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 of the configuration areas by using those links or access the configuration areas by using 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*.
Signaling HA	A sub-field that is displayed under High Availability (HA) when HA is enabled. The Signaling HA feature maintains a copy of the signaling information on the standby device so that all signaling states can be restored upon switchover.
DNS Configuration	
Primary	The IP address of the primary DNS server.
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.
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	

Table continues…

Name	Description
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.

Changing the management IP from the EMS web interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **System Management**.
3. Find the device whose IP address you want to change, and click **Edit**.

   For an Avaya SBCE, the system displays the following warning:

   ```
   Any changes to the management network on this device will reboot
   the device.
   ```

   For an EMS, the system displays the following warning:

   ```
   Any changes to the management network on this device will reboot
   the device, drop any active calls, and require each connected SBC
   to be manually restarted using Application Restart in System
   Management.
   ```

4. In the **Management IP** field, type the new management IP, and click **Finish**.

   Ensure that you include appropriate netmask and gateway details for the new IP. When you change any information in the **Network Settings** section, the device restarts to complete the change. If you change the management IP of the EMS, the EMS web interface displays a new URL. After the system restarts, you must use the new URL to go to the EMS.

   Note:

   From Release 6.3, you can change the management IP through the CLI. For more information about changing the management IP through the CLI, see the Changing Management IP section in the Avaya SBCE CLI commands chapter.

5. **(Optional)** Find the Avaya SBCE device on the System Management page, and click **Restart Application**.

Note:

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 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.

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.

Failover scenarios

Keep alive or heartbeat failure: The secondary Avaya SBCE sends a keep alive request or heartbeat every 500ms 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 not available, 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 detects that the secondary has more active links than the primary, 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 no links are available.

From Release 6.3, 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.

Configuring High Availability

Before you begin

You must obtain 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.

About this task

Use the System Management page to configure the Standard High Availability (HA) configuration. The devices can be co-located or geographically dispersed.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **System Management**.
3. On the System 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.

   Note:

   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 to announce that the secondary Avaya SBCE is now receiving requests. The GARP 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 one way audio. The 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.
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. Select the **Signaling HA** check box.

   High-Availability (HA) 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.

10. Click **Finish**.

    From Release 7.0, Avaya SBCE provides 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.

    From Release 7.1, Avaya SBCE supports an EMS HA active/active configuration. If the EMS hardware fails, the system will not be out of service. The system can switch to the other EMS in the HA pair without manual intervention.

Related links

Adding an Avaya SBCE device on page 41

HA Node Status States

When creating a new Security Rule, refer to this table for information on the Domain DoS selections in the sixth Security Rule pop-up window.

HA Node Status States

Status	Description
Primary	Avaya SBCE is active and handling call traffic.
Secondary	Avaya SBCE is inactive and in stand-by mode.
Down	Avaya SBCE has been detected as offline by the Primary SBC. This status might indicate 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 its initialization procedure.
HAElection	Avaya SBCE is determining whether or not to go into active or standby mode.
Synchronizing	Avaya SBCE is replicating data from the other SBC.
Unconfigured	Avaya SBCE has been configured as an HA device but has not yet received the configuration from EMS.
Unknown	EMS does not recognize the HA status Avaya SBCE is reporting.

Upgrade of the EMS software

The Element Management System (EMS) or GUI interface can be upgraded when necessary by using the System Management feature from the Task Pane. For more information about the EMS software upgrade procedures, see *Upgrading Avaya Session Border Controller for Enterprise*.

Obtaining a license file from Avaya PLDS

Before you begin

Obtain the following:

- Organization name. This name can be obtained from the sales order.
- Device hostname. If you choose to not use the default name, the hostname is assigned when you first install the device.

About this task

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

Procedure

1. Start a secure shell (SSH) connection with the standalone device (combined SBCE/EMS) or with the separate EMS device, if applicable.

   The system displays the dollar sign ($) prompt.

2. At the dollar sign ($) prompt, type `sudo su`.

   The system 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 system 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 to display the initial login screen.
2. Type `sudo su` after the dollar sign ($) prompt.

   The system displays the new pound sign (#) prompt.

3. Type `ipcs-options` after the pound sign (#) prompt.

   The system displays the Avaya SBC Runtime Options screen will display.

4. Scroll to View TimeZone.
5. Click **Select**, and press `Enter`.

   The current time zone screen is displayed. If there is no time zone set, the window will state that.

Setting the EMS server time zone

Procedure

1. Start a secure shell (SSH) connection to the Stand-By server to display the initial login screen.
2. Type `sudo su` after the dollar sign ($) prompt.

   The system will display the new pound sign (#) prompt.

3. Type `ipcs-options`.

   The system displays the Avaya SBCE Runtime Options screen.

4. Scroll to **Configure TimeZone**.
5. Click **Select**, and press `Enter`.

   The select time zone screen is displayed.

6. Scroll down and select the correct time zone from the alphabetical list.

   Note:

   Click the **Skip** tab, and press `Enter` to accept the default GMT time zone.

7. Tab down to **Select** and press `Enter`.

   The system saves the new time zone setting.

Next steps

Exit the Avaya SBCE Runtime Options screen.

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

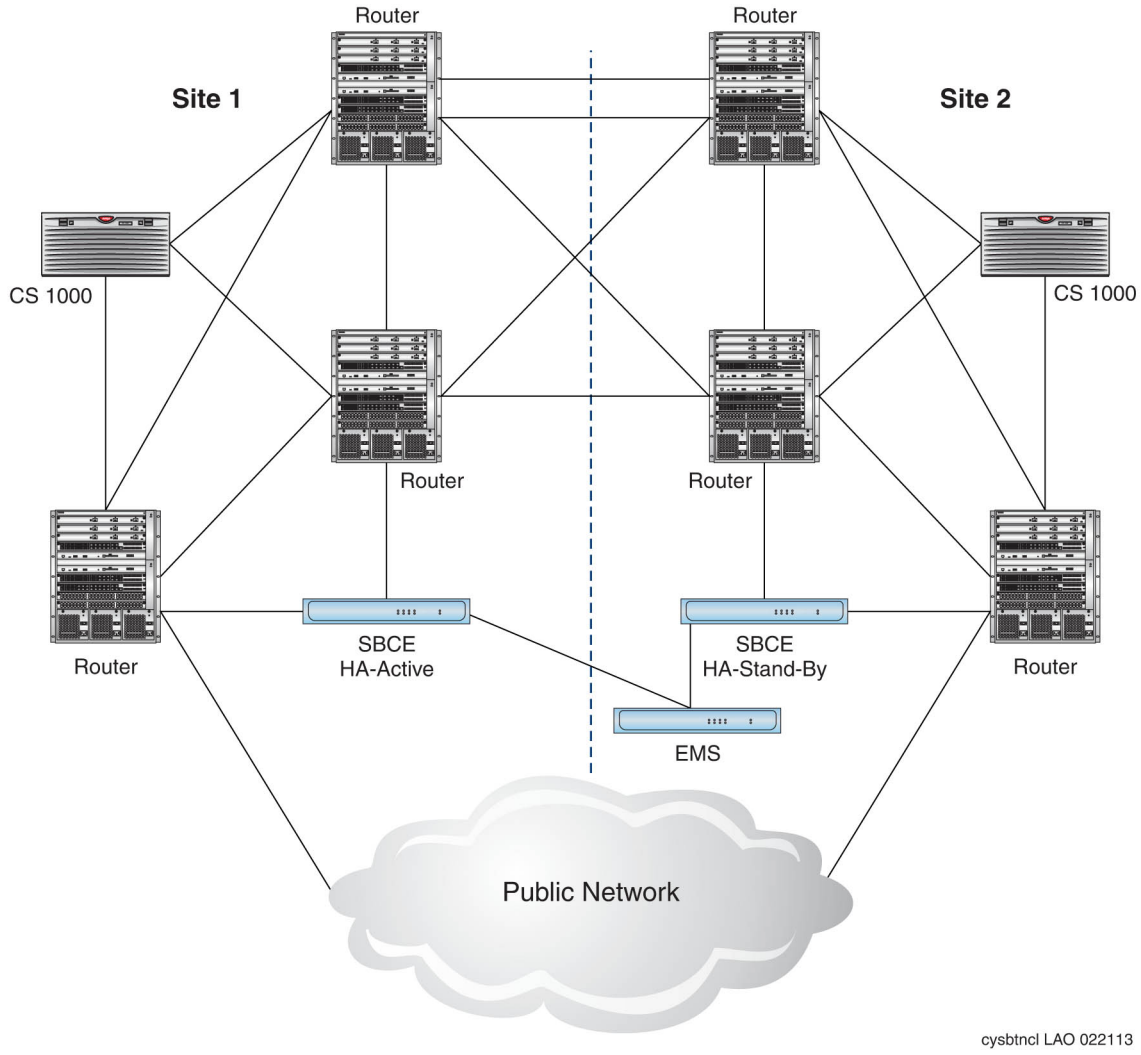
The following sections contain the information necessary to deploy two Avaya SBCE security devices in a High-Availability configuration where they are not geographically co-located.

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

Note:

Most Avaya SBCE device models can be used in the HA implementation illustrated in the following graphic. The Portwell Cad Avaya SBCE cannot be used for high availability deployment.

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 eth1 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.
Avaya SBCE	
M1 interface or management eth5 IP	The Avaya SBCE devices use this IP to: • Communicate with EMS and access the server box through SSH port 222 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.
A1 internal interface towards PBX or eth3 IP	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 or eth1 IP	This IP cannot be on the same subnet as the M1 IP.
M2 connection or eth4 IP	This interface is a layer 2 connection between the two Avaya SBCE devices. This interface does not require an IP.

The maximum delay between the EMS M1 and the Avaya SBCE M1 can be configured. For Avaya SBCE Release 6.2.1Q16, the default maximum delay on the M2 to M2 connection between the Avaya SBCE devices is 500 ms. The default value for the maximum round trip delay is 500 ms for the M1 IPs among all server boxes. You can change this value on the EMS web interface from the **HA pairs** tab on **Device Specific Settings** > **Advanced Options**. You can configure separate maximum delay values for the M2 and M1 interfaces.

Important:

The A1 and B1 IPs 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 that the MAC of the new Primary Avaya SBCE interfaces 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 the Avaya EMS security device.
3. Log on to the EMS web interface.
4. In the left navigation pane, click **System Management**.

   The system displays the System Management page.
5. On the System Management page, click **Edit** corresponding to the Primary HA security device.

   The system displays the Edit Device page.
6. On the Edit Device page, in the **High Availability (HA) Network Settings** section, do the following:
   a. In the **IP** field, type the IP address of the Primary HA Avaya SBCE security device.
   b. In the **Netmask** field, type the netmask of the Primary HA Avaya SBCE security device.
   c. In the **Gateway** field, type the gateway IP address of the Primary HA Avaya SBCE security device.

   The Signaling HA feature maintains a copy of the signaling information on the standby device so that all signaling states can be restored upon switchover.

   Note:

   When the High Availability (HA) check box is selected, an additional check box becomes visible and selectable, the **Signaling HA** check box. When the **Signaling HA** check box is selected, the system displays a warning message that the standby device will be restarted when you select **OK**. Signaling HA 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. Signaling HA will maintain state information for calls on UDP transport only. In an event when a particular call leg uses TCP transport, signaling HA will not be available for that call and Avaya SBCE falls back to Media HA where only audio information is replicated
7. Click **Finish**.
8. Repeat Step 5 through Step 7 for the Secondary HA security device.

Configuring RTCP monitoring

The RTP Control Protocol (RTCP) monitoring feature in Avaya SBCE updates RTCP packets with appropriate End Point IP and Hop Information.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. On the **RTCP Monitoring** tab, select the **RTCP Monitoring** check box to enable the RTCP feature.

RTCP Monitoring field descriptions

Name	Description
RTCP Monitoring	Specifies whether RTCP monitoring is enabled or not.
Node Type	Configures the node type based on the role of the Avaya SBCE device. The options are: Core, DMZ, and 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 prognosis server using core SBCE-1 private IP-B.

46xx settings file configuration for RTCP monitoring

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-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 user deployment are the same as the configuration steps for the core Avaya SBCE.

Do not use relay configuration for conversion between TCP and TLS.

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

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. 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 **RTCP**.
   c. In the **Remote Domain** field, type the domain in use.
   d. In the **Remote IP** field, type the prognosis server IP.
   e. In the **Remote Port** field, type the port number 5005.
   f. In the **Remote Transport** field, click **UDP**.
   g. In the **Published Domain** field, type the domain in use.
   h. In the **Listen IP** field, click the network name, and click the Core SBCE Relay IP or Core SBCE (external/public) Signaling IP-A.

i. In the **Connect IP** field, click the network name, and type the Core SBCE (Internal/ private) signaling IP-A.

j. In the **Listen Transport** field, click **UDP**.

k. Select the **Use Relay Actors** check box, and select **End-To-End-Rewrite**, **Hop-by-Hop Traceroute**, and **Bridging**.

Note:

Use control and click simultaneously to select or clear multiple items.

l. Click **Finish**.

4. In the left navigation pane, click **Device Specific Settings** > **Advanced Options** > **RTCP Monitoring**.
5. On the RTCP Monitoring page, do the following:
   a. In the **RTCP Monitoring** field, select the **Enable** check box.
   b. In the **Node Type** field, click **Core**.
   c. In the **Relay IP** field, click the network name, and click Core SBCE Relay IP address / Core SBCE Private IP-A.
   d. Click **Save**.

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.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. 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 **RTCP**.
   c. In the **Remote Domain** field, type the domain in use.
   d. In the **Remote IP** field, type the DMZ SBCE Relay listen IP.
   e. In the **Remote Port** field, type the port number 5005.
   f. In the **Remote Transport** field, click **UDP**.

g. In the **Published Domain** field, type the domain in use.
h. In the **Listen IP** field, click the Remote Avaya SBCE relay IP.

   This IP must be different from the IP used for SIP signaling and media.

i. In the **Connect IP** field, type the Remote Avaya SBCE internal signaling IP.
j. In the **Listen Transport** field, click **UDP**.
k. Select the **Use Relay Actors** check box, and select **End-To-End-Rewrite**, **Hop-by-Hop Traceroute**, and **Bridging**.

   Note:

   Use control and click simultaneously to select or clear multiple items.

l. Click **Finish**.

4. In the left navigation pane, click **Device Specific Settings** > **Advanced Options** > **RTCP Monitoring**.
5. On the RTCP Monitoring page, do the following:
   a. In the **RTCP Monitoring** field, select the **Enable** check box.
   b. In the **Node Type** field, click **Remote**.
   c. In the **Relay IP** field, click **None**.
   d. Click **Save**.

Changing blacklist rules

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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Firewall**.
3. On the **Blacklist** tab, click **Add**.
4. In the **Name** field, type the name of the blacklist rule.
5. In the **Interface/VLAN** field, select the interface or VLAN on which Avaya SBCE must receive packets from the blacklisted IPs.
6. In the **Source Address** field, type a valid IP4 address that must be blacklisted.
7. In the **Source Port/Sequence** field, type a port number or port sequence.

If you do not specify a value for this field, the system uses a default wildcard (*) character and accepts any value.

8. In the **Protocol** field, select a transport protocol.

   You must select a protocol when you enter a source or destination port.

   If you do not specify a value for this field, the system uses a default wildcard (*) character and accepts any value.

9. In the **Destination Address** field, type a valid IPv4 address that must be blacklisted.

   If you do not specify a value for this field, the system uses a default wilcard (*) character and accepts any value.

10. In the **Destination Port/Sequence** field, type a port number or port sequence.

    If you do not specify a value for this field, the system uses a default wilcard (*) character and accepts any value.

11. Click **Finish**.

    The system 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.

12. **(Optional)** To edit an existing blacklist rule, click **Edit**, and update the blacklist rule.

Related links

Firewall field descriptions on page 60

Firewall field descriptions

Blacklist tab

Name	Description
Name	The name of the blacklist rule.
Interface/VLAN	The interface or VLAN for which the rule is applicable.
Source Address	The IP address from which data must be blocked.
Source Port/Sequence	The port number from which data must be blocked.
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 blocked.
Destination Port/Sequence	The port number to which sending data must be blocked.

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

Changing blacklist rules on page 59

Chapter 5: Domain Policy, Routing, and Message Flow Administration

Governing Unified Communications with Domain Policies

This chapter explains how to create, manage, and assign Domain Policies, also referred 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 have the flexibility to govern Unified Communications through the enforcement of business rules. Different rules can be applied 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 a packet is received by Avaya SBCE, 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 routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained to be 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 are matched 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.

There are two types of endpoint flows:

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

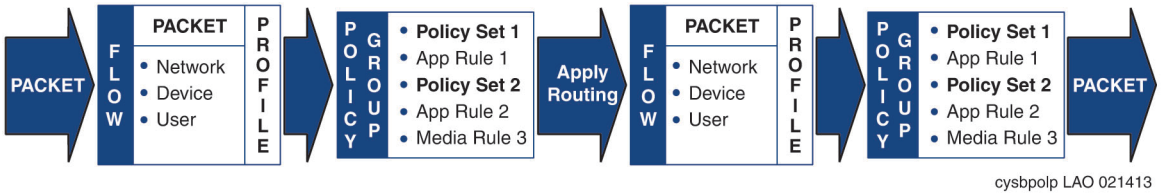
Domain Policies

- 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. 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, and ToD rules.
- Rules: To determine the processing method, privileges, and authentication method of packets.
- Session Policies: Applied based on the source and destination of a media session. For example, which codec is to be applied to the media session between the source and destination.

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

Example



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.

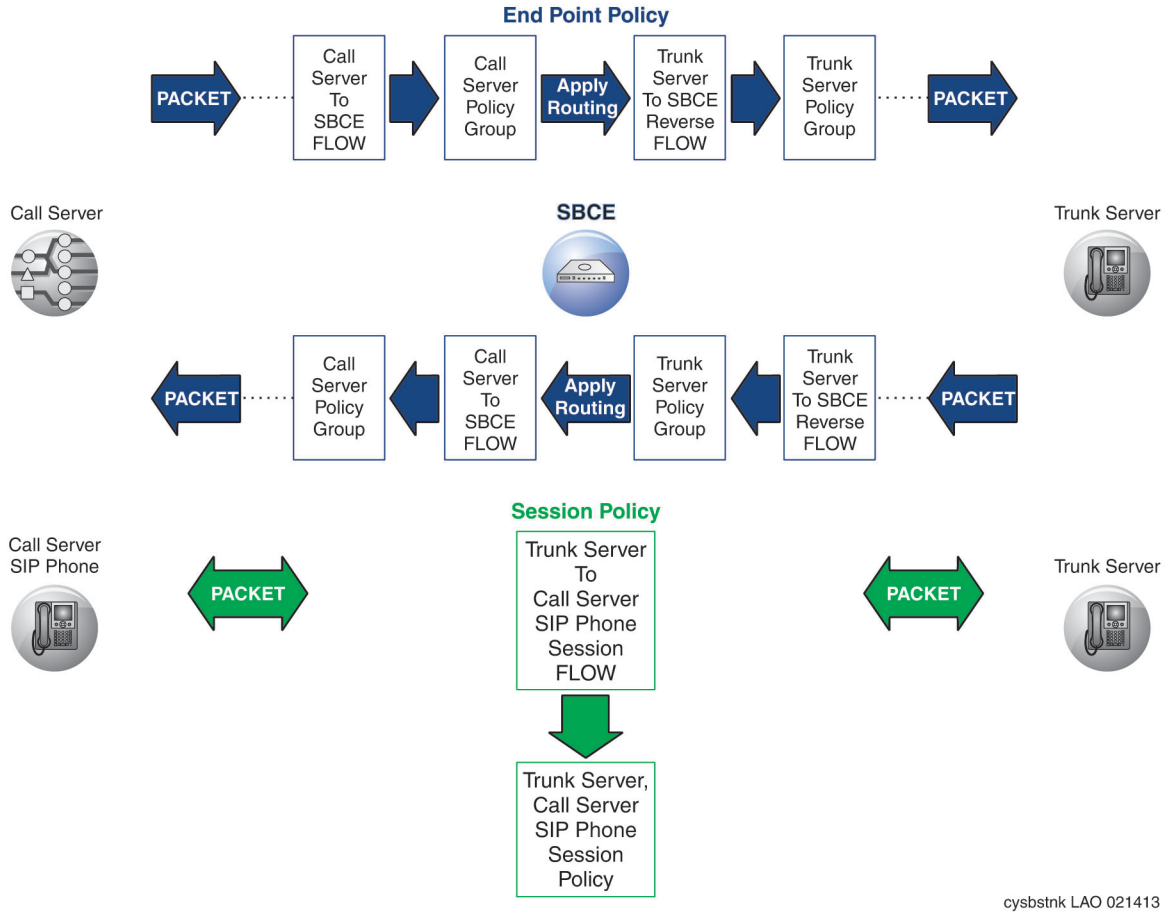
Call coming from Trunk Server

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.

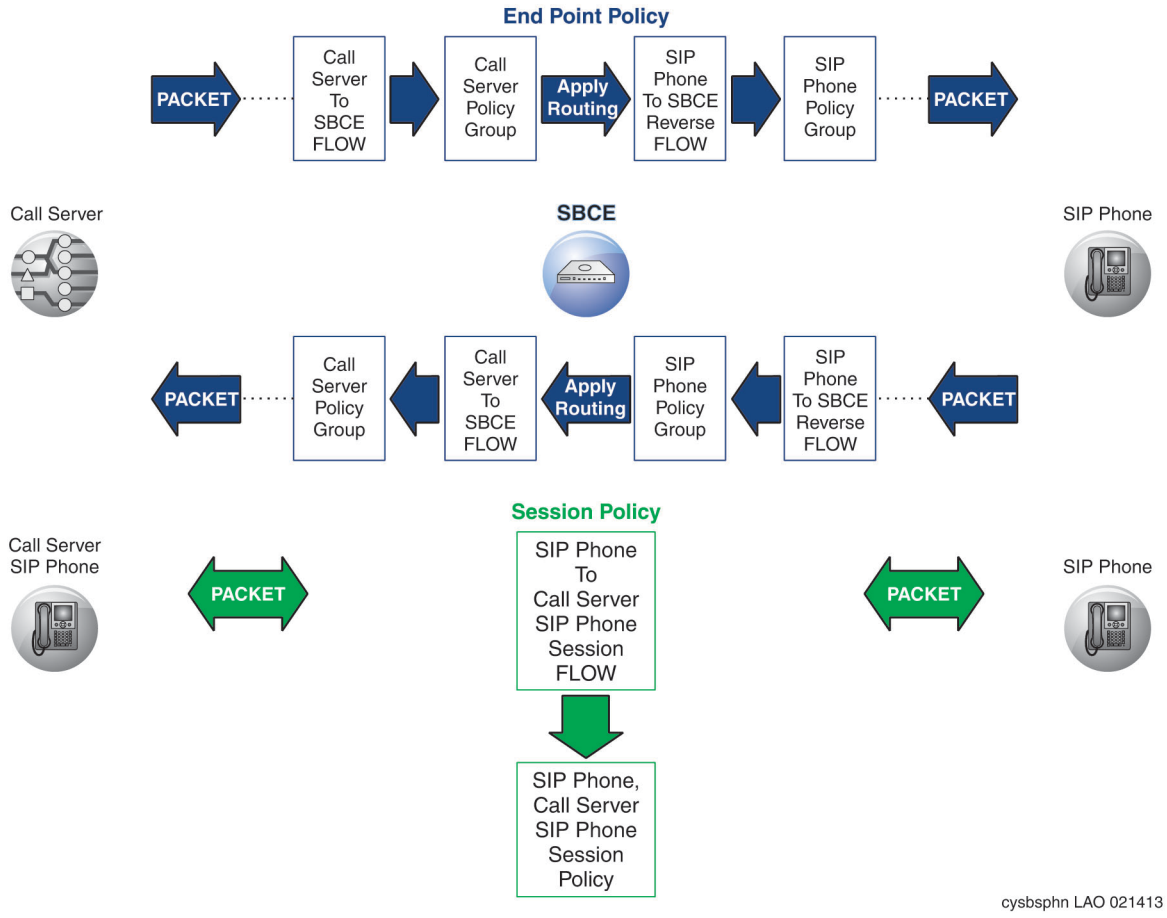
Call coming from SIP Phone

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

This section provides an overview of the process of configuring rules and policies, including descriptions of the Avaya SBCE architecture, the associations of rules and policies, an introduction to rules and profiles, creating policy groups, creating session policies, and points to remember regarding the configuration process.

While configuring rules and policies, consider the following points:

- Rules are grouped in policy sets.
- Policy sets are grouped in endpoint policy groups.
- Endpoint policy groups are assigned to endpoint flows. Subscriber and server.
- Session policies control codec negotiation, media forking, and media anchoring.
- Session policies are assigned to Session Flows, subscriber, and server.

Architecture

The following figure illustrates the Avaya SBCE architecture that 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 this 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:

The standard platform device and the Portwell platform device can be deployed in either architecture.

Example

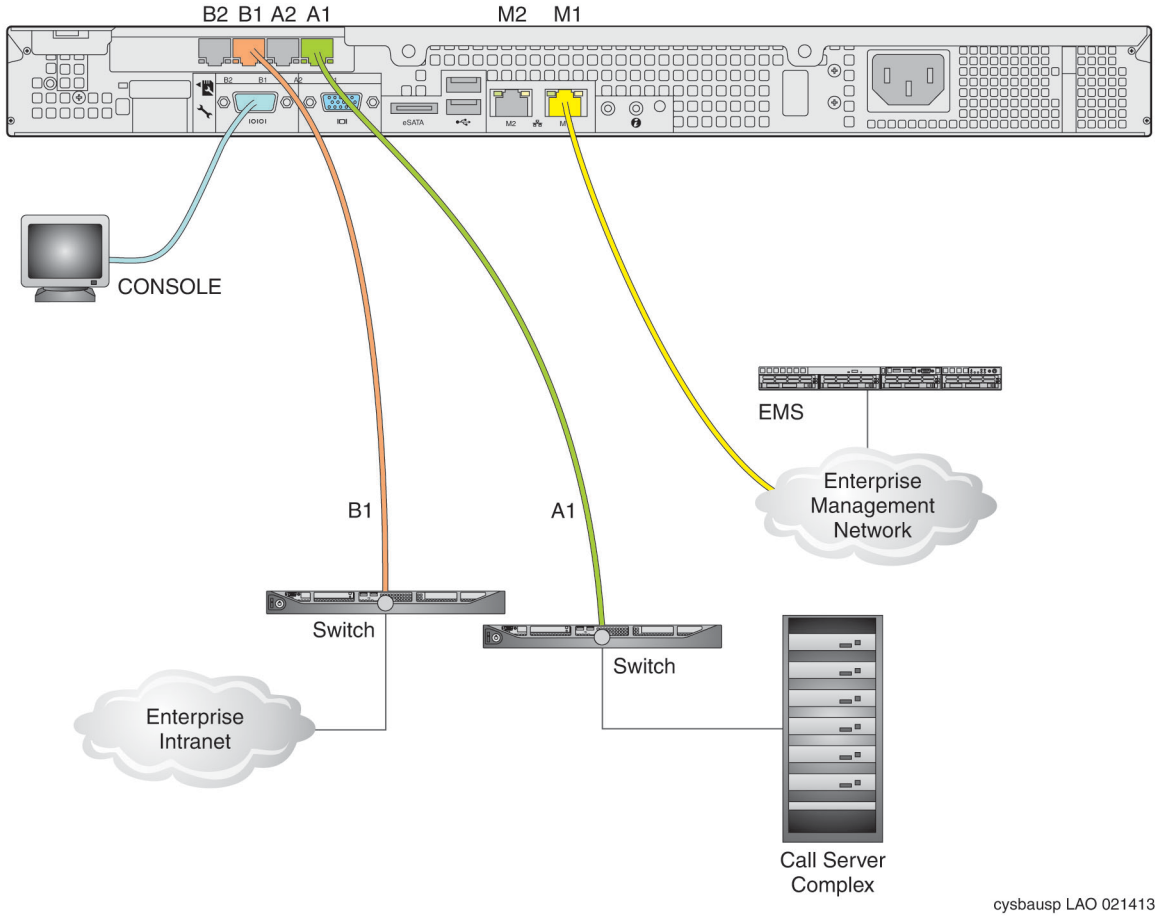


Figure 1: Avaya SBCE architecture using a standard platform

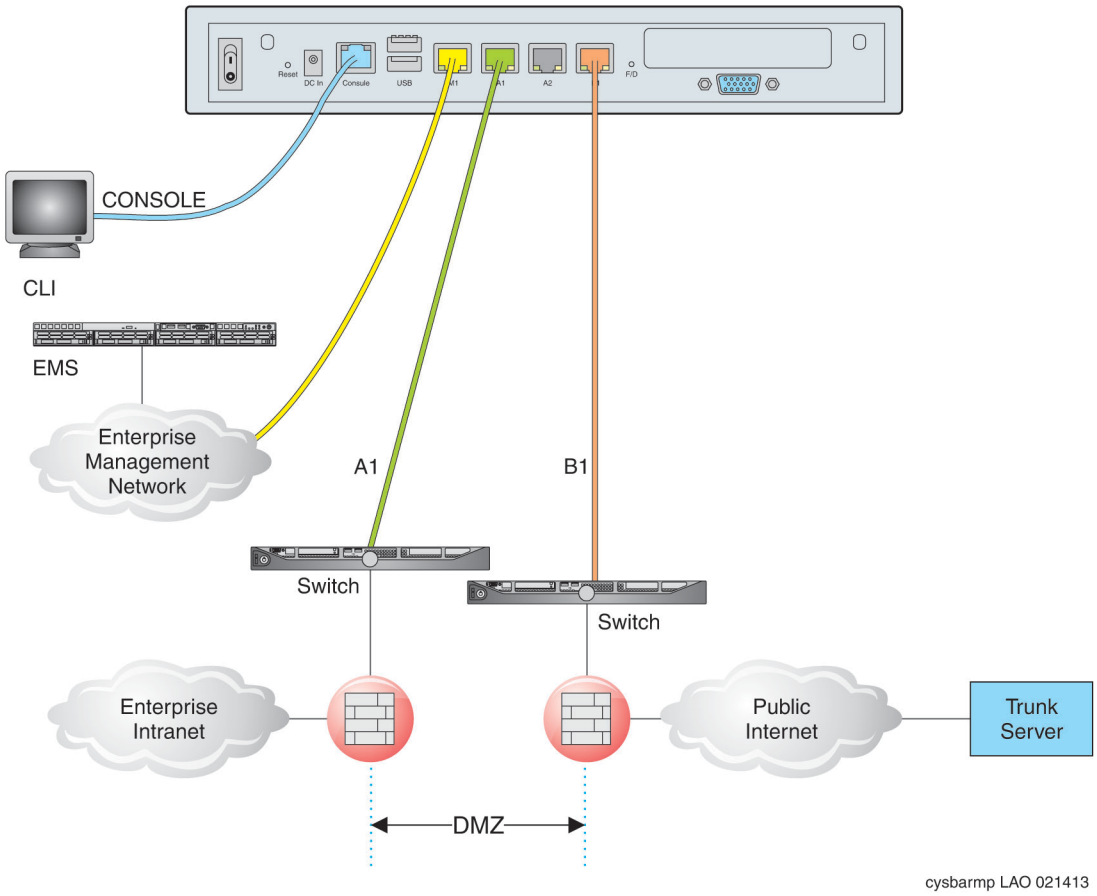


Figure 2: Avaya SBCE architecture using a micro platform

Rule and policy associations

The following image provides the list of rules and policies. For example, application, border, and media rules with domain policies:

Example

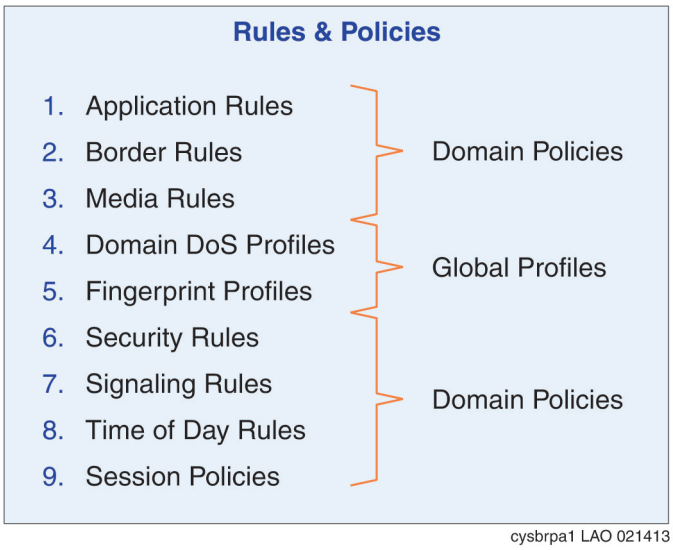


Figure 3: List of rules with the policies

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

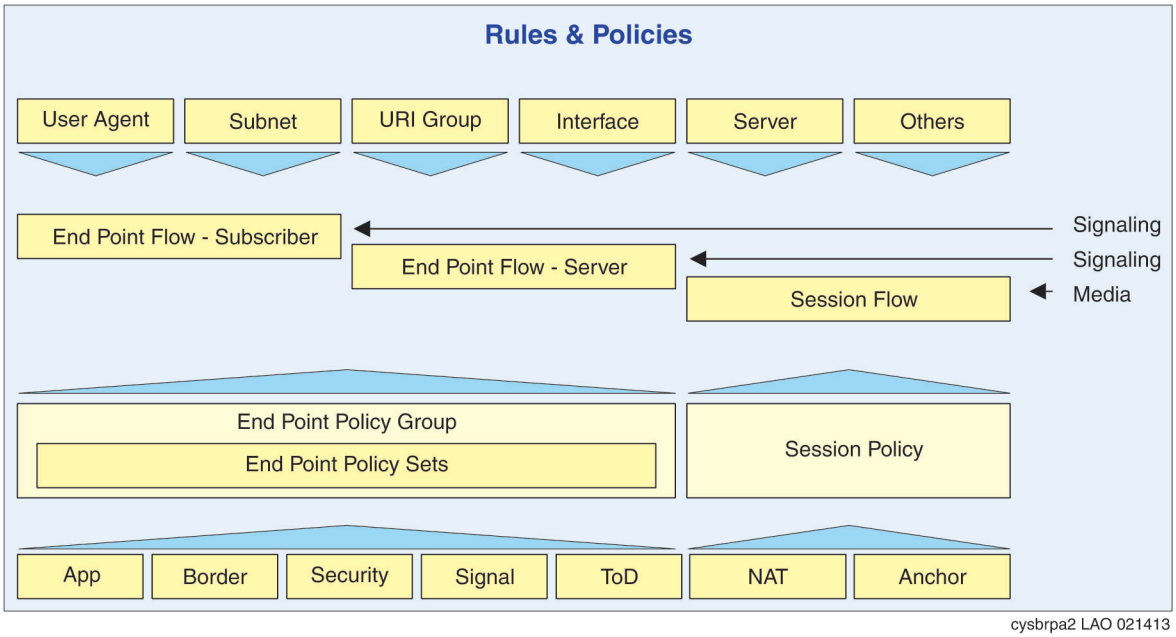


Figure 4: Types of signaling and media flows with the policies and policy groups and sets

The following image depicts the session and subscriber flows with the policies:

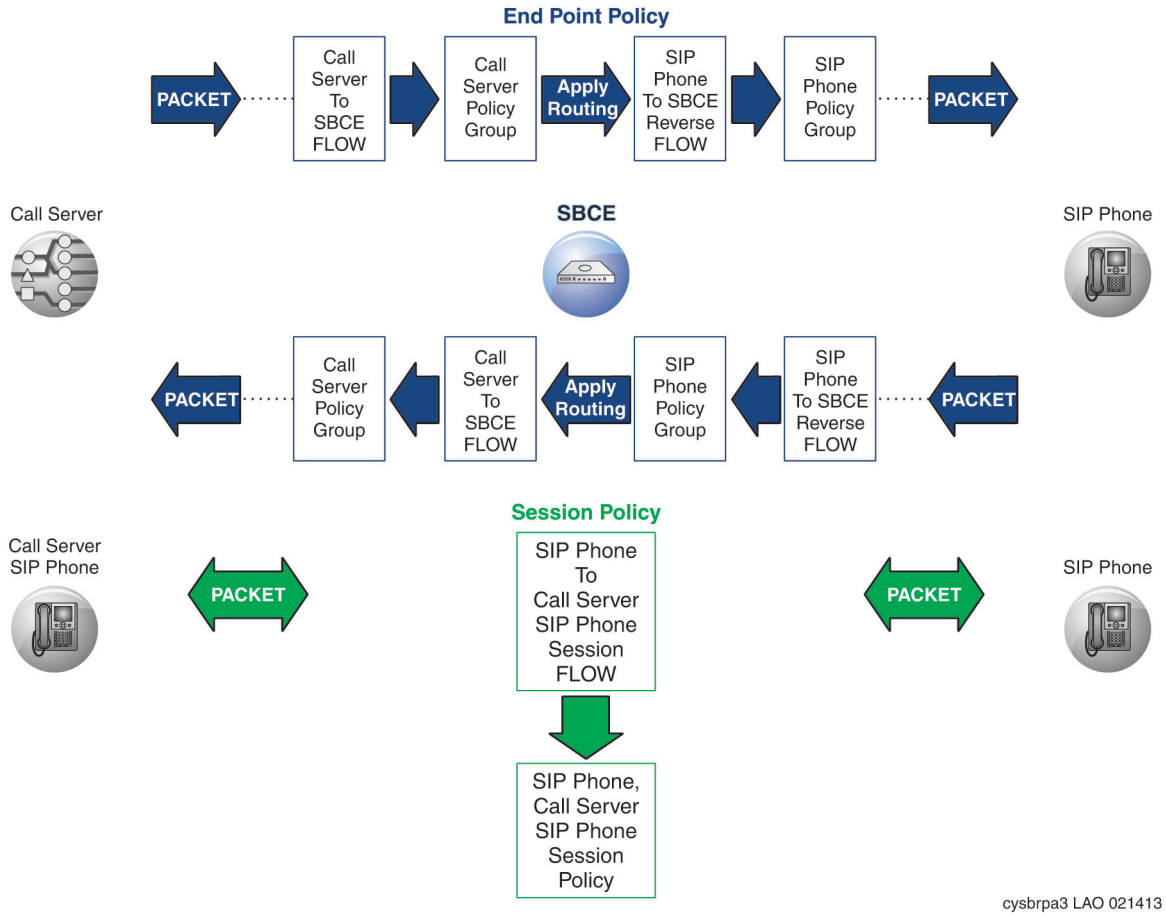


Figure 5: Session and subscriber flows with the policies

Rules and policies checklist

No.	Task	Reference	Notes
1	Configure application rules.	Creating a new application rule on page 88	
2	Configure border rules.	Creating a new border rule on page 91	
3	Define media rules.	Creating a new media rule on page 94	
4	Define domain DoS rules.	Adding a New Domain DoS Profile on page 222	
5	Create security rules.	Creating a new security rule on page 103	
6	Define signaling rules.	Creating a new signaling rule on page 108	Block Option Request Headers

Table continues…

No.	Task	Reference	Notes
			with 403 Forbidden.
7	Set time-of-day rules.	Creating a new ToD rule on page 197	
8	Create a policy group.	Creating a new policy group on page 123	

SIP message processing

SIP messaging involves the following processes:

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

SIP registration processing

An inbound SIP registration from a remote worker can be received on a TCP or TLS socket. The SIP routing system routes the SIP REGISTER requests from the remote worker to the call server.

The SIP routing system tries to find a matching subscriber flow for a new registration. If no subscriber flow match is found, the routing system rejects the new registration with a `SIP 403 Forbidden` error response.

Subscriber flow matching

The routing system uses the **URI Group**, **SIP Signaling Interface**, **Via Host**, **Contact Host**, **User Agent**, and **Source Subnet** fields of the Subscriber Flow configuration as an additional matching criterion to determine a Subscriber 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 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.

The SIP routing system then compares the rest of the fields **Via Host**, **Contact Host**, and the subnet of the source IP address of the SIP request to match the provisioned values of Subscriber Flow.

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.

If a Subscriber Flow match is found, the system proceeds with Inbound Policy Invocation.

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 Route Resolution phase.

Route resolution

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.

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/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 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 76

Server flow matching

The routing system uses the **URI Group** and **SIP Received 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 To` 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 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 75

Server flow matching for a call to a server on page 79

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 75

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/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 an additional matching criterion 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 is matched, the SIP routing system then validates if the destination IP address of the incoming SIP request matches the provisioned the **IP Address** field of the Received Interface configuration to decide a match. If either of the **URI Group** or **Received Interface** fields does not match the SIP routing, the system skips to the next server flow, looking for a match from the set of server flows associated with the server configuration.

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 the SIP request was originally received by the Avaya SBCE 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 as there is no outbound server flow 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:

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

All messages including the SIP responses and the in-dialog requests and responses are properly routed by the SIP routing system. 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 84.

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

Table continues…

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

Table continues…

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

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

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

Example 2

Table 8: Signaling Interface – CCE-Sig-Interface

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

Table 9: Media Interface – CCE-Med-Interface

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

Table 10: Routing Profile – To-CCE-ASM

Field	Value
URI Group	*

Table continues…

Field	Value
Next Hop Server 1	10.32.15.8
Transport	TLS

Table 11: Server Configuration – CCEASM

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

Table continues…

Field	Value
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

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. A customized Application Rule or the default Application Rule can be selected 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

Use the following procedure to create a new Application Rule.

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

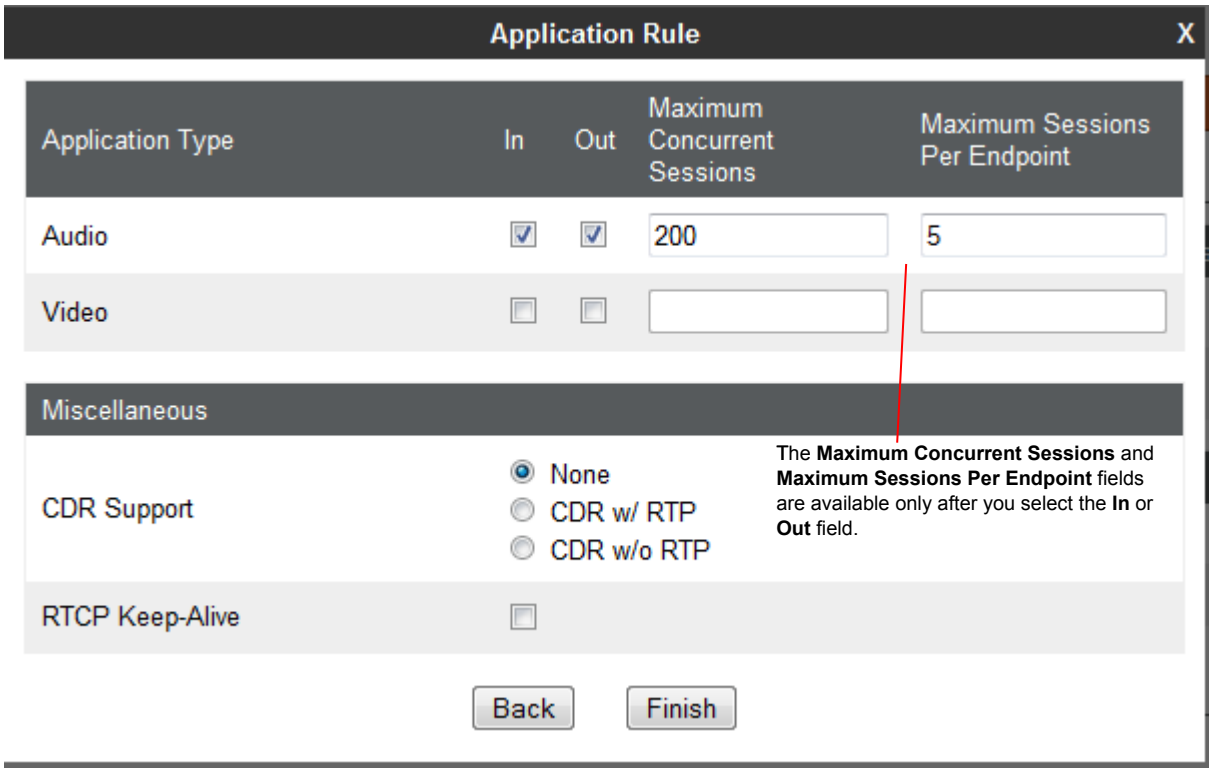
1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Application Rules**.

   The left application pane displays the existing Application Rule sets, and the content pane displays the parameters comprising the selected Application Rule set.
3. In the left Applications Rules pane, click **Add**.
4. In the Application Rule window, enter a name for the new application rule and click **Next**.

   The system displays the second Application Rule window.
5. Enter the requested information in the appropriate fields.

6. Click **Finish** to save, exit, and return to the Application Rules page.

Example



Application Rule screen field descriptions

Name	Description
Application Type	The type of SIP application for which this Application Rule is being configured: Audio and Video.
In	Check box indicating that this application rule applies to the audio and video traffic entering the enterprise network.
Out	Check box indicating that this application rule applies to the audio and video traffic originating from within the enterprise network.
Maximum Concurrent Sessions	The maximum number of concurrent application sessions that can be active for the selected application type. Additional application requests are blocked when this threshold is exceeded.
Maximum Sessions Per Endpoint	The maximum number of application sessions that can be active for an endpoint. Additional application requests are blocked when this threshold is exceeded.
CDR Support	None: Call detail records are not provided. With RTP: Call detail records with call quality and call statistics are provided in addition to change in call states. Without RTP: Call detail records with change in call states are provided.
RTCP Keep-Alive	Enables the RTCP Keep-Alive feature.

Cloning an existing Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Application Rules**.

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

   The system displays the Clone Rule window.
5. Enter a name for the new Application rule and click **Finish**.

   The system displays the Application Rules page. The Application pane shows the newly cloned Application Rule.

Editing an existing application rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Application Rules**.

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

   The system displays the Editing Rule window.
5. Edit the appropriate fields.
6. After making the appropriate edits, click **Finish**.

   The system displays the Application Rules screen. The Application pane displays the newly edited application rule.

Renaming an existing Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the Task Pane, select the **Application Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Application Rule sets, and the content pane displays the parameters comprising the selected Application Rule set.
3. In the Application Pane, select the name of the Application Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.

The system displays the Rename Rule pop-up window.

5. In the **Clone Name** field, type the new name of the Application Rule, and click **Finish** to save your changes.

   The system displays the Application Rules screen with the newly renamed Application Rule.

Deleting an existing Application Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Application Rules**.

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

   The system displays the confirmation window.
5. Click **OK** to continue with the deletion of the Application Rule.

   The system displays the Application Rules screen without the selected 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 left 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.
3. In the Applications pane, click **Add**.

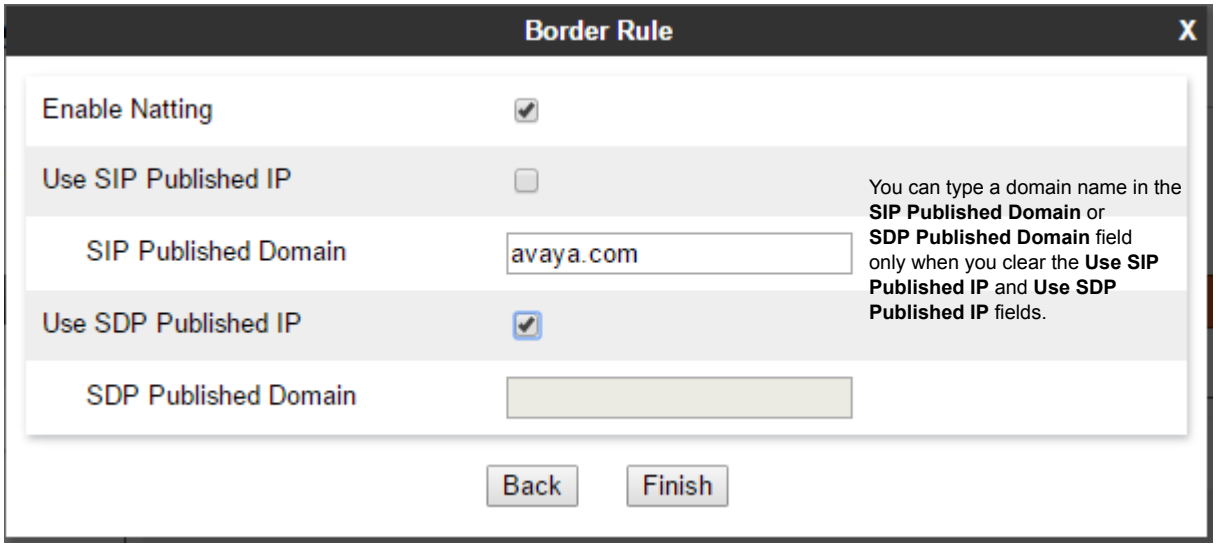
   The system displays the Border Rule window.
4. Enter a name for the new border rule, and click **Next**.

The system displays the second Border Rule window.

5. Enter relevant information in the second Border Rule window.
6. Click **Finish** to save and exit.

   The system displays the Border Rules screen.

Example



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 **Device Specific Settings** > **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.

Table continues…

Name	Description
	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.

Cloning a border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left 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.
3. In the Application pane, select the name of the border rule that you want to clone.
4. In the upper-right corner of the page, click **Clone**.

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

   The Application pane displays the newly cloned border rule.

Editing an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Border Rules**.

   The left Application pane displays the existing border rules, and the Content pane displays the parameters for the selected border rule.
3. In the Application pane, select the border rule that you want to edit.
4. In the lower-center section of the page, click **Edit**.

   The system displays the Editing Rule window.
5. Edit the required fields.
6. After making the required edits, click **Finish**.

   When you select the edited border rule in the Application pane, the system displays the changed details in the Content pane.

Renaming an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.

The left Application Pane displays the existing border rules, and the Content pane displays the parameters for the selected border rule.

3. In the Application Pane, select the name of the Border Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.

   The system displays the Rename Rule pop-up window.
5. In the **New Name** field, type the new name of the Border Rule and click **Finish** to save your changes.

   The system displays the Border Rules screen, with the newly renamed Border Rule.

Deleting an existing border rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Border Rules**.

   The left Application pane displays the existing border rule sets, and the Content area displays the parameters for the selected Border Rule set.
3. In the Application pane, click the border rule that you want to delete.
4. In the upper right corner of the page, click **Delete**.

   The system displays a confirmation window.
5. Click **OK**.

   The left Application pane does not display the selected 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 on to the EMS web interface with administrator credentials.
2. 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 for the selected Media Rule set.

3. In the Applications pane, click **Add**.

   The system displays the Media Rule window.

4. Enter a name for the new Media Rule, and click **Next**.
5. Enter the appropriate audio and video encryption information, and click **Next**.
6. Enter appropriate information in the Audio Codec and Video Codec sections and click **Next**.

   In the Audio Codec and Video Codec section, if codec prioritization is required, you can select the **Codec Prioritization**, and **Allow Preferred Codecs Only** fields, and select required codecs in the **Preferred Codecs** field. In the Audio Codec section, if transcoding is required, select the **Transcode When Needed** field. 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.

7. Select the **Silencing Enabled** check box.

   When you select the **Silencing Enabled** check box, the Media Silencing feature is enabled.

8. Select the **BFCP Enabled** check box.

   With this setting, Avaya SBCE relays Binary Floor Control Protocol (BFCP) control messages to control presentation channel. The system displays the next Media Rule window.

9. Select the **FECC Enabled** check box.

   Use this setting to enable mixed encryption support for audio, main video, and Far End Camera Control (FECC).

10. If you have environments with both IPv4 and IPv6 hosts, do the following:

    a. Select the **ANAT Enabled** check box.

       You must enable Alternate Network Address Types (ANAT) semantics when you have environments with both IPv4 and IPv6 hosts. Release 7.1 onwards, Avaya SBCE supports IPv6 addresses to SIP trunk servers.

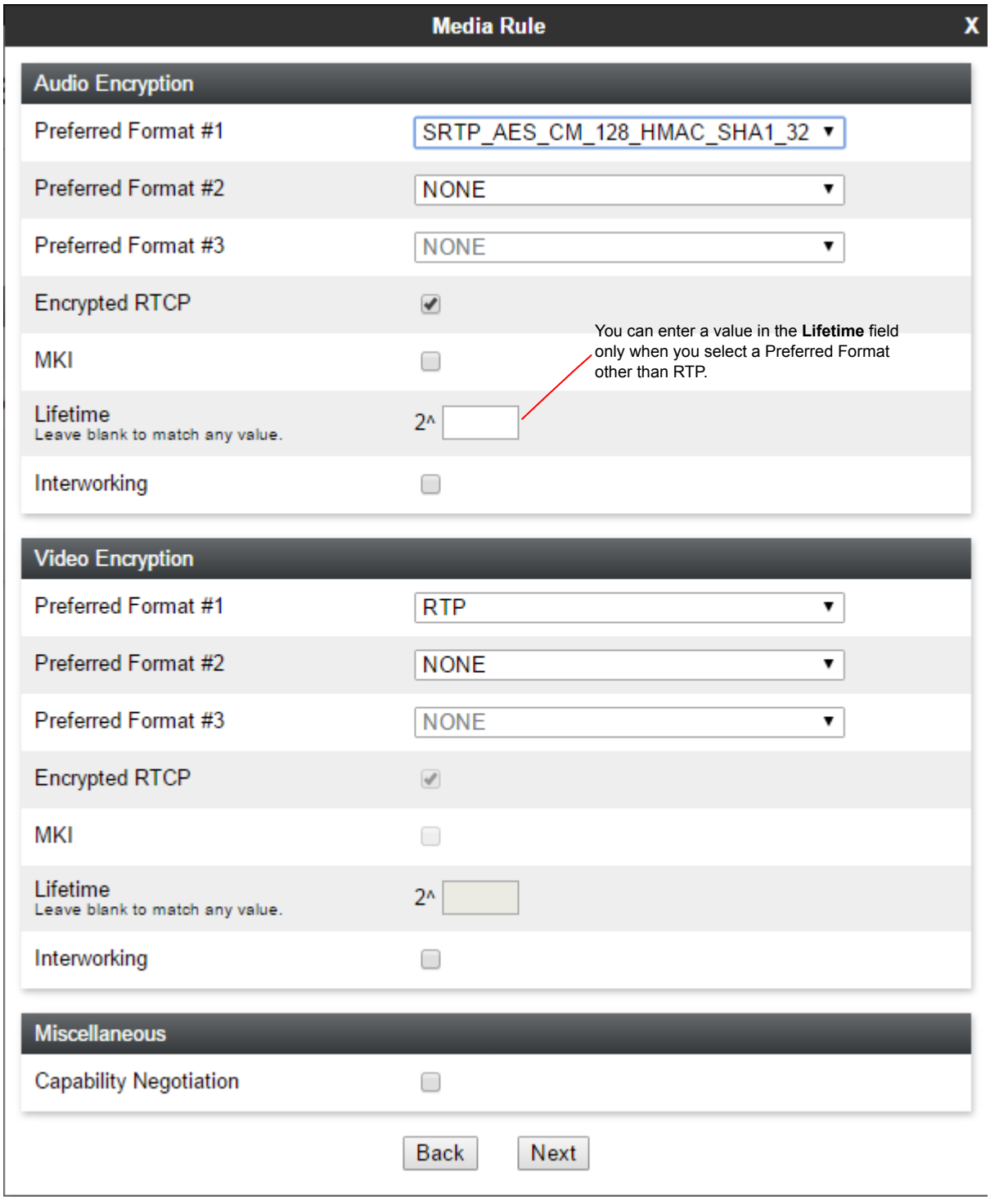
    b. In the **Preference** field, select whether the IP address is an IPv4 or IPv6 address.

    c. Click the **Remote** field to indicate that the address at the remote end is ANAT enabled, and click **Next**.

11. Enter appropriate information in the Media QoS Marking section.
12. Click **Finish**.

    The left Application pane displays the new media rule.

Example



Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 130

Media Rules field descriptions

Media 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.
	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 When Needed	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.
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**.
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 7.1 does not support transcoding for video codecs.
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**.

Advanced tab

Name	Description
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.

Table continues…

Name	Description
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	Indicated whether Far End Camera Control is enabled. 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

Table continues…

Name	Description
	• Minimize Monetary Cost • Normal Service • Other...
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.

Cloning an existing Media Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Media Rules**.

The left application pane displays the existing Media Rule sets, and the content pane displays the parameters comprising the selected Media Rule set.

3. In the Application pane, select the name of the media rule that you want to clone.
4. In the upper- right section of the screen, click **Clone**.

   The system displays the Clone Rule window.
5. In the **Clone Name** field, type a name for the new Media Rule, and click **Finish**.

   The left Application pane displays the newly cloned Media Rule.

Editing an existing Media Rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Media Rules**.

   The left application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected Media Rule set.
3. In the Application pane, click the name of the Media Rule set that you want to edit.

   The Content area displays the parameters for the selected media rule set.
4. Click the tab corresponding to the Media Rule parameter that you want to edit.
5. Click **Edit**.

   The system displays a Media Rule window for editing.
6. Edit the required fields.
7. Click **Finish**.

   When you select a rule in the Application pane, the Content pane displays the edited parameters.

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.

Renaming an existing media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Media Rules**.

   The left application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected media rule set.
3. In the Application pane, select the Media Rule that you want to rename.
4. In the upper-right section of the Content pane, click **Rename**.

   The system displays the Rename Rule window.
5. In the **New Name** field, type the new name for the Media Rule, and click **Finish**.

   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 left navigation pane, click **Domain Policies** > **Media Rules**.

   The left application pane displays the existing media rule sets, and the content pane displays the parameters comprising the selected media rule set.
3. In the upper-right corner of the page, click **Delete**.

   The system displays the confirmation window.
4. Click **OK**.

   The deleted media rule is not displayed in the left navigation pane.

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. See Installing a scrubber rules Package on page 227.

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 left navigation pane, click **Domain Policies** > **Security Rules**.

   The left Application pane displays the existing security rule sets, and the Content pane displays the parameters of the selected security rule set.
3. In the Application pane, click **Add**.

   The system displays the Security Rule window.
4. In the **Rule Name** field, type a name for the new security rule, and click **Next**.

   The system displays the second Security Rule window.
5. Enter the appropriate authentication information, and click **Next**.

   The system displays the third Security Rule window.
6. In the **From/To Blacklist** field, type a blacklist URI group to be used for checking the validity of subscribers using the network.

   When you enter a blacklist URI group, all calls from the devices in the group are rejected.

   Note:

   A blacklist URI group is a list of callers from where the subscribers do not want to receive calls. You can create a blacklist URI group in **Global Profiles** > **URI Groups**.
7. Click **Next**.

   The system displays the fourth Security Rule window.
8. Select the appropriate scrubber information, and click **Next**.

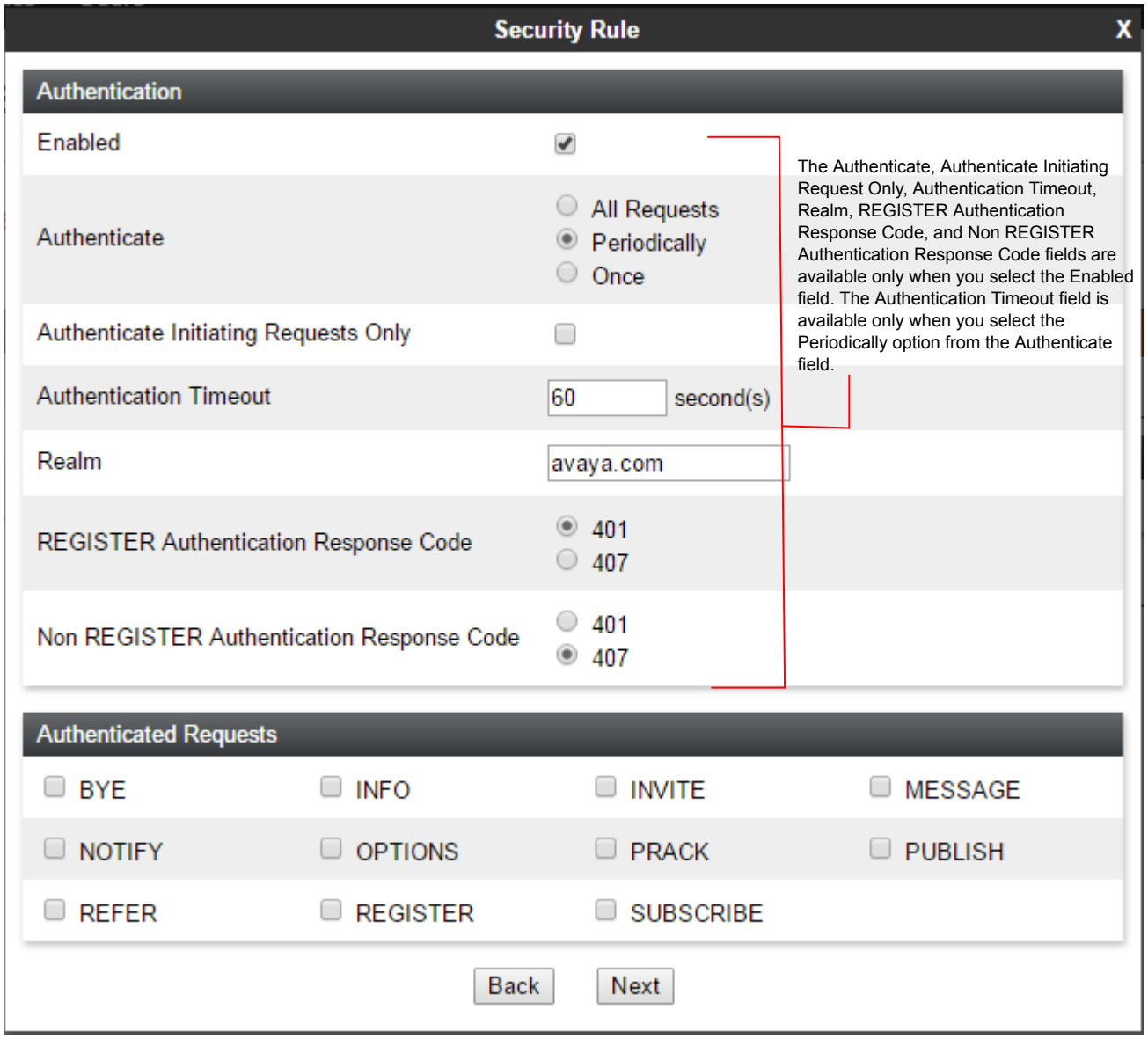
   The system displays the fifth Security Rule window.

Note:

New scrubber packages are added here. These packages are created by the VIPER team and then packaged and released by the engineering team after testing. For more information about scrubber packages, see Protocol Scrubber on page 226 and Installing a Scrubber Rules Package on page 227.

9. Enter the appropriate domain DoS profile information, and click **Finish**.

Example



Authentication field descriptions

When creating a new Security Rule, refer to this table for information on the authentication selections in the second Security Rule pop-up window.

Name	Description
Authentication	
Enabled	Indicates whether SIP requests are authenticated. SIP requests are authenticated according to the parameters specified by the remaining fields: Authenticate, Authenticate Initiating Requests Only, Authentication Timeout, and Realm. If you select this check box, the remaining fields become active and must be defined. If you do not select the check box, SIP requests are not authenticated and the remaining fields are deactivated. With the Authentication feature, Avaya SBCE challenges the user instead of the call server, and the user is not challenged again by the call server. This reduces the lead of the authentication mechanism from the call server.
Authenticate	Indicates how frequently the authentication is performed. • **All Requests**: Authenticate each SIP request. • **Periodically**: Authenticate at a periodic interval, the frequency of which is determined by the **Authentication Timeout** field. • **Once**: Authenticate once only.
Authenticate Initiating Requests Only	Indicates whether the initiating SIP requests are authenticated. If you enable this check box, only initiating SIP requests will be authenticated.
Authentication Timeout	The time, in seconds, that the authentication will be maintained by the Avaya SBCE security device. This field is active only when you select the **Periodically** option for the **Authenticate** setting.
Realm	The name of the authentication realm that will authenticate SIP proxy users.
REGISTER Authentication Response Code	The options are: 401 and 407.
Non REGISTER Authentication Response Code	The options are: 401 and 407.
Authentication Requests	Indicates which SIP requests require authentication. • BYE • INFO • INVITE • MESSAGE • NOTIFY • OPTIONS • PRACK • PUBLISH • REFER

Table continues…

Name	Description
	• REGISTER • SUBSCRIBE

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 checkbox 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.

Cloning an existing security rule

Procedure

1. Log in to the EMS web interface as with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Security Rules**.

   The left Application pane displays the existing security rule sets, and the Content pane displays the parameters of the selected security rule set.
3. In the Application pane, select the name of the security rule that you want to clone.

4. In the upper-right section of the Content pane, click **Clone**.

   The system displays the Clone Rule window.

5. Enter a name for the cloned security rule, and click **Finish** .

   The Application pane displays the newly cloned security rule.

Editing an existing security rule

Procedure

1. Log in to the EMS web interface as with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Security Rules**.

   The left Application pane displays the existing security rule sets, and the Content pane displays the parameters of the selected security rule set.

3. In the Application pane, select the name of the security rule set that you want to edit.
4. In the Content pane, click the security rule parameter tab whose values you want to edit.

   The Content pane displays the corresponding parameters for that Security Rule parameter tab.

5. Click **Edit**.

   The system displays the Edit screen for the selected parameters tab.

6. Edit the required fields, and click **Finish**.

   The Content pane displays the edited parameters.

Renaming an existing security rule

Procedure

1. Log in to the EMS web interface as with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Security Rules**.

   The left Application pane displays the existing security rule sets, and the Content pane displays the parameters of the selected security rule set.

3. In the Application pane, select the name of the security rule that you want to rename.
4. In the upper-right section of the Content pane, click **Rename**.

   The system displays the Rename Rule window.

5. In the **New Name** field, type the new name for the Security Rule, and click **Finish**.

   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 left navigation pane, click **Domain Policies** > **Security Rules**.

   The left Application pane displays the existing security rule sets, and the Content pane displays the parameters of the selected security rule set.

3. In the Application pane, select the security rule that you want to delete.
4. In the upper-right section of the Content pane, click **Delete**.

   The system displays the delete confirmation window.

5. Click **OK**.

   The Application pane does not display 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 left navigation pane, click **Domain Policies** > **Signaling Rules**.

   The left Application pane displays the existing Signaling Rule sets, and the Content pane displays the parameters of the selected Signaling Rule set.

3. In the Application pane, click **Add**.

   The system displays the first signaling rule window.

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

   The system displays the second signaling rule window.

5. Select the appropriate signaling information, and click **Next**.

   The system displays the third security rule window.

6. Enter the appropriate signaling information, and click **Next**.

The system displays the fourth security rule window.

7. Select the appropriate signaling information, and click **Next**.
8. Enter the appropriate values, and click **Finish**.

   The Application pane displays the newly created signaling rule, and the Content pane displays the parameters if the new signaling rule is selected.

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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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.
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...
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

Table continues…

Name	Description
	• 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**.
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.
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 left navigation pane, click **Domain Policies** > **Signaling Rules**.

   The left Application pane displays the existing Signaling Rule sets, and the Content pane displays the parameters of the selected signaling rule set.
3. In the left Application pane, select the name of the signaling rule set that you want to edit.
4. Select the Signaling Rule Parameter tab whose values you want to edit.

   The Content pane displays the corresponding parameters for that signaling rule parameter tab.
5. In the lower-center section of the Content pane, click **Edit**.

   The system displays the edit screen for the selected parameters tab.
6. Edit the required fields, and click **Finish**.

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. On the task pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. 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 system displays the selected Signaling Rule information window.
4. Click the **Requests** tab.
5. Click **Add In Request Control** or **Add Out Request Control**.

   The system displays the corresponding Add Request Control pop-up window.
6. Select the appropriate information.
7. Click **Finish** to save and exit.

   The system 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. On the task pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. Select the signaling rule where you want to add In Request parameters.
4. Click the **Requests** tab.
5. Click **Add In Request Control**.

6. In the **Method Name** field, click **OPTIONS**.
7. In the **In Dialog Action** field, click **Allow**.
8. In the **Out of Dialog Action** field, click **Block with...**.
9. In the fields below **Out of Dialog Action**, type `200` and `OK`.
10. 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. On the Task pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. 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 system displays the selected Signaling Rule information.
4. Click the **Responses** tab.
5. Click **Add In Response Control** or **Add Out Response Control**.

   The system displays the corresponding Add Response Control pop-up window.
6. Select the appropriate information in the Add Response Control window.
7. Click **Finish** to save and exit.

   The system 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:

A default Signaling 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. On the Task pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. 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 system displays the selected Signaling Rule information window.
4. Click the **Responses** tab.
5. Click **Add In Response Control** or **Add Out Response Control**.

   The system displays the corresponding Edit Response Control pop-up window.
6. Edit the appropriate information in the Edit Response Control pop-up window.
7. Click **Finish** to save and exit.

   The system 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. On the Task Pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. 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 system displays the selected Signaling Rule information window.
4. Click the **Request Headers** tab.
5. Click **Add In Header Control** or **Add Out Header Control**.

   The system displays the corresponding Add Header Control pop-up window.
6. Select the appropriate information.
7. Click **Finish** to save and exit.

   The system displays the selected Signaling Rule information window again.

Editing Request Header parameters

About this task

Use the following procedure to edit existing Request Header parameters.

⚠ Caution:

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

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the Task Pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. 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 system displays the selected Signaling Rule information window.
4. Click the **Request Headers** tab.
5. Click **Add In Header Control** or **Add Out Header Control**.

   The system displays the corresponding Add Header Control pop-up window.
6. Edit the appropriate information in the Add Header Control pop-up window.
7. Click **Finish** to save and exit.

The system 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. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. Select 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 system displays the selected Signaling Rule information window.
4. Select the **Response Headers** tab.
5. Select **Add In Header Control** or **Add Out Header Control**.

   The system displays the corresponding Add Header Control pop-up window.
6. Select the appropriate information on the Add Header Control pop-up window.
7. Click **Finish** to save and exit.

   The system 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. From the Task Pane, select the **Signaling Rules** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. Select 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 system displays the selected Signaling Rule information window.
4. Click the **Response Headers** tab.
5. Locate the row corresponding to the response header that you want to edit, and click **Edit**.

   The system displays the corresponding Edit Response Control pop-up window.
6. Edit the appropriate information in the Edit Response Control pop-up window.
7. Click **Finish** to save and exit.

   The system displays the selected Signaling Rule information window.

Editing signaling QoS parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the Task Pane, click the **Signaling** function from the **Domain Policies** feature.

   The left application pane displays the existing Signaling Rule sets, and the content pane displays the parameters comprising the selected Signaling Rule set.
3. In the Application Pane, select the name of the Signaling Rule where you want to edit the QoS parameters.
4. Select the **QoS Parameters** tab in the upper section of the screen.

   The system displays the Signaling QoS pop-up window.
5. Edit the appropriate fields.
6. Click **Finish**.

   The system 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 Task plane, select **Signaling Rules** section from the **Domain Policies** feature in Task Pane.
3. Click the **UCID** tab.
4. Click **UCID** > **Edit**.

UCID Screen

The following figure shows the UCID parameter screen:



Cloning an existing signaling rule

Procedure

1. Log in to EMS web interface with administrator credentials.
2. On the left navigation pane, click **Domain Policies** > **Signaling Rules**.

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

   The system displays the Clone Rule window.
5. Enter a name for the new signaling rule, and click **Finish**.

   The Application pane displays the newly cloned signaling rules.

Renaming an existing signaling rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Signaling Rules**.

   The left Application pane displays the existing Signaling Rule sets, and the Content pane displays the parameters of the selected Signaling Rule set.
3. In the left Application Pane, select the name of the signaling rule that you want to rename.
4. In the upper-right section of the screen, click **Rename**.

   The system displays the Rename Rule window.

5. Enter a new name for the signaling rule, and click **Finish**.

   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 left navigation pane, click **Domain Policies** > **Signaling Rules**.

   The left Application pane displays the existing signaling rule sets, and the Content pane displays the parameters of the selected Signaling Rule set.
3. In the Application pane, select the name of the signaling rule that you want to delete.
4. In the upper-right section of the screen, click **Delete**.

   The system displays the delete confirmation window.
5. Click **OK**.

   The Application pane no longer displays the deleted signaling 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 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. On the Task 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.

   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.
3. In the Application pane, click **Add**.

   The system displays the Policy Group window.
4. In the **Group Name** field, type a name for the new policy group, and click **Next**.

   The system displays the second Policy Group window where you must define the policy group parameters.
5. Enter the relevant parameters, and click **Finish**.

   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	Name of the Policy Group.
Application Rule	The application rule that determines which applications use this policy group.

Table continues…

Name	Description
Border Rule	The border rule that will determine which applications will use this policy group.
Media Rule	The media rule that will be used to match media packets.
Security Rule	The security rule that will determine which Avaya SBCE security policies will be applied when this policy group is activated.
Signaling Rule	The Signaling Rule that will be used to match SIP signaling packets.

Viewing an existing policy group summary

About this task

As previously stated, 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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The system 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.
3. On the Policy Group page, click **Summary**.

   The system displays the Policy Group Summary page.
4. Use the scroll bar to view the entire report. 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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The system displays the existing End Point Policy Groups.
3. From the Application Pane, select the Policy Group with the policy sets you want to edit.

   The system displays the Policy Sets currently assigned to the selected Policy Group.
4. Click the **Edit** option corresponding to the policy set that you want to edit.

   The system displays the Edit Policy Set page.
5. Edit the desired fields, and click **Finish** to save and exit.

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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

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

   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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The system displays the existing End Point Policy Groups.
3. From the Application Pane, select the Policy Group with the policy sets you want to delete.
4. Click the **Delete** option corresponding to the policy sets you want to delete.

   The system displays a delete confirmation pop-up screen.
5. Click **OK** to delete the selected policy set.

   The system 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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The system displays the existing End Point Policy Groups.
3. From the Application Pane, select the Policy Group that you want to delete.
4. Click the **Delete** option in the upper-right portion of the Content area.

   The system displays a delete confirmation message.
5. Click **OK** to delete the selected policy group.

   The system displays the End Point Policy Groups screen again.

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 left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.
3. In the Applications pane, click **Add**.

   The system displays the Session Policy window.
4. In the **Policy Name** field, type a name for the new session policy, and click **Next**.

   The system displays the second Session Policy window.
5. Select the **Media Anchoring** check box to enable or disable media anchoring.

   Disabling Media Anchoring keeps the media traffic within the remote branch network if both calling parties reside inside the network.
6. In the **Media Forking profile** field, click a Media Forking profile.

   This field is active only if the **Media Anchoring** check box is selected. If you have not created any Media Forking profile, the default value is **None**.

   Note:

   The Media Forking feature is not available on the Portwell platform.
7. Click **Finish**.

Cloning an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.
3. Select the Session Policy that you want to clone, and click **Clone**.
4. In the **Clone Name** field, type a name for the new session policy, and click **Finish**.

   The Application pane displays the newly cloned session policy.

Editing an existing session policy

Session Policies are comprised of Codec Prioritization and Media Anchoring parameters. These parameters can be easily edited by selecting the appropriate parameters tab and changing the desired fields. These procedures are described in the following sections.

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.
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.

Editing media forking parameters

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.
3. 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.

4. Click the **Media** tab.
5. Click **Edit**.

   The system displays the Media page.
6. Select a Media Forking profile, and click **Finish**.

   The Content area displays the edited media forking parameters when you click the media tab of the 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 left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.
3. In the Application Pane, select the name of the session policy that you want to rename.
4. In the upper-right section of the Content pane, click **Rename**.

   The system displays the Rename Policy window.
5. In the **New Name** field, type a new name for the session policy, and click **Finish**.

   The Application pane displays the renamed session policy.

Deleting an existing session policy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.
3. In the Application Pane, select the name of the session policy that you want to delete.
4. In the upper-right section of the screen, click **Delete**.

   The system displays the delete confirmation window.
5. Click **OK** .

   The Application pane no longer displays the deleted session policy.

Media unanchoring

To enhance bandwidth usage for endpoints within the same subnetwork and to allow direct media to flow between these endpoints, unanchor media for sessions. Use this feature to enhance bandwidth usage when you connect to a managed MPLS network or a cloud network.

From Release 7.1, 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 **Domain Policies** > **Session Policies**.
3. On the Session Policies page, in the Session Policies section, click an existing session policy and then click the **Media** tab.
4. Clear the **Media Anchoring** field.
5. 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.
6. 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.

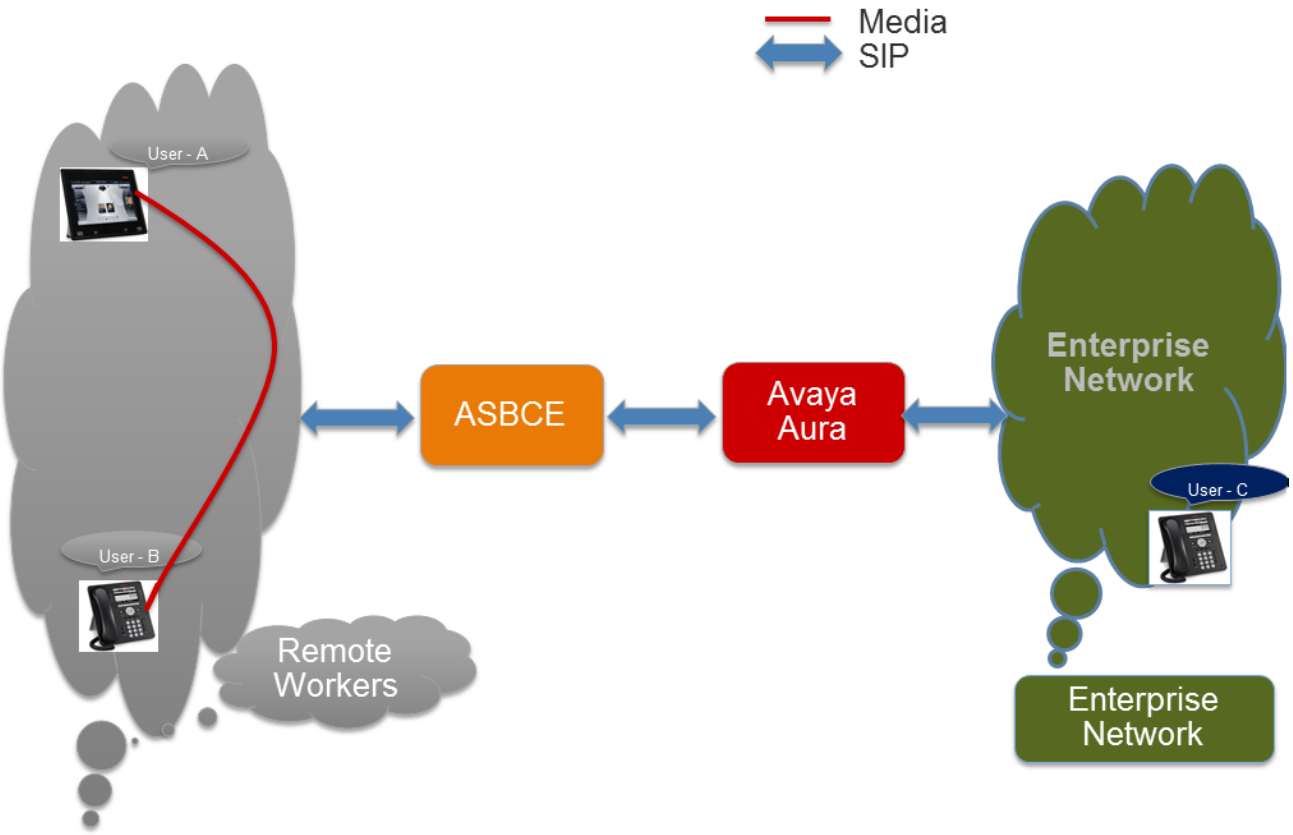
Media unanchoring scenarios

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

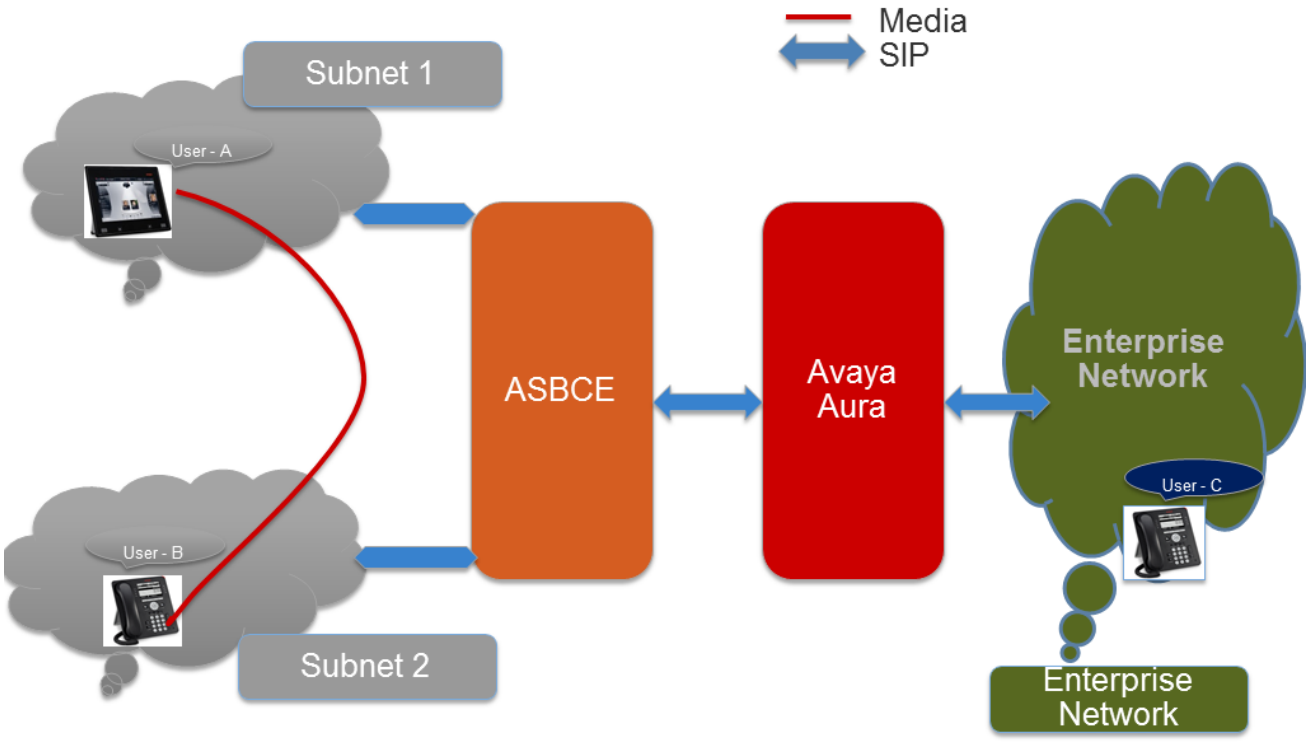
This section covers a few scenarios in which Media unanchoring can be used.

Remote workers in the same subnet



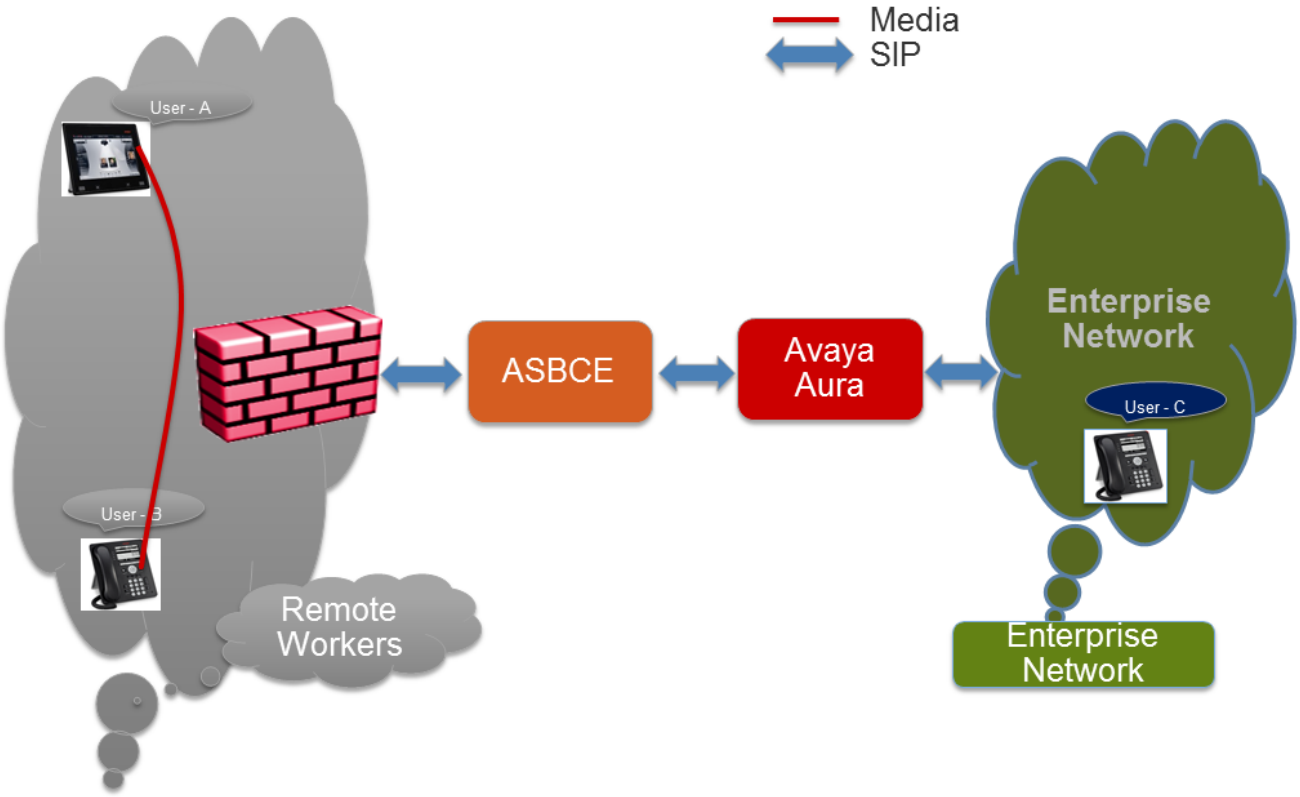
As the endpoints are in the same subnet, the Avaya SBCE can be configured to flow the media directly between the endpoints.

Remote workers in two different subnets



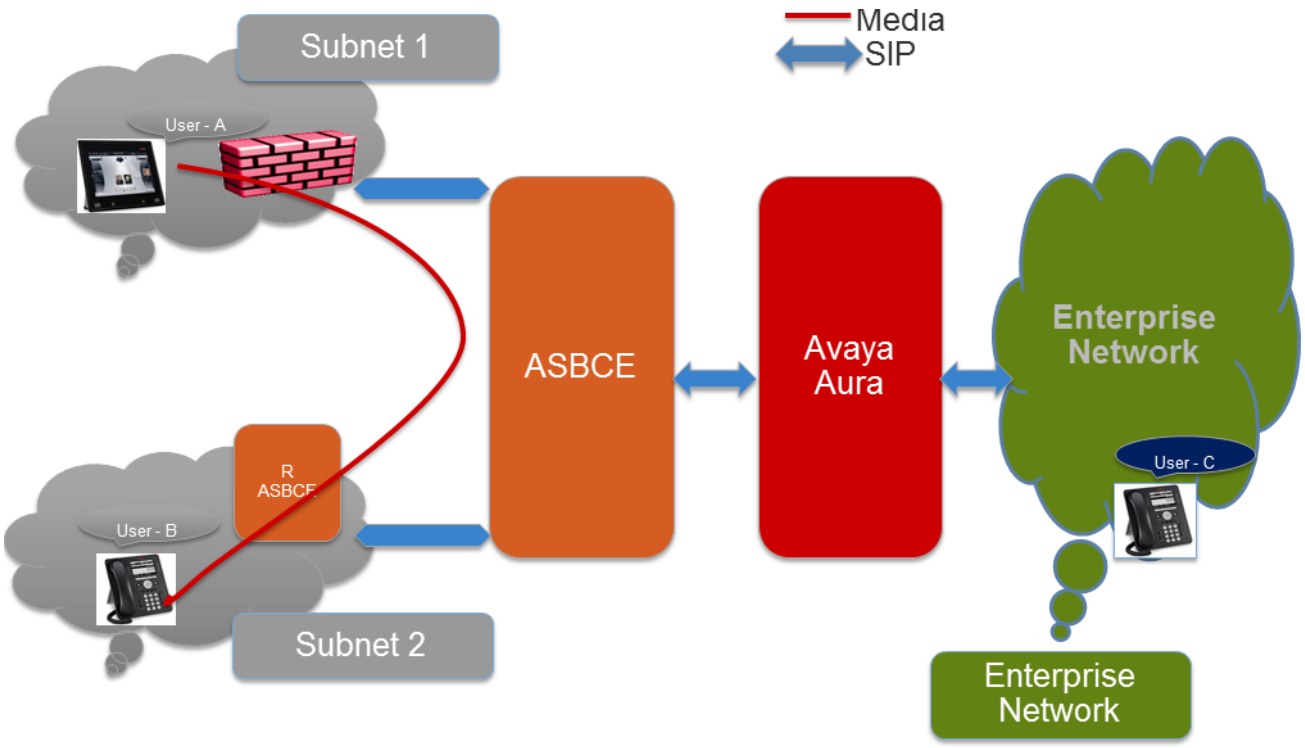
Avaya SBCE can be configured to release the media between two different subnets. The subnets must be reachable to flow the media.

Remote workers behind the same NAT



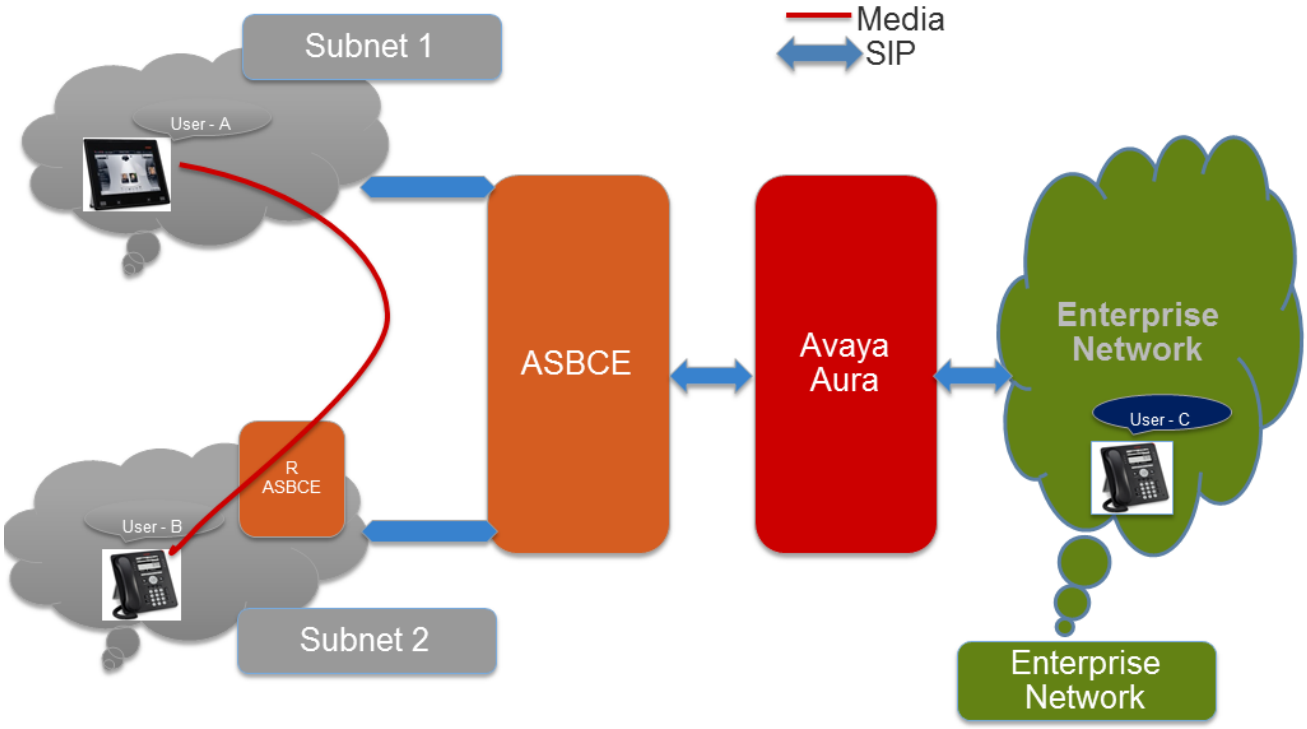
When Avaya SBCE detects that both remote workers in the call are behind the same NAT device, Avaya SBCE can enable media flow directly between the remote workers.

Remote branch office with Avaya SBCE



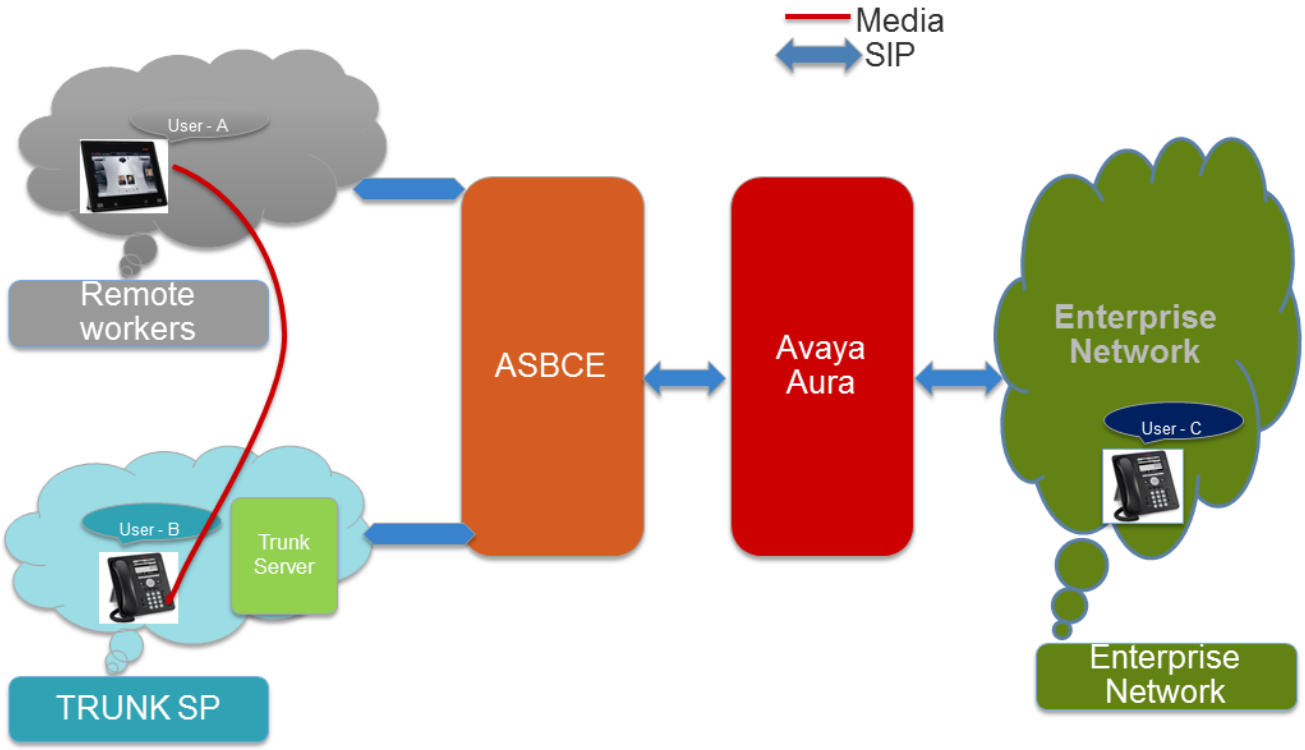
In this scenario, the endpoints belong to two different subnets. However, one of the endpoints is behind a NAT device, and the other subnet has remote Avaya SBCE. The Core Avaya SBCE can be configured to release the calls between these subnets by using the remote Avaya SBCE. To release the media from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

Remote branch office with Avaya SBCE



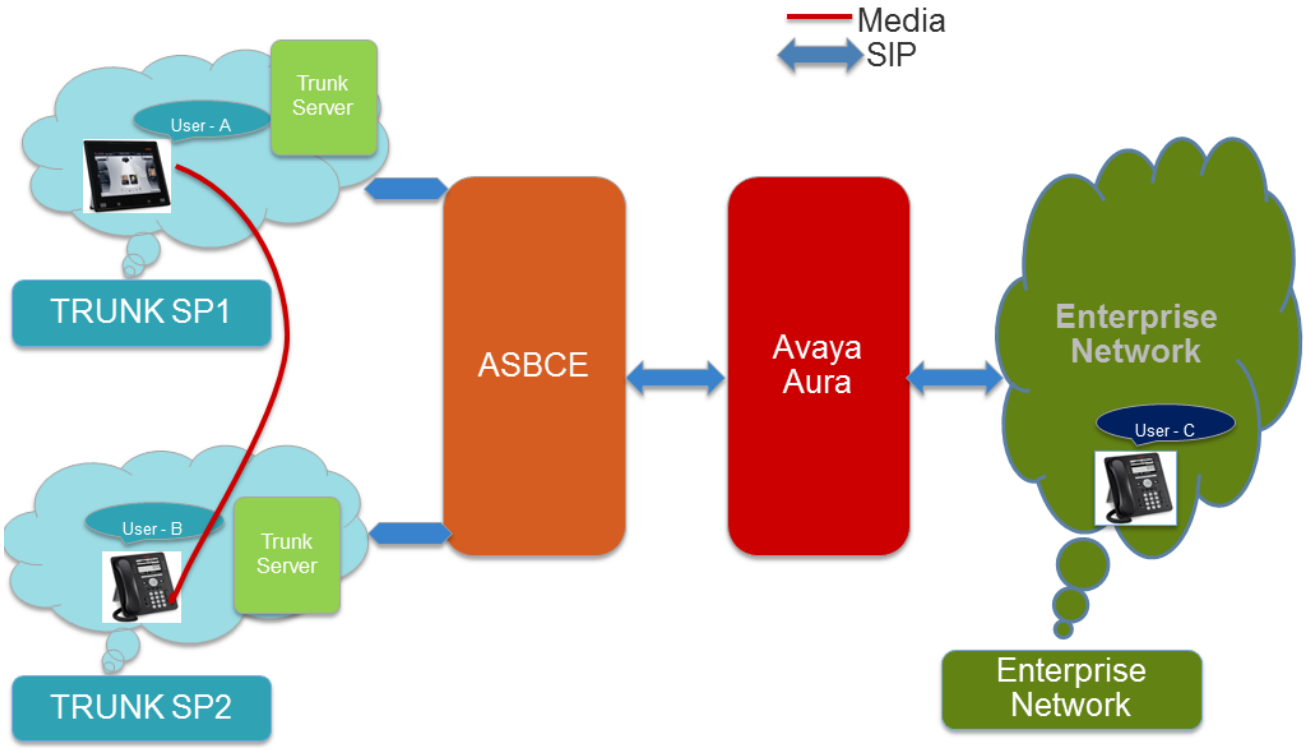
In this scenario, the endpoints belong to two different subnets, and one of the subnets has remote Avaya SBCE. The Core Avaya SBCE can be configured to release the calls between these subnets.

Calls between remote workers and Trunk users with same Avaya SBCE



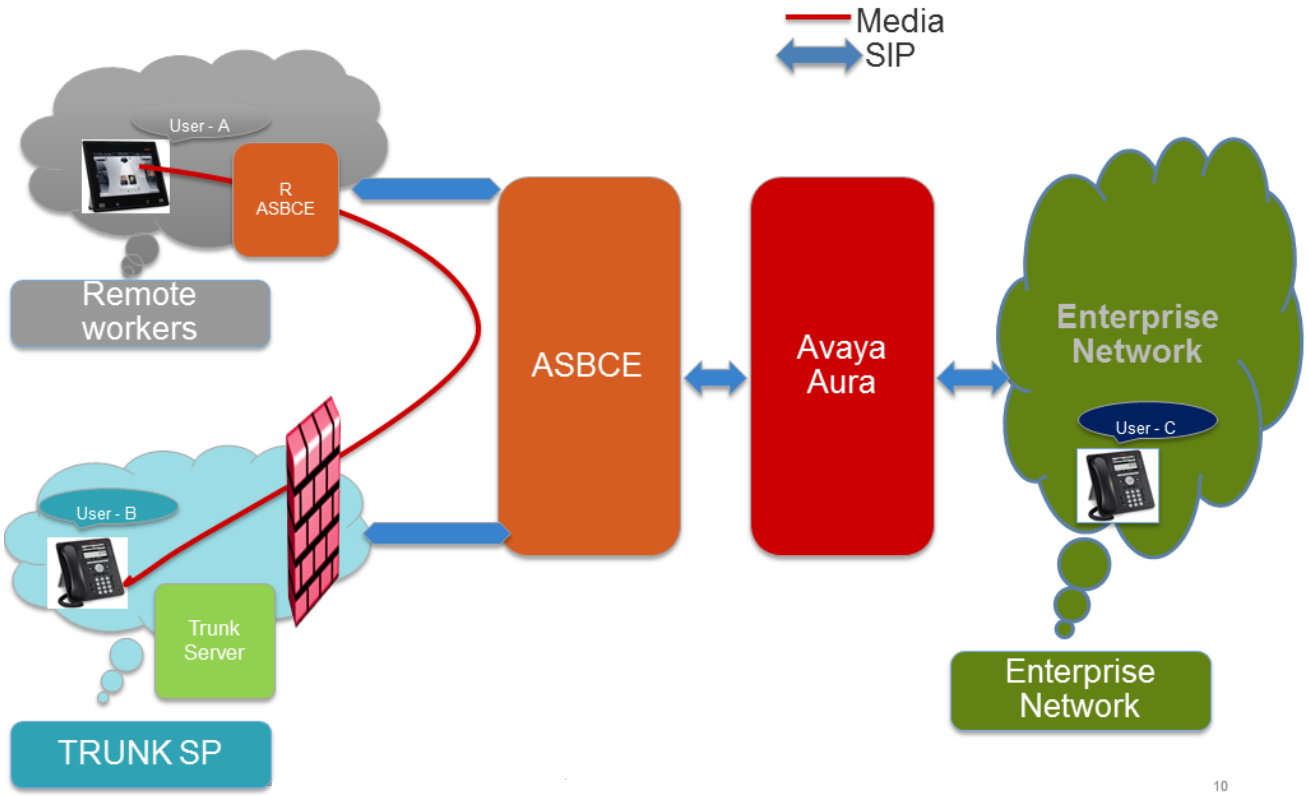
In this scenario, a call is established between remote worker from one subnet to the trunk subnet user. As these endpoints pass through the same Avaya SBCE, the Avaya SBCE device can be configured to release media between these endpoints. Both subnets must be reachable.

Calls between two trunks with the same Avaya SBCE



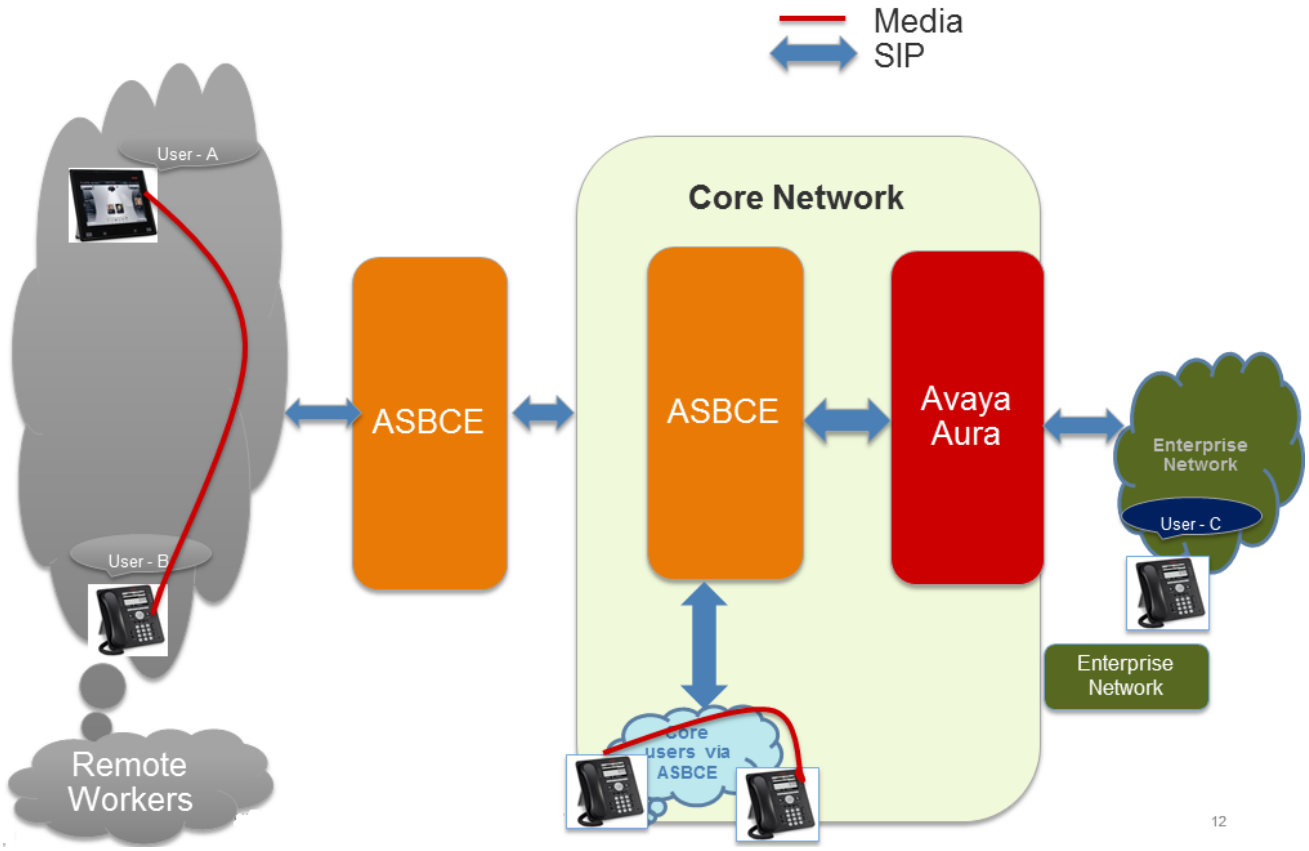
In this scenario, a call is established between two different trunk subnet users. As the endpoints pass through the same Avaya SBCE, the Avaya SBCE device can be configured to release media between these endpoints. Both subnets must be reachable.

Trunk behind firewall and Remote branch office with Avaya SBCE



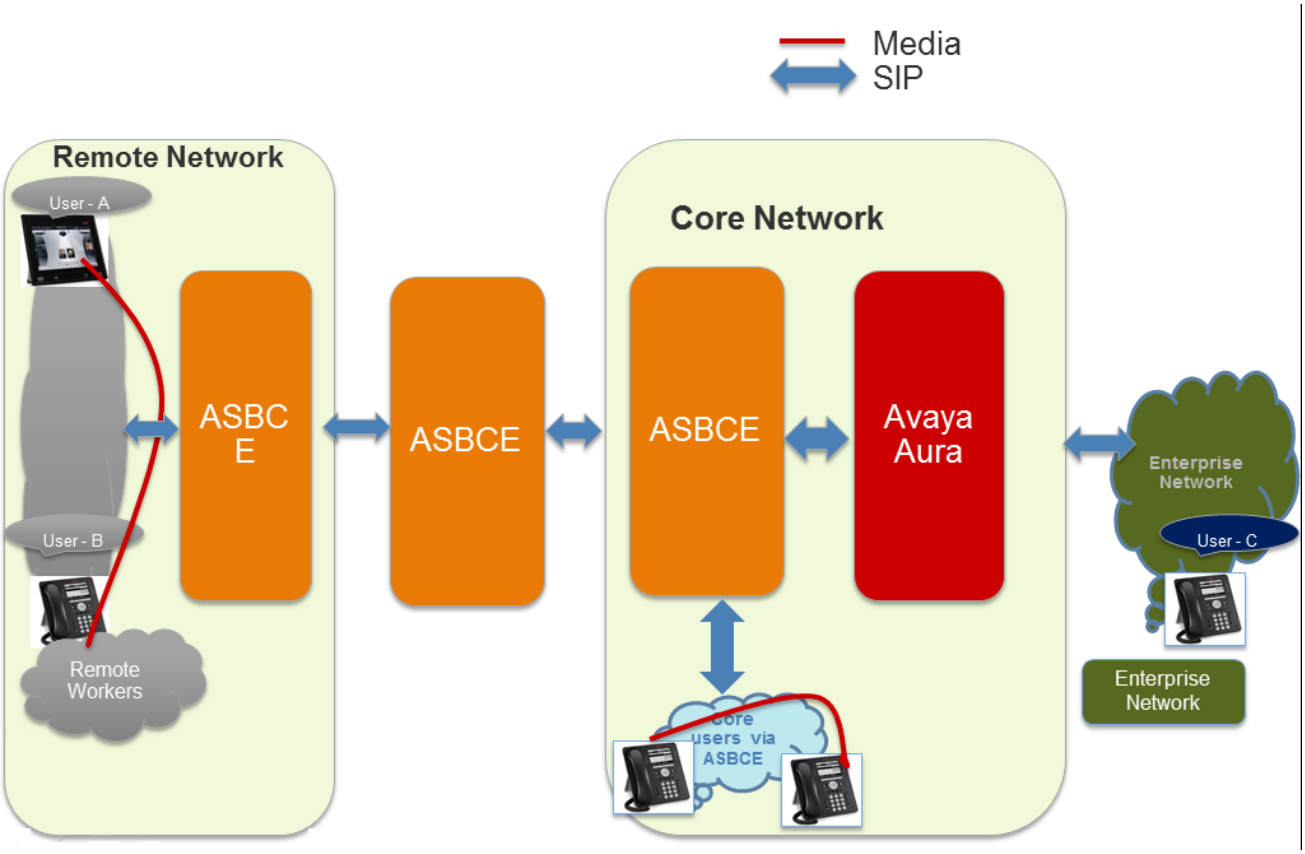
In this scenario, one subnet belongs to the trunk connected to Avaya SBCE, and the other subnet has a remote worker connected to Avaya SBCE with remote Avaya SBCE. The core Avaya SBCE can be configured to release calls between these subnets, by using the remote Avaya SBCE. To release the media from core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

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 new subscriber endpoint flow

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The Application pane lists the registered Avaya SBCE security devices for which the new flow is applied. In the content area, the system displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBCE security devices.
3. From the application pane, select the Avaya SBCE Device for which the new Subscriber End-Point Flow will be created.

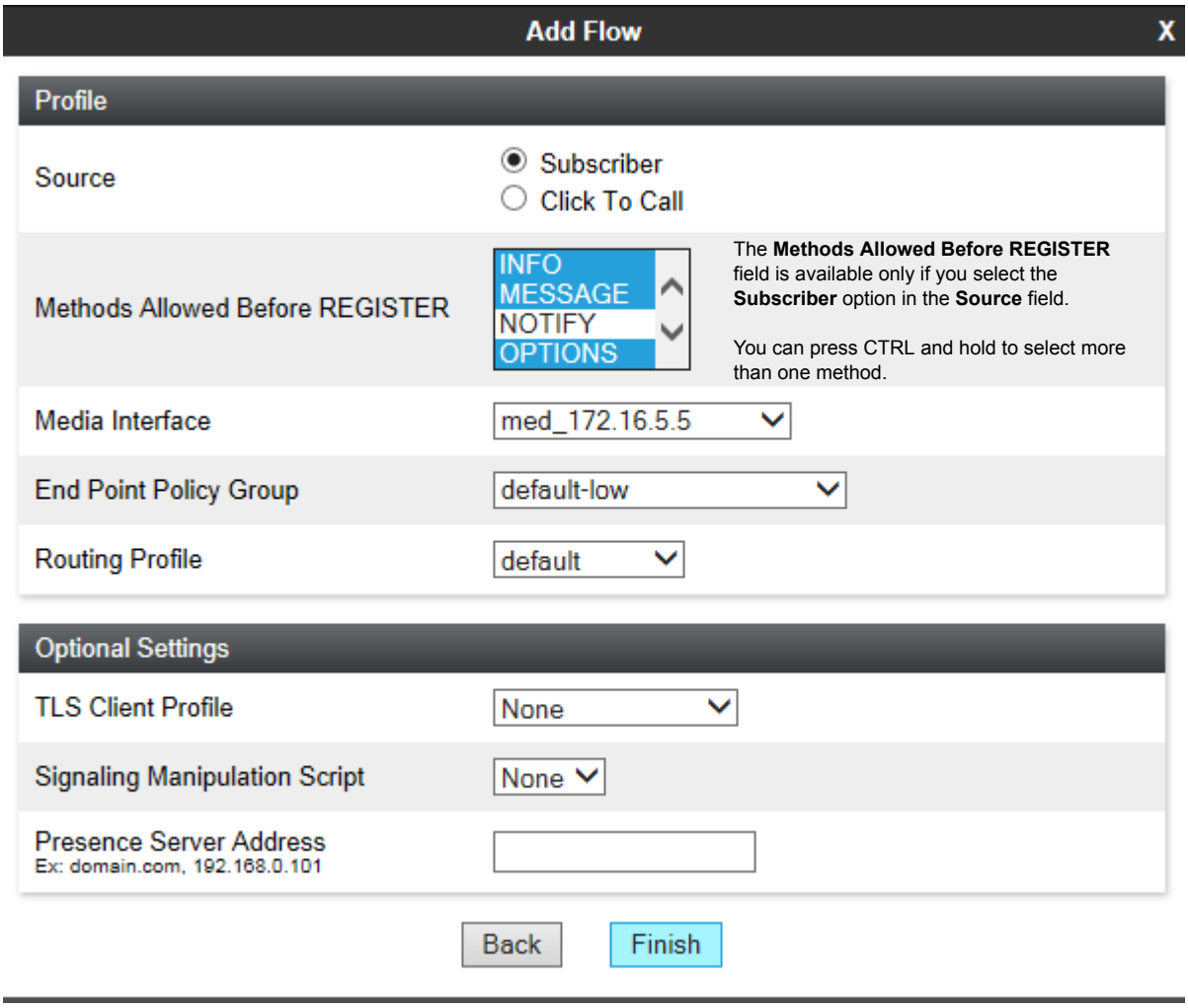
   The system displays the End-Point Flows screen showing the flows that are currently defined for that Avaya SBCE device.
4. Click the **Subscriber Flows** tab.
5. Click **Add**.

   The system displays the Add Flow window.
6. Enter the requested information in the appropriate fields, and click **Next**.

   Alternatively, click the cancel button to close the window and cancel the add flow operation.
7. 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.

Example



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.
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.

Table continues…

Name	Description
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.
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.
Server Configuration	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.

Table continues…

Name	Description
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.
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**.

Creating a server flow

About this task

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

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The Application Pane lists the registered Avaya SBCE security devices for which the new flow is applied. The content area displays a specifically ordered list of Subscriber or Server call flows for the selected Avaya SBCE security devices.
3. From the Application Pane, select the Avaya SBCE Device for which the new Server End-Point Flow is created.

   The system displays the End-Point Flows screen showing the flows that are currently defined for that Avaya SBCE.
4. Click the **Server Flows** tab.
5. Click **Add**.

   The system displays the Add Flow window.
6. Enter the requested information in the appropriate fields, and click **Finish**.

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 left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The left application pane displays the existing devices sets. Separate tabs display the parameters comprising the server end-point flows and subscriber end-point flows for a selected device.
3. Click the **Subscriber Flows** tab.

The content area displays the existing Subscriber endpoint flows for the selected device.

4. Locate the Subscriber endpoint flow that you want to clone, and click **Clone**.

   The system displays the Clone Flow screen.

5. In the **Flow Name** field, type a name for the Subscriber Flow.
6. Edit any other parameters, if necessary, and click **Finish**.

   Alternatively, click the **Cancel** button to cancel the cloning operation and close the window without saving.

   The system 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 left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The application pane displays the existing devices. Separate tabs displays the parameters comprising subscriber endpoint flows and server endpoint flows for a selected device.

3. Click the **Server Flows** tab.

   The content area displays the existing Server endpoint flows for the selected device.

4. Locate the Server end-point flow that you want to clone, and click **Clone**.

   The system displays the Clone Flow screen.

5. In the **Flow Name** field, type a name for the new server flow.
6. Edit any other parameters, if necessary, and select **Finish**.

   Alternatively, click the Cancel icon to cancel the cloning operation and close the window without saving.

   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 left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The Application pane displays the existing devices. Separate tabs display the parameters comprising subscriber endpoint flows and server endpoint flows for the selected device.

3. Click the **Subscriber Flows** tab or the **Server Flows** tab.

   The content area displays existing endpoint flows for the selected device.

4. Locate the flow that you want to edit, and click **Edit**.

   The system displays the Edit Flow screen.

5. 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.

6. Click **Finish**.

Reordering the precedence of endpoint flows

Procedure

1. Log in to the EMS web interface with administrator credentials..
2. In the left navigation pane, click **Device Specific Settings** > **End Point Flows**.
3. Click the **Subscriber Flows** tab or the **Server Flows** tab.

   The Content Area displays the existing endpoint flows for the selected 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**.

   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 left navigation pane, click **Device Specific Settings** > **End Point Flows**.
3. Select the **Subscriber Flows** tab or the **Server Flows** tab.
4. Locate the flow that you want to delete, and click **Delete**.

   The system displays a delete confirmation window.

5. 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 left navigation pane, click **Device Specific Settings** > **Session Flows**.
3. In the Application pane, click the Avaya SBCE Device for which you want to create a new session flow.

   The Content Area displays the session flows currently defined for that Avaya SBCE device.
4. Click **Add**.

   The system displays the Add Flow screen.
5. Enter the requested information.
6. Click **Finish**.

   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 left navigation pane, click **Device Specific Settings** > **Session Flows**.

   The Application pane displays the registered Avaya SBCE security devices for which the new flow is applied. The Content Area displays a specifically ordered list of Session Flows for the selected Avaya SBCE security devicè.
3. Click the Avaya SBCE Device for which you want to clone the new Session Flow.

   The Content Area displays the session flows currently defined for that Avaya SBCE device.
4. Locate the session flow that you want to clone, and click **Clone**.

   The system 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.
7. Click **Finish**.

   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 left navigation pane, click **Device Specific Settings** > **Session Flows**.

   The Application Pane lists the registered Avaya SBCE security devices for which the new flow is applied. The Content Area displays a specifically ordered list of Session Flows for the selected Avaya SBCE security device.
3. In the application pane, click the Avaya SBCE Device whose Session Flow you want to edit.

   The Content Area displays the session flows currently defined for that Avaya SBCE device.
4. Locate the Session flow that you want to edit, and click **Edit**.

   The system displays the Edit Flow screen.
5. Edit the existing fields.
6. Click **Finish**.

   The system 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 left navigation pane, click **Device Specific Settings** > **Session Flows**.

3. Click the Avaya SBCE Device whose session flows you want to reorder.

   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**.

   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 left navigation pane, click **Device Specific Settings** > **Session Flows**.

   The Application Pane displays the registered Avaya SBCE security devices for which the new flow will be applied. The Content Area displays a specifically ordered list of Session Flows for the selected Avaya SBCE security device.
3. Click the Avaya SBCE Device whose session flow you want to delete.
4. Locate the session flow that you want to delete, and click **Delete**.

   The system displays a confirmation screen is displayed to confirm whether you want to proceed with deletion.
5. Click **OK**.

   The system deletes the 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 left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.

3. In the **Reverse Proxy** tab, click **Add**.
4. 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 Avaya SBCE IP address.
   d. In the **Listen Protocol** field, click the protocol published towards remote workers for the SSO service.

      If you select the HTTPS protocol, the system enables the **Listen TLS Profile** field.
   e. In the **Listen TLS Profile** field, click a server profile.
   f. In the **Listen Port** field, type the port published towards remote workers for SSO service.

      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 IDE Server.

      For security reasons, you must use HTTPS.
   h. In the **Server TLS Profile** field, click a server profile.
   i. In the **Connect IP** field, click the IP address that Avaya SBCE uses for communicating with IDE Server.
   j. In the **Server Addresses** field, type the IDE server IP address and port number, and click **Next**.
   k. In the **Whitelisted IPs** field, type the IP addresses from which traffic is allowed.

      If required, type a maximum of five IP addresses separated by commas.
   l. Click **Finish**.

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

About this task

Use the following procedure to manually create a new URI group.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **URI Groups**.

   The system displays the URI Groups window.
3. In the Application pane, click **Add**.

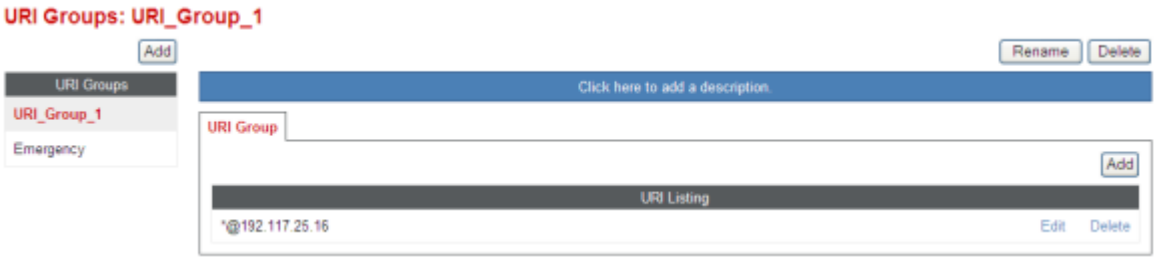
   The system displays the URI Group window.
4. Enter a name for the new URI group and then click **Next**.

   The system displays the second URI Group window.
5. Complete the fields.

   For information about the field description, see Add URI Group field descriptions.
6. Click **Finish**.

   The Content pane displays the new URI group.

Example



Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 130

Add URI Group field description

When creating a new URI group, refer to the following table for information about the fields in the second Add URI Group screen.

Name	Description
Group Name	Name of the URI group.
Scheme	URI scheme. The options are: • **sip/sips:** For Session Initiation Protocol or Secure Session Initiation Protocol. • **tel:** For telephone.

Table continues…

Name	Description
URI Type	**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. The Emergency group is created to define special numbers that must not be restricted by any dial-out restrictions imposed by Domain Policies. The Avaya SBCE administrators must put all applicable emergency numbers for the country for special handling.

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.

Related links

Managing SIP options on page 178

Adding an additional URI to an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **URI Groups**.

   The left Application pane displays the existing media rule sets, and the Content pane displays the URIs that comprise the URI group.
3. In the Application pane, click the URI group to which you want to add an additional URI.

The **URI Group** tab on the Content pane displays a list of SIP URIs assigned to the selected **URI Group**.

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

   The system displays the Add URI window.

5. Add the required URIs.

   For information about the fields, see Add URI Group field description.

6. Click **Finish**.

   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 130

Editing an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **URI Groups**.

   The left Application pane displays the existing media rule sets, and the Content pane displays the URIs that comprise the URI group.

3. 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.

4. In the Content pane, click **Edit** for URI that you want to edit.

   The system displays the Edit URI window.

5. Make the required changes to URI.
6. Click **Finish**.

   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 left navigation pane, click **Global Profiles** > **URI Groups**.

   The Application pane displays the existing URI groups. The Content pane displays URIs that comprise the URI group.

3. 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.

4. In the Content pane, click the **Delete** option that corresponds to the URI that you want to delete.

   The system displays a delete confirmation screen.

5. Select **OK** to perform the delete operation, or select **Cancel** to stop the delete operation.

   The system 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 an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **URI Groups**.

   The left Application pane displays the existing media rule sets, and the Content pane displays the URIs that comprise the URI group.

3. In the Application pane, click the URI Group that you want to rename.
4. In the Content pane, click **Rename**.

   The system displays the Rename Group window.

5. In the **New Name** field, enter a new name for the existing URI Group.
6. Click **Finish**.

   The URI Groups page displays the renamed URI Group.

Deleting an existing URI group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **URI Groups**.

   The left Application pane displays the existing media rule sets, and the Content pane displays the URIs that comprise the URI group.

3. In the Application pane, click the URI Group that you want to delete.
4. In the Content pane, click **Delete**.

   The system displays the delete confirmation window.

Note:

If the selected URI Group is associated with a security policy or a call flow, the system 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.

5. To delete the selected URI Group, click **OK**.

   The Application pane does not show the deleted URI group name.

Related links

Unanchoring media for existing session policies

Unanchoring media for existing session policies on page 130

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 global parameters.
  - Authenticate RADIUS settings.
  - Manage SNMP settings.
  - Manage routing profiles.
  - Manage trace settings.
  - Manage syslog settings.
  - Authorize user agents.
- Manage device-specific settings.
  - 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 of the topics in this overview section, refer to the appropriate sections in the chapters listed below:

- 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 159.
Enable Interfaces	See Enabling interfaces on page 160.
Configure URI Groups	See Creating a new URI group on page 151.
Configure Routing Profiles	See Creating a new routing profile on page 201.

Table continues…

Task	Description
Interworking Profiles	See Adding a new Server Interworking Profile on page 250.
Add Servers (Call/Trunk)	See Creating an Avaya call server profile (advanced services only) on page 330 and Adding a new SIP Server profile on page 240.
TLS Certificates	See Creating a Certificate Signing Request on page 265 and Installing certificates on page 267.
TLS Profiles	See Creating a new TLS server profile on page 280.
Domain Policy Group	See Creating a new policy group on page 123.
Signaling Interface	See Adding a new signaling interface on page 213.
Media Interface	See Adding a new Media Interface on page 215.
Subscriber Flow	See Creating a new subscriber end-point flow on page 141.
Server Flow	See Creating a new server endpoint flow on page 145.
Session Flow	See Creating a new session flow on page 148 and Creating a new session policy on page 126.

Reconfiguring Avaya SBCE

About this task

Management interfaces, for example, M1 and M2, and media interfaces, for example, A1, A2, B1, and B2, must not be configured 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:

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 in 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 GUI, navigate to **System management** > **Devices** and click **Uninstall**.
2. Initiate 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 GUI.

Enabling interfaces

Procedure

1. Click **Device Specific Settings** > **Network Management** > **Interfaces**.
2. On the Interfaces page, enable the required interfaces.

Backup / Restore system information

The Backup/Restore feature provides the ability to backup or create a snapshot of the EMS security configuration to a user-definable location or to a local EMS server. The location must be secure and physically separate from the Avaya SBCE equipment chassis for later retrieval or restoration. You can download the snapshot using the download link provided in the **Snapshot** tab.

Note:

A configuration backup can be taken manually and restored as needed, or automatic snapshots can be configured.

Designating a Snapshot Server

About this task

A snapshot contains information such as certificates and keys, which can be misused to gain unauthorized access to the Avaya SBCE server. The administrator must ensure that the storage directory on remote server is accessible only to authorized users.

The directory with the snapshot must not have read/write/execute permission for unauthorized users.

To back up to a remote server, before using the Backup/Restore feature, you can designate a server as a snapshot server to hold the backup files or save the files to the local EMS server.

Caution:

A snapshot can only be restored 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 must be configured with the same original management IP used when the snapshot was created or the system may need to be manually rebooted. If the EMS server hardware group or the Avaya SBCE product version do not match, the restore operation will fail and the system settings will revert to the earlier state.

Procedure

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

2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore page.

3. Click the **Snapshot Servers** tab.

   The system displays the available snapshot server profiles in the content area.

4. On the Snapshot Servers page, click **Add**.

   The system displays the Add Snapshot Servers page.

5. Add the requested information in the fields.

6. Click **Finish**.

Next steps

Making a System Snapshot on page 161

Add Snapshot Server field descriptions

Name	Description
Profile Name	A descriptive name to refer to the snapshot server being configured.
Server Address (ip:port)	The IP address and port number of the snapshot server to which backup files or snapshots are transferred by using secure FTP (SFTP).
User Name	The user name of the administrative account that is authorized to make system backups.
Password	The password assigned to authenticate the administrative account.
Confirm Password	The password that you reenter for confirmation.
Repository Location	The path (directory) on the snapshot server where the backup files will be stored and retrieved from.
Host Key	The key used to authenticate the login of the host.

Making system snapshots

Before you begin

Designate a snapshot server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. Select **Backup/Restore** from the Task Pane.

   The system displays the Backup/Restore screen in the content area.

3. Click **Create Snapshot**.

The system displays the Create Snapshot window.

In a deployment with multiple Avaya SBCEs, if any of the Avaya SBCEs is out of service, you cannot create a snapshot.

4. Enter a name to designate this snapshot (backup) file, and click **Create**.

   A snapshot (backup) of the EMS security configuration is made and saved to the designated snapshot server. A banner is displayed on the Create Snapshot pop-up window informing you that the snapshot has been successfully created. When the process is complete, the newly created snapshot is displayed in the content area of the snapshots screen.

Restoration of a system snapshot

The two methods of restoring a snapshot to the EMS server are manual and automatic.

Manual

The manual method of restoring a snapshot to EMS is a two-step process. The snapshot is first retrieved from the snapshot server to the local workstation and then uploaded to EMS for reconfiguration. See the following procedures to restore EMS to a previous snapshot configuration:

- Retrieving a snapshot file
- Restoring a snapshot file

Automatic

The automatic method of restoring a snapshot to EMS is a single-step process that restores EMS to the previous configuration without further intervention. See the Restoring a snapshot file automatically section.

Caution:

During the manual and automatic process of restoring a snapshot file, EMS goes in the offline mode when the files are being transferred and the device is being reconfigured.

No Avaya SBCE detection or mitigation features are available for the entire duration of the restore procedure, making the system vulnerable to intrusions and attacks.

Restoration procedures must be done only during times of relative system inactivity or during scheduled periods of maintenance.

Snapshots can be restored to an EMS system of the same hardware category, manufacturer, and model of EMS and the network of Avaya SBCE. The following table lists the hardware categories:

Hardware Model	No. of NICs	Hardware Category
CAD 0208	4	110
Dell 210	2	EMS
Dell 210	6	310
Dell R320	6	310

Table continues…

Hardware Model	No. of NICs	Hardware Category
Dell R620	6	310
Dell R630	6	310
HP DL360 G8	6	311
HP DL360 G9	6	311
VMWare	2	EMS
VMWare	4	110
VMWare	6	310

Related links

Retrieving a snapshot file on page 163
Restoring a snapshot file manually on page 163
Restoring a snapshot file automatically on page 164

Retrieving a snapshot file

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the Task Pane, click **Backup/Restore**.

   The system displays the Backup/Restore screen in the content area.
3. Click the **Snapshot** tab.
4. In the drop-down box, click the snapshot server or the local server on which you have created the snapshot.
5. Click the checkbox corresponding to the snapshot file that you want to retrieve and then click **Download**.

   The system saves the snapshot file on default download directory.

Next steps

Restoring a Snapshot File

Restoring a snapshot file manually

Before you begin

Retrieve a snapshot file.

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 uncompressed 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.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the Task pane, click **Backup/Restore**.

   The Content area displays the Backup/Restore screen.
3. Select the corresponding **Restore by File** option.

   The system displays the Restore by File pop-up window.
4. Click **Browse**.

   The system displays a dialog pop-up window.
5. Select the desired snapshot file, and click **Open**.

   The system enters the selected snapshot file in the **Restore Point File** field of the Restore by File window.
6. Click **Finish**.

   The system displays a warning window for confirmation to proceed with the restoration procedure.
7. Click **OK**.

   The EMS server goes offline and the snapshot file transferred to the EMS server, where the file is uncompressed and used to reconfigure the EMS software to a previous configuration.

   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 2 to 3 minutes to reboot after backup configuration.

Restoring a snapshot file automatically

Before you begin

Create a system snapshot.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the Task pane, click **Backup/Restore**.

   The Content area displays the Backup/Restore screen.
3. Using the drop-down menu in the Content Area, select the snapshot server that contains the snapshot file that you want to retrieve.

   The system displays all snapshot files on the selected snapshot server in the content area.

4. Select the snapshot file that you want to restore to the EMS by clicking the corresponding **Restore** option.

   The system displays a warning pop-up window, asking for confirmation to proceed with the automatic restoration procedure.

5. Click **OK**.

   The EMS 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 2 to 3 minutes to reboot after backup configuration.

Related links

Retrieving a snapshot file on page 163
Restoring a snapshot file manually on page 163

Deleting a system snapshot

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore screen.

3. Select the local server or the designated snapshot server from where you want to delete the file.
4. Select the file and click the corresponding **Delete** option.

   The system displays a warning message, asking for a confirmation to delete.

5. Click **OK**.

   The system deletes the snapshot file.

Configuring automatic snapshots

About this task

Use this procedure to take automatic backups on a designated server or on the local EMS server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore page.

3. Click the **Automatic Snapshot Configuration** tab.

   The system displays the Automatic Snapshot Configuration page. The **Summary** section displays the configuration for a previously saved backup, if one existed. Otherwise, the default setting of **Never** is displayed.

4. In the **Configuration** section, do the following:

   a. Select the snapshot frequency.

      The options are Never, Daily, Weekly, and Monthly.

   b. When the Weekly or Monthly option is selected, the system displays a group of Day(s) checkboxes. For example, Su, Mo, Tu, We, Th, Fr, and Sa.

   c. When the Monthly option is selected, the system displays an additional row of checkboxes for occurrence. For example, 1st, 2nd, 3rd, 4th, and Last.

5. In the **Time** field, select the time.

   When you type in the **Time** field, the system displays a Select Time pop-up.

6. Click **Save**.

Backup / Restore field descriptions

Snapshots tab

Name	Description
Date	The date and time at which the system captured the snapshot.
Build	The build number of the snapshot.
Description	The description of the snapshot.

Snapshot Servers tab

Name	Description
Name	A descriptive name to refer to the snapshot server being configured.
SFTP Host	The IP address and port number of the snapshot server to which backup files or snapshots are transferred by using secure FTP (SFTP).
User Name	The user name of the administrative account that is authorized to make system backups.
Location	The path (directory) on the snapshot server where the backup files will be stored and retrieved from.
Host Key	The key used to authenticate the login of the host.

Automatic Snapshot Configuration tab

Name	Description
Next Scheduled Backup	Information about the next scheduled backup.

Table continues…

Name	Description
	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 system 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 system displays this field only when the **Frequency** field is set to Monthly or Weekly.
Occurance	The week of the month on which the system begins automatic backup. The system displays this field only when the **Frequency** field is set to Monthly.

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 Avaya SBCE EMS web interface with administrator credentials.

2. From the task pane, select **System Management**.

   The system displays the System Management screen in the content area.

3. Click the **Shutdown** option corresponding to the Avaya SBCE security device you want to shutdown.

   The system displays a pop-up window to confirm your selection.

4. Click **OK**.

   The system displays a notification pop-up window when the device is successfully shut down.

Rebooting an Avaya SBCE security device

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Select **System Management** from the Task Pane.

   The System Management screen will be displayed in the Content Area, defaulting to the Devices tab display.

3. Click the **Reboot** option corresponding to the Avaya SBCE security device you want to reboot.

   A pop-up window will be displayed asking you to confirm your selection.

4. Click **OK**.

   A notification pop-up window will be displayed when the device has been successfully rebooted.

Restarting an Avaya SBCE application

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. From the task pane, select **System Management**.

   The system displays the System Management page.

3. On the **Devices** tab, click **Restart Application** corresponding to the Avaya SBCE security device that you want to restart.

   The system displays a confirmation pop-up.

4. Click **OK**.

   The system displays a notification pop-up when the device is successfully restarted.

Viewing device configuration

Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. From the task pane, select **System Management**.

   The system displays the System Management screen in the content area.
3. Click the **View** option corresponding to the Avaya SBCE security device whose configuration you want to view.

   The system displays a Device Configuration pop-up window.
4. Click the Cancel icon after viewing the configuration information.

Editing device configuration

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. From the task pane, select **System Management**.

   The system displays the System Management screen in the content area.
3. Click the Edit option corresponding to the Avaya SBCE security device whose configuration you want to edit.

   The system displays the Edit Device Configuration pop-up window.
4. Make the necessary changes, or click the **Cancel** icon to close the window without saving your changes.
5. Click **Finish**.

   The changes are saved to the Avaya SBCE configuration file. If you want to make additional changes to the Avaya SBCE configuration, see Chapter 8, Server and Network Interface Configuration.

Deleting device configuration

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. From the task pane, select **System Management**.

   The system displays the System Management page.
3. On the **Devices** tab, click **Uninstall** corresponding to the Avaya SBCE security device that you want to delete.

The system displays a confirmation pop-up to confirm your selection.

4. Click **OK**.

   The system 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 Avaya SBCE EMS web interface with administrator credentials.
2. From the task pane, select **System Management**.

   The system displays the System Management screen in the content area.
3. Click the **Updates** tab to display the System Management Updates screen.
4. Select an upgrade package.
5. 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 on to the Avaya SBCE EMS web interface with administrator credentials.
2. From the task pane, click **System Management**.

   The system displays a list of installed Avaya SBCE security devices in the content pane on the Devices tab.
3. Click the **Edit** button corresponding to the Avaya SBCE security device whose configuration you want to edit.

   The system displays the Edit Device Configuration pop-up window.
4. Select the **High Availability (HA)** checkbox.
5. In the **Device Pair** field, click a device.
6. Click **Finish** to save and exit.

From Release 7.0, Avaya SBCE provides 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Troubleshooting** > **Debugging**.

   The system displays the **Subsystem Logs** tab.
3. In the **Devices** section, select the Avaya SBCE device for which you want to manage log files.
4. Check or clear the field corresponding to the type of execution log that you want to enable or disable.
5. Click **Save**.

   The system 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.

Table continues…

Name	Description
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

Table continues…

Name	Description
SSH	Controls log levels for a third-party SSH library used for backup or restore and remote actions. The options are: • Inherit • Debug • Info • Warn • Error

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:

- View system-generated Call Detail Records (CDRs).
- Enable or disable Avaya SBCE security features.
- Configure SIP signaling message options.
- Designate signaling and media port ranges.
- Configure RTCP monitoring.
- Configure load monitoring.

Viewing a CDR file

Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.

   The system displays a list of installed Avaya SBCE security devices in the **Devices** section.
3. In the **Devices** section, select the Avaya SBCE device whose CDR files you want to view.

   The system displays a list of available CDR files in the content area for the selected Avaya SBCE security device.

   Note:

   The types of CDRs listed here are defined in the Application Rules screen in Miscellaneous area in the Edit Application Rule pop-up window. For more information, see *Application Rules*.
4. Select the CDR file that you want to view.

   The system displays a dialog box.
5. Click **Open with**, and select `EXCEL.EXE` to view the CDR file.
6. Click **OK**.

CDR file content

In the CDR file display, the value in the State column identifies the state of the call process at the time specified in the Time Stamp column on the associated information line. For example, Initiated, Established, or Terminated.

Definitions

State	Time Stamp
Initiated	The start time of the call
Terminated	The end time of the call
Established	The time that the call is established and the conversation can begin

Calculations

Terminated Time minus Initiated Time = Total Time
Terminated Time minus Established Time = Billable Time

Advanced Options field descriptions

CDR Listing

Name	Description
File Name	Specifies the name of the CDR file.
File Size (in bytes)	Specifies the size of the CDR file.
Last Modified	Specifies when the file was last modified.

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.

SIP Options tab

Name	Description
DNS Caching	Enables DNS Caching.
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 **Device Specific Settings** > **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.
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.
Port	Specifies the port number for RTCP monitoring.

Load Monitoring tab

Name	Description
Load Balancer Type	Type of load balancer.

Table continues…

Name	Description
	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.
Load Balancer IP	IP address of the load balancer.
Load Balancer Port	Port used by the load balancer.
Transport	Transport protocol used by the load balancer.
Listen IP	Load balancer listen IP address.

Security feature control

With the **Feature Control** tab of the **Advanced Options** function, you can enable or disable systemwide 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: **Global Parameters** > **DoS/DDoS**.

See DoS Security Features on page 218.

Managing security features

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. Click **Device Specific Settings** > **Advanced Options**.
3. Select **Advanced Options** in the Task Pane.

   The system displays a list of installed Avaya SBCE security devices in the application pane.
4. In the application pane, select the Avaya SBCE device whose security features you want to manage.
5. Click the **Feature Control** tab.

   The system displays the Feature Control screen.
6. 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.

7. 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. Click the **SIP Options** tab.

   Make your selections.
4. Click **Save**.

SIP options tab display field descriptions

Name	Description
DNS Caching	To enable or disable DNS Caching.
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.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. Click the **Network Options** tab.
4. 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 Avaya SBCE EMS web interface with administrator credentials.
2. Click **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options** in the Task Pane.

   The system displays a list of installed Avaya SBCE security devices in the application pane.
4. In the application pane, select the Avaya SBCE device whose security features you want to manage.
5. Select the **Port Ranges** tab in the Content Area.

   The system displays the Port Ranges screen.
6. Enter the beginning and ending port numbers for each field.
7. 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 using the **Signaling Interface** and **Media Interface** functions of the **Device Specific Settings** feature in the task pane.

Note:

The fixed ports for TCP, UDP, or TLS defined under **Device Specific Settings** > **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.
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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. On the Advanced Options page, click the **RTCP Monitoring** tab.
4. Select the **RTCP Monitoring** check box.
5. In the **Node Type** field, click one of the following options:
   - For DMZ Avaya SBCE configuration, click **DMZ**.

- For CORE Avaya SBCE configuration, click **Core**.
- For remote Avaya SBCE, click **Remote**.

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

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.

7. For CORE Avaya SBCE configuration, in the **Port** field, type the port number used for RTCP monitoring.
8. 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. Click **HA Pairs**.

   The system displays a list of installed Avaya SBCE security devices in the **Devices** section.
4. In the **Devices** section, select the Avaya SBCE security device.
5. Click **Edit**.

   The system displays the Edit HA Pairs Options page.
6. In the **Keep Alive Interval (Direct)** field, type the value in milliseconds.
7. In the **Max Retries tries** field, type the value for the number of retries.
8. 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 Avaya SBCE EMS web interface with administrator credentials.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.

   The system displays the Radius screen.
3. Select **Add**.

   The system displays the Add Server screen.
4. Enter the requested information into the appropriate fields.
5. Click **Finish**.

   The system 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 milliseconds) allowed for a successful authentication to be completed. If no successful authentication is completed within this time, the connection is automatically terminated and an incident is generated.
Max Retry	The maximum number of times a user can attempt to authenticate before the connection is terminated.
Ignore Session Expire	Checkbox used to indicate whether the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Selecting this box will cause the Avaya SBCE to maintain the current session upon receipt of the SESSION EXPIRE message. Leaving the box blank will cause the Avaya SBCE to terminate 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

Table continues…

Name	Description
	authenticate a user. Two selections are currently supported: Active Standby and Round Robin.
Authentication Protocol	The authentication protocol to be used for RADIUS authentication. Available options are: None, EAP_TTLS/EAP_ PAP, and 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 will be encrypted.
Confirm Server Secret	Respecifies the shared secret maintained between the Avaya SBCE security device and the active RADIUS server with which communications between the two will be encrypted.
Accounting Server	Checkbox indicating whether this RADIUS server is also to be designated as an Accounting Server and to receive CDRs. Selecting this box indicates that RADIUS server is also an Accounting Server and can receive CDRs. Leaving the box blank indicates that RADIUS server is not an Accounting Server and does not receive CDRs.

Editing an existing RADIUS server profile

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.

   The system displays the Radius screen.
3. Select the **Edit** button corresponding to the server profile that you want to edit.

   The system displays the Edit Server pop-up window.
4. Make your changes to the existing fields.
5. Click **Finish**.

   The system updates and saves the RADIUS server configuration.

Deleting an existing RADIUS server profile

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.

   The system displays the Radius screen.
3. Select **Delete** corresponding to the server profile that you want to delete.

   The system displays a confirmation pop-up window.
4. Click **OK** to confirm.

   The system deletes the selected RADIUS server configuration and updates the RADIUS tab.

Media Forking overview (Standard Platform only)

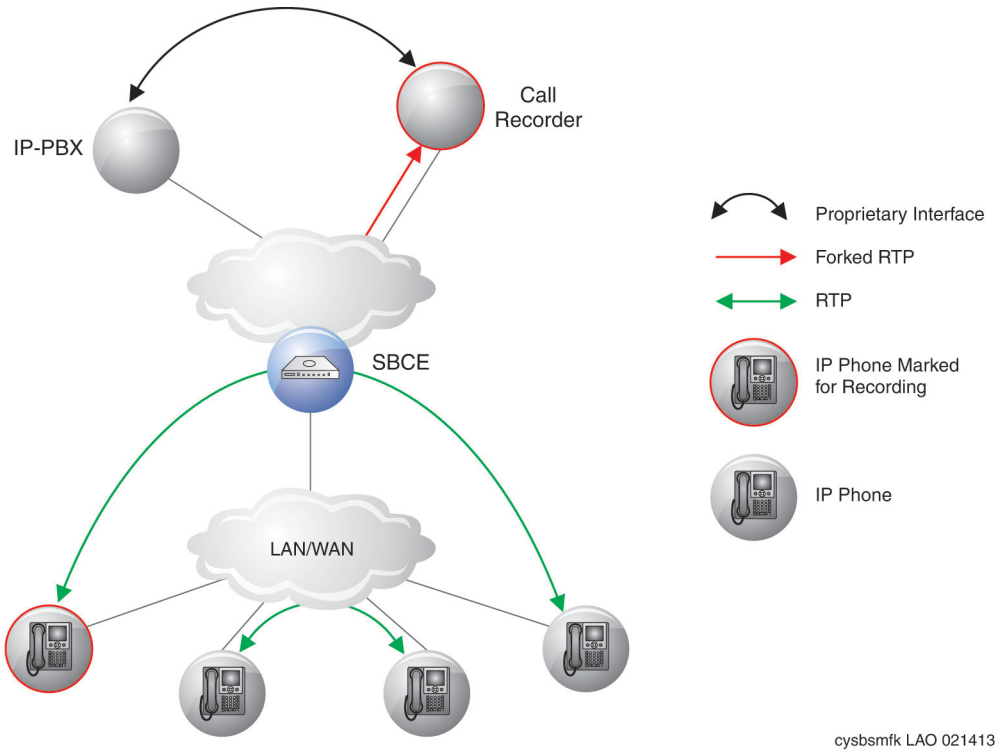
The Media Forking feature allows the Avaya SBCE device to fork media packets according to a designated Media Forking Profile. This solution addresses problems faced by call recorders deployed for quality assurance and compliance.

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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Media Forking**.
3. Enter a profile name, and click **Next**.

   The system displays the Add Media Forking Profile Edit screen.
4. Make the appropriate selections and entries.
5. Click **Finish**.

   The system displays the Media Forking Profile Information screen.

Media Forking Profile field descriptions

Note:

For configuring IP-PBX and the recording device, please refer to the individual manuals.

Name	Description
Call Scenario	Designate the type of call to be forked: • Hairpin Calls • Non-Hairpin Calls
Media Type	Select the part of the call to mirror: • Mirror Audio Stream • Mirror Video Stream • Mirror Other Streams
Mirror RTCP Stream	Designate whether to mirror the RTCP stream.
Quick Record Port	Specify the port number.
Ethernet Interface	Specify the interface.
Enable VLAN Tagging	If yes, select the **Enable VLAN Tagging** check box, and specify a VLAN ID and a protocol.
VLAN ID	Specify a VLAN ID. The range is 1 to 4095.
VLAN Protocol	Specify a protocol. The options are IEEE 802.1Q and Cisco ISL.
Destination MAC	Enter the correct destination MAC address.
Source MAC	Enter the correct 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:

- **Global Profiles** > **Media Forking**
- **Domain Policies** > **Session Policies** > **Media Forking**

Procedure

1. Click **Domain Policies** > **Session Policies**.

   The system displays the Session Policies page.
2. Select a Session Policy to add a Media Forking Profile.
3. Click **Media** > **Edit**.

   The system displays the Media page.
4. Select the **Media Anchoring** check box.

   The system enables the **Media Forking Profile** field.

5. In the **Media Forking Profile** field, click 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, see *Domain Policy Administration*. Ensure that the session flow matches with the required call recorders.

SNMP settings

About this task

Provisioning SNMP parameters (v1/v2 and 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 task pane, select the **SNMP** function from the Device Specific Settings feature.

   The system displays the SNMP screen that shows the contents of the SNMP v1/v2 tab. The Content Area contains two user-selectable tabs SNMP v1/v2 and SNMP v3 that provide access to global SNMP parameters.

   For new installations of Avaya SBCE 7.1, SNMP v1/v2 configuration is unavailable. From Release 7.1, vulnerable SNMP v1/v2 profile configuration has been removed to improve security. For Avaya SBCE instances that upgrade from an older release, options to configure SNMP v1/v2 profiles are still available.
3. Proceed to next the sections to 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.

Adding a new SNMP v1/v2 community

About this task

Use the following procedure to configure user access for SNMP v1/v2 information.

For new installations of Avaya SBCE 7.1, SNMP v1/v2 configuration is unavailable. From Release 7.1, vulnerable SNMP v1/v2 profile configuration has been removed to improve security. For Avaya SBCE instances that upgrade from an older release, options to configure SNMP v1/v2 profiles are still available.

Procedure

1. In the left navigation pane, click **Device Specific Settings** > **SNMP** > **SNMP v1/v2**.
2. In the Application Pane, in the Devices list, select the device for adding a new SNMP community. For example, EMS.
3. Click **Add**.

   The system displays the Add Community window.
4. In the **Community Name** field, type the name of the community that has access to the SNMP v1/v2 information.

   This name is the SNMP user password for that account.
5. In the **Trap IP address** field, type the IP address that receives the SNMP traps.
6. In the **Port** field, type the port number used for SNMP traps.

   If you do not enter a port number, the system uses port 162.
7. **(Optional)** To add more Trap IP addresses, click **Add**.

   You can add up to four Trap IP addresses for an SNMP v1/v2 community.
8. Click **Finish**.

Note:

For optimum security, enable only SNMP v3 with authentication and privacy modes. You can enable SNMP versions v1 and v2c, if required. However, customers must take responsibility for risks that can result from using SNMP versions v1 and v2c.

Editing an existing SNMP v1/v2 Community

Procedure

1. In the navigation pane, click **Device Specific Settings** > **SNMP**.
2. Click the **SNMP v1/v2** tab.

   For new installations of Avaya SBCE 7.1, SNMP v1/v2 configuration is unavailable. From Release 7.1, vulnerable SNMP v1/v2 profile configuration has been removed to improve security. For Avaya SBCE instances that upgrade from an older release, options to configure SNMP v1/v2 profiles are still available.
3. Select the **Edit** option corresponding to the community that you want to edit.

   The system displays the Edit SNMP Community window.
4. Edit the fields, and click **Finish**.

   The system saves the new field values and updates the SNMP v1/v2 tab.

Deleting an existing SNMP v1/v2 community

Procedure

1. In the navigation pane, click **Device Specific Settings** > **SNMP**.
2. Select the **Delete** option corresponding to the SNMP v1/v2 community that you want to delete.

   The system displays a confirmation pop-up window to confirm your selection.
3. Click **Yes** to delete the SNMP user.

   The system deletes the selected SNMP user and updates the **SNMP v1/v2** tab.

SNMP field descriptions

Add Community screen

Name	Description
Community Name	The name of the community that has access to the SNMP v1/v2 information.
Trap IP Address	The IP address that receives the SNMP traps. Users can specify up to four destinations with different IP addresses.
Port	The port number for SNMP traps. The default port number is 162.

SNMPv1/v2 tab

Name	Description
Community Name	The name of the community that has access to the SNMP v1/v2 information.
Set	The current status of SNMPv1/v2 traps.
Traps	The IP address that receives the SNMP traps. Users can specify up to four destinations with different IP addresses.

Add User screen

Name	Description
User Name	The assigned name or designation of the user being granted access to SNMP v3 data.
Authentication Scheme	The scheme to be used to authenticate the user before granting access to SNMP data. • **noAuthNoPriv**: The user is not authenticated and SNMP data is not encrypted. • **authNoPriv**: The user is authenticated, but SNMP data is not encrypted. • **authPriv**: The user is authenticated, and the SNMP data is encrypted.
AuthPassPhrase	The user password for authentication. This field is unavailable if you use the noAuthNoPriv Authentication Scheme.
Confirm AuthPassPhrase	The AuthPassPhrase for verification. This field is unavailable if you use the noAuthNoPriv Authentication Scheme.
Authentication Protocol	The type of authentication algorithm to be used 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 verification. This field is unavailable if you use the noAuthNoPriv or AuthNoPriv Authentication Scheme.

Table continues…

Name	Description
Privacy Protocol	The type of authentication algorithm used to encrypt the SNMP data (PrivPassPhrase). The types of authentication protocol available for SNMP data are: • AES • DES This field is unavailable if you use the noAuthNoPriv or AuthNoPriv Authentication Scheme.
Privilege	The type of privileges, Read or Read/Write, available to the user.
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.

SNMPv3 tab

Name	Description
User Name	The assigned name or designation of the user being granted access to SNMP v3 data.
Auth Schema	The scheme to be used to authenticate the user before granting access to SNMP data. • **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.
Auth Protocol	The type of authentication algorithm to be used 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
Priv Protocol	The privacy protocol used.
Privilege	The type of privileges, Read or Read/Write, available to the user.
Traps	The IP address, port, and trap profile in the format *IP address*:*Port*[*Trap Profile*]. Users can specify up to five destinations with different IP addresses.

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: Enabled or Disabled.

Adding SNMP v3 access

About this task

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

Procedure

1. In the Content Area, select the SNMP v3 tab.
2. Click **Add**.

   The system displays the Add User pop-up window.
3. Enter the requested information into the appropriate fields.
4. Select **Finish**.

   The SNMP v3 screen displays the new SNMP v3 account.

   Note:

   SNMP administration can also be done 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 for Release 7.0.1*.

Editing an existing SNMP v3 account

Procedure

1. In the Content Area, select the SNMP v3 tab.
2. Select the Edit option corresponding to the SNMP v3 account that you want to edit.

The system displays the Edit User pop-up window.

3. Edit the desired fields.
4. Click **Finish**.

Deleting an existing SNMP v3 account

Procedure

1. In the Content Area, select the SNMP v3 tab.
2. Select the Delete option corresponding to the SNMP v3 account that you want to delete.

   The system displays a confirmation pop-up window to confirm your selection.
3. Select **Yes** to delete the SNMP user.

   The system deletes the selected SNMP v3 user and updates the SNMP v3 tab.

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 system uses the default trap profile for SNMP v1 and v2 users.

Procedure

1. In the left navigation pane, click **Global Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
2. Click **Add**.
3. In the **Profile Name** field, type the name of the profile.
4. Click **Finish**.

   The system displays the new profile with a list of SNMP traps, which are grouped in the Security and Systems categories. All traps are enabled by default.

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%

Table continues…

Trap name	Description	Level
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
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. In the left navigation pane, click **Global Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
2. Select the profile that you want to edit.

   Note:

   You cannot edit the default SNMP profile.
3. Click the description pane above the **SNMP Traps** tab.

   The system displays an Update Description window.
4. In the **Update Description** field, type a description of the new profile and click **Finish**.
5. Locate the category of the trap that you want to change, and click **Edit**.
6. Select or clear traps as required, and click **Finish**.

   The system displays the updated SNMP trap profile.

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. In the left navigation pane, click **Global Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
2. Click the profile that you want to delete.
3. Click **Delete**.

   The system displays a message to confirm whether you want to continue deleting the profile.
4. Click **OK**.

   The system deletes the SNMP profile.

Cloning an SNMP trap profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
2. Click the profile that you want to clone.
3. Click **Clone**.
4. In the **Clone Name** field, type a name for the cloned profile.
5. Click **Finish**.

Renaming an SNMP trap profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **SNMP Traps**.

   The system displays the SNMP Traps Profiles screen with the existing trap profiles.
2. Click the profile that you want to rename.
3. Click **Rename**.
4. In the **New Name** field, type a new name for the profile and click **Finish**.

Adding a management server

Procedure

1. In the left navigation pane, click **Device Specific Settings** > **SNMP**.
2. Click the **Management Servers** tab.
3. Click **Add**.

   The system displays the Add IP Address screen.

4. In the **IP Address(es)** field, type one or more server IP addresses separated by commas or new lines.
5. 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. In the left navigation pane, click **Device Specific Settings** > **SNMP**.
2. Click the **Traps Severity Settings** tab.

   The **Traps Severity Settings** tab contains the following trap severities: Critical, minor, major, and informational. The tab also contains the status for each trap severity.
3. Click the status displayed against the trap severity that you want to disable.

   The system 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 system displays **Enabled** against a trap severity, when you click **Enabled**, the system disables all traps with that severity .
4. 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.

Related links

Creating a new Time of Day rule on page 197
Cloning an existing Time of Day rule on page 198
Editing an existing Time of Day rule on page 199
Renaming an existing Time of Day rule on page 199
Deleting an existing Time of Day rule on page 200

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 left navigation pane, click **Global Profiles** > **Time of Day Rules**.

   The left Application pane displays the existing ToD Rule sets, and the content pane displays the parameters of the ToD Rule set.
3. In the Applications pane, click **Add**.

   The system displays the ToD Rule window.
4. Enter a name for the new ToD Rule and click **Next**.

   The system displays the second ToD Rule window.
5. Enter the appropriate ToD parameters, and click **Finish**.

   The Navigation pane displays the newly added Time-of-Day Rules.

Related links

Time of Day (ToD) rules on page 196
Time of Day field descriptions on page 197

Time of Day field descriptions

Name	Description
Rule Name	Specifies the name of the rule
Date	
Start Date	Specifies the day on which the ToD rule will automatically take effect. Click the Calendar icon to select the desired day.
Now	Indicates that the ToD rule is to take effect immediately.
End Date	Specifies the day on which the ToD rule will automatically end. Click the Calendar icon to select the desired day.
Never End	Indicates that the ToD rule is to remain in effect in perpetuity or until such time as an End Date is distinctly defined.
Time	

Table continues…

Name	Description
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.

Related links

Creating a new Time of Day rule on page 197

Cloning an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Time of Day Rules**.

   The left application pane displays the existing ToD Rule sets, and the content pane displays the parameters comprising the selected ToD Rule set.
3. In the Application Pane, select the name of the ToD Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.

   The system displays the Clone Rule pop-up window.
5. Enter a name for the new ToD Rule, and select **Finish** to save your changes.

   The system displays the ToD Rules screen again, showing the newly cloned ToD Rule.

Related links

Time of Day (ToD) rules on page 196

Editing an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global 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.
3. 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.
4. Click **Edit**.

   The system displays the Edit Time of Day Rule screen.
5. Edit the appropriate fields.
6. Click **Finish** to save and exit.

   The system displays the ToD Rules screen again.

Related links

Time of Day (ToD) rules on page 196

Renaming an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Time of Day Rules**.

   The left Application pane displays the rule sets, and the content pane displays the parameters of the selected ToD Rule set.
3. On the Application Pane, select the name of the ToD Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.

   The system displays the Rename Rule pop-up window.
5. Enter the new name for the ToD Rule, and select **Finish** to save your changes .

   The system displays the ToD Rules screen again, showing the newly-renamed ToD Rule.

Related links

Time of Day (ToD) rules on page 196

Deleting an existing Time of Day rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Time of Day Rules**.

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

   The system displays a delete confirmation pop-up window.
5. Click **OK**.

Related links

Time of Day (ToD) rules on page 196

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.

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, click **Global Profiles** > **Routing**.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected routing profile.
3. In the Application Pane, click **Add**.
4. Type a distinctive name for the new Routing Profile, and click **Next**.
5. Enter the requested information into the appropriate fields.

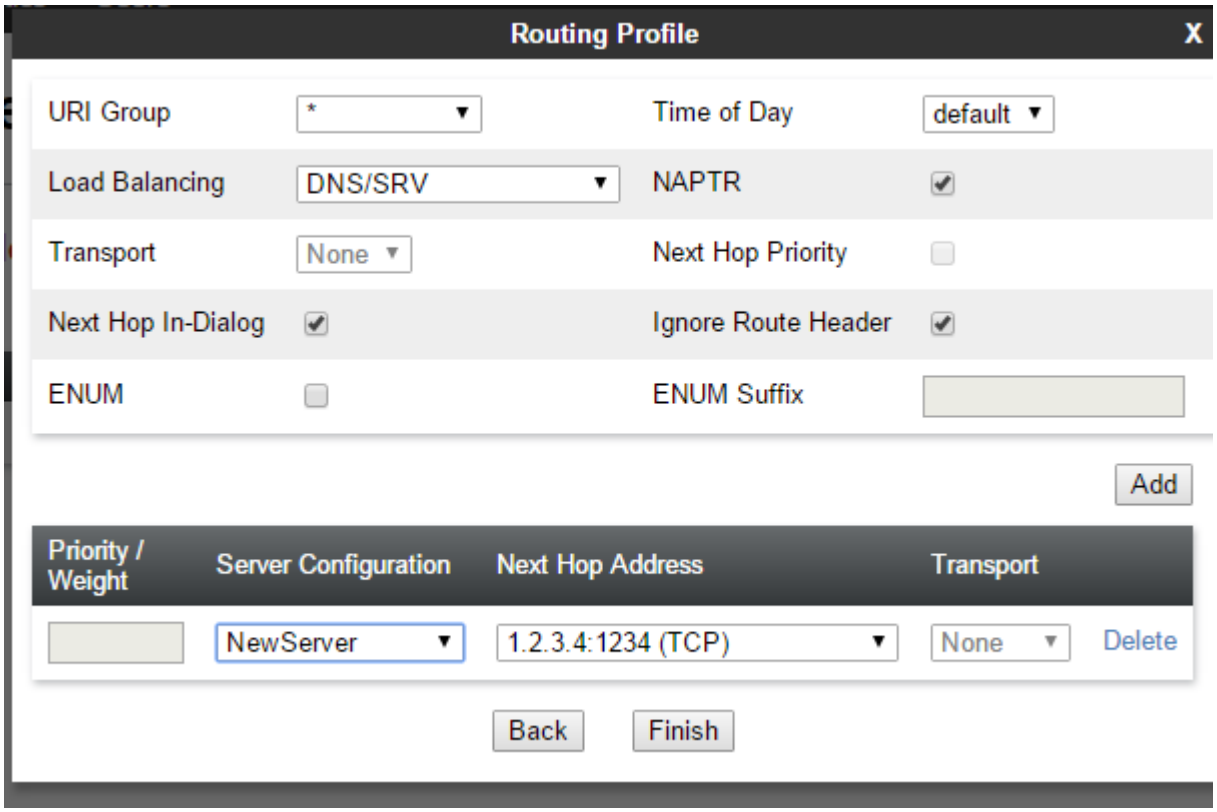
   To use alternate routing, ensure that you set the **Trans Expire** field on the **Timers** tab from **Global Profiles** > **Server Interworking** to an appropriate short duration. Any request sent from the server times out if a response is not received within the time set as the transaction

expiration timer. Therefore, alternate routing does not work if the **Trans Expire** field is set to the default value of 32 seconds.

6. Click **Finish**.

   The Application Pane displays the new Routing profile.

Example



Add routing profile field descriptions

Name	Description
URI Group	Specifies the URI Group to which the next hop routing profile applies. The options are: • * • Emergency
Time of Day	Specifies time of day for the trunk server to resolve the routing profile. **Note:** For remote users, do not use the **Time of Day** profile to resolve the routing profile.

Table continues…

Name	Description
Load Balancing	Specifies the type of load balancing option. The options are: • Priority • Round-Robin • Weighted Round-Robin • DNS/SRV
Transport	Specifies the next hop address that you must configure. Alternately, select the transport type. The system uses the routing profile transport type to route the message.
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 will try to use the same routing entry to route the message.
NAPTR	Activates or deactivates Naming Authority Pointer. When you select the Load Balancing algorithm as DNS/SRV, the system enables the NAPTR check box. If you disable NAPTR, you must specify the transport protocol.
Next Hop Priority	Specifies if the Next Hop Priority option is enabled and SBC fails to route the message using resolved routing entry from message, that is using request URI or Route Header, then the system will send the message to the alternate routing entry from the routing profile.
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.
Add	Adds a next hop address.
Priority / Weight	Specifies the priority and weight assigned for load balancing options.
Server Configuration	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.

Table continues…

Name	Description
	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 Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Applications Pane, select the routing profile to which you want to add a new routing rule.
4. Select **Add** in the Content Area.

   The system displays the Add Routing Rule pop-up window.
5. In the Add Routing Rule pop-up window, enter the desired fields and click **Finish** when done.

   The system saves the new routing rule and updates the Add Routing Rule display.

Editing a routing rule

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.

3. In the Applications Pane, select the routing profile.
4. Click the **Edit** option corresponding to the routing rule that you want to edit.

   The system displays the Edit Routing Rule pop-up window.
5. Edit the desired fields.
6. Select **Finish**.

   The system saves the changes and updates the Routing Profile display.

Deleting a routing rule

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Applications Pane select the routing profile whose routing rule you want to delete.
4. Click the **Delete** option corresponding to the routing rule that you want to delete.

   The system displays the Delete Confirmation pop-up window.
5. Click **OK**.

   The system deletes the routing rule and updates the Routing Profile display.

Reordering routing rule precedence

About this task

Use the following procedure to reorder the precedence of Session Flows.

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Applications Pane select the routing profile whose routing rules you want to reorder.
4. Change the number in the Order column to reflect the order or precedence in which you want the routing rules to be executed.
5. Click **Update Order**.

   The system 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 Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Application Pane, select the routing profile that you want to clone.
4. In the Content Area, click **Clone**.

   The system displays the Clone Profile pop-up window.
5. Provide a name for the cloned Routing profile.
6. Click **Finish**.

   The system clones and renames the Routing profile.

Renaming an existing routing profile

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Application Pane, select the routing profile that you want to rename.
4. In the Content Area, click **Rename Profile**.

   The system displays the Rename Profile pop-up window.
5. Enter a new name for the routing profile.
6. Click **Finish**.

   The system renames the selected routing profile and updates the Routing Profile screen.

Deleting an existing routing profile

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the Routing function from the Global Profiles feature.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected Routing profile.
3. In the Application Pane, select the routing profile that you want to delete.
4. Click **Delete**.

   The system displays the Delete Confirmation pop-up window.
5. Click **OK**.

   The system 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Syslog Management**.

   The system displays the Syslog Management page.
3. In the **Devices** section, click the Avaya SBCE security device for which you want to configure log-level information.

4. In the **Facility** field, click the desired log collection facility for each class of logs and the types of information to be collected.

   The options are: Platform, Trace, Security, Protocol, Incident, Registrations, and Audit.

   The types of information level are: Info, Notice, Warning, Error, Critical, Alert, and Emergency.

5. Click **Save**.

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 system reserves log collection facilities LOG_LOCAL5 and LOG_LOCAL6 for audit logs.
All	Selects all information levels for a log class.

Table continues…

Name	Description
	If you select the **All** check box in the table header, the system 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 system 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 system selects the Notice information level for all log classes.
Warning	Selects the Warning information level for a log class. If you select the **Warning** check box in the table header, the system 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 system 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 system 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 system 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 system 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

Table continues…

Name	Description
	The system reserves log collection facilities LOG_LOCAL5 and LOG_LOCAL6 for audit logs.
Destination location	The path where the system 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 system 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

Table continues…

Name	Description
	• 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Parameters** > **User Agents**.

   The system displays the User Agents page.
3. On the User Agents page, click **Add**.

   The system displays the Add User Agents page.
4. In the **Name** field, type a name to identify the user agent.
5. In the **Regular Expression** field, you can either type an exact match of the internal ID of the user agent phone, or you can type a regular expression matching multiple phones with similar IDs.
6. 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Parameters** > **User Agents**.
3. On the User Agents page, click **Edit** corresponding to the user agent type that you want to edit.

   The system displays the Edit User Agent page.
4. Edit the user agent as necessary, and click **Finish**.

   The system displays the changes made to the user agent in the User Agents display.

Viewing authorized user agents (Advanced Services only)

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Parameters** > **User Agents**.

   The system displays the User Agents page.

Deleting an existing user agent (Advanced Services only)

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Parameters** > **User Agents**.
3. On the User Agents page, click **Delete** corresponding to the user agent type that you want to delete.

   The system displays a delete confirmation pop-up window.
4. Click **OK**.

   The system deletes the user agent from the User Agents display.

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 Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the **Signaling Interface** function of the Device Specific Settings feature.

   The system displays the Signaling Interface screen.
3. Click **Add**.

   The system displays the Add Signaling Interface pop-up window.
4. Enter the requested information into 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.
5. Click **Finish**.

   The system displays the new configuration in the Signaling Interface screen.

Add signaling interface field descriptions

Name	Description
Name	The name of this profile.
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 certificate for TLS port specified above. The checkbox is disabled when no TLS Port value is specified.
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 enable 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. In the Signaling Interface display, select the **Edit** option corresponding to the Signaling Interface configuration that you want to edit.

   The system displays the Edit Signaling Interface pop-up window.

2. Edit the configuration as necessary, and click **Finish**.

   The system saves the changes and updates the Signaling Interface screen.

Viewing an existing signaling interface

Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. On the Task Pane, select the **Signaling Interface** function of the Device Specific Settings feature.

   The system displays the Signaling Interface page.

3. In the Application Pane, select the Avaya SBCE device to display the Signaling Interface parameters for that device.

Deleting an existing signaling interface

Procedure

1. In the Signaling Interface display, select the **Delete** option corresponding to the Signaling Interface configuration that you want to delete.

   The system displays the delete confirmation pop-up window.

2. Click **OK**.

   The system deletes the Signaling Interface configuration.

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. On the Task Pane, select the **Media Interface** function of the Device Specific Settings feature.

   The Media Interface screen is displayed.
3. In the Application Pane, select the Avaya SBCE device whose parameters you want to view.

   The system displays the Media Interface parameters for the device.

Adding a new media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the Task Pane, select the **Media Interface** function of the Device Specific Settings feature.

   The system displays the Media Interface screen.
3. Click **Add** on the Media Interface tab.

   The system displays the Add Media Interface pop-up window.
4. Enter the requested information into the appropriate fields in the new information line.
5. Select **Finish**.

   The system displays the new configuration in the Media Interface display.

Add media interface field descriptions

Name	Description
Name	The name of this profile.
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 for media traffic.

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 SBCEwith the ports in the data firewall. If the user has no data firewall, no action is required.

Editing an existing media interface

Procedure

1. In the Media Interface display, select the **Edit** option corresponding to the Media Interface configuration that you want to edit.

   The system displays the Edit Media Interface pop-up window.

2. Edit the configuration as necessary, and select **Finish**.

   The system saves the changes and updates the Media Interface display.

Deleting an existing media interface

Procedure

1. In the Media Interface display, select the **Delete** option corresponding to the Media Interface configuration that you want to delete.

   The system displays the Delete Confirmation pop-up window.

2. Click **OK** to confirm.

   The system deletes the Media Interface configuration.

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 230

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 218.

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. The current release of Avaya SBCE supports DoS activity reporting for certain time periods.

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: **Device Specific Settings** > **Advanced Options** > **Feature Control**.

For more information, see the *Security Configuration and Best Practices Guide*.

Viewing DoS/DDoS settings

About this task

Use the following procedure to view the current DoS/DDoS settings.

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. In the task pane, click **Global Parameters** > **DoS / DDoS**.

   The DoS Settings page displays the **Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Whitelist** tabs.
3. 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 218

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.

Table continues…

DoS attack type	Description
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.
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.

Editing DoS/DDoS settings

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. Click **Global Parameters** > **DoS/DDoS**.

   The system displays the DoS Settings screen.
3. Select the tab containing the DoS/DDoS settings that you want to edit.

   The Content Area displays the selected DoS/DDoS settings.
4. Click the **Edit** icon corresponding to the DoS/DDoS settings that you want to edit.

   The system displays the Edit Response screen.
5. On the Edit Response screen, perform one of the following actions:
   - Edit the fields, and click **Finish**.
   - Click **Cancel**. The system restores the fields to the previous values and closes the window without saving.

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.

Table continues…

Name	Description
	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.
Threshold (over 3 seconds)	The maximum number of sessions that can be started within 3 seconds.
Action	The action to be performed when any thresholdis 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 timeslots in which DoS attacks are monitored. The options are: • Morning (0600–1159) • Afternoon (1200–1759) • Evening (1800–2359)

Table continues…

Name	Description
	• 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.
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.

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.

Viewing a Domain DoS profile

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. Click **Global 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.
3. Select the Domain DoS profile you want to view.

   The Content Area displays the Rate Limit parameters corresponding to the selected Domain DoS profile.

Adding a new Domain DoS profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **Domain DoS**.
2. Click **Add**.

   The system displays the Add Domain DoS window.
3. In the **Profile Name** field, type the new profile and click **Next**.
4. Choose the Traffic Type.

   If you choose Trunk Traffic in the **Traffic Type** field, you can only enter the number of maximum number of concurrent sessions. If you choose Remote User or Trunk Traffic and Remote Users for the **Traffic Type** field, you must enter the maximum number of concurrent sessions and the number of remote users.

Note:

When you click **Recalculate Values** on the **Rate Limit** tab after the profile has been created, the system displays a Recalculate Thresholds window. The fields on this window are the same as those on the Add Domain DoS window.

5. Click **Finish**.

   The system saves the new Domain DoS profile and displays the Domain DoS screen.

Cloning an existing Domain DoS profile

About this task

Use the following procedure to make a copy or clone of an existing Domain DoS profile.

Procedure

1. From the left navigation pane, click **Global Profiles** > **Domain DoS**.
2. From the application pane, click the Domain DoS profile you want to clone.
3. Click **Clone**.

   The Clone Domain DoS window is displayed.
4. In the **New Name** field, type a name for the cloned profile and click **Finish**.

   The system saves the cloned Domain DoS profile and displays the Domain DoS screen.

Renaming an existing Domain DoS profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **Domain DoS**.
2. Click the Domain DoS profile that you want to rename.
3. Click **Rename**.

   The system displays the Rename Domain DoS window.
4. In the **New Name** field, type a new name for the profile and click **Finish**.

   The system saves the new name and displays the Domain DoS screen.

Editing an existing Domain DoS profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **Domain DoS**.
2. Click the Domain DoS profile that you want to edit.

3. In the **Rate Limit** tab, navigate to the SIP service or method that you want to edit and click **Edit**.
4. In the Edit Domain DoS window, edit the fields as desired.
5. 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 224

Domain DoS profile field descriptions

Domain DoS screen

Name	Description
Traffic Type	The type of traffic.
Max Concurrent Sessions	Maximum number of concurrent sessions
Number of Remote Users	Number of remote users for the DoS profile
SIP Service	SIP service affected by the DoS attack. The available options include TOTAL, Registrations, Calls, Presence Updates, Subscriptions, Misc.
SIP Method	The SIP Method that is displayed here in the Edit window is a reflection of the service, that is, All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or OPTIONS edited from the Domain DoS screen.
Initiated Threshold (per 10 seconds)	The maximum number of sessions that can be started within a 10 second period.
Pending Threshold	The maximum number of pending session initiations.
Failed Threshold (per 10 seconds)	Maximum number of failed session initiations.
Action	The action to be performed should any of the above thresholds be exceeded. The following options are available: • 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

Table continues…

Name	Description
	Note: The SIP Challenge action should not be selected 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 the 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: 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

Deleting a Domain DoS profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **Domain DoS**.
2. Click the Domain DoS profile that you want to delete.
3. Click **Delete**.

   The system displays a confirmation window to confirm your selection.
4. Click **OK**.

   The system deletes 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 on to the EMS web interface with administrator credentials.

2. In the left navigation pane, click **Device Specific Settings** > **Troubleshooting** > **DoS Learning**.

   The system displays the Learned Information screen with a list of installed Avaya SBCE devices.

3. Select the Avaya SBCE security device whose DoS activity you want to learn.
4. In the **Learned Information** tab, select the time period for which you want to learn the DoS activity.
5. Select **Update**.

   The **Learned Information** tab displays the DoS activity detected for the specified time period.

Related links

DoS Learning field descriptions on page 226

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 225

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 102.

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 229 and Installing a scrubber rules Package on page 227 respectively.

Viewing scrubber rules

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the navigation pane, click **Global Parameters** > **Scrubber**.

   The system displays the Scrubber screen.
3. Click the **Rules** tab.

   The system displays all installed scrubber rules and templates.

Installing a scrubber rules package

Procedure

1. In the navigation pane, click **Global Parameters** > **Scrubber**.

2. Click the **Packages** tab.
3. Click **Install Package**.

   The system displays the Install Scrubber Package window.
4. Click **Browse** and navigate to the directory containing the chosen scrubber package.
5. Select the scrubber package.
6. Click **Install**.

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

   Note:

   The Scrubber must be enabled in the Security Rules of Domain Policies before it takes effect. Once the Scrubber is enabled in the Security Rules of Domain Policies, a list of packages would be needed for the Security Rule.

Related links

Security rules on page 102

Configuring scrubber actions

Procedure

1. In the left navigation pane, click **Global Parameters** > **Scrubber**.
2. On the **Rules** tab, select a package and click **Edit**.
3. 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

Scrubber 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.

Enabling or disabling an installed Scrubber Rules package

Before you begin

Ensure that the Scrubber Rules package is installed and enabled.

About this task

Note:

Use this procedure to enable the package so that the rules take effect.

Procedure

In the Content Area, click the **Toggle** button corresponding to the scrubber package that you want to enable or disable.

The selected scrubber package is enabled or disabled.

Deleting a Scrubber Rules package

Procedure

1. In the Content Area, click the **Delete** icon corresponding to the scrubber package that you want to delete.

   The system displays a Delete Confirmation pop-up window.

2. Click **OK**.

   The system deletes the selected Scrubber package.

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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.

   The system displays the existing topology hiding profiles and the corresponding topology headers.
3. Click **Add**.

   The system displays the Topology Hiding Profile screen.
4. In the **Profile Name** field, type a name for the new profile and click **Next**.
5. In the **Header** field, click one of the following options:
   - Request-Line
   - From
   - To
   - Record-Route
   - Via
   - SDP
   - Refer-To
   - Referred-By
6. In the **Criteria** field, click one of the following options:
   - IP/Domain
   - IP
   - Domain
7. In the **Replace Action** field, click one of the following options:
   - Auto
   - Next Hop
   - Destination IP
   - Overwrite
   - Signaling Interface

   If you select the **Overwrite** action, you must type an IP address in the **Overwrite Value** field.

8. Click **Finish**.

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

Related links

Protocol scrubber on page 226

Topology Hiding Profiles field descriptions

Name	Description
Header	The name of the header that will be changed with topology hiding. The options are: • **Request—Line** • **From** • **To** • **Record-Route** • **Via** • **SDP** • **Refer-To** • **Referred-By**
Criteria	The criteria that are changed with topology hiding. The options are: • **IP/Domain** • **IP** • **Domain** **Note:** Ensure that the values in the **Header** field and the **Criteria** field with topology hiding are same. For example, if you are not sure about the value of the **Header** field, configure the **Criteria** field with topology hiding as **IP/Domain**. If the **Header** is: • **IP** : Configure the **Criteria** field with topology hiding as IP. • **Domain** : Configure the **Criteria** field with topology hiding as Domain.
Replace Action	The data that replaces the header.

Table continues…

Name	Description
	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**.

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.

Note:

Before Avaya SBCE Release 4.0.4, this section was titled Adding a New Topology Hiding Rule. From Release 4.0.4, Topology Hiding rules are now based on headers instead of rules and URI groups.

Procedure

1. In the left navigation pane, click **Global Profles** > **Topology Hiding**.
2. In the application pane, click the Topology Hiding Profile to which you want to add a new Topology Hiding Header.
3. Click **Edit**.

   The system displays the Edit Topology Hiding Profile window.
4. Click **Add Header** button.

   The system adds a new Header description row.

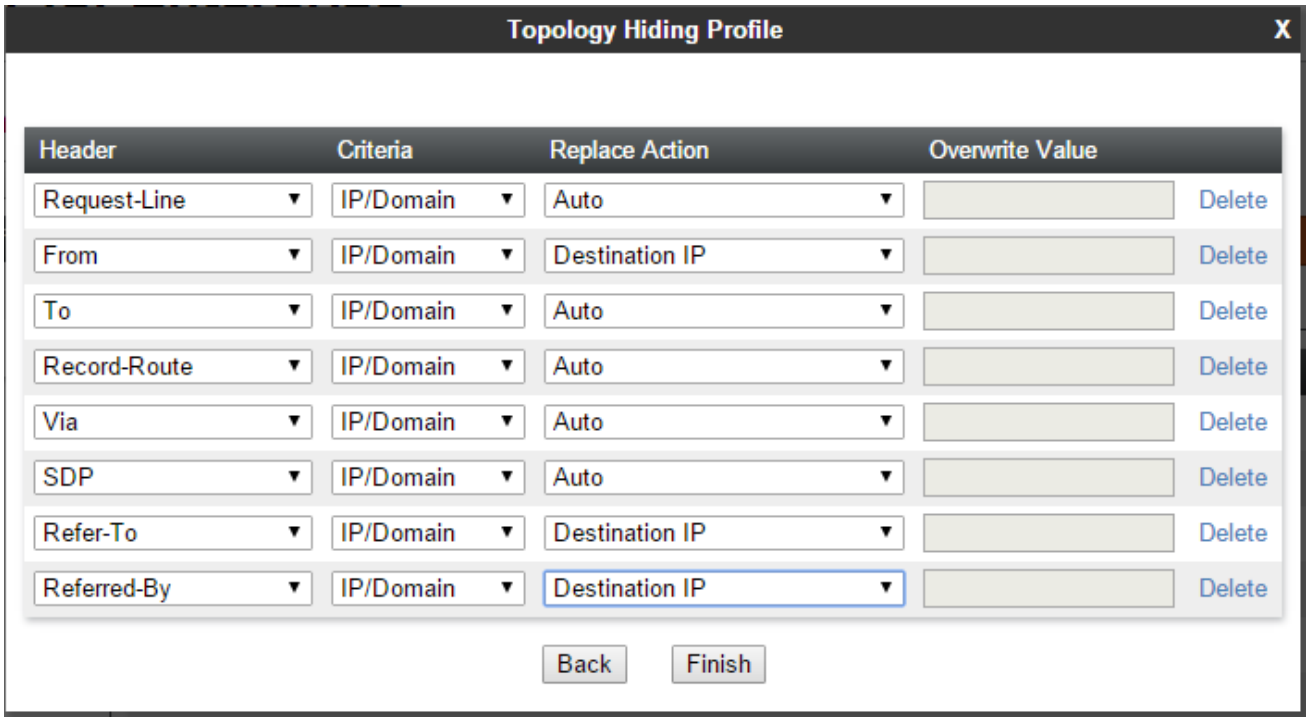
   Note:

   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.
5. In the new **Header** field, use the default value or select another unused Header parameter name for the new Topology Hiding Header.
6. 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.
7. Click **Finish**.

The Topology Hiding Profile screen now contains the new header.

Example



Editing a Topology Hiding Header

About this task

Use this procedure to edit and delete headers added to a Topology Hiding Header.

Procedure

1. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.
2. Click the Topology Hiding Profile containing the Topology Hiding header that you want to edit.
3. In the **Topology Hiding** tab, click **Edit**.
4. Select new values, as required, for the **Header**, **Criteria**, and **Release Action** fields.
5. Click **Finish**.

Deleting a Topology Hiding profile

Procedure

1. In the left navigation pane, click **Global Profles** > **Topology Hiding**.
2. Click the Topology Hiding Profile that you want to delete.

3. Click **Delete**.

   The system displays a message to confirm whether you want to proceed with deleting the profile.

4. Click **OK**.

Deleting a Topology Hiding header

Procedure

1. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.
2. Click the Topology Hiding Profile that contains the Topology Hiding Header you want to delete.
3. In the **Topology Hiding** tab, click **Edit** .
4. In the Edit Topology Hiding Profile window, locate the Topology Hiding Header that you want to delete, and click **Delete**.

   The system removes the deleted header from the Edit Topology Hiding Profile window.

5. Click **Finish**.

Cloning a Topology Hiding profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.
3. Click the Topology Hiding Profile that you want to clone.
4. Click **Clone**.

   The system displays the Clone Profile window.

5. 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.

Renaming a Topology Hiding profile

Procedure

1. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.
2. Click the Topology Hiding Profile that you want to rename.
3. In the Content Area, click **Rename Profile**.

The system displays the Rename Profile window.

4. In the **New Name** field, type a new name and click **Finish**.

   The application pane displays the renamed profile.

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 235 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 236, 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.

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	

Table continues…

Main Header names	Headers affected by Main Header	Header affecting this header
Referred-By		From
PAsserted Identity		From
Destination Headers		
To	ReferTo	
Request Start Line		
Refer To		To
Diversion		
SDP Headers		
Origin Header		

Topology Hiding settings examples

This section provides examples of all possible combinations of topology hiding settings listed in the **Header** field. Each **Header** type is combined with each combination of the **Criteria** type and **Replace Action** type along with a description of the resulting action or effect.

Topology Hiding examples for Request-Line Header

1. Topology Hiding replaces the **Request-Line** header with the next hop address or domain from the routing profile. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the **Request-Line** header with the next hop address or domain from the routing profile. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **Request-Line** header with the Destination **IP/Domain** from the SIP message. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain
   - Replace Action: Destination IP
4. Topology Hiding replaces the **Request-Line** header with the **Overwrite Value**. This scenario occurs in the following settings:
   - Header: Request-Line
   - Criteria: IP/Domain
   - Replace Action: Overwrite

Topology Hiding examples for From header

Note:

The **From** header setting affects the **Referred-By** header and the **P-Asserted-Identity** header. The **To** header setting does not affect **Referred-By** and **P-Asserted-Identity**. When you select the **From** header settings, the **Referred-By** header and **P-Asserted-Identity** header are automatically updated.

1. If the SIP message is from the Subscriber side, then Topology Hiding replaces the **From** Header with the next hop address or domain from the routing profile. If the SIP message is from the Call Server side or Trunk Server side, then Topology Hiding replaces the **From** Header with the Signaling Interface. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Auto
2. Topology Hiding replaces the **From** header with the next hop address/domain from the Routing profile. This scenario occurs in the following setting:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **From** header with the Destination IP from the SIP Message. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Destination IP
4. Topology Hiding replaces the **From** header with the Signaling Interface IP/Domain. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Signaling Interface
5. Topology Hiding replaces the **From** header with the Overwrite Value. This scenario occurs in the following settings:
   - Header: From
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Overwrite

Topology Hiding examples for To header

Note:

The **To** header setting only affects the **Referred-To** header.

1. If the SIP message endpoint type is Subscriber, then Topology Hiding replaces the **To** header with the Next Hop Address used by the Signaling Interface. If the SIP message

endpoint type is Call Server or Trunk Server, then Topology Hiding replaces the **To** header with the Next Hop Address. This scenario occurs in the following settings:

- Header: To
- Criteria: IP/Domain or IP or Domain
- Replace Action: Auto

2. Topology Hiding replaces the **To** header with the Next Hop Address/Domain from the Routing profile. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Next Hop
3. Topology Hiding replaces the **To** header with the Destination IP from the SIP Message. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Destination IP
4. Topology Hiding replaces the **To** header with the Signaling Interface IP/Domain. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Signaling Interface
5. Topology Hiding replace the **To** header with the **Overwrite Value**. This scenario occurs in the following settings:
   - Header: To
   - Criteria: IP/Domain or IP or Domain
   - Replace Action: Overwrite

Topology Hiding examples for Record-Route header

Topology Hiding stores the IP/Domain from the outbound message **Record-Route** header and then removes the **Record-Route** header from the outbound message. When the inbound message is received, Topology Hiding puts the stored IP/Domain in a **Record-Route** header and adds the header to the inbound message. This scenario occurs in the following settings:

- Header: Record-Route
- Criteria: IP/Domain or IP or Domain
- Replace Action: Auto

Topology Hiding examples for Via header

Topology Hiding stores the IP/Domain from the outbound message **Via** header and then removes the **Via** header. When the inbound message is received, Topology Hiding puts the stored IP/Domain

in a **Via** header and adds the header to the inbound message. This scenario occurs in the following settings:

- Header: Via
- Criteria: IP/Domain or IP or Domain
- Replace Action: Auto

If Trunk and Call server support Via header format RFC 3261, Avaya 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.

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

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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. Click **Add**.

   The system displays the Add Server Configuration Profile page.
4. In the **Profile Name** field, type a name for the new server profile, and click **Next**.
5. On the Add Server Configuration Profile page, type the requested information in the appropriate fields.

6. Click **Next**.

   The system displays the Add Server Configuration Profile - Authentication page.

7. On the Add Server Configuration Profile - Authentication page, type the requested information in the appropriate fields.

8. Click **Next**.

   The system displays the Add Server Configuration Profile - Heartbeat page.

   Note:

   The system does not display the Add Server Configuration Profile - Heartbeat page for Remote Branch Office servers.

9. On the Add Server Configuration Profile - Heartbeat page, type the requested information in the appropriate fields.

10. Click **Next**.

    The system displays the Add Server Configuration profile - Advanced page.

11. On the Add Server Configuration profile - Advanced page, type the requested information in the appropriate fields.

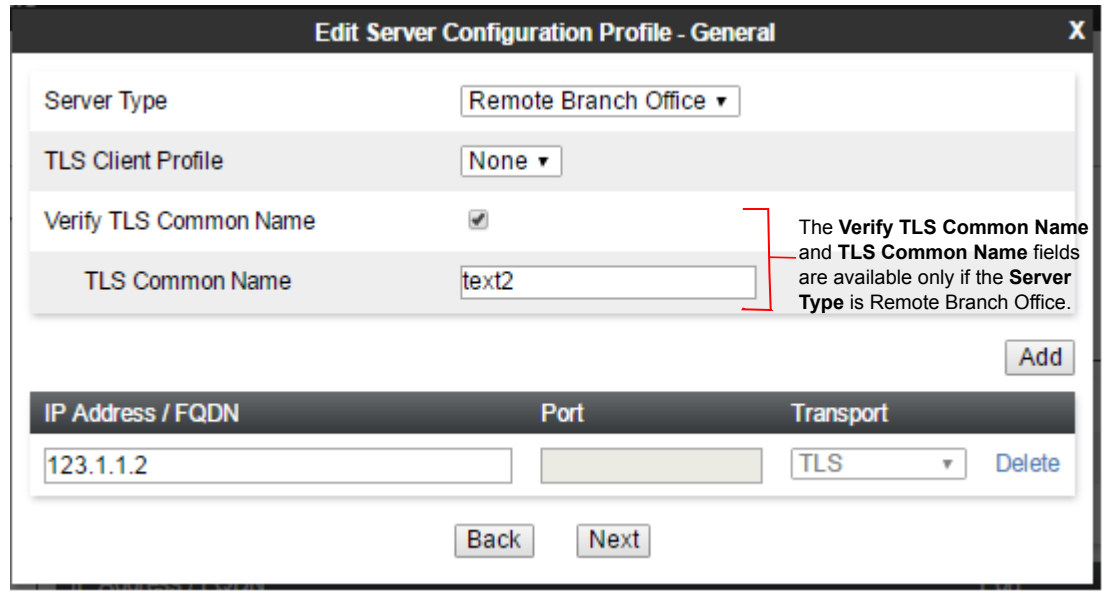
    Note:

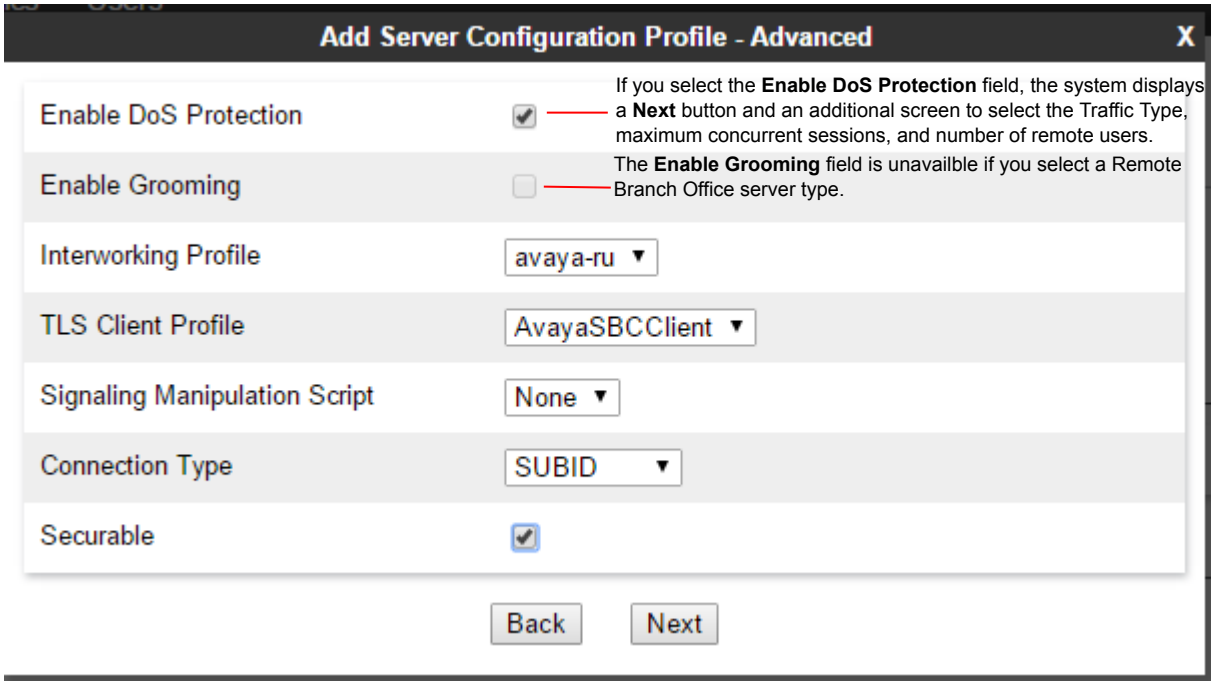
    When you select the **Enable DoS Protection** check box, the system displays **Next** at the bottom of the page. When you click **Next**, the system displays a second Add Server Configuration Profile - Advanced page, prompting for the number of users on this Call Server.

12. **(Optional)** If you select the **Enable DoS Protection** check box, type the requested information in the appropriate fields.

13. Click **Finish**.

Example





Add Server Configuration profile field descriptions

General tab

Name	Description
Profile Name	The name of the server profile.

Table continues…

Name	Description
Server Type	The type of SIP server for which this profile is being defined. The options are: • **Trunk Server**: Used while configure a trunk server. • **Call Server**: Used to configure a call server. • **Media Server**: Used to configure a media server. • **Remote Branch Office**: Used to configure a branch office in a remote site that connects to the enterprise through Avaya SBCE. • **Recording Server**: Used to configure a Recording Server to record SIP sessions.
SIP Domain	Specifies the SIP domain that is used to validate the host name in a certificate. You must specify a SIP Domain when: • You have enabled extended host name validation. • Custom host name is left 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 TLS profile. If the custom host name is left blank, Avaya SBCE then looks for the SIP Domain specified in server configuration.
TLS Client Profile	Specifies the TLS Client profile to be used for the SIP server.
IP Addresses/ FQDNs	The IP address or Fully-Qualified Domain Name (FQDN) of the SIP server. You can add multiple IPs and FQDNs. **Note:** 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. • if the Remote Branch Office is 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 TLS common name must be verified during TLS handshake. **Note:** The system displays this field only when the **Server Type** is **Remote Branch Office**.
TLS Common Name	The string used to verify whether TLS connection from the IPO is valid. If the TLS Common Name configured in server configuration does not match the TLS Common Name provided by the IPO, Avaya SBCE rejects the TLS connection. Use any of the following values for the **TLS Common Name** field: • **FQDN** • IP Address • Name

Table continues…

Name	Description
	• Domain beginning with a wild card (*) **Note:** The system displays this field only when the **Server Type** is **Remote Branch Office**.
Port	The port number. **Note:** 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, and TLS. The **Transport** field is set to **TLS** when the **Server Type** is **Remote Branch Office**.

Authentication tab

Name	Description
Enable Authentication	Indicates whether the SIP server requires authentication. If selected, the field indicates that authentication is required and the remaining fields are activated. If cleared, the field indicates no authentication is required and the remaining fields remain inactivated.
User Name	The user name required for authentication.
Realm	The realm from which the legitimate authentication request will be 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. Checking this box indicates that a heartbeat is established and maintained and the remaining fields are activated. An empty check box indicates that no heartbeat is maintained and the remaining fields remain inactivated.
Method	Specifies the method in which the heartbeat is maintained. The options are: **OPTIONS**, **PING**, and **REGISTER**.
Frequency	Specifies the frequency with which the heartbeat signal is sent.
From URI	Specifies the source of the heartbeat signal.
To URI	Specifies the destination of the heartbeat signal.

Advanced tab

Name	Description
Enable DoS Protection	Indicates whether DoS protection is enabled for the SIP server. **Note:** 1. When you select the **Enable DoS Protection** check box, the system displays **Next** at the bottom of the page. When you click **Next**, the system displays a second Add 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 system displays two new tabs: **DoS Whitelist** and **DoS Protection** on the Server Configuration page. The system 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. If grooming changes are done on a production system, you must restart the application to clean up the stale connections. **Note:** 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 when: • one server flow is associated with the server OR • all server flows associated with the server must use the same signaling manipulation script **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.
Connection Type	Specifies the manner in which the connection will be established. The options are: **SUBID**, **PORTID**, and **MAPPING**.
Securable	Specifies whether the server is securable Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. From Release 7.0 onwards, 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.

Table continues…

Name	Description
Enable FGDN	Enables a Failover Group Domain Name (FGDN) using which, Avaya SBCE routes 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 is tolerant to both IPv4 and IPv6 addresses.
Traffic Type	Specifies the traffic type. The options are Trunk Traffic, Remote Users, and Trunk Traffic and Remote Users. The system 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 system displays this field only when you select the **Enable DoS Protection** field.
Number of Remote Users	Specifies the number of remote users. The system displays this field only when you select the **Enable DoS Protection** field. **Note:** When you select the Remote Users or Trunk Traffic and Remote Users option, the system enables the **Number of Remote Users** field.

DoS Whitelist tab

Name	Description
URI/Domain	Specifies the URI or domain to be whitelisted. The system 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	Maximum number of concurrent sessions
SIP Service	SIP service affected by the DoS attack. The available options include TOTAL, Registrations, Calls, Presence Updates, Subscriptions, Misc.
SIP Method	The SIP Method such as All, REGISTER, INVITE, SUBSCRIBE, PUBLISH, or 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.

Table continues…

Name	Description
Failed Threshold (per 10 seconds)	Maximum number of failed session initiations.
Action	The action to be performed should any of the above thresholds be exceeded. The following options are available: • 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 Avaya phones 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.

Viewing a SIP Server profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. Select the Server Configuration function of the Global Profiles feature from the Task Pane.

   The Server Configuration screen displays a list of available Server Configuration profiles in the Application Panel.

Editing a SIP Server profile

About this task

You can edit SIP server profiles on the **General**, **Authentication**, **Heartbeat**, and **Advanced** tabs.

On the Advanced page, if you select the **Enable DoS Protection** check box and save the settings, the system displays the two additional tabs: **DoS Whitelist** and **DoS Protection** on the Server Configuration page.

Procedure

1. In the Server Profiles section, select the server profile that you want to edit.
2. Select the tab, and click **Edit**.

   The system displays the Edit Server Configuration Profile page.
3. Click **Finish**.

DoS Whitelist

When you configure DoS protection while adding or editing the SIP Server profile on the Edit Server Configuration Profile - Advanced page, the system displays the DoS Whitelist page on the Server Configuration page.

Adding a URI or Domain to DoS Whitelist

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. On the Server Configuration page, click **DoS Whitelist**.
4. Click **Add**.

   The system displays the Add Whitelist URI page.
5. In the **URI/Domain** field, type the URI or domain name.
6. Click **Finish**.

Deleting a URI or Domain from DoS Whitelist

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.
3. On the Server Configuration page, click **DoS Whitelist**.
4. Click **Delete** corresponding to the URI/Domain that you want to delete.

   The system displays a Delete Confirmation pop-up.
5. Click **OK**.

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 Server Configuration Profile - Advanced page, the system displays the DoS Protection page on the Server Configuration page.

Procedure

1. Log on to the EMS web interface using the administrator credentials.

2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.
3. On the Server Configuration page, click **DoS Protection**.
4. Click **Recalculate Values**.
5. On the Recalculate Values page, reenter the required values.

   You can reenter values for traffic type and the maximum number of concurrent sessions.
6. Click **Finish** to save the settings.
7. Click **Edit** corresponding to the SIP service or method that you want to edit.

   The system displays the Edit Server DoS page.
8. Edit the desired fields, and click **Finish**.

Cloning an existing SIP Server profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. In the Server Profiles section, click the server profile that you want to clone.
4. Click **Clone**.

   The system displays the Add Server Configuration Profile page.
5. In the **Clone Name** field, type a new name for the cloned server profile.
6. Click **Finish**.

Renaming an existing SIP Server profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. In the Server Profiles section, click the server profile that you want to rename.
4. Click **Rename**.

   The system displays the Rename Server Configuration Profile page.
5. In the **New Name** field, type a new name for the server profile.
6. Click **Finish**.

Deleting an existing SIP Server profile

Procedure

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

   The system displays the Server Configuration page.
3. In the Server Profiles section, click the server profile that you want to delete.
4. Click **Delete**.

   The system displays a Delete Confirmation pop-up.
5. Click **OK**.

Server interworking

With the Server Interworking function of the Global Profiles feature, 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 on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
3. On the Interworking Profiles page, click **Add**.

   The system displays the Interworking Profile page.
4. In the **Profile Name** field, type a name for the new interworking profile, and click **Next**.
5. On the Interworking Profile - General page, type the requested information in the appropriate fields.
6. Click **Next**.
7. On the Interworking Profile - Privacy page, type the requested information in the appropriate fields.
8. Click **Next**.
9. On the Interworking Profile - SIP Timers page, type the requested information in the appropriate fields.

10. Click **Next**.
11. On the Interworking Profile advanced settings page, type the requested information in the appropriate fields.
12. Click **Finish**.

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, and RFC 3264 - a=send only.
180 Handling	Determines how 180 Ringing messages are handled. The options are: None, SDP, and No SDP.
181 Handling	Determines how 181 Call is being Forwarded messages are handled. The options are: None, SDP, and No SDP.
182 Handling	Determines how 182 Queued messages are handled. The options are: None, SDP, and No SDP.
183 Handling	Determines how 183 Session Progress messages are handled. The options are: None, SDP, and 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. URI based routing is applied to the new **INVITE** message triggered towards the transfer target.
URI Group	Indicates the URI for enabling REFER request handing. The options are: None and Emergency. **Note:** The system enables the **URI Group** field only when you select the **Refer Handling** checkbox.
Send Hold	Indicates whether or not 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:** The system 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. The system enables the **Delayed Offer** check box only when you select the **Refer Handling** check box.

Table continues…

Name	Description
3xx Handling	Indicates whether the Avaya SBCE security device will handle the *3xx Redirection Response* messages.
Diversion Header Support	Indicates whether diversion headers are supported by the Avaya SBCE security device. **Note:** When you select the **3xx Handling** check box, the system enables the **Diversion Header Support** check box.
Delayed SDP Handling	Indicates whether delayed SDP packets are processed by the Avaya SBCE security device.
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 re-invite must be enabled. 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 back. However, if a second INVITE comes without any SDP change, while adding extra SDP parameters to Hold or Resume, then Avaya SBCE will handle **RE-INVITE**.
Prack Handling	Indicates whether Provisional Response Acknowledgement (PRACK) handling is supported by Avaya SBCE
Allow 18X SDP	Indicates whether a PRACK message is permitted in an 18x record route header.
T.38 Support	Indicates whether the T.38 FAX Relay standard is supported by the Avaya SBCE security device.
URI Scheme	Indicates the URI scheme to be used by the Avaya SBCE security device. The options are: **SIP**, **TEL**, and **ANY**.
Via Header Format	Indicates the header format used by the Avaya SBCE security device. The options are: **RFC3261** and **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 SIP refresh (Re-Invite/Update) session as the minimum session expire time value. The time range is 90 to 86400 seconds.
Init Timer	Specifies the initial request retransmission interval. This is the initial SIP request retransmission interval and corresponds to Timer T1 in RFC 3261. This timer is used when sending request over UDP.

Table continues…

Name	Description
	The time range is 50 to 1000 milliseconds.
Max Timer	Specifies the maximum retransmission interval for non-INVITE requests. This is the maximum retransmission interval 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 sent from the server times out if a response is not received within the time set as the Transaction Expiration timer. 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	The transaction expiration time for an INVITE transaction after a provisional response has been received. The time range is 180 to 300 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 **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 will insert this header from the FROM header, insert the header in P-asserted ID and change From as Anonymous user, and send out the request.
P-Preferred-Identity	Indicates that Avaya SBCE uses the P-Preferred-ID during the 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.

Table continues…

Name	Description
User Action	The action to be taken by the Avaya SBCE security device if a User Regex match is found. The options are: None, Add prefix [Value], Remove prefix [Value], Replace with [Value], and Replace [Value 1] with [Value 2].
User Values	The values to be used in the manner directed 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 to be taken by the Avaya SBCE security device if a Domain Regex match is found. The options are: None, Add prefix [Value], Remove prefix [Value], Replace with [Value], and Replace [Value 1] with [Value 2].
Domain Values	The values to be used in the manner directed 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, and To.
Action	The action to be performed. The options are: Add Parameter w/ [Value] and Remove Parameter w/ [Value].
Parameter	The parameter to be used in the action performed by 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 will 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, however record routes will not be added to the in-dialog message. If Avaya

Table continues…

Name	Description
	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, however record routes will not be added 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.
Include Enpoint 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, and Cisco.
Diversion Manipulation	Directs the Avaya SBCE security device to copy SIP Diversion header from 3xx message to Sip Request message 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.
DTMF	
DTMF Support	Indicates the type of DTMF support. The options are: **None**, **SIP NOTIFY**, and **SIP INFO**.

Viewing existing Server Interworking profiles

About this task

Use the following procedure to view existing interworking profiles.

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. Select the **Server Interworking** function of the **Global Profiles** feature from the Task Pane.

The Interworking screen displays a list of available interworking profiles in the Application Pane.

Editing the Server Interworking profile parameters

About this task

To edit the server interworking parameters, you can edit the parameters of the **General**, **Timers**, and **Advanced** tabs.

Use the following procedure edit the parameters.

Procedure

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

   The system displays the parameters for that tab.
4. Click **Edit**.

   The system displays the corresponding Editing Profile page.
5. Edit the required parameters, and click **Finish**.

Adding a new URI Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click **URI Manipulation**.

   The system displays the URI Manipulation page.
4. Click **Add**.
5. On the Add Rule page, type the requested information in the appropriate fields.
6. Click **Finish**.

Editing an existing URI Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
3. Click **URI Manipulation**.

   The system displays the URI Manipulation page.
4. On the URI Manipulation page, click **Edit**corresponding to the Regex expression that you want to edit.

   The system displays the Edit Regex page.
5. Edit the required regex parameters, and click **Finish**.

Deleting an existing URI Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click **URI Manipulation**.
4. On the URI Manipulation page, click **Delete** corresponding to the regex expression that you want to delete.

   The system displays a Delete Confirmation pop-up window.
5. Click **OK**.

Adding a new Header Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click **Header Manipulation**.

   The system displays the Header Manipulation page.
4. Click **Add**.

5. On the Add Rule page, type the requested information in the appropriate fields.
6. Click **Finish**.

Editing a Header Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click **Header Manipulation**.
4. On the Header Manipulation page, click **Edit** corresponding to the header manipulation rule that you want to edit.

   The system displays the Edit Rule page.
5. Edit the required parameters, and click **Finish**.

Deleting a Header Manipulation rule

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click **Header Manipulation**.
4. On the Header Manipulation page, click **Delete** corresponding to the header manipulation rule that you want to delete.

   The system displays a Delete Confirmation pop-up window.
5. Click **OK**.

Cloning a Interworking profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
3. On the Interworking Profiles page, click the interworking profile that you want to clone.
4. Click **Clone**.

The system displays the Clone Profile page.

5. In the **Clone Name** field, type a name for the cloned interworking profile.
6. Click **Finish**.

Renaming an existing Interworking profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
3. On the Interworking Profiles page, click the interworking profile that you want to rename.
4. Click **Rename**.

   The system displays the Rename Profile page.
5. In the **New Name** field, type a name for the interworking profile.
6. Click **Finish**.

Deleting an Interworking profile

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
3. On the Interworking Profiles page, click the interworking profile that you want to delete.
4. Click **Delete**.

   The system displays a Delete Confirmation pop-up window.
5. Click **OK**.

Networks and interfaces management

With the Network Management function of the Device Specific Settings feature, 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.
3. On the Network Management page, click **Interfaces**.
4. Click **Add VLAN**.
5. On the Add VLAN page, type the appropriate values in all the fields.
6. Click **Finish**.

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.
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 a data interface only.

Tagging a VLAN

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.
3. On the Network Management page, click **Interfaces**.
4. Click **Add VLAN**.
5. 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**.

Changing the administrative state of an interface

About this task

Use the following procedure to change the administrative state of an interface.

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.

   The system displays the Network Management page.
3. On the **Interfaces** tab, in the Devices section, click the Avaya SBCE security device of which you want to change the administrative state.
4. In the **Status** column, click **Enabled** or **Disabled**.

   The system displays a confirmation pop-up window.
5. Click **OK**.

Deleting an existing interface

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.

   The system displays the Network Management page.
3. On the **Interfaces** tab, in the Devices section, click the Avaya SBCE security device of which you want to delete the interface.
4. Click **Delete** corresponding to the interface that you want to delete.

   The system displays a Delete Confirmation pop-up window.
5. Click **OK**.

Viewing an existing interface or network

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.
3. On the Network Management page, click **Interfaces** or **Networks**.

Adding a new network

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.
3. On the Network Management page, click **Networks**.
4. Click **Add**.
5. On the Add Network page, enter the appropriate values in all the fields.
6. Click **Finish**.

Editing network management parameters

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.

   The system displays the Network Management page.
3. On the **Networks** or **Interfaces** tab, in the Devices section, click the Avaya SBCE security device of which you want to edit the parameters.
4. Click **Edit** corresponding to the interface or network that you want to edit.

   The system displays the Edit VLAN or Edit Network page.
5. Edit the required fields, and click **Finish**.

Chapter 9: TLS Management

TLS Parameter Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. TLS enables clients to authenticate servers or servers to authenticate clients. Avaya SBCE security products utilize TLS primarily to facilitate secure communications with remote users.

Avaya SBCE is preinstalled with several certificates and profiles that can be used to quickly set up secure communication using TLS, which 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, Avaya recommends using System Manager or third-party certificates. For more information about how to configure third-party certificates, see Certificate Management on page 264 and TLS profile management on page 276.

Certificate Management

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management** > **Certificates**.

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, accessible at https://www.openssl.org/. For tips and tricks regarding working with certificates using OpenSSL, see Tips and tricks for working with TLS on page 286.

Certificate Signing Requests

The EMS GUI provides a basic built-in tool to assist in generating a Certificate Signing Request (CSR) specifically for use on the EMS.

Generating a CSR through the built-in tool that is provided in the Avaya SBCE is not mandatory, but recommended because the tool generates a CSR that is guaranteed to be compatible with an Avaya SBCE.

Related links

Installing third-party certificates on page 265

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.

You must also have the corresponding unencrypted, 2048–bit RSA private key.

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`*.

   Here, *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. Go to the directory to which the certificate and private key are copied.
4. As a root user, 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 264

Creating a Certificate Signing Request

Procedure

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

   The system displays the Certificates screen.
3. Click **Generate CSR**.

The system displays the TLS Management Generate CSR window.

4. Enter the appropriate information in the TLS Management Generate CSR screen, and click **Generate CSR**.

   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected. Do not clear these check boxes.

Related links

TLS Certificates screen field descriptions on page 272

Recommended 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: 1024-bit or greater
- Key Usage: keyUsage=keyEncipherment,digitalSignature
- 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 a PKCS#12 format (.p12 or .pfx), use the following procedure to extract the certificate and key.

Note:

PKCS#12 was formerly called as PFX.

Procedure

1. Copy the keystore file to the `/home/ipcs/` directory on 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 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. In the left navigation pane, click **TLS Management** > **Certificate**.
2. Click **Generate CSR**.
3. 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.
4. Use the following settings if you want to generate CSR using alternate methods:
   - Certificate: keyUsage = keyEncipherment
   - Private Key: SHA1 hash with at least 1024-bit size or SHA256 with 2048–bit size

   These settings are generated automatically when you generate CSR using the Avaya SBCE EMS web interface.
5. If you generate CSR using the Avaya SBCE EMS web interface, download the CSR to your computer.
6. 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. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate**.
4. 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.
5. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
6. In the **Key** field, select one of the following options:
   - **Use Existing Key from Filesystem**: 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.
7. **(Optional)** In the **Key File** field, click **Browse** and browse to the location of the key file
8. 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.
9. Click **Upload**.

   The system uploads the signed X.509 certificate, and the key file, if necessary, to the EMS.

Next steps

Synchronize the certificate to Avaya SBCE through a secure shell (SSH) session.

Related links

TLS Certificates screen field descriptions on page 272

Synchronizing and installing certificate in a multi-server deployment

About this task

A multi-server deployment can consist of one or more Avaya SBCE HA pairs or multiple individual Avaya SBCE servers. Use this procedure to synchronize and install certificates for each Avaya SBCE server in the multi-server deployment.

Procedure

1. Using a terminal emulation program such as PuTTY, start a secure shell (SSH) connection to each Avaya SBCE individually in a multiple server deployment.
2. In the **Host Name (or IP address)** field, type the IP address of an individual SBCE box.
3. In the **Port** field, type `222` and click **Open**.

   A short delay might occur before connecting.
4. To log in to Avaya SBCE, use ipcs login and password.
5. At the $ prompt, type `sudo su` and press `Enter`.

   The system displays a prompt to enter the password.
6. At the password prompt, type the ipcs password.
7. At the # prompt, type `clipcs` and press `Enter`.

   The system displays the CLIPCS console commands level, which is one level below root-level. For a list and descriptions of available CLIPCS commands, see “CLIPCS Console Commands”.
8. At the # prompt, type `certsync` and press `Enter`.

   Avaya SBCE synchronizes with EMS and displays the list of available certificates.
9. Type `certinstall` *`certificate_file_name`*, where *certificate_file_name* is the name of the certificate file that you want to install.

   If the **`certinstall`** command does not accept the certificate file name that you enter, rename the file with extension .crt and enter the filename again.
10. When the system requests the key passphrase, enter the passphrase.

    If you used the CSR generation utility that is built into Avaya SBCE, the passphrase is the password you entered in the Generate CSR screen.

11. At the # prompt, type `exit` and press `Enter`.

    The system exits the program level and displays the $ prompt.

12. At the $ prompt, type `exit` and press `Enter`.

    The system exits the secure shell session. You can also exit the session by clicking the Cancel (X) button in the upper-right portion of the window.

13. Use the EMS web interface to restart the Avaya SBCE application.

Related links

clipcs commands and descriptions on page 314

Installing certificate on a single server Avaya SBCE

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Certificates**.
3. Click **Install**.
4. In the **Type** field, click **Certificate**.
5. In the **Name** field, type a name for the certificate.

   If you have not downloaded the Private Key, you must type the name you provided in the **Common Name** field while generating CSR. If you have downloaded the Private Key, you can type any name for the certificate.

6. In the Certificate File section, click **Browse** to upload the certificate file.
7. In the **Key** field, select one of the following options:
   - If you have not downloaded the Private Key, click **Use Existing Key from Filesystem**.
   - If you have downloaded the Private Key, click **Upload Key File** and upload the key that you downloaded while generating CSR.

   After uploading the certificate to Avaya SBCE, verify whether the file is available in `/usr/local/ipcs/cert/certificates`.

   For a single server Avaya SBCE, you need not run the **`certsync`** command. You must run the **`certsync`** command only for synchronizing certificates for Avaya SBCE deployed in an HA or multi-server deployment.

8. Using a SSH client, such as PuTTY, start a secure shell (SSH) connection to the Avaya SBCE server.
9. In the **Host Name or IP address** field, type the IP address of an Avaya SBCE server.
10. In the **Port** field, type `222`, and click **Open**.
11. To log in to Avaya SBCE, use ipcs login and password.

12. Go to directory `/usr/local/ipcs/cert/key`.
13. Type `enc_key` *`filename passphrase`*.

    In this command, *filename* is the name of the encryption key file, and *passphrase* is the passphrase you used while generating the CSR.
14. Use the EMS web interface to restart the Avaya SBCE server.

Viewing certificate details

Procedure

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

   The system displays the Certificates screen.
3. Locate the Avaya SBCE certificate that you want to view, and click **View**.

   The system displays the View Certificate window.
4. 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 left navigation pane, click **TLS Management** > **Certificates**.

   The system displays the Certificates screen.
3. Locate the Avaya SBCE certificate that you want to delete, and click the **Delete**.

   The system displays the delete confirmation window. If the certificate is currently in use by a reverse proxy or TLS profile, the system displays a message to indicate that the certificate is in use. You cannot delete certificates that are currently in use.
4. Click **OK** to confirm.

   The system 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.

Install Certificate

Name	Description
Type	The type of certificate that you want to install. Options are: **Certificate**, **CA Certificate**, or **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

Table continues…

Name	Description
	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 existing key from the filesystem or select a file containing another key.
Key File	The button that is displayed when you select **Upload Key File** in the **Key** field. Depending on the browser, click **Browse** or **Choose File** to locate the file.

Generate CSR

Name	Description
Country Name	The name of the country within which the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Locality Name	The locality (city) where the certificate is being created.
Organization Name	The name of the company or organization creating the certificate.
Organizational Unit	The group within the company or organization creating the certificate.
Common Name	The name used to refer to or identify the company or group creating the certificate. 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 cannot provide wildcard (*) characters in this 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. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **CA Certificate**.
4. In the **Name** field, type a name for the certificate.
5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

Related links

TLS Certificates screen field descriptions on page 272

Viewing Certificate Authority details

Procedure

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

   The system displays the View CA Certificate window.
4. 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 left navigation pane, click **TLS Management** > **Certificates**.

   The system displays the Certificates screen in the Content Area.
3. Locate the Avaya SBCE certificate authority (CA) certificate that you want to delete, and click **Delete**.

   The system displays the delete confirmation window. If the certificate is currently in use by a reverse proxy or TLS profile, the system displays a message to indicate that the certificate is in use. You cannot delete certificates that are currently in use.
4. Click **OK**.

The Certificates screen is displayed without 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.
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 Option

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate Revocation List**.
4. In the **Name** field, type the name of the certificate.
5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

Viewing Certificate Revocation List details

Procedure

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

4. After viewing the certificate revocation list information, click the Cancel icon.

Deleting Certificate Revocation Lists

Procedure

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

   The system displays the Certificates screen without 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.
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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the **New Profile** window.
4. Enter the requested information in the appropriate fields.
5. Click **Finish**.

   The system installs and displays the new TLS client profile.

TLS client profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS server profile pop-up window field descriptions on page 280.

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**.

Name	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
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.

Table continues…

Name	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 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.
Custom Hostname Override	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.
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. Available selections are: • Default: The cipher suite recommended by Avaya. • FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility.

Table continues…

Name	Description
	• 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.

Editing a Client Profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click the client profile that you want to edit.

   The system displays the configuration of the selected client profile in the content area.
4. Click **Edit**.

   The system displays the Edit Profile window.
5. 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 277

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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. In the applications pane, click the client profile that you want to delete.
4. Click **Delete**.

   The system displays a confirmation window to confirm your selection.
5. Click **OK**.

   The system 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The system displays the Server Profiles screen.
3. Click **Add**.

   The system displays the New Profile window.
4. Enter the requested information into the appropriate fields.
5. Click **Finish**.

   The TLS Server profile is created, installed, and listed in the application pane.

TLS server profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS Client Profile Pop-up Screen Field Descriptions on page 277

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**.

Field	Description
TLS Profile	
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
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.
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.

Table continues…

Field	Description
	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. Available selections 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.

Editing a server profile

Procedure

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

2. In the left navigation pane, click **TLS Management** > **Server Profiles**.
3. Click the server profile that you want to edit.

   The configuration of the selected server profile is displayed in the content area.
4. From the content area, click **Edit**.

   The system displays the Edit Profile window.
5. 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 Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The system displays the Server Profiles screen.
3. Click the server profile that you want to delete.
4. Click **Delete**.

   The system displays a confirmation window to confirm your selection.
5. Click **OK**.

   The system 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.	
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 265.	
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 267.	
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	

Table continues…

No.	Task	Description	✔
		• Value: N/A For more information, see Creating a server profile on page 280.	
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 277.	
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 214.	
7	Update the subscriber flow.	To enable the Avaya SBCE in establishing a TLS connection back towards the phone, you	

Table continues…

No.	Task	Description	✔
		must update the subscriber flow to use the TLS client profile. For more information, see Editing existing endpoint flows on page 146.	
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 247.	

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`.

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
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 on to the EMS web interface.
2. On the toolbar, click **Alarms** or click on the specific alarm you want to view from the **Alarms (past 24 hours)** section of the Dashboard screen.

   The system displays the Alarms Viewer screen.
3. 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.
Details	The specific or descriptive name of the active alarm.

Table continues…

Name	Description
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. To clear the selected alarm or all alarms, on the Alarms screen, click **Clear Selected** or **Clear All**.

   The system displays a confirmation pop-up window.

2. 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:

Incidents can only be viewed. They cannot be edited or deleted.

Procedure

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

   The system 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.

3. 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.

   The options for Incidents category selections include:

   - 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

4. To ensure that the system displays all required incidents, periodically click **Refresh** to refresh the display.
5. Click **Clear Filters**.

   The system clears the filtering criteria of the **Device** and **Category** fields and sets the value of the fields to All.

6. Click **Generate Report** and select the start and end date to generate the report.

Incident Viewer field descriptions

Search Criteria

Name	Description
Device	A drop-down list to select the device for which you want to view incidents.
Category	A drop-down list to select the category of the incident.

Table continues…

Name	Description
	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

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.
Category	The category of the incident.
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.

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 on to the EMS web interface with administrator credentials.
2. On the **Status** toolbar, click **SIP Statistics**.

   The system 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**

   On the **SIP Summary** tab, you can view information such as the number of:
   - Active calls
   - User registrations
   - Calls through the Avaya SBCE after the last restart

Related links

Statistics Viewer field descriptions on page 293

Statistics Viewer field descriptions

SIP Summary tab

Name	Description
Active TCP Registrations	The number of active SIP registrations with TCP transport.

Table continues…

Name	Description
Active UDP Registrations	The number of active SIP registrations with UDP transport.
Active TLS Registrations	The number of active SIP registrations with TLS transport.
Concurrent Sessions (Active Calls)	The number of active SIP calls.
Active SRTP Calls	The number of active calls using media as SRTP.
Total Registrations	The number of SIP registration requests received.
Total Registrations Rejected	The number of rejected registrations.
Total TCP Registrations	The number of SIP registrations received with TCP transport.
Total UDP Registrations	The number of SIP registrations received with UDP transport.
Total TLS Registrations	The number of SIP registrations received with TLS transport.
Total Calls	The number of SIP calls received.
Total Calls Rejected due to Policy Violations(s)	The number of SIP calls rejected by Avaya SBCE because of policy violation.
Total Calls Failed	The number of failed SIP calls.
Total Calls Rejected due to Concurrent Session Limit	The number of SIP sessions dropped by Avaya SBCE because the maximum number of concurrent sessions was exceeded.

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.

Table continues…

Name	Description
	This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Policy tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the policy group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

From URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
URI Group	Selects the source URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

To URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the destination URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Transcoding Summary

Name	Description
Streaming	Specifies whether live statistics are displayed.
Total Active Transcoding Sessions	The number of active transcoding sessions.
Total Transcoding Sessions	The number of transcoding sessions.

Table continues…

Name	Description
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.

Related links

Viewing system SIP statistics on page 293

Real Time SIP Server Status

Avaya SBCE Release 6.3 onwards, you can view the current status of the configured SIP servers. The system 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.
3. Click the **Heartbeat** tab.
4. Select the **Heartbeat** check box.

   This option enables the heartbeat. After enabling the heartbeat, configure the server flow for this server.
5. In the left navigation pane, click **Device Specific settings** > **Endpoint flows** > **Server flows**.

   For more information about creating server flows, see Creating Flow toward Call Server on page 381.

   Note:

   In a high availability failover scenario, the system 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 on to the EMS web interface with administrator credentials.
2. On the **Status** toolbar, click **Server Status**.

   The system displays the Status screen.

   The system displays server information, such as Server Profile, FQDN, IP address, Transport, Port, Status (UP/DOWN/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.
Status	The status of the server.
TimeStamp	The date and time when the server status was updated.

User registration

From Avaya SBCE Release 6.3 onwards, you can view the list of users that are registered through Avaya SBCE. 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 on to the EMS web interface.
2. On the **Status** toolbar, click **User Registrations**.

The system displays the list of registered users.

3. For complete details of a registered user, click the user details.

   The system 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.
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 on to the EMS web interface with administrator credentials.
2. Select the **Logs** option from the toolbar, and click the **System Logs** menu.

   The system 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.

Related links

Syslog Viewer field descriptions on page 299

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.

Table continues…

Name	Description
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 following options are available: • All • Platform • Trace • Security • Protocol • Incidents • Registration • Audit • GUI • Unknown
Severity	Severity of the logs to be displayed. The following options are available: • 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.

Table continues…

Name	Description
Severity	Severity of the message.
Class	Class of the message.
Summary	Summary of the message.

Related links

Viewing system logs on page 299

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 on to the EMS web interface with administrator credentials.
2. On the toolbar, click **Logs** > **Audit Logs**.

   The system 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 system displays the report output.
5. To see additional details about a particular log line in a report, select the log line.

   The system displays the Audit Log Details page.
6. On the **Device Specific Settings** > **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`.

Related links

Audit Logs field descriptions on page 302

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.

Related links

Viewing audit logs on page 301

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

   The system 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 system 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.

Related links

Diagnostics field descriptions on page 303

Diagnostics field descriptions

Full Diagnostic tab

Name	Description
EMS Link Check	Checks the EMS link.
Ping: SBC to EMS	Sends a ping from Avaya SBCE to EMS.
Ping: EMS to SBC via VPN	Sends a ping from Avaya SBCE to EMS through VPN.
SSH Test: EMS to SBC	Connects EMS to Avaya SBCE through SSH.
SBC Link Check: A1	Checks the Avaya SBCE A1 interface.
Ping SBC [A1] to Gateway	Sends a ping from the Avaya SBCE A1 interface to the Gateway.
Ping SBC [A1] to Primary DNS	Sends a ping from the Avaya SBCE A1 interface to the Primary DNS.

Ping Test

Name	Description
Source Device / IP	The IP address of the device originating the ping.
Destination IP	The IP address to which the ping is sent.

Related links

Viewing diagnostics results on page 302

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 on to the EMS web interface with administrator credentials.
2. On the toolbar, click **Users**.

   The system displays the Active Users page.

Related links

Active Users field descriptions on page 304

Active Users field descriptions

Name	Description
User Name	The user 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.

Related links

Viewing administrative users on page 303

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 on to the EMS web interface with administrator credentials.

2. In the left navigation pane, click **Device Specific Settings** > **Troubleshooting** > **Trace**.
3. In the **Devices** section, click the Avaya SBCE device for which you want to configure packet capture.
4. Click **Packet Capture**.

   The system displays the Packet Capture page.
5. On the Packet Capture page, do the following:
   a. In the **Interface** field, click `Any` or the required interface. The default value is Any.
   b. In the **Local Address** field, click `All` or the required local address. You can type the port number for the required local address. The default value is All.
   c. In the **Remote Address** field, type the remote IP address and port.

      The default value is *.
   d. In the **Protocol** field, click the protocol.

      The options are: All, TCP, and UDP.
   e. In the **Maximum Number of Packets to Capture** field, type the number of packets to capture the data. You can enter values between 1 to 10,000.

      Note:

      Do not capture more than 10,000 packets. The system displays a warning message.
   f. In the **Capture Filename** field, type the name of the file to capture the data.
   g. Click **Start Capture**.

      The system displays a message that `A packet capture is currently in progress. This page will automatically refresh until the capture completes.`
   h. Click **Stop Capture**.

      The system stops capturing the data and saves the packet capture file in the pcap format on the Captures page.
6. On the Captures page, click **Refresh**.

   The system displays the file with the file size information in bytes and the date when the file is last modified.
7. On the Captures page, click the file name.

   The system displays the File Download window.
8. On the File Download window, click **Save** or open the file directly.

   The system displays the Save As window.
9. Navigate to a directory for saving the Packet Capture (pcap) file and click **Save** to save the file to the new directory.

10. 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 protocols are: • 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.

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.

You can log in as a root user and run the following set of commands: **`gui-user`**, **`gui-snapshot-create`**, **`gui-snapshot-restore`**, **`traceSBC`**, and **`clipcs`**. The second set of commands are **`clipcs`** commands.

Root-level console commands

You can enter the following new root-level console commands at the root prompt:

- **`# gui-user`**
- **`# gui-snapshot-create`**
- **`# gui-snapshot-restore`**

Console Command - gui-user

The **`gui-user`** console command allows the user to modify GUI user settings from the command line. The general structure of the command is:

`gui-user` action options

Action

The action must be one of the following:

- -a or --add: Add user mode, used for configuring a new user.

  When using the –a option, the following options are also required:

  - -n or --name

Comments on this document? infodev@avaya.com

  - -p or --password
  - -r or --role
- -e or --edit=*username*: Edit user mode, used for changing parameter fields for an existing user. This option also allows you to change the username.

  Note:

  username is required and must be the username of an existing user.
- -d or --delete=*username*: Delete user mode, used for deleting a user.

  Note:

  The username is required and must be the username of an existing user. Any specified options, except debug and quiet, will be ignored.
-
- --version: Displays the command version, which is equal to the GUI version.
- --help: Displays detailed information about the command, possible arguments, and a few examples.

Options

Can be any combination of the following:

- n or --name: Specifies the username to set. This option is required when using –a (add) option.
- -p or --password: Specifies the password to set. This option is required when adding a user with the –a (add) option, editing using the –e (edit) option, or specifying the -n (name) or –t (type) flags.
- -c or --contact-info: Specifies the contact info to set.
- -N or --real-name: Specifies the real name to set.
- -r or --role: Specifies the user role to set. Can be admin, manager, or supervisor. Required when using –a (add) option.
- -t or --type: Specifies the user type to set. Can be legacy, local, ASG, or radius. These user types are relevant for the add and edit operations. For more information, see New administrative account field descriptions. on page 35
- -s or --status: Specifies the user status to set. Can be ok or disabled.
- --debug: Outputs debug logs to stdout when executing the command.
- --quiet: Suppresses all output. If both the **quiet** option and **debug** option are specified, the **quiet** option takes precedence.

When the command is run, an exit code is returned. Any relevant details for a failure are passed to stderr. A list of possible returned exit codes:

- -1 – User has no permission to run this command (this command must be run as the root user).
- 0 – Completed successfully.
- 1 – Invalid command syntax. This exit code is returned if no action is specified or one of the required options was missing.

- 2 – Validation failed. One or more of the options did not pass validation.
- 3 – User does not exist. This usually happens when trying to edit or delete a user that does not exist.
- 4 – User exists. This usually happens when trying to add a user or changing a username to one that already exists.
- 5 – User is required. This usually happens if a username was not specified when trying to edit or delete a user.
- 6 – Role is required. This usually happens if a role is not specified when adding a new user.
- 7 – Action failed. This usually happens if the connection to the database could not be established or some other library failed.
- 1000 – An unknown error has occurred.

Examples

Command	Usage
gui-user --edit *test-user* **--status disabled**	Edits an existing user named test-user and disables the user. This command exits with code 0.
gui-user –e *test-user* **–u** *fred*	Edits an existing user named test-user and changes the username to fred using the shorthand options. This command exits with code 0.
gui-user –d *test-user*	Deletes a user named test-user using shorthand options. **Note:** While this command is syntactically correct if you follow the progression from the previous examples, the command fails. This error occurs because the user named test-user was renamed to fred. The user was renamed to fred in the first example. Therefore, the command fails with error code 3.
gui-user –e *test-user* **–p** *password*	Changes the password.

Console command-gui-snapshot-create

Use the **gui-snapshot-create** console command to create a snapshot from the command line. The structure of the command is:

gui-snapshot-create options description

Description

The description can be any string value and does not need to be quoted. If not specified, the description has the default value Restore Point through CLI.

Options

The following options are available for this command:

- --version: Displays the command version that is equal to the GUI version. Usually, the GUI version matches ipcs-version.
- --help: Displays detailed information about the command, possible arguments, and a few examples.

- --debug: Sends the output of debug logs to stdout when executing the command.
- --quiet: Suppresses all output. If both the quiet option and debug option are specified, the quiet option takes precedence.

When the command is run, an exit code is returned. Any relevant details for a failure are passed to stderr. The following are examples of the returned exit codes:

- 0 – Completed successfully.
- 1 – Invalid command syntax.
- 2 – Snapshot creation partially successful. This exit code occurs when a snapshot was created successfully, but could not be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This exit code occurs if the snapshot creation fails.
- 1000 – An unknown error has occurred.

Examples

A few sample commands with descriptions are listed here:

- `gui-snapshot-create`: Creates a new snapshot with the default description Restore Point via CLI.
- `gui-snapshot-create --quiet This is a test snapshot`: Creates a new snapshot with the description This is a test snapshot. The system does not send any output to stdout or stderr.

Console Command-gui-snapshot-restore

With the **`gui-snapshot—restore`** console command, you can restore a snapshot from the command line. The general structure of the command is:

`gui-snapshot-restore` options *file*

File

Use the absolute or relative path for a valid snapshot file.

Options

Use one of the following options:

- --version: Displays the command version, which is equal to the GUI version. The GUI version usually matches the ipcs-version.
- --help: Displays detailed information about the command, possible arguments, and a few examples.
- --debug: Sends debug logs to stdout when running the command.
- --quiet: Suppresses all output. If both the quiet option and debug option are specified, the quiet option takes precedence.

After the command runs, the system returns an exit code. Any relevant details for a failure are passed to stderr. A list of possible returned exit codes follows:

- 0 – Completed successfully.
- 1 – Invalid command syntax.

- 2 – Snapshot creation partially successful. This exit code occurs when a snapshot is created successfully, but cannot be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This exit code occurs if the snapshot creation failed.
- 1000 – An unknown error occurred.

Examples

A few sample commands with descriptions are listed here:

- `gui-snapshot-restore /home/ipcs/snapshot folder/snapshot.zip`: Restores from a snapshot file named snapshot.zip in /home/ipcs/snapshot folder/.
- `gui-snapshot-restore ../snapshots/snapshot-1.2.3.zip`: Restores from a snapshot file named snapshot-1.2.3.zip in the sibling of the parent directory, named snapshots.

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 **Device specific settings** > **Troubleshooting** > **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.

Table continues…

Command	Description
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.
certupdate	Updates the certificate key.
certinstall	Installs certificates.
certsync	Synchronizes certificates.
!<cmd>	Executes <cmd> in shell.

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.

Accessing Avaya SBCE

Logging in to EMS through VGA connection

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 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 system 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`.

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

   The system displays the super user command line prompt (#).
9. On the root level prompt (root@), type `clipcs` and press `Enter`.

   The system starts the Avaya SBCE console.

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

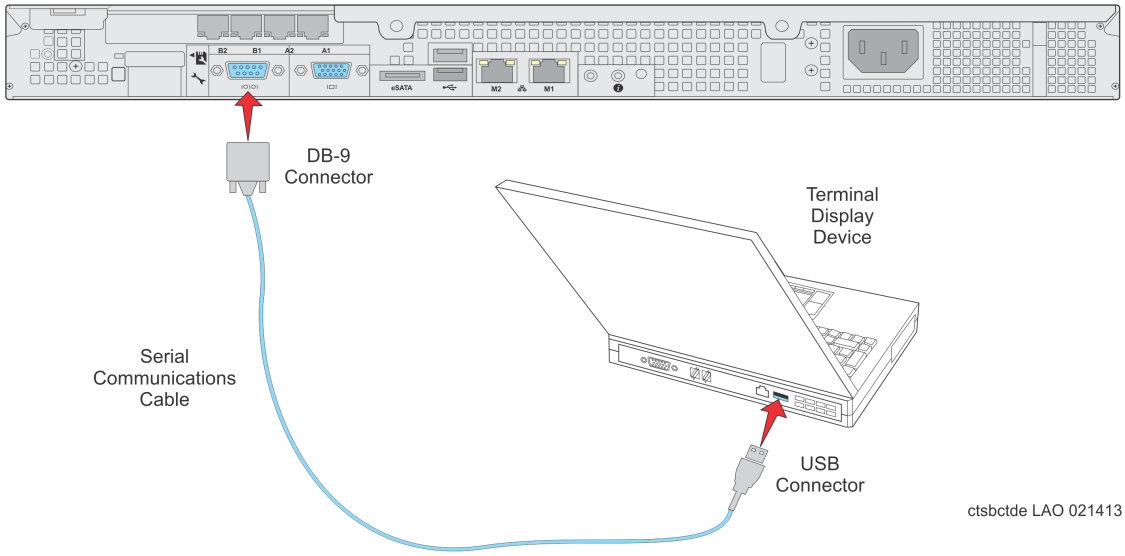
1. Find the Console port on the Avaya SBCE equipment chassis or, for the Element Management System (EMS), the UART (serial COM) port.

   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.

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*
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	**SBCEConfigurator.py change-sbce-ip** *sbce-old-ip sbce-new-ip*

Table continues…

#	Command	Description	Usage
		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.	
9	**factory-reset**	Resets Avaya SBCE to the factory default state. 1. To uninstall the Avaya SBCE device in a multiple server deployment from GUI, click **System 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**

Changing the management IP from the EMS web interface

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **System Management**.
3. Find the device whose IP address you want to change, and click **Edit**.

   For an Avaya SBCE, the system displays the following warning:

```
Any changes to the management network on this device will reboot
the device.
```

For an EMS, the system displays the following warning:

```
Any changes to the management network on this device will reboot
the device, drop any active calls, and require each connected SBC
to be manually restarted using Application Restart in System
Management.
```

4. In the **Management IP** field, type the new management IP, and click **Finish**.

   Ensure that you include appropriate netmask and gateway details for the new IP. When you change any information in the **Network Settings** section, the device restarts to complete the change. If you change the management IP of the EMS, the EMS web interface displays a new URL. After the system restarts, you must use the new URL to go to the EMS.

   Note:

   From Release 6.3, you can change the management IP through the CLI. For more information about changing the management IP through the CLI, see the Changing Management IP section in the Avaya SBCE CLI commands chapter.

5. **(Optional)** Find the Avaya SBCE device on the System Management page, and click **Restart Application**.

   Note:

   If you change the management IP address of the EMS, restart each Avaya SBCE connected to the EMS.

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

IP, gateway, and network mask change

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.

To change EMS IP, you must regenerate VPN certificates on the EMS server and all Avaya SBCE servers connected to EMS. Change in management IP also 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.

Regenerating VPN certificates when Avaya SBCE is unreachable

Procedure

1. Log on to the EMS server as a super user.
2. Type `SBCEConfigurator.py generate-client-vpn-cert` *`SBC_MGMT_IP`* and press `Enter`.

   Here, *SBC_MGMT_IP* is the Avaya SBCE management 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 on the EMS device 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 on to the Avaya SBCE server as a super user.
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 on to the Avaya SBCE server as a super user.
2. Type `SBCEConfigurator.py change-nw—passphrase` *New Passphrase*.

   The system restarts for enabling the new passphrase.

Regenerating self-signed certificates

Procedure

1. Log on to the EMS web interface as a super user.
2. Run the following command: **`SBCEConfigurator.py change-ssl-certs`**.

Changing DNS IP and FQDN

Procedure

1. Log on to the Avaya SBCE server as a super user.
2. Type `SBCEConfigurator.py change-dns—ip—fqdn` *DNS IP FQDN*.

   The system changes the DNS IP and FQDN.

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

Remote worker overview

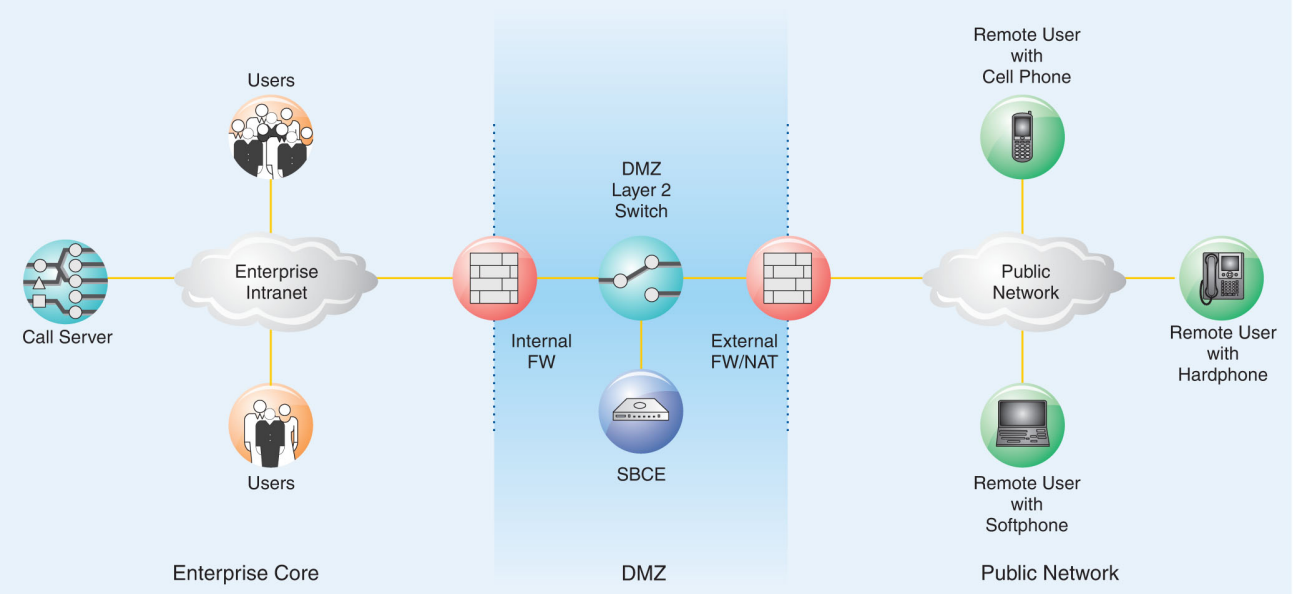
Avaya SBCE delivers security to a SIP-based enterprise network. This chapter describes how to configure Avaya SBCE for Avaya Aura® remote worker.

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

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 290 and Viewing current system alarms on page 289.
- 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.

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 330	
2.	Create an external signaling interface for the phone network.	Creating an external signaling interface toward phone network on page 332	
3.	Create an internal signaling interface for the Avaya call server.	Creating an internal signaling interface toward Avaya call server on page 333	
4.	Create an external media interface for the phone network.	Creating an external media interface toward phone network on page 334	
5.	Create an internal media interface for the Avaya call server.	Creating an internal media interface toward Avaya call server on page 334	
6.	Create a PPM Mapping profile.	Creating PPM Mapping Profile on page 335	
7.	Creating a reverse proxy service for PPM traffic.	Creating a reverse proxy service for PPM traffic on page 338	
8.	Configure reverse proxy service for downloading file or firmware.	Creating reverse proxy service for file or firmware download on page 339	
9.	Create a media rule.	Creating a media rule on page 344	
10.	Create a server flow.	Creating server flow on page 347	
11.	Configure application rules for concurrent sessions per endpoint and maximum concurrent sessions.	Creating application rules on page 344	
12.	Create an endpoint policy.	Creating an endpoint policy on page 345	
13.	Create a routing profile to the Avaya call server.	Creating a routing profile to Avaya call server on page 346	
14.	Create a subscriber flow.	Creating a subscriber flow on page 348.	
15.	If you are setting up an Avaya Scopia® remote worker, administer BFCP and FECC.	Administering Binary Floor Control Protocol on page 405 Administering Far End Camera Control on page 407	
16	Add a URI group for emergency numbers.	Creating a new URI group on page 151	
17	Enable the URI group by selecting the emergency URI group in the **E911 URI Group**	Managing SIP options on page 178	

Table continues…

No.	Task	Link	✔
	field from **Device Specific Settings** > **Advanced Options** > **SIP Options**.		

Cloning Avaya-ru profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Click an Avaya-ru profile, and then click the **Clone** button.
4. In the Clone Profile window, type the profile name.
5. 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 left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.
4. Enter a name for the server profile.
5. Click **Next**.

   The system displays the Add Server Configuration Profile – General window.
6. In the **Server Type** field, click **Call Server**.
7. In the **IP Address/Supported FQDNs** field, enter the IP address or FQDN of Session Manager.
8. In the **Transport** field, click the supported transport protocol.

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.

9. 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.

10. Click **Next**.

    The system displays the Add Server Configuration Profile – Authentication window.

11. 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.

12. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat window.

13. If you use the heartbeat feature, select the **Enable Heartbeat** check box to establish a heartbeat.

    Note:

    - The system enables the **Method**, **Frequency**, **From URI**, and **To URI** fields.
    - For a single Session Manager instance, leave these fields blank.

14. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.

15. Select the **Enable Grooming** check box.
16. In the **Interworking Profile** field, select the interworking profile as Avaya_ru.

    Note:

    You can clone the Avaya_ru profile and use the cloned profile if any changes are to be made to the profile.

17. In the **TLS Client Profile** field, click the default TLS profile.
18. For the other fields, do not change the default parameters.
19. Click **Finish** to save and exit.

Related links

Cloning Avaya-ru profile on page 330

Creating an external signaling interface for a phone network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Signaling Interface**.

   The left Application pane displays the list of signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
3. In the upper-right corner of the Content pane, click **Add**.

   The system displays the Add Signaling Interface window.
4. In the **Name** field, type a descriptive name for the external signaling interface for the phone network.
5. In the **IP Address** field, select the IP address of the external signaling interface.
6. Depending on the transport protocol that you are using for your network, do one of 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.

   The system enables the **TLS Profile** and **Enable Shared Control** fields.

   Note:

   - Avaya recommends the use of TLS as this protocol is secured and supports presence.
   - Use the B1 interface as the external signaling interface.
7. In the **TLS Profile** field, click 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.
8. 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 213

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 left navigation pane, click **Device Specific Settings** > **Signaling Interface**.

   The left Application pane displays any existing signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
3. In the right-corner of the Content pane, click **Add**.
4. In the Add Signaling Interface window, add parameters the following parameters:
   a. In the **Name** field, type the name of the internal signaling interface for the Avaya call server.
   b. In the **IP Address** field, select the IP address of the internal signaling interface.
   c. In the **TLS Port** field, type the port number `5061`.

      The system enables the **TLS Profile** and **Enable Shared Control** fields.

      Note:

      - Avaya recommends the use of TLS, as this protocol is secure and supports presence.
      - If your call server uses a different protocol, type the appropriate port numbers in the **TCP Port** /**UDP Port** fields, as applicable.
      - The default port number for TCP and UDP is 5060.
      - To use Avaya one-X® Communicator for shared control, configure the shared control port in the internal signaling interface.

   d. In the **TLS Profile** field, select the profile name of TLS.
   e. To use Avaya One-X Communicator in the shared control mode, select the **Enable Shared Control** check box.
   f. In the **Shared Control Port** field, type the 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.

g. Click **Finish**.

The system displays the new internal signaling interface.

Related links

Add signaling interface field descriptions on page 213

Creating an external media interface for a phone network

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Media Interface**.
3. On the Media Interface page, click **Add**.

   The system displays the Add Media Interface window.
4. In the **Name** field, type the name of the external media interface toward the phone network.
5. In the **IP Address** field, click the IP address of the external media interface.
6. In the **Port Range** fields, type the starting and ending port range numbers.

   The port range is from 35000 to 40000. To change the port range settings, change the values in the **Port Range** field on the Edit Media Interface page.
7. Click **Finish**.

Creating an internal media interface for an Avaya call server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Media Interface**.
3. On the Media Interface page, click **Add**.

   The system displays the Add Media Interface window.
4. In the **Name** field, type a descriptive name for the internal media interface of the Avaya call server.
5. In the **IP Address** field, click the IP address of the internal media interface.

6. In the **Port Range** field, type the starting and ending port range numbers.

   The port range is from 35000 through 40000. If you want to change the port range settings, go to **Device Specific Settings** > **Advanced Options** > **Port Ranges** page.

7. Click **Finish**.

   The system displays the new external and internal media interfaces.

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 left 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**.

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
Server Address	The IP address or FQDN of the server.
SBC Device	Session Managerame 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.
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.

Adding a reverse proxy policy

Procedure

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

2. In the navigation pane, click **Global Profiles** > **Reverse Proxy Policy**.
3. Click **Add**.
4. In the **Rule Name** field, type the name of the reverse proxy policy, and click **Next**.
5. Provide appropriate values in the **General**, **Timeout**, and **Route/Connection Limiting** fields.
6. Click **Finish**.

   The system creates a reverse proxy profile. While creating a reverse proxy service, you can associate the reverse proxy service with the reverse proxy policy you created.

   Note:

   You cannot edit the default reverse proxy profile. Instead you can clone the default profile.

Related links

Add reverse proxy policy field descriptions on page 337

Add reverse proxy policy field descriptions

Name	Description
Allow Web Sockets	Permits Web Sockets if selected.
Request Max Body Size	Specifies the maximum size in megabytes allowed for the body of a proxied request.
Client Body Timeout	Specifies the maximum time in seconds allowed between two successive read operations on an HTTP request before the proxied request is timed out.
Client Header Timeout	Specifies the maximum time in seconds in which the header of an HTTP request can be read before the request is marked as timed out. If the reverse proxy module is unable to read the request in this time period, the module will respond with an HTTP 408 error response.
DNS Resolver Timeout	Specifies the maximum amount of time in seconds allowed to resolve a DNS record.
TLS/SSL Session Timeout	Specifies the period in seconds in which SSL/TLS session parameters may be reused before they must be renegotiated.
Enable Rate Limiting	Enables rate limiting. With rate limiting, you can restrict excessive SIP requests from a host and avoid a DoS attack.

Table continues…

Name	Description
Total Number of Clients	Specifies the maximum number of concurrent clients allowed by this policy. This field is available only when you select the **Enable Rate Limiting** check box.
Maximum Simultaneous Connections	Specifies the maximum number of simultaneous connections allowed by this policy. This field is available only when you select the **Enable Rate Limiting** check box.
Average Request Rate	Specifies the number of requests permitted to be process every second or minute for an IP address. If the number of requests exceed the rate specified in this field, the requests are rejected with an HTTP 503 response if a Burst per Client value is not defined.. This field is available only when you select the **Enable Rate Limiting** check box.
Burst per Client	Specifies the number of requests allowed to burst per IP address or client. If set to zero, bursting is disabled and any requests above the Average Request Rate threshold are rejected. If set to number above zero, this is the number of requests that can be queued for processing. If the number of requests is below this threshold, the requests are processed at a rate which does not exceed the Average Request Rate threshold. Any requests sent after this threshold has been exceeded, are rejected with an HTTP 503 error response. This field is available only when you select the **Enable Rate Limiting** check box.

Related links

Adding a reverse proxy policy on page 336

Creating a reverse proxy service for PPM traffic

About this task

Use the following procedure for each Avaya SBCE.

Procedure

1. Log on to EMS.

2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.
3. In the **Reverse Proxy** tab, click **Add**.
4. 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.

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.

Procedure

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

2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.
3. In the **Reverse Proxy** tab, click **Add**.
4. 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.
5. In the **Reverse Proxy Policy Profile** field, click a reverse proxy policy profile.
6. 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.
7. Click **Finish**.

Related links

Relay Services field descriptions on page 341

Relay Services field descriptions

Application Relay tab

Field	Description
Name	Specify a name for the application relay.
Service Type	Specify a service type. The options are: XMPP, RTCP, LDAP, SCEP, HTTP, CES, and Other.
Remote Configuration	
Remote IP/FQDN	Specify the server IP address or FQDN as follows: • For RTCP (Core Avaya 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.

Table continues…

Field	Description
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.
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.

Table continues…

Name	Description
	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.
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.
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

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 a reverse proxy service for file or firmware download on page 339

Creating a media rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Domain Policies** > **Media Rules**.
3. Create a new media rule.

   Note:

   When you use SRTP as preferred format, disable **Encrypted RTCP** as Avaya Aura® does not support encrypted RTCP.
4. Click **Finish**.

Related links

Creating a new Media Rule on page 94

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 left navigation pane, click **Domain Policies** > **Application Rules**.
3. 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 on to the EMS web interface with administrator credentials.
2. In the left 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.
3. Create a new policy group.
4. 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Routing** .
3. On the Routing Profile page, click **Add**.
4. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
5. Click **Next**.

   The system displays the second Routing Profile page.
6. **(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.
7. **(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.
8. 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.
9. 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.
10. 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.
11. Select the **Next Hop In-Dialog** check box.

If you select this option, Avaya SBCE processes the next-hop configuration for in-dialog message as well.

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 **Device Specific Settings** > **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.
3. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow window.
4. In the **Flow Name** field, type a flow name.
5. In the **Server Configuration** field, click the name of the Avaya call server profile.
6. Keep the default value for the **URI Group**, **Transport**, and **Remote Subnet** fields.
7. In the **Received Interface** field, click the name of the interface pointing toward the phone network, for example, Sig_Intf_Ext_to_Phone_Net.
8. 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.
9. In the **Media Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Med_Intf_1.
10. In the **End Point Policy Group** field, click the created endpoint policy.
11. In the **Routing Profile** field, keep the default value.
12. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
13. 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 left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The system displays the End Point Flows page.
3. In the **Subscriber Flows** tab, click **Add**.

   The system displays the Add Flow window.
4. Create a User Agent.
5. In the **Flow Name** field, type `Subscriber_Flow_1`.
6. 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.
7. In the **Signaling Interface** field, click the name of the interface that receives all SIP traffic from the phone network. In this example, the interface selected is Sig_Intf_1.
8. Click **Next**.

   The system displays the second Add Flow window.
9. In the Profile section, in the **Source** field, click **Subscriber**.
10. In the **Media Interface** field, select the name of the interface that receives all media traffic from the phone network.

    For example, the name of the interface can be Med_Intf_Ext_to_Phone_Net.
11. 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.
12. 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.
13. If you require TLS transport, in the **TLS Client Profile** field, select an appropriate TLS profile.
14. In the **File Transfer Profile** field, leave the default value: None.
15. 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.

16. **(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.
17. Click **Finish**.

Related links

Adding a new user agent (Advanced Services only) on page 211
Add URI Group field description on page 152
User agents (Advanced Services only) on page 211

Configuring application relay for IM

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **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, complete the fields.
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 348	
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 350	
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 338	

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 **Device Specific Settings** > **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 left 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 **Presence**.
7. 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
8. In the **SBC Device** field, click the Avaya SBCE device.
9. In the **Signaling Interface** field, select a corresponding external signaling interface of Avaya SBCE.
10. 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. On the Advanced Options page, click the **RTCP Monitoring** tab.
4. Select the **RTCP Monitoring** check box.

   Note:

   For relay settings, do not use an IP address that is already in use for SIP signaling and media bandwidth efficiency.
5. In the **Node Type** field, click **Core**.
6. 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.

7. In the **Port** field, type the port number used for RTCP monitoring.
8. 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 341

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 left navigation pane, click **Global Profiles** > **URI Groups**.

   The system displays the URI Groups window.
3. In the Application pane, click **Add**.

   The system displays the URI Group window.
4. 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`.

5. Click **Next**.
6. In the **URI Type** field, click **Plain**.
7. 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.
8. Click **Finish**.
9. In the left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The Application pane lists the registered Avaya SBCE security devices for which the new flow is applied. In the content area, the system displays an ordered list of call flows, Subscriber or Server, for the selected Avaya SBCE security devices.
10. From the application pane, select the Avaya SBCE Device for which the new Subscriber End-Point Flow will be created.

    The system displays the End-Point Flows screen showing the flows that are currently defined for that Avaya SBCE device.
11. Click the **Subscriber Flows** tab.
12. Click **Add**.

    The system 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 329.		
2.	Configure DMZ Avaya SBCE.	Remote worker configuration checklist on page 329.		
2a.	Configure the server interworking profile.	Creating a server interworking profile on page 361.	1. Clone avaya-ru server interworking profile and name the profile as avaya-ru-b2b. 2. In **Advanced** tab, in the **Record Routes** field, click **None**.	
2b.	Configure the server.	Creating an Avaya call server profile on page 330.	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 348.		
2d.	Creating a reverse proxy service for file or firmware download.	Creating reverse proxy service for file or firmware download on page 339.		
2e.	Configure application relay settings for IM.	Application relay settings for IM on page 341.		

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 329.		
2.	Configure DMZ Avaya SBCE.	Remote worker configuration checklist on page 329.		
2a.	Configure the server interworking profile.	Creating a server interworking profile on page 361.	1. Clone avaya-ru server interworking profile and name it as avaya-ru-b2b. 2. In **Advanced** tab, in the **Record Routes** field, click None.	
2b.	Configure the server.	Creating an Avaya call server profile on page 330.	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 348		
2d.	Configure reverse proxy for file download.	Creating reverse proxy service for file or firmware download. on page 339		
2e.	Configure application relay settings for IM.	Configuring application relay for IM. on page 349		
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	

Table continues…

No	Task	Reference	Notes	✔
			same. Therefore, you can use the same profile between the two SBCs. 2. In **Advanced** tab, in the **Record Routes** field, click None.	
3c.	Configure server.		When the Avaya 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 341		

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 **Device Specific Settings** > **Advanced Options**.
3. On the Advanced Options page, click the **RTCP Monitoring** tab.
4. Select the **RTCP Monitoring** check box.

   For relay settings, do not use an IP address that is already in use for SIP signaling and media bandwidth efficiency.
5. 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**.

6. 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.

7. For Core Avaya SBCE configuration, in the **Port** field, type `5005`.

   For other configurations, do not change the values.

8. 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 341

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:

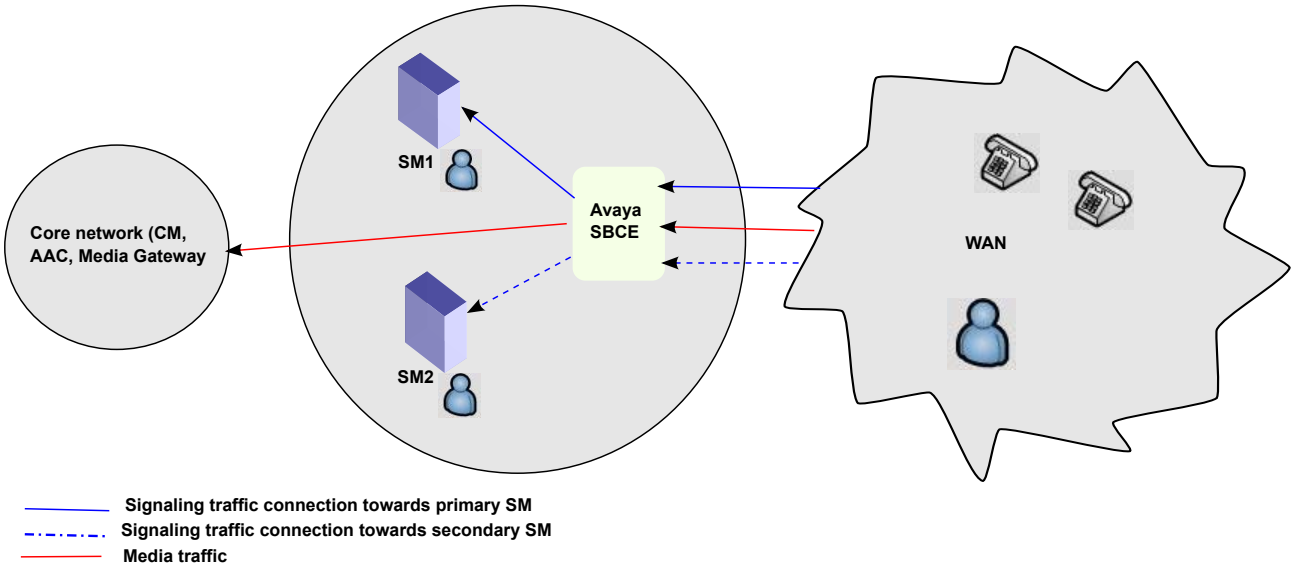
In the following sections:

- 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 361.
2.	Create two external signaling interfaces and two internal signaling interfaces.		Creating an external signaling interface toward phone network on page 332. Creating an internal signaling interface toward Avaya call server on page 333.
3.	Create two external media interfaces and two internal media interfaces.		Creating an external media interface toward phone network on page 334. Creating internal media interface toward Avaya call server on page 334.
4.	Create a media rule.		Creating a media rule on page 344.
5.	Create a server interworking profile.		Creating a server interworking profile on page 361.

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 344.
7.	Create an endpoint policy.		Creating an endpoint policy on page 345.
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 330.
9.	Create a reverse proxy for file download.		Creating a reverse proxy service for file or firmware download on page 339.
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 346.
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 348.
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 145.
13.	Configure an application relay for IM.		Configuring application relay for IM on page 349.

Note:

For more information about remote worker configuration, see Remote worker configuration checklist on page 329.

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

Procedure

1. Log on to the EMS web interface with adminsrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.

   The system displays the Network Management page.
3. Click **Networks** > **Add**.
4. In the Add Network dialog box, type the internal and external IP addresses corresponding to the primary and secondary Session Manager interfaces A1 and B1.
5. Click **Finish**.

Creating a server interworking profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Interworking**.

   The system displays the Interworking Profiles page.
3. Select the **avaya—ru** profile, and click **Clone**.

   The system displays the Clone Profile window.
4. In the **Clone Name** field, type `avaya-ru-multism`.
5. Click **Finish**.
6. Click the new **avaya-ru-multism** profile, and click **Timers**.
7. Click **Edit**.
8. In the **Trans Expire** field, type `4`.
9. Click **Finish**.

Configuring application relay settings for multiple Session Manager

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **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 339
Configuring application relay for IM on page 349
Topology Hiding settings examples on page 236

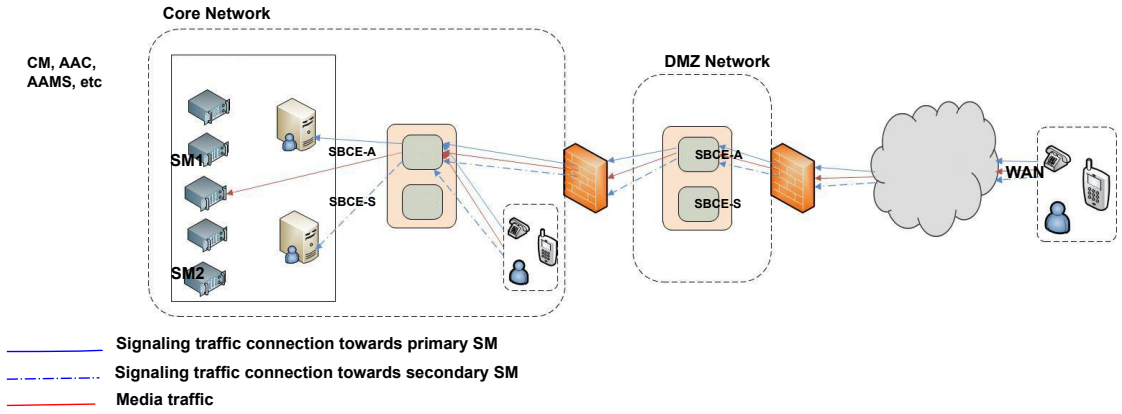
Multiple Session Manager support with back-to-back Avaya SBCEs

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.	
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.	

Table continues…

No.	Task	Notes	✔
		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 339.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Configuring application relay for IM on page 349.	

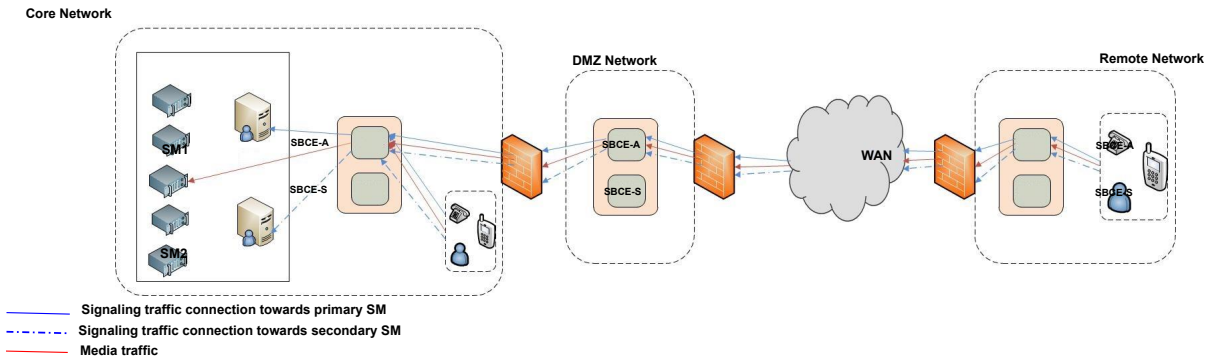
Configuration for Multi-Session Manager support with back-to-back-to-back Avaya SBCEs

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.	
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 339.	
2e.	Configure an **Application Relay** to support IM for remote workers.	See Relay Services field descriptions on page 341.	

Table continues…

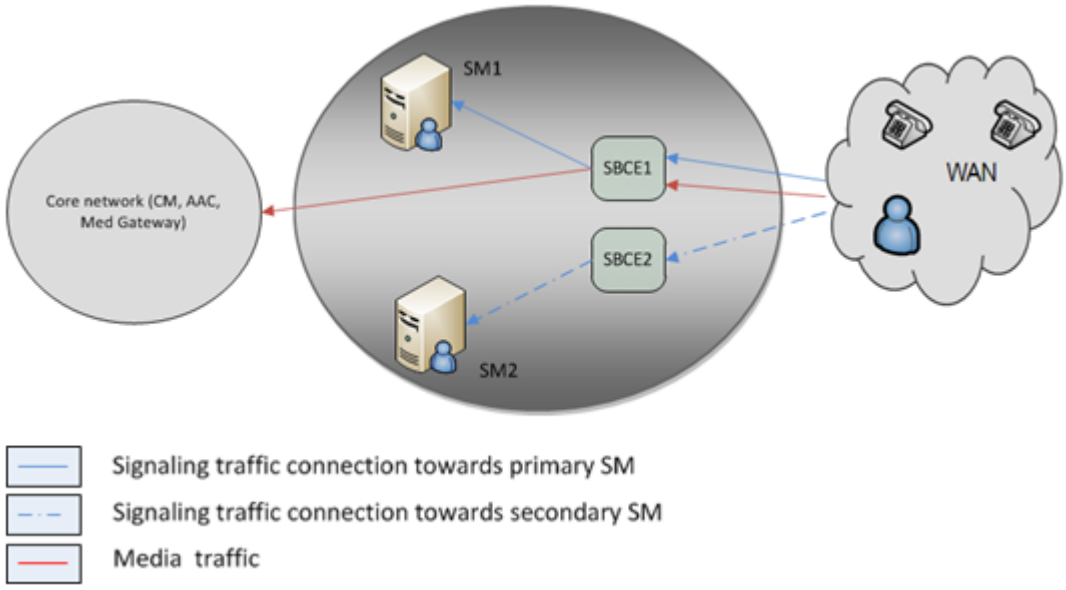
No.	Task	Details	✔
3.	Configure the remote Avaya SBCE.		
3a.	Do not configure public IP address in the **Network Management** feature.		
3b.	Configure server interworking profile.	Clone the avaya-ru server interworking profile and name it `avaya-ru-multism`. The server interworking profile configuration 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 339.	
3f.	Configure an application relay to support IM for remote workers.	See Configuring application relay for IM on page 349.	

Multiple Avaya SBCE deployment

In a Geo-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.

Multiple Avaya SBCE deployment in the non-HA mode

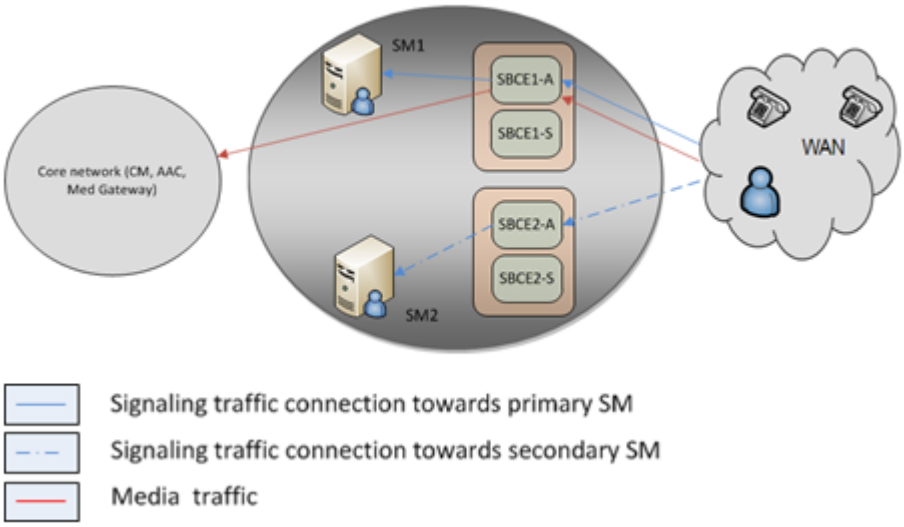
In the following diagram, SBCE1 and SBCE2 are two different physical devices deployed in different data centers. The endpoints have one connection with SBCE1 corresponding to the primary Session Manager, SM1. The second connection with SBCE2 corresponds to the secondary Session Manager, SM2.



Multiple Avaya SBCE 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.



Multiple Avaya SBCE deployment checklist

Use the following checklist to configure the multiple Avaya SBCE deployment.

Note:

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

For more information about remote worker configuration, see Remote worker configuration checklist on page 329.

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 361		
2	Create two external signaling interfaces and two internal signaling interfaces.	Creating an external signaling interface toward phone network on page 332		
3	Create two internal signaling interfaces.	Creating an internal signaling interface toward Avaya call server on page 333		

Table continues…

No.	Task	Reference	Notes	✔
4	Create two external media interfaces.	Creating an external media interface toward phone network on page 334		
5	Create two internal media interfaces.	Creating internal media interface toward Avaya call server on page 334		
6	Create a server interworking profile.	Creating a server interworking profile on page 361		
7	Create two server profiles, one for the primary and another for the secondary Session Manager.	Creating an Avaya call server profile on page 330		
8	Create two routing profiles for the primary and secondary Session Managers.	Creating a routing profile to Avaya call server on page 346	Do not use alternate routing in a Multi-Session Manager deployment. Do not configure the **Next Hop Server 2** field.	
9	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 335		
10	Configure reverse proxy service for downloading file or firmware.	Creating reverse proxy service for file or firmware download on page 339		
11	Create an endpoint policy.	Creating an endpoint policy on page 345		
12	Create a media rule.	Creating a media rule on page 344		
13	Create two subscriber endpoint flows corresponding to the primary and secondary Session Managers.	Creating a subscriber flow on page 348.	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.	

Table continues…

No.	Task	Reference	Notes	✔
14	Create two server flows, one for Session Manager 1 and one for Session Manager 2.	Creating a new server endpoint flow on page 145		
15	Create application rules.	Creating application rules on page 344	Ensure that voice sessions are set as per the user license in the application rules and enable video.	
16	Configure application relay for IM.	Configuring application relay for IM on page 349		
17	Create a reverse proxy service for PPM traffic.	Creating a reverse proxy service for PPM traffic on page 338		

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 372. 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

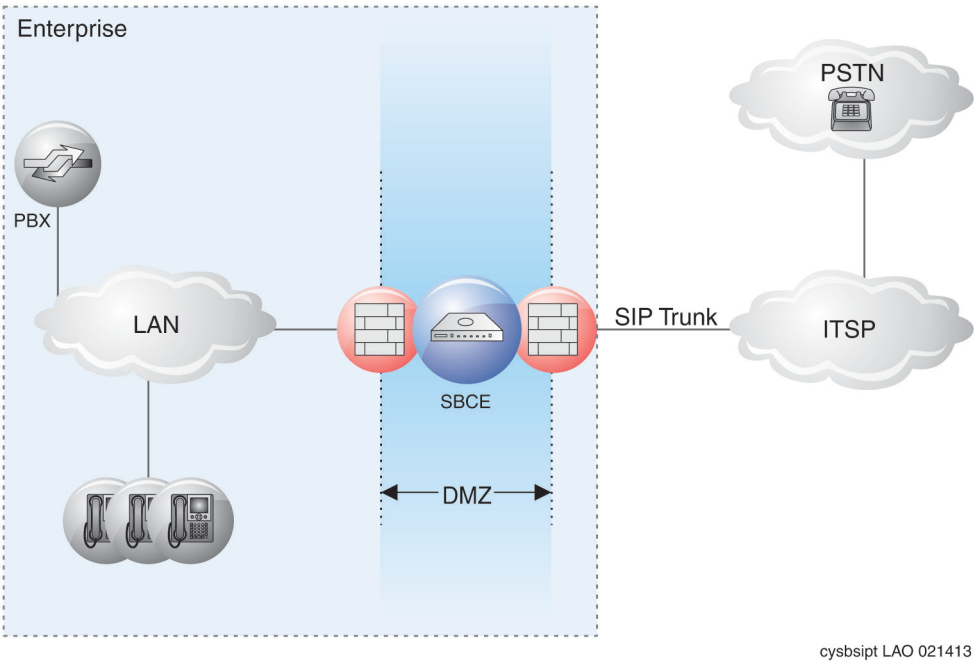


Figure 6: Avaya SBCE deployed in the enterprise DMZ

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 routing profile for call server and trunk server.	Creating Routing Profile for Call Server on page 373.	
2	Create Topology Hiding Profile for trunk server and call server.		
3	Create interworking profiles.	Creating Interworking Profiles on page 375.	
4	Create server profiles,	Creating Server Profile for Call Server on page 375 and Creating Server Profile for Trunk Server on page 377.	
5	Create signaling interfaces.	Creating External Signaling Interface toward Trunk Server on page 378 and Creating Internal	

Table continues…

No.	Task	Reference	✔
		Signaling Interface Toward Call Server on page 379.	
6	Create media interfaces.	Creating External Media Interface toward Trunk Server on page 380 and Creating Internal Media Interface Toward Call Server on page 380.	
7	Create server flows.	Creating Flow toward Call Server on page 381 and Creating Flow toward Trunk Server on page 381.	
8	Perform server-specific configuration for SIP trunking.	Configuring SBCE for Avaya Trunk on page 382..	

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 left navigation pane, click **Global Profiles** > **Routing**.
3. 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.
4. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
5. Click **Next**.

   The system displays the second Routing Profile window.
6. **(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.
7. **(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.
8. 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.

9. In the **Transport** field, enter **TCP** or **TLS**. If you define the transport type here, the system deactivates the common **Transport Type** field.
10. 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.
11. Select the **Next Hop In-Dialog** check box. If you select this option, Avaya SBCE processes the next-hop configuration for in-dialog message as well.
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 Topology Hiding profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Topology Hiding**.

   The left Application pane displays the Topology Hiding profiles, and the Content pane displays the parameters of the selected profile.
3. In the Application pane, click the default profile.
4. In the Content pane, click **Clone**.

   The system displays the Clone Profile window.
5. In the **Clone Name** field, type the name in the `SBCE_to _Call_Svr` format and click **Finish**.

   The system displays the cloned profile in the application pane.
6. To modify the cloned profile, in the left navigation pane, click the cloned profile.
7. In Content pane, click **Edit**.

8. After you have modified the values, click **Finish** to save, submit, and exit.

Related links

Topology Hiding settings examples on page 236

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 left navigation pane, click **Global 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.
3. Click **Add**.
4. In the **Profile Name** field, type a name for the new profile.
5. Enter required information in the Interworking profile screens, and click **Finish**.

   The system displays the newly created interworking profile.
6. Click the **Advanced** tab, and click **Edit**.
7. 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 382
Adding a new Interworking profile on page 250

Creating Server Profile for Call Server

Procedure

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

2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.

3. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.

4. In the **Profile Name** field, type a call server name and click **Next**.

   The system displays the second Server Configuration Profile window.

5. In the **Server Type** field, click **Call Server**.

6. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or of the FQDN.

7. In the **Transport** field, select the transport protocol that you want to use.

8. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.

9. Click **Next**.

   The system displays the Add Server Configuration Profile – Authentication screen.

10. **(Optional)** If you use server authentication, type the related information on this screen.

11. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.

12. **(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.

13. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.

14. **(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.

15. In the **Interworking Profile** field, select the profile name for the type of call server.

16. In the **TLS Client Profile** field, select the client profile to be used for the server.

17. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.

18. In the **Connection Type** field, click a connection type.

19. Click **Finish**.

Creating Server Profile for Trunk-side server

Procedure

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

   The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.
3. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.
4. In the **Profile Name** field, type a trunk server name and click **Next**.

   The system displays the second Server Configuration Profile window.
5. In the **Server Type** field, click **Trunk Server**.
6. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or its FQDN.
7. In the **Transport** field, select the transport protocol that you want to use.
8. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.
9. Click **Next**.

   The system displays the Add Server Configuration Profile – Authentication screen.
10. **(Optional)** If you use server authentication, type the related information on this screen.
11. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.
12. **(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.
13. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.
14. **(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.
15. In the **Interworking Profile** field, select the profile name for the type of trunk server.
16. In the **TLS Client Profile** field, select the client profile to be used for the server.

17. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.
18. In the **Connection Type** field, click a connection type.
19. Click **Finish**.

Creating external signaling interface toward Trunk-side server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Signaling Interface**.

   The left Application pane displays the list of signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
3. In the upper-right corner of the Content pane, click **Add**.

   The system displays the Add Signaling Interface window.
4. In the **Name** field, type a descriptive name for the external signaling interface for the phone network.
5. In the **IP Address** field, select the IP address of the external signaling interface.
6. 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.
7. 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.

8. 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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Signaling Interface**.

   The left Application pane displays any existing signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
3. In the right-corner of the Content pane, click **Add**.
4. 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 213

Creating External Media Interface toward Trunk Server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.
3. In the upper-right corner of the Application pane, click **Add**.

   The system displays the Add Media Interface window.
4. In the **Name** field, enter a descriptive name for the external media interface toward the phone network.
5. In the **IP Address** field, click the IP address of the external media interface.
6. In the **Port Range** fields, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.
7. Click **Finish**.

Creating Internal Media Interface toward call server

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.
3. In the Applications pane, click **Add**.

   The system displays the Add Media Interface window.
4. In the **Name** field, type a descriptive name for the internal media interface of the Avaya call server.
5. In the **IP Address** field, click the IP address of the internal media interface.
6. In the **Port Range** field, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.
7. Click **Finish**.

Creating call server flow

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **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.
3. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow window.
4. In the **Flow Name** field, enter a flow name.
5. In the **Server Configuration** field, click the name of the Avaya call server profile.
6. Keep the default value for the **URI Group**, **Transport**, and **Remote Subnet** fields.
7. In the **Received Interface** field, click the name of the interface pointing toward the SIP trunk, for example, Sig_Intf_Ext_to_Trunk_Net.
8. 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.
9. In the **Media Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Med_Intf_1.
10. In the **End Point Policy Group** field, click the created endpoint policy.
11. In the **Routing Profile** field, choose the routing profile towards SIP trunk.
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.
15. Click **Finish** to save and exit.

Creating trunk server flow

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **End Point Flows**.

   The system displays the End Point Flows page.
3. In the **Server Flows** tab, click **Add**.

The system displays the Add Flow page.

4. In the **Flow Name** field, type a name for the server flow.
5. In the **URI Group**, **Transport**, and **Remote Subnet** fields, leave the default (*) values.

   Depending on customer requirements, modify these fields.
6. In the **Signaling Interface** field, click the name of the interface that receives all of the SIP traffic from the trunk server.
7. In the **Media Interface** field, select the name of the interface that receives all media traffic from the trunk.
8. 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.
9. In the **Routing Profile** field, click the name of the routing profile that points toward the trunk server.
10. In the **File Transfer Profile** field, leave the default value: None.
11. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
12. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.
13. In the **Remote Branch Office** field, keep the default value **Any** or select another remote branch office.

    The **Remote Branch Office** field lists all servers configured for remote branch office.
14. Click **Finish**.

Related links

User agents (Advanced Services only) on page 211
Add URI Group field description on page 152

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 left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration screen.

3. In the **General** tab, ensure that you see the servers created in earlier steps.
4. Click the **Advanced** tab, and ensure that the **Interworking Profile** field displays the correct profile selected for the Avaya server.
5. **(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.
6. Click **Finish** to save and exit.
7. In the left navigation pane, click **Global Profiles** > **Server Interworking**.
8. In the **Interworking Profiles** list, click an Interworking profile.

   You can clone the default `avaya-ru` profile, or create a new interworking profile.
9. Click the **Advanced** tab.
10. Click the **Edit** button at the bottom of the screen.

    The system displays the Advanced Edit window.
11. In the **Extensions** field, select **None**.
12. Click **Finish** to save and exit.
13. In the Server Interworking screen, click the **General** tab.
14. In the lower-center section of the screen, click the **Edit** button.
15. In the **Hold Support** field, click **RFC2543**.
16. 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 250

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 385.
- 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 388

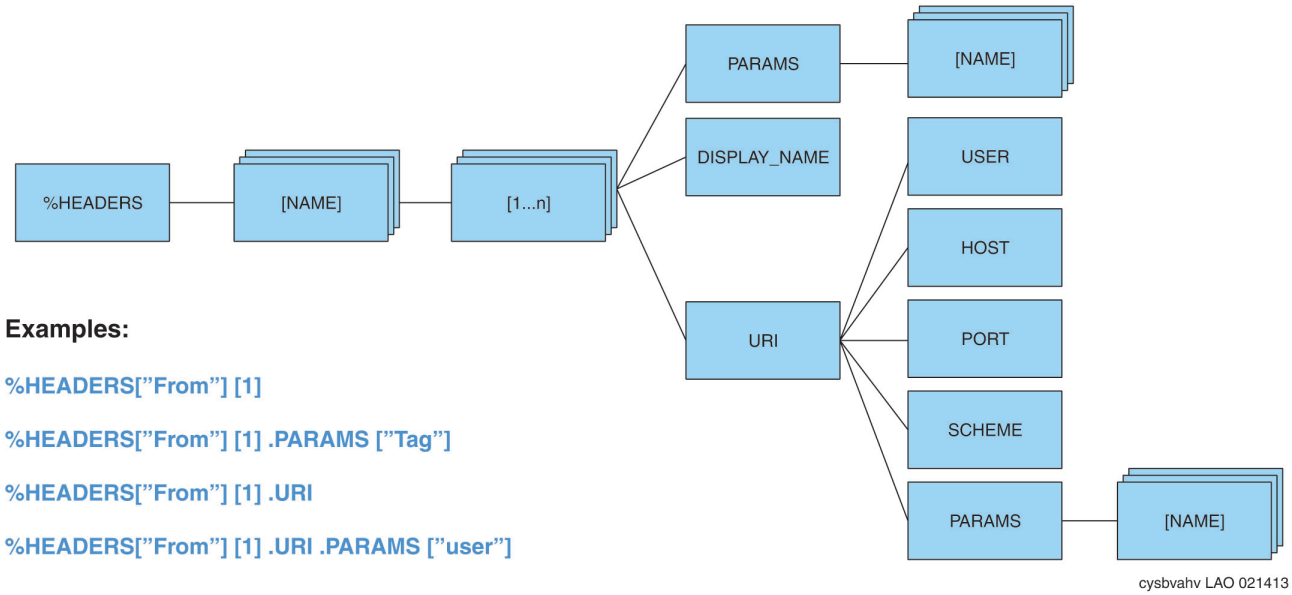
SDP Variable on page 389

Other Variables on page 390

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”]

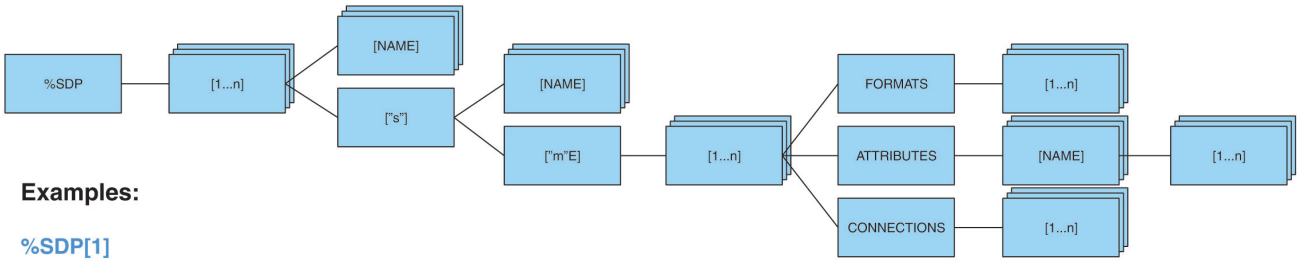
%HEADERS[”From”] [1] .URI

%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).

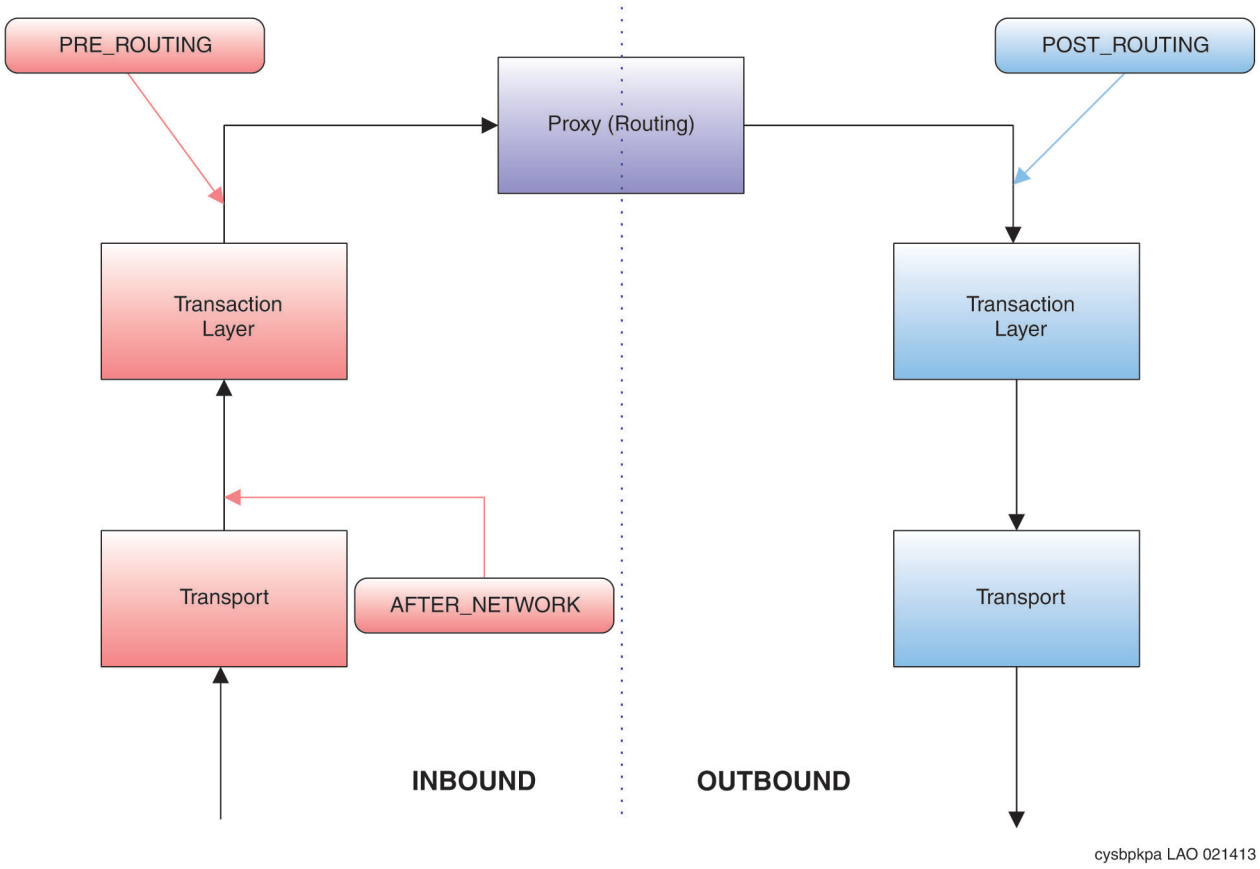
Hook points

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;`
	`    }`
	`}`

Updating the p-asserted-identity field with the value of From header if P-	`within session "ALL"`
	`{`
	`act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`

Table continues…

Description	Scripting Example
Asserted-Identity field value is anonymous	`{ 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); } } }`
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`

Table continues…

Description	Scripting Example

	{
	%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);
	}
	}

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

Table continues…

Description	Scripting Example

	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.

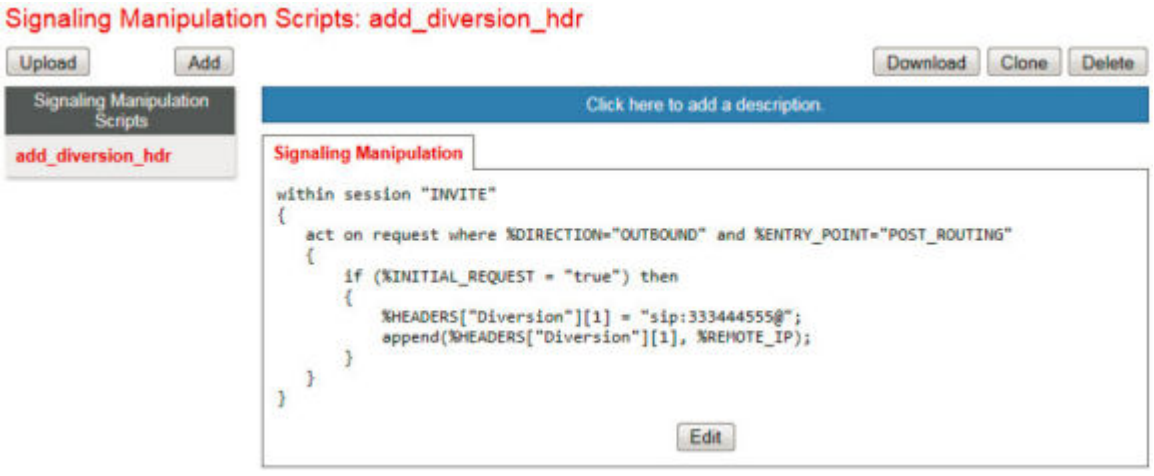
Limitations

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.
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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.
3. In the Server Configuration screen, click **Add**.
4. In the first Add Server Configuration Profile screen, type a name in the **Profile Name** field, and click **Next**.
5. In the second Add Server Configuration General screen, type the appropriate information, and then select **Next**.
6. In the third Add Server Configuration Authentication screen, type the appropriate information, and then select **Next**.
7. In the fourth Add Server Configuration Heartbeat screen, type the appropriate information, and then select **Next**.
8. In the fifth Add Server Configuration 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.
9. Select the profile name and then click the **Advanced** tab button.
10. In the Server Configuration Advanced Tab screen, select the **Edit** button.
11. In the Edit Server Configuration 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.

12. 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.

Note:

Configuring SSL VPN in Avaya SBCE is not supported in Release 7.1. However, SSL VPN is supported on single server or standalone systems.

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. On the dashboard, click **Domain Policies** > **Media Rules**.
2. On the Media Rules page, click the **Advanced** tab.
3. 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.
4. On the dashboard, click **Device Specific Settings** > **Media Interface**.
5. On the Media Interface page, click **Add**.

   The system displays the Add Media Interface dialog box.
6. In the **Name** field, type the name of the media interface.

The **IP Address** field is pre-populated with the Media Interface IP address.

7. 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 Scopia® 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. On the dashboard, click **Domain Policies** > **Media Rules**.
2. On the Media Rules page, select a media rule, and click the **Advanced** tab.
3. 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® networks with SIP at the core. For example, a consumer of an organization can call an Avaya Aura® network by using a WebRTC-enabled browser from the 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™, 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 using the Reverse Proxy feature and the media relay 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 by functionalities within the TURN/STUN server functionality built in Avaya SBCE.

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 supports only audio with G711 codec. Avaya SBCE does not support the OPUS codec, but supports G711. 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. However, the solution does not provide HA survivability, therefore, the existing calls do not work after the primary Avaya SBCE becomes nonfunctional.
- Avaya does not support incoming calls from an external Avaya SBCE network to an internal network between WebRTC-enabled browsers.

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 TURN/STUN relay service for WebRTC calls in Avaya SBCE

Before you begin

In the navigation pane, click **System Management** and verify that the System 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 displays `Commissioned`

In the navigation pane, click **Device Specific Settings** > **Network Management** and do the following:

- In the **Networks** tab, click **Add**.
- In the Add Networks window, configure A1 and B1 interfaces, where A1 is the public interface and B1 is an internal or a private interface.
- To toggle the A1 interface to `Enabled`, in the **Interfaces** tab, click **A1**.
- To toggle the B1 interface to `Enabled`, in the **Interfaces** tab, click **B1**.

About this task

Verify that the Avaya SBCE configuration settings match with the settings in Avaya Breeze™ and Avaya Media Server.

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **TURN/STUN Service**.

   The system displays the TURN/STUN page.
3. In the **TURN/STUN Configuration** tab, click **Add**.
4. In the Add TURN/STUN Server Configuration window, complete the following fields:
   a. In the **Listen Port** field, type the port number. Avaya recommends that you type `3478`. However, you can type a different port number if required.
   b. In the **Media Relay Port Range** field, type the valid port range.

      Avaya recommends that you type the port range as `50000` to `55000`. However, you can type a different port number if required.

      If you use a different port range, verify that there is no clash between other media port ranges for SIP calls.
   c. Select the **Authentication** check box. Type the related details in the **UserName**, **Password**, **Confirm Password**, and **Realm** fields.

      Avaya recommends that you select this check box for WebRTC calls.

      Warning:

      Do not change the Authentication details when a WebRTC call is in progress. Any change in authentication details causes existing calls to disconnect because the TURN processes get restarted.
   d. Select the **FingerPrint** check box. Avaya recommends that you select this check box for WebRTC calls.

   If you change the transport protocol from TCP to UDP or from UDP to TCP, the WebRTC service is impacted. For any change in the transport protocol, you must restart the application.
5. Click **Finish**.

   On the TURN/STUN service page, the system displays the message, `At least one Listen/Media Relay IP Pair is required to complete the configuration. Click here to create a new pairing.`
6. To configure a **Listen Address** and **Media Relay Address** pair, click **here** in the message.

   Note:

   Select a Listen IP interface and a Media Relay IP interface for the Avaya Breeze™ WebRTC solution.

If you change the parameters in some fields, the TURN/STUN application stops working and restarts. These fields are: **Listen Port**, **Media Relay Port Range**, or **Listen IP/ Media Relay IP** pair. Calls that run on existing address interfaces can affect service.

7. Click **Finish**.
8. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   Specify the settings to connect to the services on Avaya Breeze™.
9. Click the **Reverse Proxy** tab, and then click **Add**.
10. In the **Listen IP** field, type the IP in the URL on the external browser to access the services of Avaya Breeze™.
11. In the **Listen Port** field, type the port number that is used on the customer external computer browser to connect to the services on Avaya Breeze™.
12. In the **Connect IP** field, type the IP to connect to Avaya Breeze™.

    This URL within the Avaya SBCE IP is used to reach the WebRTC services within the enterprise.
13. In the **Server Address** field, type the Avaya Breeze™ server IP address and port number.

    The port number is either 80 or 443.
14. Click **Finish**.

Add TURN STUN Server Configuration field descriptions

Name	Description
Listen Port	Listen port number. For TURN/STUN configuration, use port 3478.
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. However, you can type a different port number if required.
Alternate Server 1 to 3	IP address of an alternate server. The load factor on a Turn server address is configured with a load factor threshold. When the load factor threshold is exceeded, the load is redirected to an alternate Turn server address on the same Avaya SBCE or a different Avaya SBCE, when the Turn server addresses on the same Avaya SBCE reaches the load factor threshold.
Authentication	Option to enable authentication.
UserName	User name for authentication.
Password	Password for authentication.

Table continues…

Name	Description
Confirm Password	Password confirmation for authentication.
Realm	Realm used for TURN authentication.
Fingerprint	Option to enable fingerprint.
UDP	Option to enable UDP. If you change the transport protocol from UDP to TCP, the WebRTC service is affected. For any change in the transport protocol, you must restart the application.
UDP Relay	Option to enable UDP relay.
TCP	Option to enable TCP. If you change the transport protocol from TCP to UDP, the WebRTC service is affected. For any change in the transport protocol, you must restart the application. From Release 7.1, the TCP field is available.
TCP Relay	Option to enable TCP relay. From Release 7.1, the TCP relay field is available.
TLS	Option to enable TLS. This field is unavailable by default.
DTLS	Option to enable DTLS. This field is unavailable by default.

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.

From Release 7.1, 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 7.1 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/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.

Checklist for configuring Avaya SBCE for SIPREC

No.	Task	Reference	✔
1	Configure a Recording Server.	Configuring a Recording Server on page 415	
2	Create a routing profile for the Recording Server.	Creating a new routing profile on page 201	
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 416	
4	Assign the recording type and routing profile in Session Policies.	Creating a new session policy for the Recording Server on page 417	
5	Create an application rule for the Recording Server.	Creating a new Application Rule on page 88	

Table continues…

No.	Task	Reference	✔
6	Create a media rule with appropriate codec prioritization for the Recording Server. **Note:** For SRTP calls, ensure interworking is enabled.	Creating a media rule for the Recording Server on page 417	
7	Create an endpoint policy group for the Recording Server.	Creating a new endpoint policy group on page 123	
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 417	
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 419	
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	Creating a server flow on page 145	

Table continues…

No.	Task	Reference	✔
	interface, and Avaya SBCE interface towards recorder is set as the signaling interface for the server flow.		

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 on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Global Profiles** > **Server Configuration**.

   The system displays the Server Configuration page.
3. Click **Add**.

   The system displays the Add Server Configuration Profile page.
4. In the **Profile Name** field, type a name for the new server profile, and click **Next**.
5. In the **Server Type** field, click **Recording Server**.
6. In the **IP Address/FQDN** field, type the IP address of the Recording Server.
7. In the **Port** field, type the port number.
8. In the **Transport** field, click a transport protocol.
9. Click **Next**.
10. On the Add Server Configuration — Heartbeat page, type the requested information in the appropriate fields.

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

    The system displays the Add Server Configuration — Advanced page.
12. 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.

13. 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.

14. **(Optional)** If the Transport type is TLS, select the appropriate TLS client profile.
15. Click **Finish**.

Next steps

Configure routing profile.

Related links

Creating a new routing profile on page 201

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 left navigation pane, click **Domain Policies** > **Signaling Rules**.

   The left Application pane displays the existing Signaling Rule sets, and the Content pane displays the parameters of the selected Signaling Rule set.

3. Click the Signaling Rule that the Avaya SBCE must use for the Recording Server.
4. Click the **UCID** tab.
5. Click **Edit**.
6. Select the **Enabled** check box.
7. 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.

8. 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.

9. Click **Finish**.

Creating a media rule for the Recording Server

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. 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 for the selected Media Rule set.
3. In the Applications pane, click **Add**.

   The system displays the Media Rule window.
4. Enter a name for the new Media Rule, and click **Next**.
5. Enter the appropriate audio and video encryption information, and click **Next**.
6. **(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.
7. **(Optional)** Select the **Allow Preferred Codecs Only** check box.
8. **(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.
9. **(Optional)** In the **Available** column, select the preferred audio and DTMF dynamic codecs that the recorder supports, and click **>**.
10. **(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.
11. Click **Next**.
12. **(Optional)** Enable BFCP, FECC, and ANAT if required.
13. 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 left navigation pane, click **Domain Policies** > **Session Policies**.

   The left Application pane displays the existing session policies, and the Content pane displays the parameters of the selected session policy.

3. In the Applications pane, click **Add**.

   The system displays the Session Policy window.

4. In the **Policy Name** field, type a name for the new session policy, and click **Next**.

   The system displays the second Session Policy window.

5. Select the **Media Anchoring** check box.
6. Select the **Recording Server** check box.
7. In the **Recording Type** field, select the type of recording required.

   The available options are Full Time and Selective.

8. **(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.

9. **(Optional)** To configure Avaya SBCE to terminate the session when Recording Servers do not respond, select the **Call Termination on Recording Failure** check box.
10. In the **Routing Profile** field, click the routing profile that Avaya SBCE must use for the Recording Server.
11. 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 145
Adding a session flow for the Recording Server on page 419
Session Policy field descriptions on page 128

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 left navigation pane, click **Device Specific Settings** > **Session Flows**.
3. In the Application pane, click the Avaya SBCE Device for which you want to create a new session flow.

   The Content Area displays the session flows currently defined for that Avaya SBCE device.
4. Click **Add**.

   The system 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 on to the EMS web interface.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the New profile screen.
4. In the **Profile Name** field, type `AvayaCESClient`.

5. In the **Certificate** field, click a certificate.
6. In the **Peer Verification** field, click **Required**.
7. In the **Peer Certificate Authorities** field, click a certificate.
8. In the **Verification Depth** field, type `1`.
9. In the **Renegotiation Time** field, type `0`.
10. In the **Renegotiation Byte Count** field, type `0`.
11. In the **Ciphers** field, click **Default**.
12. Click **Finish**.

Configuring CES proxy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **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

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.

This section describes the configuration in Avaya SBCE to use the Call Preservation feature.

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 426	
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 426	

Table continues…

No.	Task	Reference	✔
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 427	
4	Add the routing rule to the trunk server flow.	Creating a routing rule for Call preservation on page 427	
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 427	
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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **FGDN Groups**.
3. 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.
4. In the **Group Name** field, type a name for the group.
5. In the **FGDN(s)** field, type the FGDNs as administered in Session Manager.
6. Click **Finish**.

FGDN Group field descriptions

Name	Description
Group Name	The name of the FGDN group.
FGDN(s)	The failover group domain name.

Table continues…

Name	Description
	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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Configuration**.
3. Click the server profile for the Session Manager in the FGDN group.
4. Click the **Heartbeat** tab.
5. 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
6. Click the **Advanced** tab.
7. Click **Edit**.
8. Select the **Enable FGDN** check box.
9. **(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.
10. Click **Finish**.

Related links

Add Server Configuration profile field descriptions on page 242

Creating a routing rule for Call preservation

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Routing**.

   The Application Pane displays the Existing routing profiles. The Content Area displays the routing rules comprising a selected routing profile.
3. In the Application Pane, click **Add**.
4. Type a distinctive name for the new Routing Profile, and click **Next**.
5. In the **Load Balancing** field, click **DNS/SRV**.

6. In the **Server Configuration** field, click **Custom**.
7. 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.
8. Click **Finish**.

Related links

Add routing profile field descriptions on page 202

Adding the routing rule to the trunk server flow

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **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 **Routing Profile** field, click the routing rule you created.
7. Click **Finish**.

Related links

Endpoint flow field descriptions on page 142

Changing transaction expiry time in Server Interworking

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Global Profiles** > **Server Interworking**.
3. Click the interworking profile for the Session Manager instances in the FGDN.
4. Click the **Timers** tab.
5. Click **Edit**.
6. 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 251

Chapter 22: Avaya SBCE configuration for transcoding

From Release 7.1, Avaya SBCE supports transcoding. 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.

This section describes the configuration in Avaya SBCE to support the transcoding feature.

Checklist for configuring Avaya SBCE for transcoding

No.	Task	Description	✔
1	Enable the transcoding feature.	Enabling the transcoding feature on page 430	
2	Administer codec prioritization.	Administering codec prioritization on page 431	
3	Add the media rule, which has transcoding enabled, to an endpoint policy group.	Configuring endpoint policy group on page 431	
4	Add the endpoint policy group to a server flow.	Configuring a server flow for transcoding on page 432	

Enabling the transcoding feature

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Advanced Options**.
3. Click the **Feature Control** tab.

4. Select the **Transcoding** check box.

   Active transcoding calls are lost when the transcoding feature is disabled.

5. Click **Save**.

Administering codec prioritization

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. 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 for the selected Media Rule set.

3. In the Applications pane, click **Add**.

   The system displays the Media Rule window.

4. Enter a name for the new Media Rule, and click **Next**.
5. Enter the appropriate audio and video encryption information, and click **Next**.
6. Select the **Codec Prioritization** and **Transcode When Needed** 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.

7. **(Optional)** To remove all codecs that are not included in the Preferred Codecs list , select the **Allow Preferred Codecs Only** check box.
8. 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.
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 left navigation pane, click **Domain Policies** > **End Point Policy Groups**.

   The system displays the existing End Point Policy Groups.

3. From the Application Pane, select the Policy Group with the policy sets you want to edit.

   The system displays the Policy Sets currently assigned to the selected Policy Group.
4. Click the **Edit** option corresponding to the policy set that you want to edit.

   The system displays the Edit Policy Set page.
5. In the **Media Rule** field, click the transcode-enabled media rule.
6. 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 on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **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 23: 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	Provides a high-level functional and technical description of characteristics and capabilities of Avaya SBCE.	• Sales engineers • Solution architects • Implementation engineers
Implementation		
Deploying Avaya Session Border Controller for Enterprise	Provides hardware installation and preliminary configuration procedures for deploying Avaya SBCE into a SIP enterprise VoIP network.	Implementation engineers
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Provides procedure to deploy Avaya SBCE on VMware.	Implementation engineers
Upgrading Avaya Session Border Controller for Enterprise	Provides procedures for upgrading the software.	Implementation engineers
Maintenance		
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Provides the troubleshooting and maintenance procedures for Avaya SBCE.	• Sales engineers • Implementation engineers

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.

2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

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.

Course code	Course title
5U00090E	Knowledge Access: Avaya Session Border Controller
5U00160E	Knowledge Collection Access: Avaya Unified Communications Core Support

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 http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.

6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

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 task pane, click **Device Specific Settings** > **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.
3. In the Devices list in the Application Pane, click the Avaya SBCE device.

4. Click the **Networks** tab.
5. In the **Networks** tab, click **Add.**

   The system displays the Add Network screen.
6. Type the IP address information, and click **Finish**.
7. Create a reverse proxy service for file or firmware download.

Related links

Adding a new signaling interface on page 213
Creating a reverse proxy service for file or firmware download on page 339

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.

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 *un*trusted 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

accessing Avaya SBCE
through SSH ... 316
active users
field descriptions ... 304
act on statements
scripting language
act on statements ... 386
statement
act on statements ... 386
add
Domain DoS profile ... 222
signaling interface ... 213
subscriber flow ... 142
Topology Hiding header ... 232
adding
adding ... 115–117, 119
custom recording tone ... 418
Header Manipulation rule ... 257
internal IP in System Manager ... 328
interworking profile ... 250
management server ... 195
media forking profile ... 185
network ... 263
network interface ... 260
new recording tone ... 418
new user agent ... 211
regex expression ... 256
request header parameters ... 117
request parameters ... 115
response header parameters ... 119
response parameters ... 116
reverse proxy policy ... 336
routing rule to trunk server flow ... 428
session flow for recording server ... 419
SIP Server profile ... 240
SNMP v1/v2 Community ... 188
URI Manipulation rule ... 256
Adding a new media interface ... 215
Adding a New RADIUS Server ... 182
Adding a Routing Rule ... 204
adding a URI
adding a URI ... 153
URI group ... 153
Adding Media Forking Profile to Session Policy ... 186
adding network ... 263
adding network interface ... 260
Adding SNMP v3 Access ... 192
add interworking profile general
field descriptions ... 251
Add Media Forking Profile
field descriptions ... 185
Add Media Interface Pop-up Window Field Descriptions ... 215
Add RADIUS Server
field descriptions ... 182
add reverse proxy policy
field descriptions ... 337
add routing profile
fields descriptions ... 202
add Server Configuration profile
field descriptions ... 242
add session flow
add session flow criteria ... 148
field descriptions ... 148
add snapshot server ... 161
add snapshot server window field descriptions ... 161
Add SNMP v1/v2 community
field descriptions ... 189
add URI group
add URI group criteria ... 152
field descriptions ... 152
add user
user administration ... 35
add user agent
field descriptions ... 211
administering
BFCP ... 405
codec prioritization ... 431
FECC ... 407
Administration
Administration Parameters ... 22
ASG Configuration ... 22
User ... 22
Administration screen
field descriptions ... 37
administrative account
editing ... 36
privileges ... 37
administrative accounts
creating ... 35
administrative state
editing ... 262
administrative users ... 303
advanced option
configuration ... 173
advanced options
field descriptions ... 175
alarms ... 289
managing
alarms ... 289
application pane ... 21
application relay
IM ... 341
application relay configuration
RTCP monitoring ... 56

application rule 88, 90, 91, 94
counter 80
processing 80
Application Rule
field descriptions 89
application rules
creating 344
architecture
architecture
micro platform 67
standard platform 67
ASG
install 40
audit logs
field descriptions 302
viewing 301
authentication
authentication 104
field descriptions 104
Avaya SBCE
reconfigure 159
Avaya SBCE device
adding 41
Avaya SBCE for Avaya Trunk
configuration 382
Avaya SBCE SIP trunk configuration
checklist 372

B

back-to-back
single Session Manager 354
back-to-back-to-back
checklist 355
SBC 365
SBCEs 362, 364
backup 160
backup/restore
field descriptions 166
basic configuration checklist 158
BFCP
overview 405
BFCP administration 405
blacklist rules
changing 59
border rule 91, 93
Border Rule screen
field descriptions 92
built-in structures 390
functions 390
regular expressions
functions 390
variables and arrays
built-in structures 388

C

CA
certificates 273
CA certificates
deleting 274
viewing 274
cadf file
uploading 187
call flow
call flow 81–84
example 81–84
call flow call processing
call flow call processing 82
example 82
call flow inbound policy invocation
call flow inbound policy invocation 82
example 82
call flow outbound policy invocation
call flow outbound policy invocation 83
example 83
call flow route resolution
call flow inbound route resolution 83
example 83
call flow server flow matching
call flow server flow matching 82, 83
example 82, 83
call flow splitting
increasing capacity 80
call flow transmit to network
call flow transmit to network 84
example 84
call from remote worker
subscriber flow matching
call from remote worker 74
call handling
WebRTC 408
call preservation 425
configuration checklist 425
call server
securing SIP phones 65
securing SIP trunk 63
SIP phones
call server 65
SIP trunk
call server 63
call server profile
creating 330
CDR file content 174
certificate
extract 266
certificate authority certificates
deleting 274
viewing 274
certificate file
uploading 267
certificate management 264

certificate revocation list 275
certificate revocation lists
deleting 276
viewing 275
certificates 267
CA 273
deleting 271
installing 267
viewing 271
CES
CA certificate 421
CES CA certificate
extract 421
CES proxy
configuration 423
change password
field descriptions 32
changing
administrative state 262
blacklist rules 59
calling party presentation 397
DNS IP 324
FQDN 324
gateway IP on a single server 321
gateway IP on Avaya SBCE 323
gateway IP on secondary EMS 323
hostname 324
management IP 46, 320
management IP on a single server 321
management IP on Avaya SBCE 323
management IP on secondary EMS 323
network mask 321
network mask details on Avaya SBCE 323
network mask details on secondary EMS 323
network passphrase 324
transaction expire 428
changing IP, gateway, and mask address on EMS 322
Changing IP address of the primary EMS server on the secondary EMS server 323
changing NTP address on Avaya SBCE devices 322
changing primary EMS IP on unreachable SBCE 322
checklist
configuring transcoding 430
establishing end-to-end TLS communications 283
multiple session border controller deployment
multiple Session Border Controller 368
multiple session manager configuration
multiple session manager 359
Presence server configuration 350
clearing
alarms 290
Client Profile
management 276
client TLS profile
create 422
clipcs
select 316
clipcs command line interface
clipcs command line interface 314
commands descriptions 314
clipcs console 314
clipcs console commands 315
clipcs top commands
instance commands 316
clone
SIP Server Profile 249
cloning
application rule 90
border rule 93
cloning 90, 93, 100, 106, 121, 127, 145, 146, 148, 198
Domain DoS profile 223
interworking profile 258
media rule 100
security rule 106
server endpoint flow 146
session flow 148
session policy 127
signaling rule 121
SNMP trap profle 195
subscriber endpoint flow 145
ToD rule 198
Topology hiding profile 234
Cloning an existing routing profile 206
code blocks
statements
code blocks 387
codec prioritization 101
administering 431
codec prioritizations
codec prioritizations 128
field descriptions 128
command line interface
overview 308
Command Line Interface 31
commands
clipcs console 314
instance
commands 315
commissioning
Avaya SBCE device 43
communications session
establish 318
communications settings
terminal program 318
concurrent sessions
counter 80
config/firmware
files download 437
configuration
endpoint policy group 80
File server 438
phone 439
configuration checklist
back-to-back 363

configuration checklist *(continued)*
back-to-back-to-back ... 365
configure
application relay settings ... 362
configuring
application relay ... 349
automatic snapshots ... 165
Avaya SBCE for other trunks ... 383
CES proxy ... 423
emergency calls from unregistered endpoints ... 352
endpoint policy group ... 431
High Availability ... 48
packet capture ... 304
recording server ... 415
server flow for transcoding ... 432
UCID ... 416
configuring application relay
core SBCE ... 57
remote Avaya SBCE ... 58
RTCP monitoring ... 57, 58
configuring Avaya SBCE
real time trunk status ... 296
configuring HA Heartbeat Interval
configuring HA Max Retries ... 181
configuring multi-session manager
back-to-back-to-back
SBC configuration ... 365
back-to-back-to-back SBCEs ... 362, 364
configuring Presence server
checklist ... 350
configuring SBCE
simultaneous downloads ... 439
connecting terminal device ... 317
connecting to
Avaya SBCE device ... 317
connection to SBC
terminal device ... 317
console ... 314
console commands
gui-snapshot-create
console commands ... 310
gui-snapshot-restore
console commands ... 311
gui-user
console commands ... 308
root level ... 308
root level commands
console ... 308
converting
certificates to PEM format ... 286
counter
application rule ... 80
concurrent sessions ... 80
create ... 333
create internal ... 333
creating
application rule ... 88
creating *(continued)*
border rule ... 91
call server flow ... 381
client profile ... 277
client TLS profile ... 422
creating
... 88, 91, 94, 103, 108, 123, 126, 141, 145, 148, 151, 197
CSR ... 265
endpoint flow ... 141, 145
external Media Interface toward Trunk Server ... 380
External Signaling Interface toward Trunk-side Server
... 378
FGDN groups ... 426
internal Media Interface toward call server ... 380
interworking profiles ... 375
media rule ... 94, 197
new TLS server profile ... 280
policy group ... 123
PPM mapping profile for presence server ... 350
routing profile ... 373
routing rule for call preservation ... 427
security rule ... 103
server endpoint flow ... 145
Server Profile for Call Server ... 375
Server Profile for trunk server ... 377
session flow ... 148
session policy ... 126
session policy for Recording Server ... 417
signaling interface ... 332
signaling rule ... 108
SNMP trap profile ... 193
subscriber endpoint flow ... 141
Topology Hiding profile ... 230, 374
trunk server flow ... 381
URI group ... 151
Creating
server interworking profile ... 361
creating a new routing profile ... 201
CRLs
deleting ... 276
viewing ... 275
CSRs
externally generated ... 266

D

dashboard
about ... 21
alarms ... 21
component descriptions ... 288
dashboard ... 288
incidents ... 21
installed devices ... 21
notes ... 21
screen
dashboard ... 288
DB-9 connector

DB-9 connector *(continued)*
connecting terminal device 317
debugging
field descriptions 171
delete
administrative account 36
SIP Server Profile 250
Topology Hiding header 234
Topology Hiding profile 233
deleting
application rule 91, 94
CA certificates 274
certificate authority certificates 274
certificate revocation lists 276
certificates 271
client profile 279
CRLs 276
deleting
91, 94, 102, 107, 122, 125, 126, 129, 147, 150, 154, 155, 200
Domain DoS profile 225
end-point flow 147
existing user agent 212
Header Manipulation rule 258
interfaces 262
interworking profile 259
media rule 102
policy group 126
policy set 125
security rule 107
server profile 283
session flow 150
session policy 129
signaling rule 122
SNMP trap profile 194
system snapshot 165
ToD rule 200
URI from URI group 154
URI group 155
URI Manipulation rule 257
deleting an existing media interface 216
Deleting an Existing RADIUS Server Profile 184
deleting an existing routing profile 207
deleting an existing signaling interface 214
Deleting an Existing SNMP v1/v2 Community 189
Deleting an Existing SNMP v3 Account 193
deleting a routing rule 205
deleting regex rules 257
deploy
multiple SBCE in HA mode 367
multiple SBCE in non-HA mode 366
deploying
geographically dispersed Avaya SBCE HA 55
deployment
multiple SBCE 366
designating a snapshot server 160
device configuration 41
Device Management Overview 167
device specific settings
settings 27
diagnostics
field descriptions 303
diagnostics results 302
diagram
remote user topology 325
direction flags
In/Out 80
disabling
SNMP traps by severity 196
display registered users 298
display settings
field descriptions 20
Domain DoS
field descriptions 224
Domain DoS profile
rename 223
Domain DoS profiles 222
domain policies 25, 62
management 88
managing
domain policies 88
unified communications 62
DoS
security features 218
DoS/DDoS global parameters
field descriptions 219
DoS/DDoS settings
editing 219
DoS learning
field descriptions 226
DoS Protection
editing 248
recalculate values 248
DoS whitelist 248
DoS Whitelist
adding
URI or domain 248
deleting
URI or domain 248
download files
config/firmware 437

E

edit
Topology Hiding header 233
editing
administrative state 262
application rule 90
border rule 93
Client Profile 279
codec prioritization 101
Domain DoS profile 223
DoS Protection 248

SIP server profile *(continued)*
editing
..... 90, 93, 101, 107, 114, 117–119, 124, 128, 154, 199
endpoint policy group
editing 125
existing user agent 212
Header Manipulation rule 258
interfaces 263
interworking profile 256
media forking 128
media rule 101, 199
policy set 124
request header parameters 118
response header parameters 119
response parameters 117
security rule 107
server endpoint flow 146, 147
server profile 282
signaling rule 114
SIP server profile
editing 247
SNMP profile 194
subscriber endpoint flow 146, 147
URI group 154
URI Manipulation rule 257
Editing an existing Media Interface 216
Editing an Existing RADIUS Server Profile 183
Editing an Existing Routing Profile 204
editing an existing signaling interface 214
Editing an Existing SNMP v3 Account 192
editing a routing rule 204
editing device configuration 169
editing regex rules 257
editng
editing 149
session flow 149
emergency group 153
EMS software
updating 50
EMS web interface 19
Administration 22
Backup 22
button descriptions 29
Dashboard 22
Global parameters 23
Global profiles 23
log in 31
Restore 22
System Management 22
task pane 22
tool bar 20
enabling
FGDN 427
interfaces 160
transcoding 430
enabling high availability 170
endpoint
flows *(continued)*
flows
endpoint 141
endpoint administration
GROUP identifier 437
endpoint flow 141, 145, 147
cloning
endpoint flow 145
creating
endpoint flow 141
endpoint flows
managing 140
endpoint policy
creating 345
endpoint policy group
configuration 80
configuring 431
establishing end-to-end TLS communications
checklist 283
exiting the runtime options screen 52
external media interface
creating 334
external signaling interface 332
extract certificate 266
extracting
CES CA certificate 421

F

Failover Group Domain Name
enabling 427
far end camera control 407
FECC
administration 407
FGDN
enabling 427
FGDN group
field descriptions 426
FGDN groups
creating 426
field description
TLS Certificates screen 272
field descriptions
active users 304
add interworking profile general 251
add reverse proxy policy 337
add snapshot server window 161
add user agent 211
advanced options 175
alarms .....
field descriptions 289
audit logs 302
backup/restore 166
change password 32
debugging 171
diagnostics 303
display settings 20

alarms *(continued)*
DoS/DDoS global parameters 219
DoS learning 226
FGDN group 426
firewall 60
incident viewer 291
install CA certificate 275
install CRL 276
network management 260
new profile 277
new server profile screen 280
PPM Mapping Profile 336
scrubber 228
Security Rules 106
server status 297
SigMa 401
subscriber flow profile 142
syslog management 208
syslog viewer 299
System Management 42
system viewer 293
Topology Hiding Profiles 231
trace 306
TURN STUN configuration 411
files download
config/firmware 437
File server
configuration 438
firewall
field descriptions 60
firmware/config
files download 437
Forward Error Correction
FEC 406
From header
Topology Hiding examples 237
functions 390
built-in 390
built-in structures .....
functions 390

G

geographically dispersed Avaya SBCE HA pair
interface connections 53
Global Parameters
vverview 181
Graphical User Interface (GUI)
browser support 18
GROUP identifier
endpoint administration 437

H

HA failovers 47
HA node
HA node 49
HA node *(continued)*
status states 49
hardware warranty 16
Header Manipulation rule
adding 257
deleting 258
editing 258
HEADERS variable 388
High Availability
configuration 48
High-Availability pair
geographically dispersed 52
hook points 391

I

identity engine 150
In/Out
direction flags 80
inbound
call processing
inbound 73
policy invocation
inbound 75
inbound policy
invocation
inbound policy 72
incidents 290
incident viewer
field descriptions 291
increasing capacity
call flow splitting 80
InSite Knowledge Base 435
install
ASG 40
authentication file 40
installation wizard
field descriptions 44
installing 267
Avaya SBCE device 43
CA certificate 274
Certificate Revocation List 275
certificate to SBCE 269
third-party certificates 265
installing certificate
single server Avaya SBCE 270
installing rules
scrubber 227
interface
signaling 213
viewing 262
interfaces
deleting 262
existing signaling interface 214
view 214
internal IP
adding 328

internal media interface
avaya call server ... 334
create internal ... 334
creating ... 334
internal signaling interface
create ... 333
internal signaling interface ... 333
internal signaling interface toward call server ... 379
interworking profile
adding ... 250
cloning ... 258, 330
deleting ... 259
editing ... 256
renaming ... 259
IP, gateway, and network mask change ... 321

L

learned DoS parameters
setting ... 225
license file
PLDS download ... 50
load balancing ... 200
locating
SIP servers ... 76
logging
EMS web interface ... 31
logging in to EMS ... 316
logs ... 299

M

making a system snapshot ... 161
management IP
change ... 46, 320
managing
network options ... 179
SBCE logging level ... 171
server profiles ... 280
session flows ... 140
SIP options ... 178
Managing Avaya SBCE security devices ... 18
managing device-specific settings ... 212
Managing Port options ... 179
Managing security features ... 177
manipulation of P-Asserted-Identity Header ... 395
media
unachoring ... 130
unanchor ... 130
media and video
field descriptions ... 97
Media NAT ... 97
media forking ... 128
Media Forking
overview ... 184
media rule ... 94, 100–102
creating ... 344
mobile workspace
topology diagram ... 325
monitoring
RTCP ... 180
rtcp for remote worker ... 357
Monitoring RTCP
single Session Manager deployment ... 351
multi-session manager
web interface
gui ... 358

N

network
adding ... 263
viewing ... 262
network connectivity overview ... 240
network interface
adding ... 260
network interfaces
configuring ... 259
network
interface ... 259
network management
editing ... 263
field descriptions ... 260
network options
manage ... 179
networks
editing ... 263

O

options tab display field descriptions ... 178
other trunks
configuration ... 383
other variables ... 390
outbound
call processing
outbound ... 78
outbound policy
invocation
outbound policy ... 79
outbound policy call processing
invocation
outbound policy call processing ... 73
overview ... 18
basic system configuration ... 157
command line interface ... 308

P

packet capture ... 304
password
console ... 32
EMS GUI ... 32

password *(continued)*
policies 32
passwords 31
PFX
extract 266
phone
configuration 439
PKCS#12
extract 266
PLDS download
license file 50
policy group 123, 126
policy group summary 124
policy invocation
route resolution
policy invocation 75
policy set 124, 125
policy sets 125
port ranges
field descriptions 179
PPM Mapping Profile
create 335
field descriptions 336
PPM Services
Mapping Profile 25
prerequisites 41
processing
application rule 80
profile
call server 330
protocol scrubbing 226

Q

QoS parameters tab 120

R

real time
SIP Server Status 296
rebooting a device 168
recording server
configuration 415
Record Route header
Topology Hiding examples 238
regenerating self-signed certificates 324
registered users
user registrations 297
viewing
registered users 297
related documentation 433
remote access 404
remote support 404
remote worker
checklist 329
Session Manager configuration 327
Remote Worker registration
Remote Worker registration *(continued)*
limitation 326
rename
SIP Server Profile 249
renaming 155
application rule 90
border rule 93
Domain DoS profile 223
interworking profile 259
media rule 102
renaming 90, 93, 102, 107, 121, 129, 199
security rule 107
session policy 129
signaling rule 121
SNMP trap profile 195
ToD rule 199
Topology Hiding profile 234
Renaming an Existing Routing Profile 206
reordering
policy sets 125
reordering 125
reordering precedence
reordering precedence 149
session flows 149
reordering routing rule precedence 205
request header parameters 117, 118
Request Headers Parameters Tab 117
request parameters 115
response header parameters 119
Response Headers Parameters Tab 119
response parameters 116, 117
Responses Parameters Tab 116
restarting a device 168
restore 160
restore a system snapshot 162
restoring a snapshot file 163
restoring a snapshot file automatically 164
retrieving
a snapshot file 163
reverse proxy policy
adding 336
reverse proxy service
create 338
reverse proxy service for file or firmware download
create 339
route resolution
call towards a server
route resolution 76
routing profile
route resolution 72
routing
call processing toward network 79
call sever
call processing toward network 79
routing 73
toward network 73
routing profile

routing profile *(continued)*
call server ... 346
Routing Profiles ... 200
Routing Rule Management ... 204
RTCP
monitoring ... 56
RTCP monitoring
remote worker ... 356
single Session Manager ... 352
RTCP Monitoring
field descriptions ... 56
rules
application rules
rules ... 88
border ... 91
border rules
configuration ... 91
endpoint policy rules
rules ... 122
media rules
rules ... 94
security rules
rules ... 102
signaling rules
rules ... 108
Time of Day (ToD) rules
rules ... 196
rules and policies
associations ... 68
configuration ... 66
policies and rules
associations ... 68
configuration ... 66
rules and policies configuration checklist ... 70
running
scripts on the CES server ... 422
turntop command ... 409

S

SAL ... 404
SBCE
back-to-back-to-back ... 362, 364
sbceinfo commands
getapptype ... 313
getemsip ... 313
gethwtype ... 313
getversion ... 313
SBCE reconfiguration command options ... 319
scenarios
media unanchoring ... 130
Scopia and Avaya SBCE interoperability with SRTP ... 406
scrubber ... 227
field descriptions ... 228
scrubber actions
configuration ... 228
scrubber rules
scrubber rules *(continued)*
installing ... 227
viewing ... 227
SDP capability negotiation ... 100
SDP header
Topology Hiding examples ... 239
SDP variable ... 389
secure CES proxy ... 421
Security Feature Control ... 177
security rule ... 103, 106, 107
Security Rules
field descriptions ... 106
selecting
log levels ... 207
server endpoint flow ... 145–147
server flow
creating ... 347
matching
server flow ... 72
server flow for transcoding
configuring ... 432
server flow matching
call toward server
server flow matching ... 79
server interworking ... 250
server profile
management ... 280
server status
field descriptions ... 297
session
accessing clipcs remotely ... 318
flows
session ... 147
policies
session ... 126
session flow ... 148–150
session flow for recording server
adding ... 419
session flows ... 149
session manager
Avaya SBCE internal and external IP addresses ... 361
configure primary and secondary ... 361
Session Manager
disabling PPM ... 328
session policy ... 126, 127, 129
editing
session policy ... 127
field descriptions ... 128
Session Policy
media forking profile ... 186
session statement
scripting language
session statement ... 385
statement
session statement ... 385
session variables ... 386
setting

setting *(continued)*
learned DoS parameters 225
setting EMS time zone 51
settings
externally generated CSRs 266
show flow dynamic 315
shutting a device down 167
Sigma Design Overview 402
SigMa Editing the Allow Header 399
SigMa Editor
field descriptions 401
SigMa Prefix Stripping 400
SigMa Replace From Header For a Set of Users 398
SigMa Scripting Examples 392
SigMa Scripting Tutorial 395
Signaling
QoS parameters tab 120
signaling 120
signaling interface
create internal 333
field descriptions 213
signaling interface 333
signaling manipulation
scripting language
signaling manipulation 384
SigMa primer
signaling manipulation 385
SigMa scripting language
signaling manipulation 384
signaling rule 108, 114, 121, 122
field descriptions 109
signaling rule 109
simultaneous downloads
configuring SBCE 439
single sign on 150
configuring 150
identity engine server
configuring 150
SIP
call processing
SIP 73, 74
SIP message processing
high level 71
message processing
SIP high-level 71
SIPREC
codec prioritization 417
configuration 413
creating media rule 417
SIPREC feature
overview 413
SIP registration
processing 71
registration processing
SIP 71
SIP server
DoS configuration 217
SIP Server Configuration
profile management 240
SIP Server profile
adding 240
SIP servers
locating 76
SNMP Settings 187
SNMP trap profile
clone 195
create 193
delete 194
rename 195
SNMP traps
disable by severity 196
SNMP v1/v2 Community
editing 189
software warranty 16
solution
config/firmware files download 437
specifying
SigMa Script in Server Configuration 402
SRTP failover
considerations 406
SRTP support 406
statistics 293
subscriber endpoint flow 141, 145–147
subscriber flow
advanced services 348
matching
subscriber flow 71
subscriber processing toward remote worker
route resolution
subscriber processing toward remote worker 75
support 435
support under warranty 16
synchronizing
certificate to SBCE 269
syslog management
field descriptions 208
Syslog Parameter Management 207
syslog viewer
field descriptions 299
system alarms 289, 290
managing
system alarms 289
system incidents 290
system logs 299
System Management
field descriptions 42
system statistics 293
system viewer
field descriptions 293

T

tagging
VLAN 261

terminal device 317
third-party certificates
installing 265
time zone 51
tips and tricks
TLS 286
TLS
tips and tricks 286
TLS management
management 26
tls profile management 276
ToD
field descriptions 123, 197
policy 123
ToD 197
ToD rule 197–200
To header
topology hiding 237
topology diagram
remote worker 325
Topology Hiding 234
affected headers 235
Topology Hiding header
adding 232
deleting 234
editing 233
Topology Hiding headers 235
Topology Hiding profile
clone 234
create 230
deleting 233
Topology Hiding Profiles
field descriptions 231
Topology Hiding settings
examples 236
trace
call
trace 304
field descriptions 306
traceSBC command
usage 312
training 434
transaction expire
changing 428
transcoding
enabling 430
introduction 430
transcoding configuration
checklist 430
trap
description 193
troubleshooting
system 29
TURN STUN configuration
field descriptions 411
turntop
usage 408
turntop command
running 409

U

UCID 120, 121
configuration 416
unified communications 62
uniform resource identifier
groups
uniform resource identifier 151
uninstalling device configuration 169
upgrading system management 170
upload
certificate file 267
uploading
cadf file 187
URI
groups
URI 151
URI from URI group 154
URI group 151, 153–155
URI Manipulation rule
adding 256
deleting 257
editing 257
regex rules 257
user accounts
administrator account 34
user agents 211
user-defined variables 391

V

variable 388, 389
variables 385, 386, 390
variables and arrays
built-in 388
built-in structures .....
variables and arrays 388
VGA connection 316
Via header
Topology Hiding example 238
videos 434
view
existing signaling interface 214
viewing
a CDR file 174
administrative users 303
alarms 289
audit logs 301
authorized user agents 212
CA certificates 274
certificate authority certificates 274
certificate revocation lists 275
certificates 271
CRLs 275

viewing *(continued)*
device configuration 169
diagnostics results 302
Domain DoS profile 222
DoS/DDoS settings 218
incidents 290
interface 262
logs 299
network 262
policy group summary 124
scrubber rules 227
statistics 293
status of the SIP servers 297
system alarms 289
system incidents 290
system logs 299
system statistics 293
viewing 124, 289, 290, 293, 299, 302, 303
Viewing an existing media interface 215
viewing EMS time zone 51
Viewing SIP Server profile 247
VLAN
use 261

W

warranty 16
webRTC
configuring TURN/STUN 409
WebRTC
call handling 408
webRTC considerations 408
where clause 385
whitelisting
Avaya SBCE internal IP address 327