Administering Avaya Session Border Controller for Enterprise

Release 6.2
Issue 2
January 2013

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software (“Product(s)”). 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: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. “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.

License types

Designated System(s) License (DS). End User may install and use each copy 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, 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.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). 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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Feature comparison

Advanced services licenses are not available with this release of Avaya SBCE. Therefore some features described in this book are not currently available. The following table indicates which features are available with the current release and which will be available in the future.

Feature	Available in January 2013 release	Available in future
Remote management services	Yes	Yes
Signaling manipulation	Yes	Yes
SIP trunking	Yes	Yes
Media anchoring	No	Yes
Mobile workspace user	No	Yes
Reverse turing test	No	Yes
Signaling mirroring service	No	Yes
UC device configuration proxy	No	Yes

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Document number	Title	Description	Audience
Design			
	Avaya Session Border Controller for Enterprise	High-level functional and technical description of	Sales Engineers,

Document number	Title	Description	Audience
	Overview and Specification	characteristics and capabilities of the Avaya SBCE.	Solution Architects and Implementation Engineers
Implementation			
	Installing Avaya Session Border Controller for Enterprise	Hardware installation and preliminary configuration procedures for installing Avaya SBCE into a SIP enterprise VoIP network.	Implementation Engineers
	Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading: • software only from Sipera 4.0.5 to Avaya SBCE 6.2 • Avaya Aura® Session Border Controller6.0 to Avaya SBCE 6.2	Implementation Engineers

About this book

Throughout this document in text and illustrations, except when referring to a specific platform and that platform's capabilities, the term Avaya SBCE will be used to collectively refer to both the standard hardware platform and the smaller Portwell hardware platform. The term EMS will refer to either the EMS (Element Management System) internal software and its graphical user interface (GUI) running inside a stand-alone SBCE server or to a dedicated external Avaya EMS server, which can be used to manage several SBCE servers.

Document sections dealing with the two features mentioned (i.e., HA and Media Forking) above that are not supported on the Portwell platform will include in the section titles the notation, "(Standard Platform only)."

Document sections dealing with features and capabilities not supported on the Basic Services license version will include in the section titles the notation, "(Advanced Services only)."

Document sections dealing with features and capabilities that are supported on both the Advanced Services and Basic Services license versions will have section titles that do not include the "(Advanced Services only)" notation.

Also, when referring to Avaya SBCE devices, the terms *Primary* and *Secondary* are used interchangeably with the terms *Active* and *Stand-by*, respectively.

Introduction

This administration document provides an overview of the Avaya Session Border Controller Enterprise (Avaya SBCE) UC network security solutions along with an overview of how the controller can be administered using the Avaya SBCE Control Center. It primarily describes how to use the Unified Communications Policies (also referred to as Domain Policies) feature of the Avaya SBCE to configure, apply, and manage security rule sets based upon the source and destination end-point and session call flows entering or exiting the enterprise. In addition, this document provides the information necessary to allow you to effectively monitor SIP-based UC network security using the Avaya SBCE Control Center and various incident and historical reports.

Currently, there are two Avaya SBCE hardware platform versions available, the standard platform and the Portwell platform. The Portwell platform provides identical capabilities to those available in the standard platform with the exception of the exclusion of two features: (1) High-Availability (HA) support for both media and signaling (only available in the standard platform); (2) Media Forking (only available in the standard platform).

There are also two licensed versions of the Avaya SBCE based on product licensing:(1) Advanced Services (i.e. All services including Remote Worker and SIP Trunking) and (2) Basic Services (i.e., SIP Trunking only).

Managing Avaya SBCE security devices

Avaya SBCE security devices can be monitored and controlled in one of two ways: either remotely via a graphical user interface (GUI) or locally via a command line interface (CLI). GUI access is provided by Ethernet management interface ports located on each Avaya SBCE equipment chassis, which allow up to 10 simultaneous log-ons to the Avaya SBCEControl Center. Equally high-speed serial CLI access is provided by the console ports also located on the Avaya SBCE equipment chassis, which allow administrators to establish direct, physical connections to the devices using any commonly available terminal device for provisioning, management, troubleshooting, maintenance, and repair. Both the GUI and CLI interfaces can be accessed any time an Avaya SBCE security device is operational.

In addition to the management and serial terminal ports, the Avaya SBCE security devices have an interactive 32-character, 2-line LCD display for status.

Graphical User Interface (GUI)

Avaya SBCE security devices support a GUI interface through the EMS that can be accessed from any remote physical location using either a Mozilla Firefox™ (3.0 or later), Microsoft Internet Explorer™ (7.0 or later), or Google Chrome™ (4.0 and later) web browser. This provides administrators and maintenance personnel the ability to view concise, real-time, graphical representations of the security activities and operational condition of the network being monitored in addition to providing access to all the screens and windows necessary to properly configure and maintain each security aspect of a particular AAvaya SBCE device.

SBCE Control Center

The Avaya SBCE Control Center is the fully integrated, web-accessible operations and administration platform for the Avaya SBCE UC security products. It is a graphical user interface (GUI) that centralizes and simplifies the provisioning, administration, control, and monitoring of the Avaya SBCE signaling, media, and intelligence elements to reduce the overall operational burden and eliminate unnecessary system management complexity.

The Avaya SBCE Control Center contains a redundant Solid® database to store configuration and subscriber information which is continually updated by each of the deployed Avaya SBCE security elements.

The following functions can be performed using the Avaya SBCE Control Center:

- Configuration Management
- Alarm and Fault Management
- Performance Management
- Administration and Maintenance

Command Line Interface (CLI)

The 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. These tasks are executed using various commands entered via a terminal emulator such as Telnet or another commonly available serial application like HyperTerminal. The CLI interface is available whenever an Avaya SBCE equipment chassis is running. Security is provided through a combination of account login and user access privileges.

Note:

It is recommended that the Command Line Interface should only be used under the direction of authorized Avaya support personnel. Refer to Chapter 10, Command Line Interface, for information on using the CLI.

Chapter 2: Getting Started

Prerequisites

To ensure proper operation, the most recent versions of the following software programs are required to be installed on the workstation to be used for accessing the Avaya SBCE Control Center:

- Mozilla Firefox™ (3.0 or later)

or

- Windows® Internet Explorer™ (7.0 or later)

or

- Google Chrome™ (4.0 and later)

Passwords

There are two types of passwords associated with Avaya SBCE:

- Console Password
- EMS GUI Password

Console password complexity

The Console Password:

- must be at least eight (8) characters long
- must contain at least two (2) uppercase characters, not including the first character of the password
- must contain at least one (1) lowercase character
- must contain at least one (1) special character
- must contain at least two (2) digits, not including the last character of the password

- Password Authentication Module (PAM) enforces password security, and hashes are stored in: **/etc/shadow**
- maximum length is not limited
- is hashed by MD5 hash algorithm

EMS GUI password complexity

The EMS GUI Password:

- must be at least eight (8) characters long
- must contain mixed uppercase and lowercase characters
- must contain at least one (1) special character
- must contain at least one (1) number
- maximum length is not limited
- is hashed by SHA—256 hash algorithm

Password policies

Password Policies:

- Upon first-time power-up of the Avaya SBCE, user is allowed immediate access to the Avaya SBCE system via console.
- When user is configuring the box (this is where the Text-based User Interface (TUI) comes up), the system asks for root and ipcs account passwords.
- The root password is determined and set during product installation.
- All of 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.”

Note:

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

The EMS GUI Admin Login ID and Password were assigned by Avaya when the Avaya SBCE security was initially configured prior to shipment. Older installations may still use the previous default login / password: ipcs / ipcs.

Logging-in to the SBCE Control Center

The Avaya SBCE Control Center is used to provision, monitor and control the Avaya SBCE functional entities and is accessed via a web browser (either Mozilla Firefox™ or Windows® Internet Explorer™).Logging-in to the Avaya SBCE Control Center using the **Admin** account login ID and password provides unrestricted top-level access to all the features and parameters supported by the Avaya SBCE security products.

- Mozilla Firefox™ (3.0 or later)

or

- Windows® Internet Explorer™ (7.0 or later)

or

- Google Chrome™ (4.0 and later)

Caution:

Great care should be taken by the Admin when configuring or altering domain policies or network, system or security parameters as these actions will have an immediate and direct affect on the level of security provided to the enterprise. In addition, changing any of these parameters may also impact application or network availability.

Logging—in procedure

Use the following procedure to login to the Avaya SBCE Control Center for the first time:

Procedure

1. Open a new browser tab or window.
2. Enter the following URL: `https://<Control_Center_IP_Address>` where <Control_Center_IP_Address> is the IP address of the Avaya SBCE Control Center you want to access.
3. Press **Enter**.

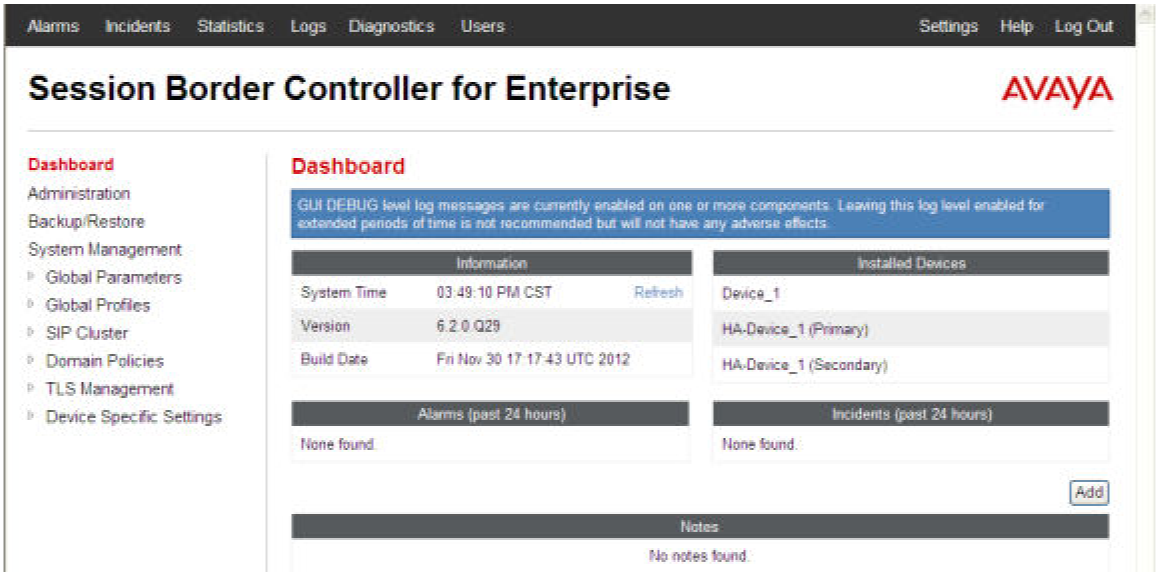
   The **Avaya SBCE Control Center** (EMS) sign-in screen is displayed
4. Enter your assigned **Login ID** and **Password** and click the **Log In** pushbutton.

   Note:

   The EMS GUI Admin Login ID and Password were assigned by Avaya when the Avaya SBCE security was initially configured prior to shipment and should have been provided to you when the equipment was delivered and installed.

The **Avaya SBCE Control Center – Dashboard Screen** is displayed.

Example



Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

Information		
System Time	03:49:10 PM CST	Refresh
Version	6.2.0.Q29	
Build Date	Fri Nov 30 17:17:43 UTC 2012	

Installed Devices
Device_1
HA-Device_1 (Primary)
HA-Device_1 (Secondary)

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

Notes
No notes found.

Control Center screen descriptions

The Avaya SBCE Control Center — Dashboard Screen is the main administrative and configuration display screen for the Avaya SBCE security system. It is the Dashboard Screen that the Avaya SBCE displays upon a successful logon and is comprised of three main sections — *Tool Bar*, *Task Pane*, and *Content Area*. Together they provide an ordered, top-level textual and/or visual representation of the security status of the monitored IP network in real-time, as well as all the user-selectable options and controls that are necessary to facilitate administration.

The Dashboard screen is the top-level display screen which provides direct access to all the features, functions, and information available on the current release of the Avaya SBCE security system. The Dashboard Screen displays the software build version, build number, and copyright information for the software running on your system.From the Dashboard Screen you can display additional, separate summary windows which contain active, up-to-the-minute alarm, incident, and statistical information as well as review and exchange textual messages with other administrative accounts. In addition, you can select wizards to either provision additional Avaya SBCE security devices into the network or define new destination-source call flows.

When a Feature and Function selection (e.g., The SIP Cluster feature and its Cluster Proxy function) is made in the Task Pane, an additional Application Pane area is displayed between the Task Pane and the Content Area.

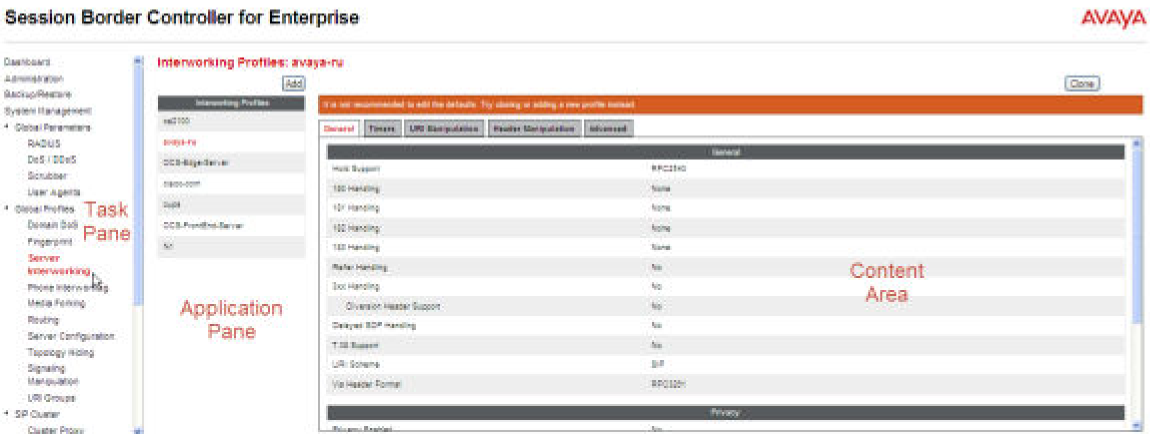
In the Application Pane, you can select a single item, such as a device, profile, rule, group, etc, to display the selected item's configuration information in the Content Area to the right.

Note:

Throughout this document, navigation instructions for each procedure will be shown as follows:

Select the <function name> function from the <feature name> feature from the Task Pane.

Example: Select the `Server Interworking` function from the `Global Profiles` feature from the Task Pane.



It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No

Tool bar

The Tool Bar appears directly beneath the Identification Bar at the top of each Avaya SBCE Control Center screen and contains several user-selectable icons (Alarms, Incidents, Statistics, Users, Logout, Help, and About) and a constantly-blinking alarm status indicator (Alarms). Descriptions of the tool bar items are provided in the table below.

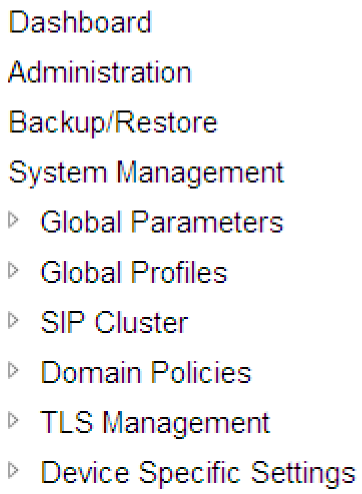
Tool bar item descriptions

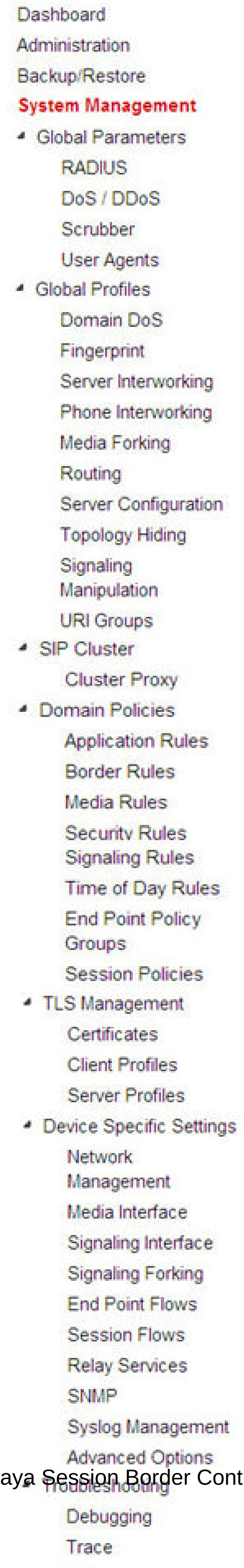
Name	Function	Description
Alarms	Alarm Viewer	Opens the Alarm Viewer window in a new window.(When alarms are present, an alarm count is displayed in red next to the function name.)
Incidents	Incident Viewer	Opens the Incident Viewer window a new window.
Statistics	Statistics Viewer	Opens the Statistics Viewer in a new window.
Logs	Logs Viewer	Opens a menu for selecting either the Syslog Viewer or the Audit Log Viewer.
Diagnostics	Diagnostics Tests	Opens the Diagnostic Test Selection window. Test selections which can then be made are: Full

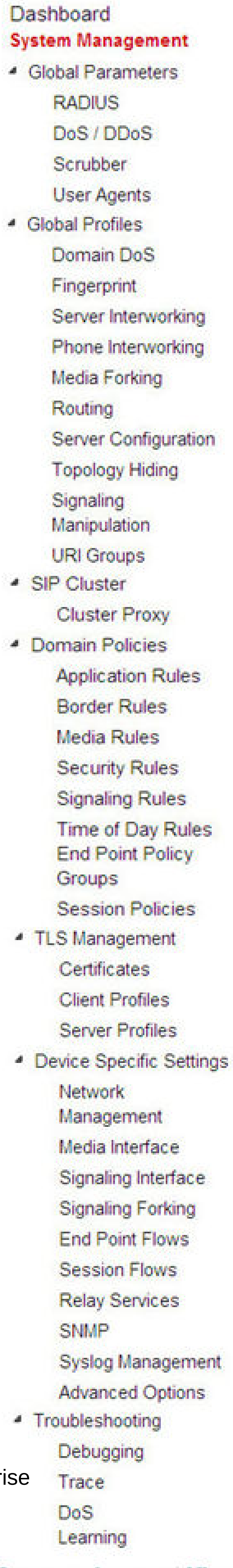
		Diagnostic, Ping Test, Application, Protocol, Octeon PFC, Octeon TCP, Octeon TLS, Octeon Memory, and Octeon Ethernet.
Users	Display Users	Opens the SBCE Active User Account window.
Help	Help	Activates system help.
Log Out	Log Out	Logs you out of the SBCE Control Center and redisplays the main login screen..

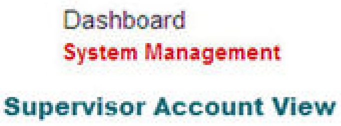
Task Pane

The Task Pane is always displayed on the left side of the Avaya SBCE Control Center and provides access to each of the functional areas of the Avaya SBCE Control Center. The functional areas to which a user is granted access is determined by the administrative privileges assigned to them by the System Administrator (Administrator, Manager, or Supervisor).




Dashboard
Administration
Backup/Restore
System Management
Global Parameters
RADIUS
DoS / DDoS
Scrubber
User Agents
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SIP Cluster
Cluster Proxy
Domain Policies
Application Rules
Border Rules
Media Rules
Securitv Rules
Signaling Rules
Time of Day Rules
End Point Policy Groups
Session Policies
TLS Management
Certificates
Client Profiles
Server Profiles
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting
Debugging
Trace


Dashboard
System Management
Global Parameters
RADIUS
DoS / DDoS
Scrubber
User Agents
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SIP Cluster
Cluster Proxy
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Time of Day Rules
End Point Policy Groups
Session Policies
TLS Management
Certificates
Client Profiles
Server Profiles
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting
Debugging
Trace
DoS Learning


Dashboard
System Management
Supervisor Account View

Dashboard

Following login, the Avaya SBCE Control Center — Dashboard Screen is displayed, from which you can view and access all the features, functions, and information available of the current release of theAvaya SBCE security system. Using this screen you can display additional separate summary windows which contain active, up-to-the-minutealarm, incident, and statistical information as well as review and exchange textual messages with other administrative accounts. Finally, you can select specific Avaya SBCE security features and functions from the Task Pane for administration and maintenance.

Note:

Depending upon which administrative user account is chosen (i.e., you can login as Administrator, Manager, or Supervisor), it will determine which specific features will be displayed in the Task Pane.

Administration

The Administration function displays the User Administation screen in the content area of theAvaya SBCE Control Center which displays a comprehensive list of all users having Admin, Manger, and Supervisor privileges. In addition, this feature screen allows you to add new user accounts, edit existing user accounts, and delete existing user accounts.

Backup/Restore

The Backup/Restore function displays the Backup/Restore window which allows you to create a back-up file containing a snapshot of the entireAvaya SBCE system configuration. In addition, the Backup/Restore window allows you to restore system files when necessary.

System Management

The System Management function displays the System Management window which contains two tabs (Installed and Updates) that allow you to either view, configure, shut down, or restart Avaya SBCE security devices.

Global parameters

Selecting the Global Parameters feature from the Task Pane allows you to configure parameters across all Avaya SBCE Appliances.

Global parameters feature descriptions

Feature	Description
RADIUS	Displays the Radius tab allowing you to provision RADIUS server parameters, such as IP address, retry timeout, etc.
DoS/DDos	SIP only. Displays the DoS Settings screen containing five tabs: Single Source DoS, Phone DoS/DDoS, Stealth DoS/DDoS, Call Walking and Toll Fraud. These tabs allow you to configure which actions the Avaya SBCE security system will perform when certain types of DoS, DDoS, and Call Walking attacks have been detected.
Scrubber	Displays the Scrubber screen containing two tabs: Packages and Rules which allow you to determine which scrubber rule sets (packages) the Avaya SBCE system will use when analyzing SIP signaling messages for anomalies.
User Agents	Displays the User Agents screen which allows you to define which types of SIP user agent are trusted end-points.

Global profiles

Selecting the Global Profiles feature from the Task Pane allows you to configure parameters across all Avaya SBCE Appliances.

Global profiles feature descriptions

Feature	Description
Domain DoS	Displays the Rate Limit screen that allows you to determine how the Avaya SBCE

	security solution will respond to suspected DoS attacks. Responses include Alert Only, Enforce Limit, Sender Intention Verification, and White List.
Fingerprint	Displays the Fingerprint screen which allows you to configure and manage the various criteria used to determine the ‘fingerprint’ of a particular SIP end-point. ⚠ **Caution:** Fingerprint parameters should only be changed after consulting Avaya’s technical support staff.
Server Interworking and Phone Interworking	Displays the interworking screen containing five tabs: General, Timers, URI Manipulation, Header Manipulation, and Advanced. These tabs allow you to edit specific SIP signaling message parameters to facilitate interoperability between various end-points and SIP implementations within the enterprise.
Media Forking	Media forking allows a duplicate stream of media to be sent to a recording or monitoring device. The stream can be used for quality assurance and compliance purposes.
Routing	Displays the **Routing Profile** which allows you to manage parameters related to routing SIP signaling messages.
Server Configuration	Displays the Server Configuration screen containing six tabs: General, Authentication, Heartbeat, Advanced, DoS White List, and DoS Protection. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. **Note:** DoS White List and DoS Protection are only activated once the DoS Protection check box is selected under the Advanced Tab.
Topology Hiding	Displays the Topology Hiding screen which allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted

	or changed to maintain the integrity of the network. Hides the topology of the enterprise network from external networks.
Signaling Manipulation	Signaling Manipulation adds the ability to add, change, and delete any of the headers and other information in a SIP message. This feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language.
URI Groups	Displays the URI Group screen. The domain(s) comprising the URI Group is/are displayed 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 End Point and Session policies. URI Groups can be added, deleted, viewed, edited cloned, and deleted using the corresponding buttons in the Application Pane and Content Area.

Domain policies

The **Domain Policies** feature, also referred to as *Unified Communication Policies*, allows you to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control, and normalize call flows.

Domain policies feature descriptions

Feature	Description
Application rules	Displays a list of existing **Application Rule** sets in the Application Pane. **Voice**, **Video**, and **IM** application states (**IN** / **OUT**) are displayed, along with the number of maximum concurrent sessions. These parameters can be changed in a pop-up window accessible from the Content Area. Application rules can be added, viewed, edited, cloned, or deleted using the

	corresponding buttons in the Application Pane and Content Area.
Border rules	Displays the **NAT Traversal** tab which allows you to manage the way in which the Avaya SBCE security device operates when deployed at the edge of the network (secure border access).
Media rules	Displays a list of existing **Media Rule** sets in the Application Pane. The **Media Encryption**, **Media Anomaly**, **Media Silencing,** and **Media QoS** parameters for an existing Media Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the parameters group you want to see or change. Media rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.
Security rules	Displays a list of existing **Security Rule** sets in the Application Pane. The **Authentication**, **Compliance**, **Fingerprint**, **Scrubber**, and **Domain DoS** parameters for an existing Security Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the group of parameters you want to see or change. Security Rule sets can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.
Signaling rules	Displays a list of existing **Signaling Rule** sets in the Application Pane. The **General**, **Requests**, **Responses**, **Request Headers**, **Response Headers** , and **Signaling QoS** parameters for an existing Signaling Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the control parameters group you want to see or change. Signaling rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.

Time of day rules	Displays a list of existing **Time-of-Day (ToD) Rule** sets in the Application Pane. The parameters of a ToD Rule set are displayed in the Content Area. These parameters can be viewed, edited, or deleted. In addition, new ToD Rule sets can be added as needed.
End Point Policy	Displays a list of existing end-point **Policy Groups** in the Application Pane. The Policy Sets comprising the Policy Group are displayed in the Content Area. A Policy Group is a completely user-definable combination of previously configured **Application**, **Border**, **Media**, **Security**, **Signaling**, and **ToD** rule sets that are applied to call flows traversing the enterprise as identified by **Sessions** feature. Policy Groups rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area. . ⚠ **Caution:** The default End Point Policy parameters should only be changed after consulting Avaya’s technical support staff.
Session Policies	Displays two tabs which control how media streams are processed by the SBCE: **Codec Prioritization** and **Media Anchoring**. Session Policies added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area. ⚠ **Caution:** The Session Policies parameters should only be changed after consulting Avaya’s technical support staff.

Device specific settings

The **Device Specific Settings** feature allows you to 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, end-point and session call flows, as well as the ability to manage system logs and control security features.

Global profiles feature descriptions

Feature	Description
Network Management	Displays the Network Management screen containing two tabs: **Network Configuration** and **Interface Configuration**. The **Network Configuration** tab allows you to manage the internal and external IP addresses assigned to a particular Avaya SBCE security device while the **Interface Configuration** tab allows you to enable or disable SBCE Ethernet interfaces (**A1**, **A2**, **B1**, and **B2**).
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).
Signaling Forking	**Note:** **For standard platform only.** Displays the **Signaling Forking** screen to where you can add or modify signaling forking profiles, which provides for the splitting and redirection of signaling packets monitoring and security purposes.
SNMP	Displays the SNMP information screen, which is used to create access accounts for granting certain users access to the SNMP information.
End Point Flows	Displays two tabs (**Subscriber Flows** and **Server Flows**) in the Content Area which allow you to determine how calls will be handled by the SBCE Together, 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.
Relay Services	Enables Web conferencing for Mobile Workspace Users. Displays two tabs (**Application Relay** and **File Transfer**). **Application Relay** enables PSOM NAT traversal. **File Transfer** enables file transfers between IM clients.
Troubleshooting	**Troubleshooting** is a subfolder function under **Device Specific Settings**. (See the next section for complete description of the **Troubleshooting** functions.)

Troubleshooting

Troubleshooting is a subfolder function under Device Specific Settings main menu item in the Task Pane. The Troubleshooting Feature provides options that are useful for troubleshooting problems.

Troubleshooting feature descriptions

Feature	Description
Debugging	Displays the debugging screen for EMS and devices, containing tabs for information on Subsystem Logs and GUI Logs.
DoS Learning	Displays the **Learned Info** screen which allows you to select a time slot (i.e., weekday/ weekend and morning/afternoon, evening/ night) for which DoS-related information will be learned and displayed, providing a snap-shot of potential threats and anomalies which may be targeting the network. **Note:** This learns “Server DoS/DDoS” only, and the learning applies to : **Global Profiles > Server Configuration > Profile > DoS Protection Tab**

Trace	Displays the **Trace** screen which allows you to define the parameters necessary to trace a media packet traversing the network..

TLS Management

The **TLS Management** feature allows you to manage the parameters defined by the Transport Layer Security (TLS) protocol specification 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.

Successful TLS management requires that the two parties to a communications session (the *client* and *server*) be properly certified, so that their identity to each other can be unquestioningly verified and trusted. The mechanism used to authenticate subscriber identities are *certificates* that are issued by a trusted Certificate Authority (CA). The **TLS Management** features allows you 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 very precisely define the manner in which you want the TLS feature to function.

TLS management feature descriptions

Feature	Description
Certificates	Displays a single Certificates tab screen that is used to handle the installation of Certificates, CA Root Certificates, and Certificate Revocation Lists (CRL).
Client Profiles	Displays a list of all currently available client profiles in the Application Pane. You can also define additional client profiles if necessary using automated field requests to solicit the information necessary to authorized a client to participate in a secure TLS session.
Server Profiles	Defines a list of all currently 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.

Application pane

When certain security features are selected from the Task Pane, a list of available items (Avaya SBCE device, VoIP server, rule set, etc.) to which that feature can be applied is displayed in the Application Pane. When the desired item is selected from the list in the Application Pane, the specific feature parameters that are assigned to that item are displayed in the Content Area of the display screen where they can be managed as desired.

Dashboard screen content area

This portion of the Avaya SBCE Control Center presents the contents of the selected features or functions that are selected from the task pane. The different screens and windows displayed by the Avaya SBCE Control Center use various pushbuttons and icons to perform certain functions.

The Content Area of the Dashboard screen is different than the Content Area that is displayed when other features are selected from the Task Pane in that it does not contain an Application Pane, nor does it contain low-level function-specific information such as feature fields or parameter values. Instead, it contains various summary areas which display top-level, system-wide information such as which alarms and incidents are currently active, links to available Quick Links, 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

Area	Description
About	Displays the system version and build date
Installed Devices	A list of all the Avaya SBCE security devices which are installed and provisioned in the enterprise VoIP network
Alarms	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	The incidents feed is a streaming feed which displays currently active system incidents. It

Area	Description
	is parsed according to the Avaya SBCE device type which generated it. More information on the listed incidents can be accessed by clicking the Incidents push-button from the Tool Bar. A separate Incidents window will be opened from which the incident can be viewed and manually cleared. Incidents are associated with security issues while alarms are associated with hardware/ connectivity issues.
Notes	This portion of the Content Area allows you to view and exchange 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.

Control center button descriptions

The buttons and icons used by the different Avaya SBCE Control Center screens and pop-up windows.

Control center pushbuttons

Pushbutton	Description
Activate Feature	Causes the currently selected features / parameters to be enabled.
Add / New	Allows you to create a new element, rule, or policy depending upon the screen currently being displayed.

Alarm Status Indicator	If there are any active alarms, a red rectangle will appear and display the current number of alarms.
Cancel	Cancels the current operation and closes the window without saving any changes.
Checkbox	Used to select or deselect specific items, features, parameters, or actions.
Clone	Causes the currently selected rule or parameter to be copied to a new record to facilitate defining new rules.
Close	Cancels the current operation and closes the window without saving any changes.
Delete	Allows you to delete the selected element or item from the currently displayed list.
Display Statistics	Displays the Statistics screen in a new window.
Edit	Allows you to edit 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 on-line help.
Incidents	Activates a separate Incidents pop-up window to display all recently reported system-wide incidences.
Logout	Logs you out of Avaya SBCE Control Center and re-displays the login screen.
Radio Button	Used to select or deselect the corresponding item.
Reboot Device	Reboot the associated Avaya SBCE security device.
Shutdown Device	Shutdown the associated Avaya SBCE security device.
Restart Application	Restart an SBCE application.
View Configuration	View the configuration of the associated Avaya SBCE security device.
Install Device	Install the associated Avaya SBCE security device into the network.

Save	Allows you to save 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 pop-up 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 pop-up window that displays all active Administrator accounts.
Swap Device	Allows you to automatically substitute 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	Causes the selected item to be uninstalled (de-commissioned) from the network.

Chapter 3: Administrative User Accounts

Administrative accounts

Administrative (Admin) user accounts are manually created and edited using the Administration feature selected from the Task Panel. Using this feature, you are able to create three levels of administrator: Admin, Manager, and Supervisor. The Admin user has full read/write access to all the features provided by the Avaya SBCE security device, which includes adding, editing, and deleting other administrative accounts. The Manager has the same access privileges as the Admin user, with the exception of not being able to add new administrative accounts. The Supervisor has the least system access; this account only has read privileges for viewing incidence and statistical logs.

Creating a new administrative account

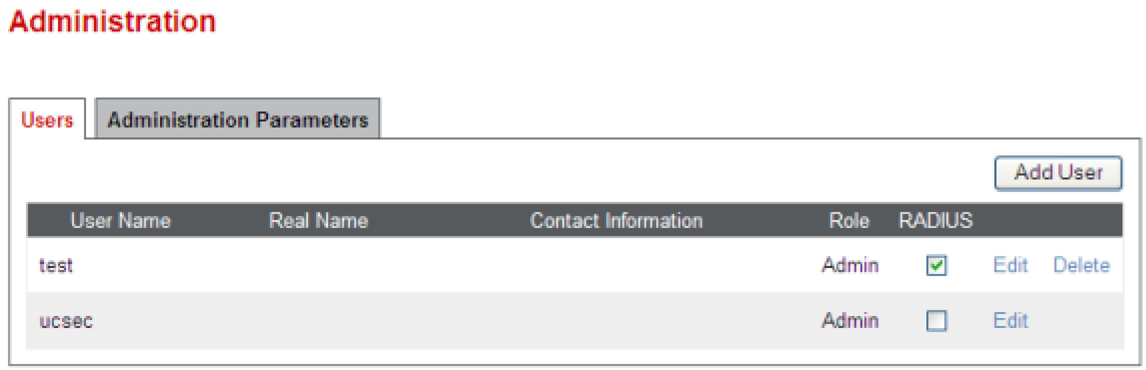
About this task

Procedure

1. Login to the SBCE Control Center as the Admin.
2. Select the **Administration** function from the Task Pane.
   The Users tab of the Administration screen is displayed.
3. Click the **Add User** button in the upper-right part of the Content Pane.
   The Add New Administrative User pop-up window is displayed.
4. Enter the appropriate information in the parameter fields. See the New administrative account field descriptions on page 46 table for more information.
5. Click **Finish** to create the new administrative account.
6. Close the window.

The new account will be displayed in the Content Area.

Example



User Name	Real Name	Contact Information	Role	RADIUS		
test			Admin	☑	Edit	Delete
ucsec			Admin	□	Edit	

New administrative account field descriptions

Use these topic descriptions

Field	Description
Real Name	Real name of the individual for whom this account is being created.
Contact Information	Contact information (e.g., email, phone, number etc.) of the owner of this account.
User Name	System name assigned to the owner of this account.
RADIUS User	Checkbox indicating that the user will be authenticated via a RADIUS server. If checked the following Password and Confirm Password fields will be deactivated.
Password	The login password being assigned to this account. Only activated if the RADIUS User checkbox is unchecked.
Confirm Password	A reliability feature to ensure the correct password has been entered in the previous field. Only activated if the RADIUS User checkbox is unchecked.
Permission	The level of administrative access to be granted to this account.

<table>
<tr><td></td><td><table>
<tr><td>Admin</td><td>Highest level of system access, having full read/write permissions for all screens and features. Can create and delete new user accounts.</td></tr>
<tr><td>Manager</td><td>Read/write access for all screens and functions, with the exception of not being able to create new user accounts.</td></tr>
<tr><td>Supervisor</td><td>Only read access to certain incidence and statistical logs.</td></tr>
</table></td></tr>
</table>

Setting administrative account privileges

About this task

Use the following procedure to configure administration parameters for all existing user accounts (i.e., Administrator, Manager, and Supervisor).

Procedure

1. Select the **Administration Parameters** tab.
   The Administration Parameters screen is displayed.
2. Enter the requested information into the appropriate fields. See the Administration parameters field descriptions on page 48 table for more information.
3. Click **Save** to save the parameter configuration.
   A notification will be displayed in the content area informing you that the new configuration has been successfully saved.

Next steps

Editing an existing administrative account on page 49

Administration parameters field descriptions

Field	Description
Local Account Password Expiration (days)	Checkbox indicating whether or not the password assigned to this user account will expire after the number of days indicated in the corresponding field. If checked, the assigned password will expire after the indicated number of days. If unchecked, the password assigned to this user account will not expire after a predetermined time period. It can be used indefinitely.
Local Account Password Expiration Notification (days)	Checkbox indicating whether or not an expiration notification should be given to the user when they log-on to the EMS informing them that their password will expire within the indicated number of days. If checked, a notification will be displayed each time the user logs-on to the EMS. If unchecked, a notification will not be displayed.
Radius Server	A checkbox indicating whether or not RADIUS user accounts are to be authenticated. If checked, RADIUS user accounts will be authenticated by the RADIUS server selected from the corresponding pull-down menu. If unchecked, RADIUS user accounts will not be authenticated.
RADIUS Authentication Protocol	A drop down containing all supported RADIUS authentication methods. This will be used instead of the configured RADIUS profile's authentication protocol. The currently supported methods are: • Password Authentication Protocol (PAP): Password is transmitted in plain text to the RADIUS server. • RFC 5090/Digest: Password uses a client and server nonce 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. This should be the same value as configured on the RADIUS server.

Editing an existing administrative account

Before you begin

Avaya SBCE

About this task

Use the following procedure to edit an existing administrative account.

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.
2. Click on **Administration** in the Task Pane.
   The users screen is displayed.
3. In the content area, click on the Edit button corresponding to the admin user account you want to edit.
   The Edit User window will pop-up.
4. Edit the desired fields.
5. Click on **Finish** to update the administrative account record and close the window.

Deleting an administrative account

Before you begin

Avaya SBCE

About this task

Use the following procedure to delete an existing administrative account.

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.
2. Click on **Administration** in the Task Pane.
   The administrative users screen is displayed.

3. In the content area, click on the Delete button corresponding to the admin user account you want to delete.
   A confirmation window will pop-up.
4. Click **OK**.

Chapter 4: Device Configuration

Prerequisites

To ensure the successful operation, of this semi-automated feature, you must first ensure that the desired Avaya SBCE security device has been properly installed and powered up according to the procedures described in “*Installing Avaya Session Border Controller*” 101–5225–062

Installing an Avaya SBCE device

About this task

Use the following procedure to add and provision anAvaya SBCE security device into an existing enterprise VoIP network.

Adding an SBCE device on page 51

Provisioning an SBCE device on page 52

Adding an SBCE device

About this task

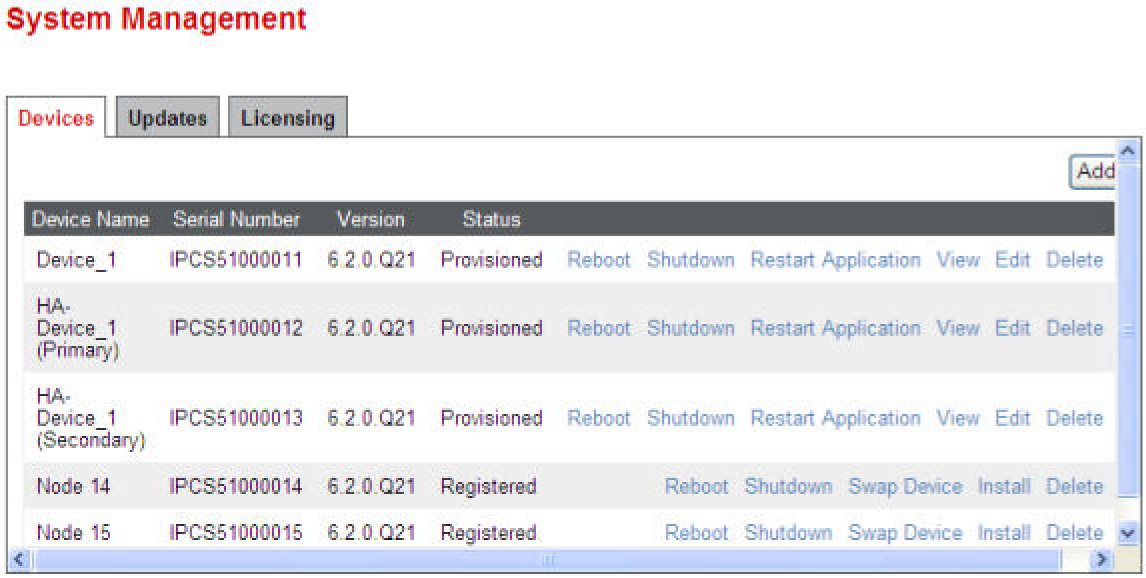
When the EMS is set up as a separate device, one or more Avaya SBCE devices must be added from the System Management function. Use the following procedure to add an Avaya SBCE device.

Procedure

1. Login to the Avaya SBCEControl Center as **Admin**.
2. Select the **System Management** function from the Task Pane.
3. In the Content Area, select the **Add** button to display the Add Device pop-up window .
4. In the Add Device pop-up window, complete the required information fields, and select the **Finish** button to save and exit.

The device list appears with the newly created device added to the list.

Example



Device Name	Serial Number	Version	Status	
Device_1	IPCS51000011	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
HA-Device_1 (Primary)	IPCS51000012	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
HA-Device_1 (Secondary)	IPCS51000013	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
Node 14	IPCS51000014	6.2.0.Q21	Registered	Reboot Shutdown Swap Device Install Delete
Node 15	IPCS51000015	6.2.0.Q21	Registered	Reboot Shutdown Swap Device Install Delete

Next steps

Provisioning an SBCE device on page 52

Provisioning an SBCE device

About this task

Use the following procedure to provision an already installed Avaya SBCE security device into an existing enterprise VoIP network.

Note:

Avaya SBCE security devices which are physically installed into the network and available for provisioning are identified in the Status column with the status of “Registered.” Each one of these un-provisioned devices will have the “Install” option available. Devices that have previously been installed and provisioned are identified with the status of “Provisioned.” Each one of these provisioned devices will have only the “View” option available.

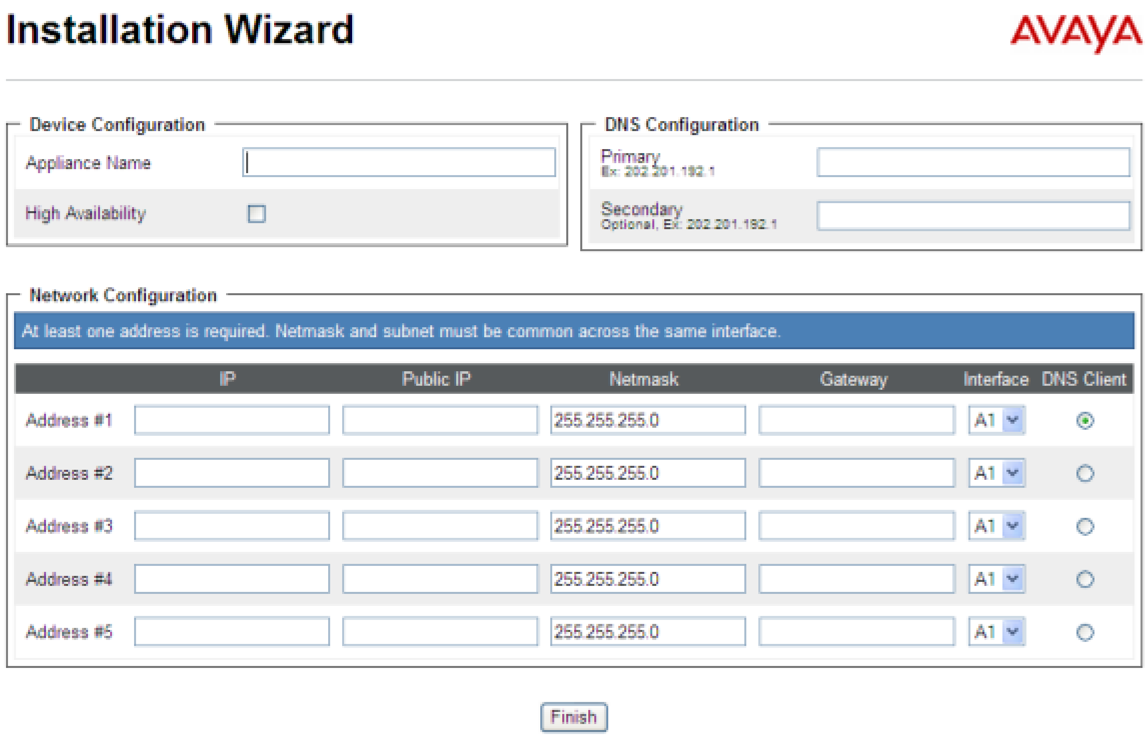
Procedure

1. Select the **System Management** feature from the Task Pane.
   The System Management screen appears.
2. Select the **Devices** tab if not already displayed.
3. Select the **Install** option corresponding to the device that you want to provision.

The Installation Wizard pop-up screen appears.

4. Enter an Appliance Name for the Avaya SBCE security device being provisioned and its deployment settings (i.e., HA and Secure Channel Type).
5. Click **Finish**.
   The Installation Wizard pop-up screen appears showing “Installation is now complete” followed by a list of links to ”Server Configuration,” Media Interface,” “Signaling Interface,” “SIP Cluster,” and “End Point Flows.” You can proceed to any of those configuration areas using those links or access those areas using the Task Pane. Details of each of those configuration areas are described in later sections of this guide.

Example



Installation Wizard

Device Configuration

Appliance Name	
High Availability	□

DNS Configuration

Primary Ex: 202.201.192.1	
Secondary Optional, Ex: 202.201.192.1	

Network Configuration

At least one address is required. Netmask and subnet must be common across the same interface.

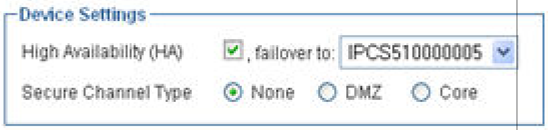
	IP	Public IP	Netmask	Gateway	Interface	DNS Client
Address #1			255.255.255.0		A1	●
Address #2			255.255.255.0		A1	○
Address #3			255.255.255.0		A1	○
Address #4			255.255.255.0		A1	○
Address #5			255.255.255.0		A1	○

Installation Wizard screen

The Installation Wizard screen provides an interface for easily configuring an Avaya SBCE security device. Screen field descriptions are provided in the table below.

Installation Wizard screen field descriptions

Feature	Description

Device Configuration	
Appliance Name	A descriptive name assigned to the Avaya SBCE security device being provisioned. This name will subsequently be used as the device host name.
High Availability (HA)	A checkbox indicating that the Avaya SBCE security device being provisioned will be part of a High-Availability (HA) pair. If checked, a drop-down window will be displayed containing a list of HA partners. Click to select the desired HA partner. **Note:** For HA configuration instructions, refer to the next section in this chapter titled, “Avaya SBCE High Availability (HA) Configurations.”  Device Settings High Availability (HA) ☑, failover to: IPCS510000005 Secure Channel Type ● None ○ DMZ ○ Core
Signaling HA	A sub-field 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 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.
Network Configuration	
IP	IP is the actual IP address of the Avaya SBCE device (whether it is publicly reachable or not) that is being configured.
Public IP	Public IP is the publicly-reachable IP address of the Avaya SBCE security device being configured and is the IP address that the device will use to access the external network. If near-end NAT is not employed, the Public IP address may be the same as the IP (actual) address.
Netmask	The subnet mask of the Avaya SBCE device being configured.

Gateway	The IP address of the device the Avaya SBCE security device will use to send local network traffic to other networks.
Interface	A drop-down menu from which you select the physical interface of the Avaya SBCE security device which will be used to interface to the external, public network (**A1**, **A2**, **B1**, and **B2**).
DNS Client	Select the **DNS Client** 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 in the **DNS Configuration** area.

High Availability (HA) configurations

About this task

The Standard High Availability (HA) configuration (devices co-located) and Geographically-Dispersed HA configuration (devices not co-located) are both performed from the **System Management** screen on two devices that have already been added using the **Add Device** function Adding an SBCE device on page 51. The two devices must be listed with a *Registered* status, as shown in the example below.

Procedure

1. ✱ **Note:**

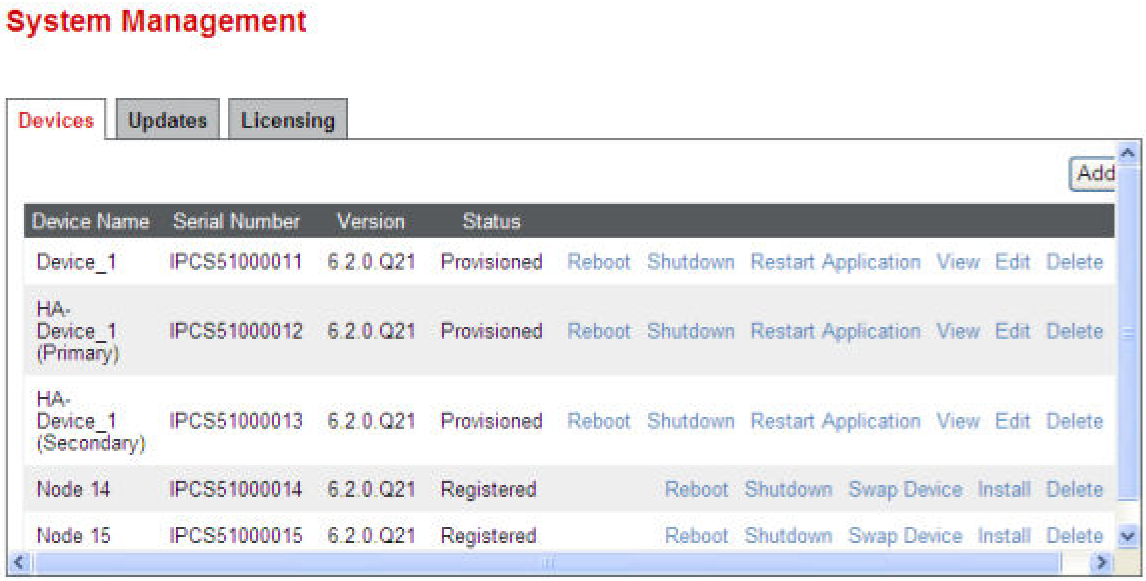
   As part of the Install Wizard design, the device you select here in Step 1 with the **Install** button in the System Management screen will be automatically configured as the “**Active**” (primary) device.The device you select in the “**failover to**” drop-down list will be automatically configured as the “**Stand-By”** (secondary) device.

   Select the **Install** button corresponding to the device you want to provision as the “*Active*” (primary) device.

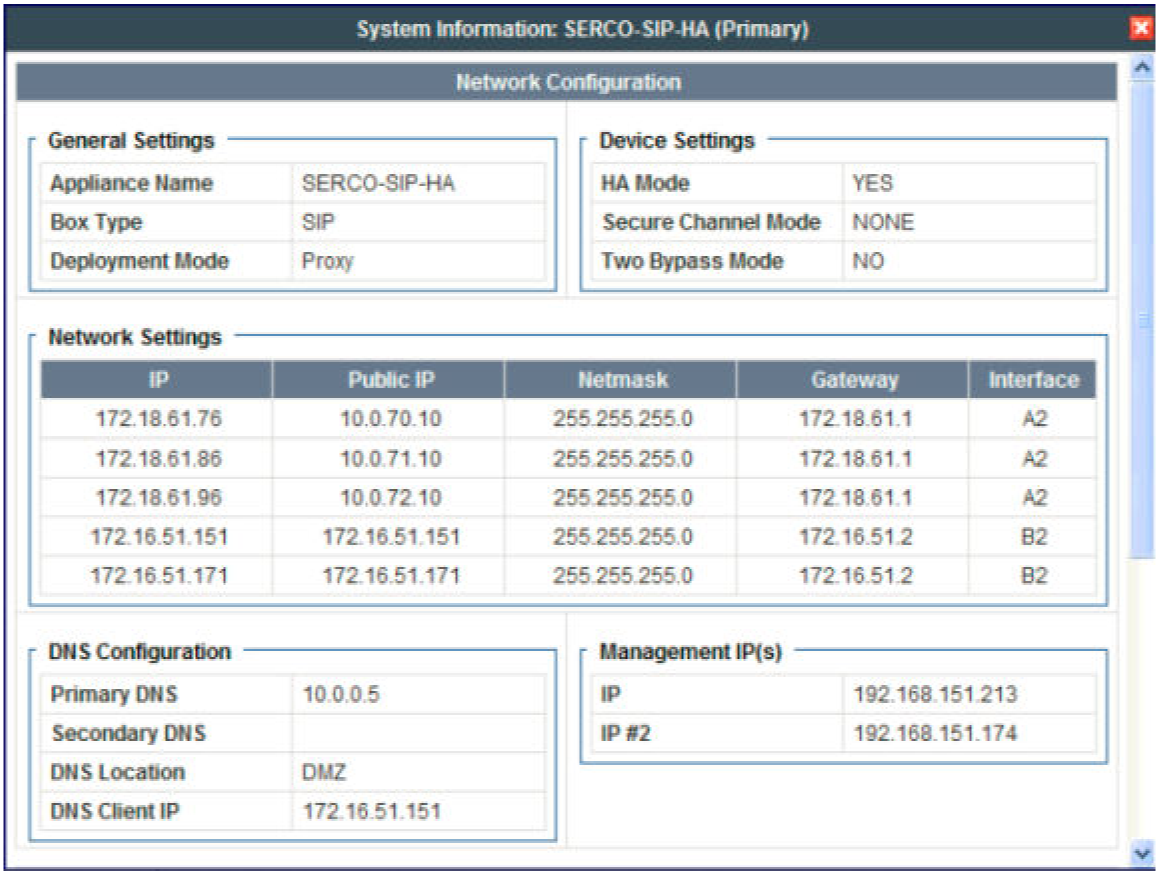
2. Enter an Appliance Name for the Avaya SBCE security device being provisioned and its deployment settings. Select the High Availability (HA) checkbox to display the drop-down list. Select the **Stand-By** (secondary) device serial number from the list. If the device you want to assign as the **Stand-By** device is not listed in the **System Management** screen, use the **Add Device** button Adding an SBCE device on page 51 to add it.

3. Complete the required configuration information in **Installation Wizard** Screen and click **Finish** to continue with the configuration process. This will display a scrollable **System Information** screen similar to the examples shown in the figures below.

Example



Device Name	Serial Number	Version	Status						
Device_1	IPCS51000011	6.2.0.Q21	Provisioned	Reboot	Shutdown	Restart Application	View	Edit	Delete
HA-Device_1 (Primary)	IPCS51000012	6.2.0.Q21	Provisioned	Reboot	Shutdown	Restart Application	View	Edit	Delete
HA-Device_1 (Secondary)	IPCS51000013	6.2.0.Q21	Provisioned	Reboot	Shutdown	Restart Application	View	Edit	Delete
Node 14	IPCS51000014	6.2.0.Q21	Registered		Reboot	Shutdown	Swap Device	Install	Delete
Node 15	IPCS51000015	6.2.0.Q21	Registered		Reboot	Shutdown	Swap Device	Install	Delete



System Information: SERCO-SIP-HA (Primary)

Network Configuration

General Settings

Appliance Name	SERCO-SIP-HA
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	YES
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

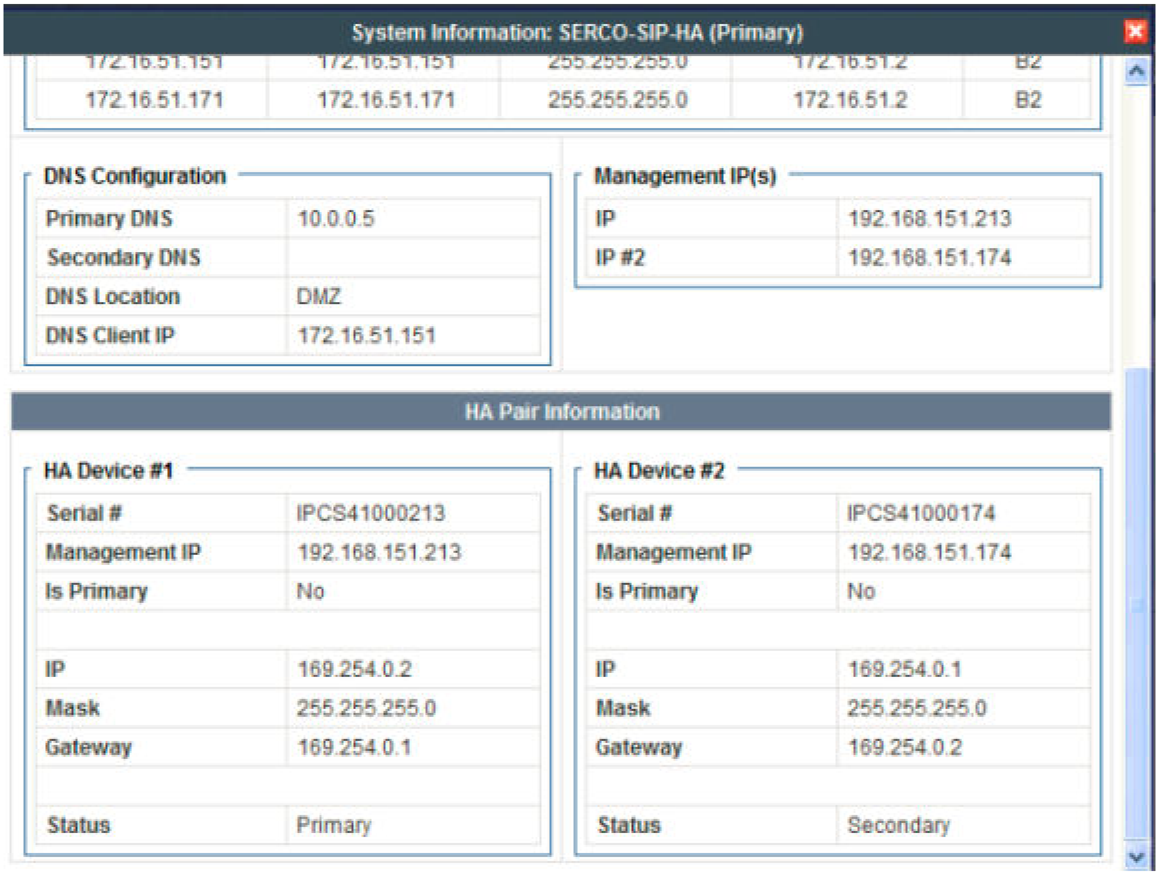
IP	Public IP	Netmask	Gateway	Interface
172.18.61.76	10.0.70.10	255.255.255.0	172.18.61.1	A2
172.18.61.86	10.0.71.10	255.255.255.0	172.18.61.1	A2
172.18.61.96	10.0.72.10	255.255.255.0	172.18.61.1	A2
172.16.51.151	172.16.51.151	255.255.255.0	172.16.51.2	B2
172.16.51.171	172.16.51.171	255.255.255.0	172.16.51.2	B2

DNS Configuration

Primary DNS	10.0.0.5
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.51.151

Management IP(s)

IP	192.168.151.213
IP #2	192.168.151.174



System Information: SERCO-SIP-HA (Primary)

172.16.51.151	172.16.51.151	255.255.255.0	172.16.51.2	B2
172.16.51.171	172.16.51.171	255.255.255.0	172.16.51.2	B2

DNS Configuration

Primary DNS	10.0.0.5
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.51.151

Management IP(s)

IP	192.168.151.213
IP #2	192.168.151.174

HA Pair Information

HA Device #1

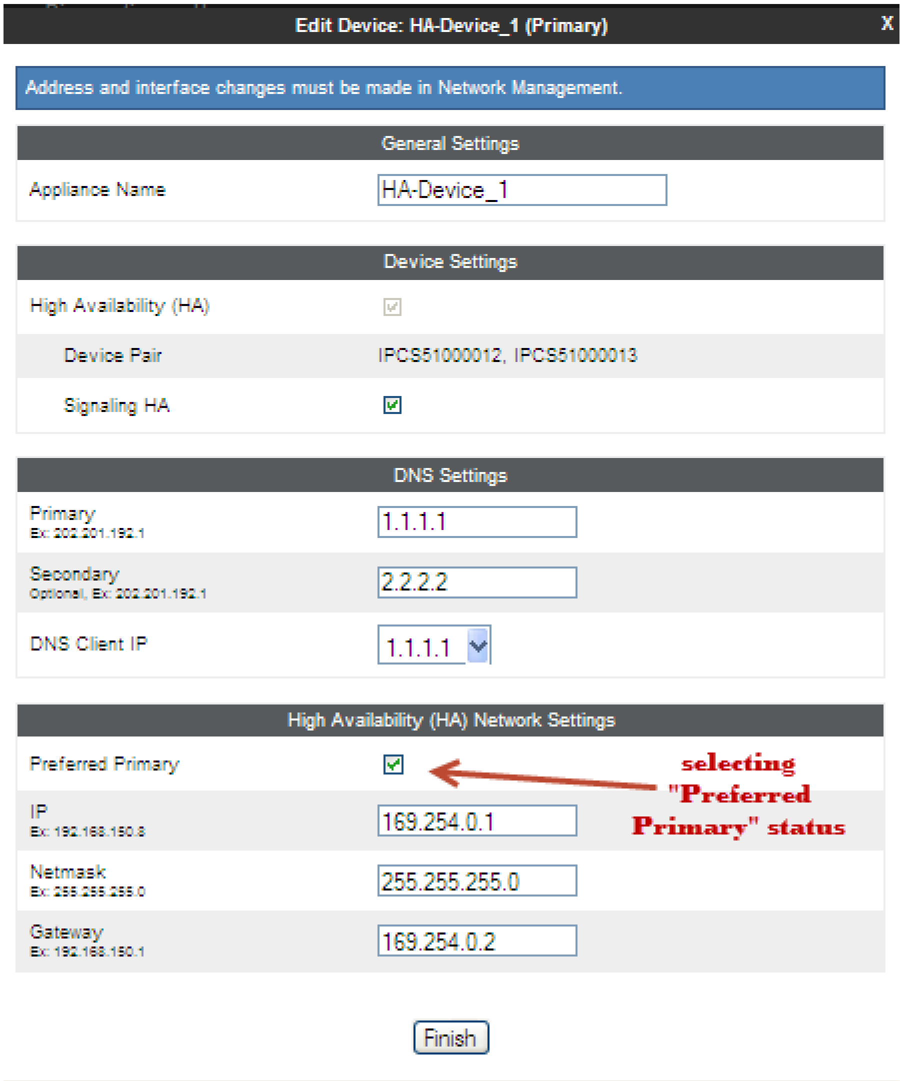
Serial #	IPCS41000213
Management IP	192.168.151.213
Is Primary	No
IP	169.254.0.2
Mask	255.255.255.0
Gateway	169.254.0.1
Status	Primary

HA Device #2

Serial #	IPCS41000174
Management IP	192.168.151.174
Is Primary	No
IP	169.254.0.1
Mask	255.255.255.0
Gateway	169.254.0.2
Status	Secondary

Preferred primary configuration

One of the nodes in the HA pair can be configured to be the “Preferred Primary” (preferred active) node. In the configuration screens, this is done by selecting the “Preferred Primary” checkbox. This is an additional configuration on top of the Parallel HA configuration, which can be configured in the HA-related screens at the time of installation. When a node is configured as “Preferred Primary” (preferred active), it means that when there is no link between the HA nodes, the “Preferred Primary” node will automatically become Primary (active) irrespective of its previous status.



Edit Device: HA-Device_1 (Primary) X

Address and interface changes must be made in Network Management.

General Settings	
Appliance Name	HA-Device_1

Device Settings	
High Availability (HA)	☑
Device Pair	IPCS51000012, IPCS51000013
Signaling HA	☑

DNS Settings	
Primary Ex: 202.201.192.1	1.1.1.1
Secondary Optional, Ex: 202.201.192.1	2.2.2.2
DNS Client IP	1.1.1.1

High Availability (HA) Network Settings	
Preferred Primary	☑
IP Ex: 192.168.150.8	169.254.0.1
Netmask Ex: 255.255.255.0	255.255.255.0
Gateway Ex: 192.168.150.1	169.254.0.2

selecting "Preferred Primary" status

The table below provides a list of HA node status states with their descriptions.HA Node Status States on page 61

Note:

In the status field on the View Device screen for each HA node, the “Preferred Primary” status will be appended to the existing node status of the respective device. For example, when one of the nodes is configured as the “Preferred Primary” node, the status field on the view device screen for one of the HA devices will be displayed as:

Primary (Preferred Primary)

or

Secondary (Preferred Primary)

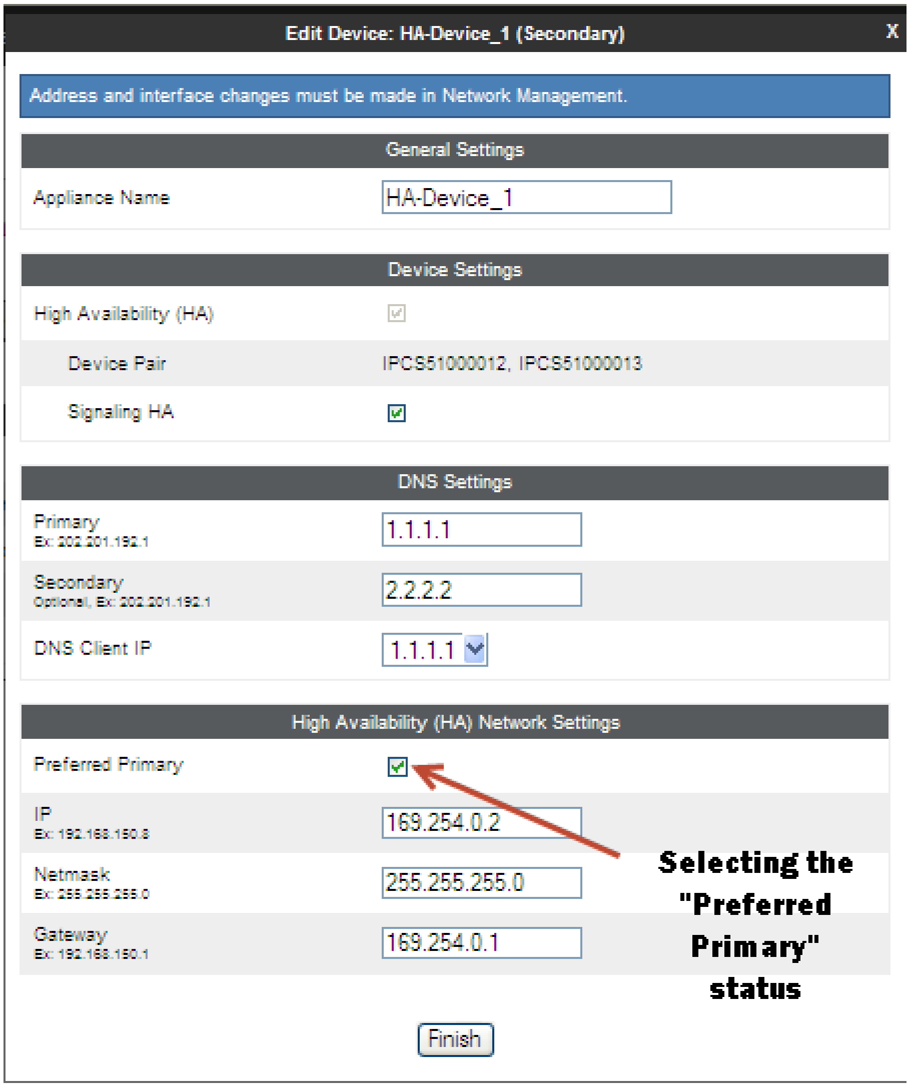
Designating an active node

Use the following procedure to configure one of the nodes in an HA pair to be the designated "***Active***" (primary) node. This is an additional configuration on top of the Parallel HA configuration, which can be configured in the HA-related screens at the time of installation. When a node is designated ***Active*** (primary), it means that when there is no link between the HA nodes, the designated ***Active*** node will automatically become ***Active*** (primary) irrespective of its previous status.

The Preferred Primary status may be viewed in lower portion of the scrollable System Information Screen in the HA Pair Information section in the **Is Primary** status boxes for HA Device #1 and HA Device #2.

Procedure

1. Select the **System Management** feature from the Task Pane.
   The **System Management** screen appears.
2. Selecting **Edit** in the row corresponding to the device you want to configure as the "Preferred Primary" device.
   An **Edit Device** pop-up screen appears.



Edit Device: HA-Device_1 (Secondary)

Address and interface changes must be made in Network Management.

General Settings	
Appliance Name	HA-Device_1

Device Settings	
High Availability (HA)	☑
Device Pair	IPCS51000012, IPCS51000013
Signaling HA	☑

DNS Settings	
Primary Ex: 202.201.192.1	1.1.1.1
Secondary Optional, Ex: 202.201.192.1	2.2.2.2
DNS Client IP	1.1.1.1

High Availability (HA) Network Settings	
Preferred Primary	☑
IP Ex: 192.168.150.8	169.254.0.2
Netmask Ex: 255.255.255.0	255.255.255.0
Gateway Ex: 192.168.150.1	169.254.0.1

Selecting the "Preferred Primary" status

3. Select the Preferred Primary checkbox in the Hgh Availability (HA) Network Settings field area to assign the Preferred Primary status to the applicable HA device.
4. Click **Finish** to save the new configuration and exit.

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	The SBC is active and handling call traffic.
Secondary	The SBC inactive and in stand-by mode.
Down	The SBC has been detected as offline by the Primary SBC. This could mean the application is not running, the network interfaces are disabled, or the hardware device is not running at all.
Initializing	Tthe SBC is going through its initialization procedure.
HAElection	The SBC is determining whether or not to go into active or standby mode.
Synchronizing	This SBC is replicating data from the other SBC.
Unconfigured	The SBC has been configured as an HA device but has not yet received the configuration from the EMS.
Unknown	The EMS does not recognize the HA status the SBC is reporting.

Updating EMS software

The **Element Management System** (EMS) or GUI interface can be upgraded when necessary using the **System Management** feature from the Task Pane. The EMS software upgrade procedures are described in the document titled, “Upgrading Session Border Controller,”

in the Chapter titled, “Software Only Upgrades.”

Updating VIPER signatures

When new scrubber packages or new VIPER signatures become available, an email is sent to the customers containing the following:

- An attachment which contains the rules SQL definitions in a tar.gz format signed with the secret signature
- The Package ID of the rules
- A description of the package
- The release date of the package
- The Vulnerability ID

> **Note:**
>
> The tar.gz file is the Scrubber package that is to be instated in the GUI from the Scrubber profile screen.

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.

Licensing

Use the following procedure for installing, viewing, and uninstalling license files:

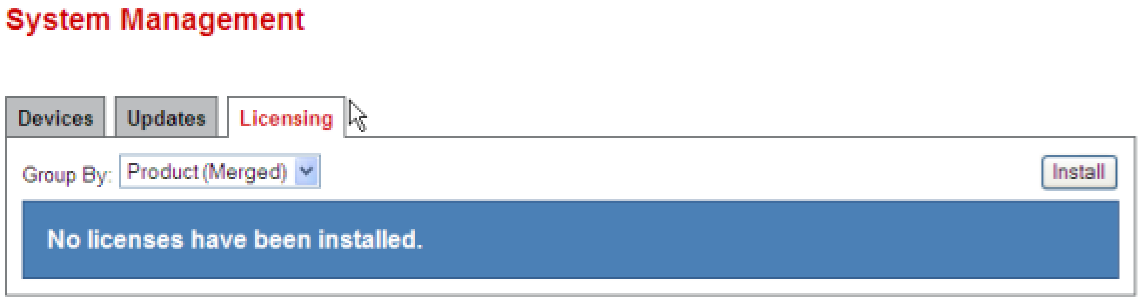
Procedure

1. Click the Install button on the right-hand portion of the System Management Licensing tab screen.
   An Install License pop-up window appears.
2. Select the **Browse** button to navigate to the location of the desired license file.
3. Select the **Append** button.
   Clicking the **Append** button will add the selected license file with any existing license files.

   > **Note:**
   >
   > Clicking the **Overwrite** button will overwrite an existing license file with the same name of the uploaded file.
4. Select the **Upload** button.
   The license is uploaded and installed and an updated License screen is redisplayed.
5. Repeat Step 2, selecting a second license file.
   You will see the values increased on the right-hand side of the Product (Merged) License screen.
6. In the drop-down list, select **License File** to display an expanded list.
7. Double-click on a license name to display a **View License** screen to view details of a license.

8. To uninstall an installed license file, selecting the corresponding checkbox and select the Uninstall button at the bottom of the screen.

Example



No licenses have been installed.

EMS switchover / takeover

EMS data is replicated on an iterative basis, determined by user-defined fields accessed from the EMS GUI interface.

EMS Replication does not support automatic “takeover” (i.e., where “takeover” is defined as the Stand-by EMS server taking over the new duty as Active EMS server).The “takeover” operation requires manual intervention by the operator in either one of two possible scenarios:

- Scenario A - Both Active and Stand-By EMS servers are up and running. The operator initiates a “Graceful Switchover” using the “EMS Switchover” option on the Avaya SBCE Runtime Options screen. This operation swaps the duties of Active and Stand-By between the two servers.
- Scenario B - The Active EMS server has failed and the Stand-By EMS server is up and running. The operator initiates a “Forced Switchover” using the “EMS Takeover” option on the Avaya SBCE Runtime Options screen. This operation just changes the duty of the Stand-By EMS server from “Stand-By” to “Active, while the failed former Active server is being maintained.

Note:

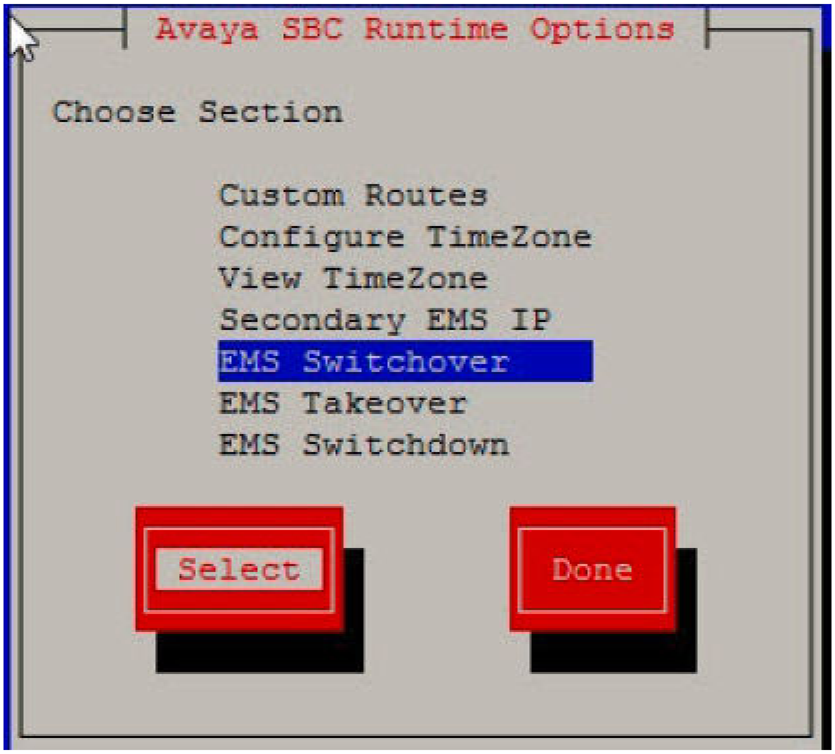
Both switchover/takeover processes may take from 5 to 10 minutes to complete as the “Active” and “Stand-By” servers each reboot and come up to the “STANDBY” and “COMMISSIONED” (Active) respectively. It takes a few minutes for the SBCE servers to receive the new VPN certificates and connect to the new “Active” EMS server.

Initiating a graceful switchover

Procedure

1. Initiate a secure shell (SSH) connection to the “Stand-By” server to display the initial login screen.
2. Enter: `sudo su` after the dollar sign ($) prompt.
   The new pound sign (#) prompt will appear.
3. Enter: `ipcs-options` after the pound sign (#) prompt.
   The Avaya SBCE Runtime Options screen will display.
4. Scroll down to select the EMS Switchover option.
5. Tab down to Select and press the Enter Key.
   The active EMS server will execute the switchover process.

Example



Initiating a forced takeover

Procedure

1. Initiate a secure shell (SSH) connection to the “Stand-By” server to display the initial login screen.

2. Enter: `sudo su` after the dollar sign ($) prompt.
   The new pound sign (#) prompt will appear.
3. Enter: `ipcs-options` after the pound sign (#) prompt.
   The Avaya SBCE Runtime Options screen will display.
4. Scroll down to select the EMS Takeover option.
5. Tab down to Select and press the Enter Key.
   The stand-by EMS server will execute the takeover process.

Viewing the EMS server time zone

About this task

Procedure

1. Initiate a secure shell (SSH) connection to the “Stand-By” server to display the initial login screen.
2. Enter: `sudo su` after the dollar sign ($) prompt.
   The new pound sign (#) prompt will appear.
3. Enter: `ipcs-options` after the pound sign (#) prompt.
   The Avaya SBC Runtime Options screen will display.
4. Scroll to View TimeZone.
5. Tab down to Select and press the Enter Key.
   The current time zone screen will be displayed. If there is no time zone set, the window will state that.

Setting the EMS server time zone

Procedure

1. Initiate a secure shell (SSH) connection to the “Stand-By” server to display the initial login screen.
2. Enter: `sudo su` after the dollar sign ($) prompt.
   The new pound sign (#) prompt will appear.
3. Enter: `ipcs-options` after the pound sign (#) prompt.
   The Avaya SBCE Runtime Options screen will display.

4. Scroll to Configure TimeZone.
5. Tab down to Select and press the Enter Key.
   The select time zone screen will be displayed.
6. Scroll down and select the correct time zone from the alphabetical list.

   > **Note:**
   >
   > Instead of selecting a particular time zone from the alphabetical list in the Select Time Zone screen, you can also tab over to **Skip** and press the **Enter** key to accept the default GMT time zone.

7. Tab down to Select and press the Enter Key.
   New time zone setting will be saved.

Next steps

To exit from the Avaya SBCE Runtime Options screen, tab down to the Select button and press the Enter key to display the previous screen, and then tab over to the Done button and press the Enter key.

Exiting the Avaya SBC Runtime Options screen

About this task

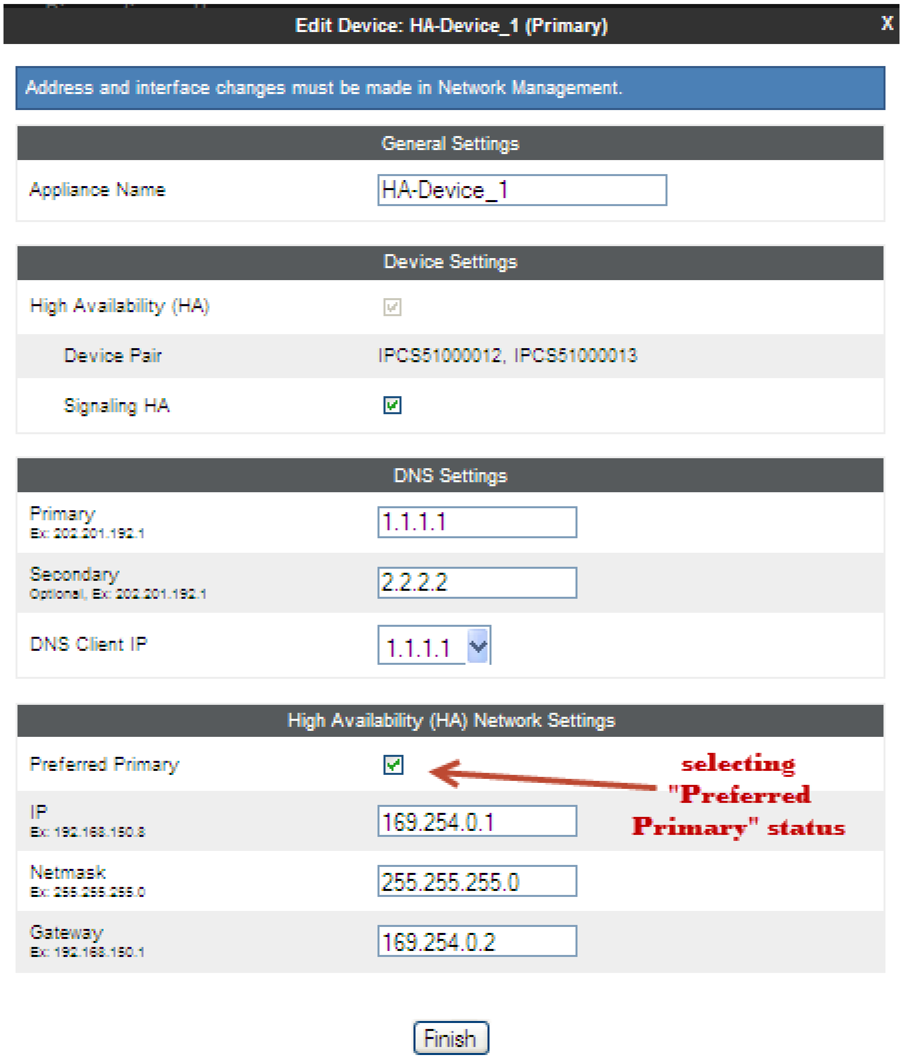
Use this procedure to exit from the Runtime Options screen.

Procedure

1. In the Runtime Options screen, tab down to the `Select` button, and then press the `Enter` key.
   This displays the previous screen.
2. Tab over to the `Done` button, and then press the `Enter` key.
   This redisplays the pound sign (#) prompt.

Preferred primary configuration

One of the nodes in the HA pair can be configured to be the “Preferred Primary” (preferred active) node. In the configuration screens, this is done by selecting the “Preferred Primary” checkbox. This is an additional configuration on top of the Parallel HA configuration, which can be configured in the HA-related screens at the time of installation. When a node is configured as “Preferred Primary” (preferred active), it means that when there is no link between the HA nodes, the “Preferred Primary” node will automatically become Primary (active) irrespective of its previous status.



Edit Device: HA-Device_1 (Primary)

Address and interface changes must be made in Network Management.

General Settings	
Appliance Name	HA-Device_1

Device Settings	
High Availability (HA)	☑
Device Pair	IPCS51000012, IPCS51000013
Signaling HA	☑

DNS Settings	
Primary Ex: 202.201.192.1	1.1.1.1
Secondary Optional, Ex: 202.201.192.1	2.2.2.2
DNS Client IP	1.1.1.1

High Availability (HA) Network Settings	
Preferred Primary	☑
IP Ex: 192.168.150.8	169.254.0.1
Netmask Ex: 255.255.255.0	255.255.255.0
Gateway Ex: 192.168.150.1	169.254.0.2

selecting "Preferred Primary" status

The table below provides a list of HA node status states with their descriptions. HA Node Status States on page 61

Note:

In the status field on the View Device screen for each HA node, the “Preferred Primary” status will be appended to the existing node status of the respective device. For example, when one of the nodes is configured as the “Preferred Primary” node, the status field on the view device screen for one of the HA devices will be displayed as:

Primary (Preferred Primary)

or

Secondary (Preferred Primary)

High-Availability pair geographically dispersed

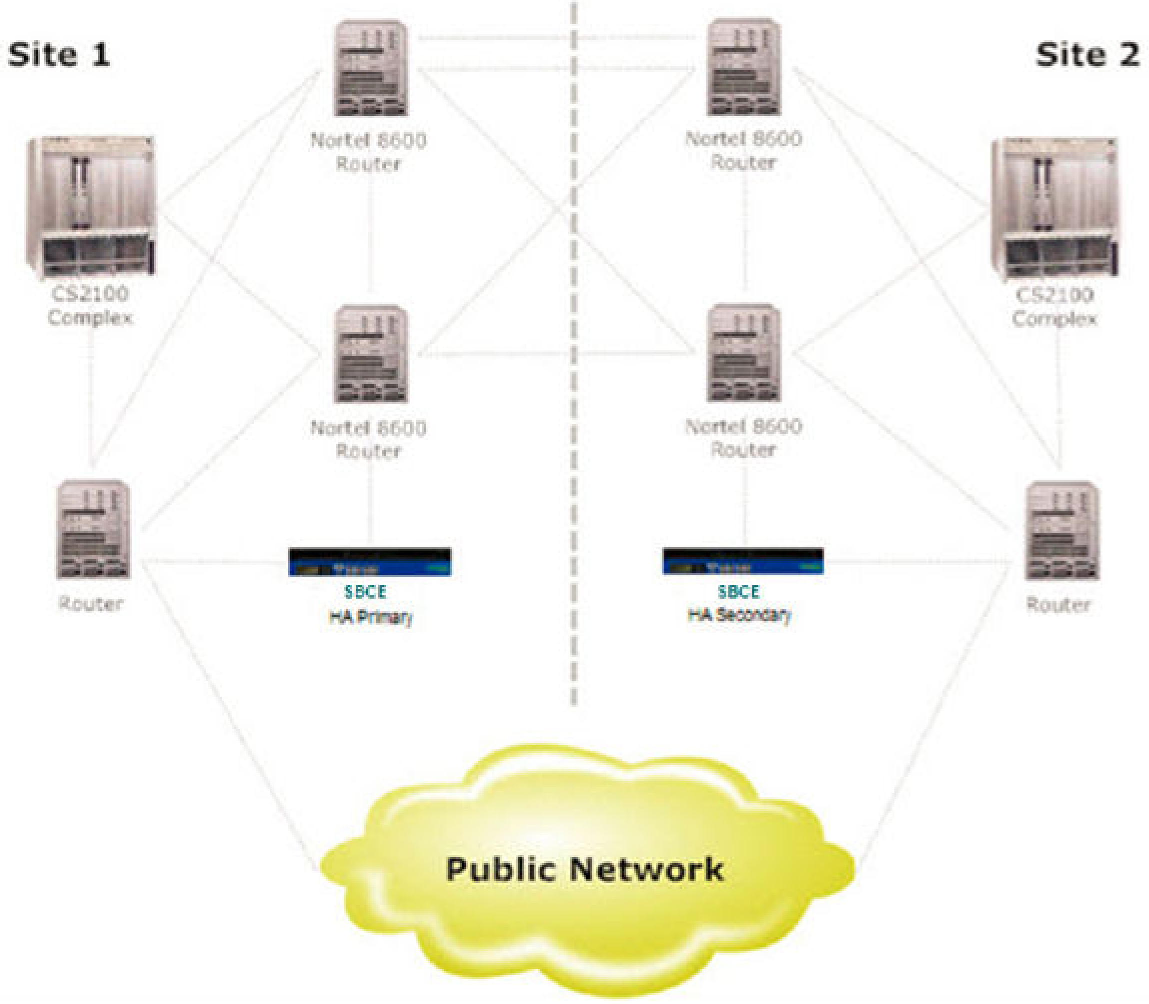
Introduction

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, as shown below.

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 the Avaya EMS which synchronizes the database in each Avaya SBCE device accesses to maintain real-time network information. Thus, if the HA Primary Avaya SBC 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.

Fig Note: Any or all of the available Avaya SBCE device models may be used in the HA implementation illustrated in this graphic. The example below illustrates the use of Avaya SBCE devices.

Example



Deploying a geographically dispersed Avaya SBCE HA configuration

About this task

Use the following procedure to deploy a geographically dispersed Avaya SBCE HA configuration.

Procedure

1. Install each Avaya SBCE security device using the procedures contained in *Installing Avaya Session Border Controller*.
2. Install the Avaya EMS security device using the procedures contained in *Installing Avaya Session Border Controller*.
3. Access the EMS GUI using the procedures contained in Chapter 2, Getting Started, of *Administering Avaya Session Border Controller*.
4. Select the System Management feature from the Task Pane.
   The System Management screen is displayed in the Content Area.
5. Click the **Edit** button corresponding to the Primary HA security device.
   The Edit Device pop-up window is displayed.
6. Enter the IP address, Netmask, and Gateway of the Primary HA Avaya SBCE security device into the High Availability (HA) Network Settings portion of the pop-up window.

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

   Note:

   When the High Availability (HA) checkbox is selected, an additional checkbox becomes visible and selectable, the Signaling HA checkbox.When the Signaling HA checkbox is selected, the warning message pop-up will warn 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 steps 5 through 7 for the Secondary HA security device.

Chapter 5: Domain Policy Administration

Governing Unified Communications with domain policies

This chapter explains how to create, manage, and assign domain policies (also referred to as *Unified Communications Policies*). These policies allow you maintain control over call flows entering or leaving the enterprise based upon a wide range of conditions and parameters.

Purpose — Unified Communications policies

UC Policies allow enterprise UC administrators the flexibility to govern their Unified Communications through the enforcement of business rules. Different rules may be applied based on user identity, domain affiliation, network identity, time of day, and time of week.

How they work

UC Policies have two high level concepts: flows and domain policies. When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

Flows

The packet field values 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 numerical value). The most particular flows should be used at the top, while those lower in the order may be more general.

Endpoint Flows

- Used to determine signaling endpoints in order to apply the appropriate endpoint policy
- There are two types of endpoint flows: subscriber flows and server 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 numerical value) is applied if Time of Day (ToD) matches. Smaller time windows should be 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

  Determine the processing method, privileges, and authentication method of packets.
- Session Policies

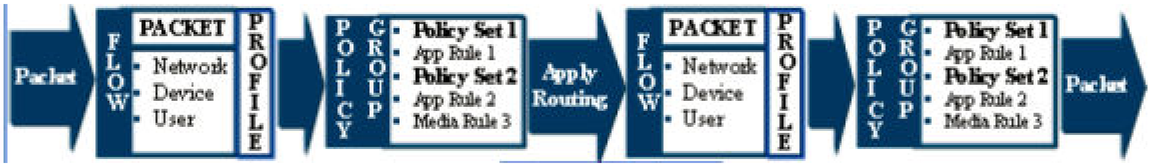
  Applied based on the source and destination of a media session (e.g., which codec is to be applied to the media session between its source and destination).

Profiles

Profiles are very similar to polices, but they are usually dependent on deployment. For example, they are dependent on which call server is being used, IP addresses being used, SIP domains, normal traffic behavior, etc. This differs from policies, in that policies are based on business and compliance requirements.

Detailed visual examples of matching flows and applying policies for securing a SIP Trunk and securing SIP Phones with Avaya SBCE are provided below.

Example



Example: call server with SBCE securing SIP trunk

This is an example of a call server and Avaya SBCEsecuring a SIP trunk.

To be created by user

- End Point Policy Groups
    - Call Server Policy Group
    - Trunk Server Policy Group
- Endpoint Flows
    - Call Server to Avaya SBCE Flow (Reverse used in opposite direction)
    - Trunk Server to Avaya SBCE Flow (Reverse used in opposite direction)
- Session Policies
    - Trunk Server/Call Server SIP Phone Session Policy
- Session Flows
    - Trunk Server to Call Server SIP Phone Flow (bidirectional)

End Point Policy

Incoming

1. Packet sent received by Avaya SBCE.
2. Avaya SBCE determines flow.
3. Call Server to Avaya SBCE Flow points to Call Server Policy Group; Avaya SBCE applies policy and routes packet to determined destination.
4. Trunk Server to Avaya SBCE REVERSE Flow points to Trunk Server Policy Group; Avaya SBCE applies policy.
5. Packet sent to Trunk Server.

Outgoing

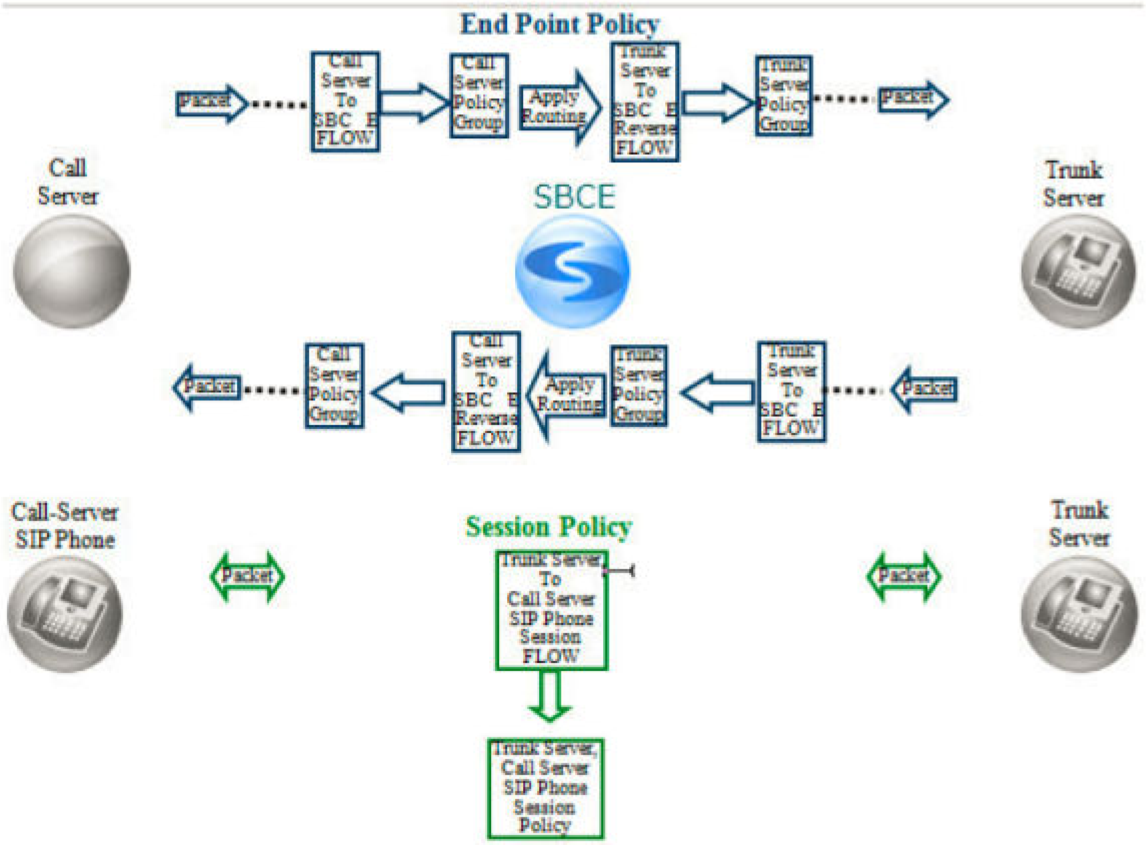
1. Packet received by Avaya SBCE
2. Avaya SBCE determines Flow.
3. Trunk Server to Avaya SBCE Flow Points to Trunk Server Policy Group; Avaya SBCE applies policy and routes packet to determined destination.
4. Call Server to Avaya SBCE REVERSE Flow points to Call Server Policy Group; Avaya SBCE applies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

Session Policy

1. Packet received by Avaya SBCE.
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 policy.
4. Packet sent.

Example


End Point Policy
Packet
Call Server To SBC E FLOW
Call Server Policy Group
Apply Routing
Trunk Server To SBC E Reverse FLOW
Trunk Server Policy Group
Packet
Call Server
SBCE
Trunk Server
Packet
Call Server Policy Group
Call Server To SBC E Reverse FLOW
Apply Routing
Trunk Server Policy Group
Trunk Server To SBC E FLOW
Packet
Call-Server SIP Phone
Session Policy
Packet
Trunk Server To Call Server SIP Phone Session FLOW
Packet
Trunk Server
Trunk Server, Call Server SIP Phone Session Policy

Example: call server with SBCE securing SIP phones

This is an example of a call server andAvaya SBCEsecuring SIP phones..

To be created by user

- End Point Policy Groups
  - Call Server Policy Group
  - SIP Phone Policy Group
- Endpoint Flows
  - Call Server to Avaya SBCE Flow (Reverse used in opposite direction)
  - SIP Phone to Avaya SBCE Flow (Reverse used in opposite direction)

- Session Policies
    - SIP Phone Session/Call Server SIP Phone Policy
- Session Flows
    - SIP Phone to Call Server SIP Phone Flow (bidirectional)

End Point Policy

Incoming

1. Packet received by Avaya SBCE.
2. Avaya SBCE determines flow.
3. Call Server to Avaya SBCE Flow points to Call Server Policy Group; Avaya SBCE applies policy and routes packet to determined destination.
4. SIP Phone to Avaya SBCE REVERSE Flow points to SIP Phone Policy Group; Avaya SBCE applies policy.
5. Packet sent to SIP Phone.

Outgoing

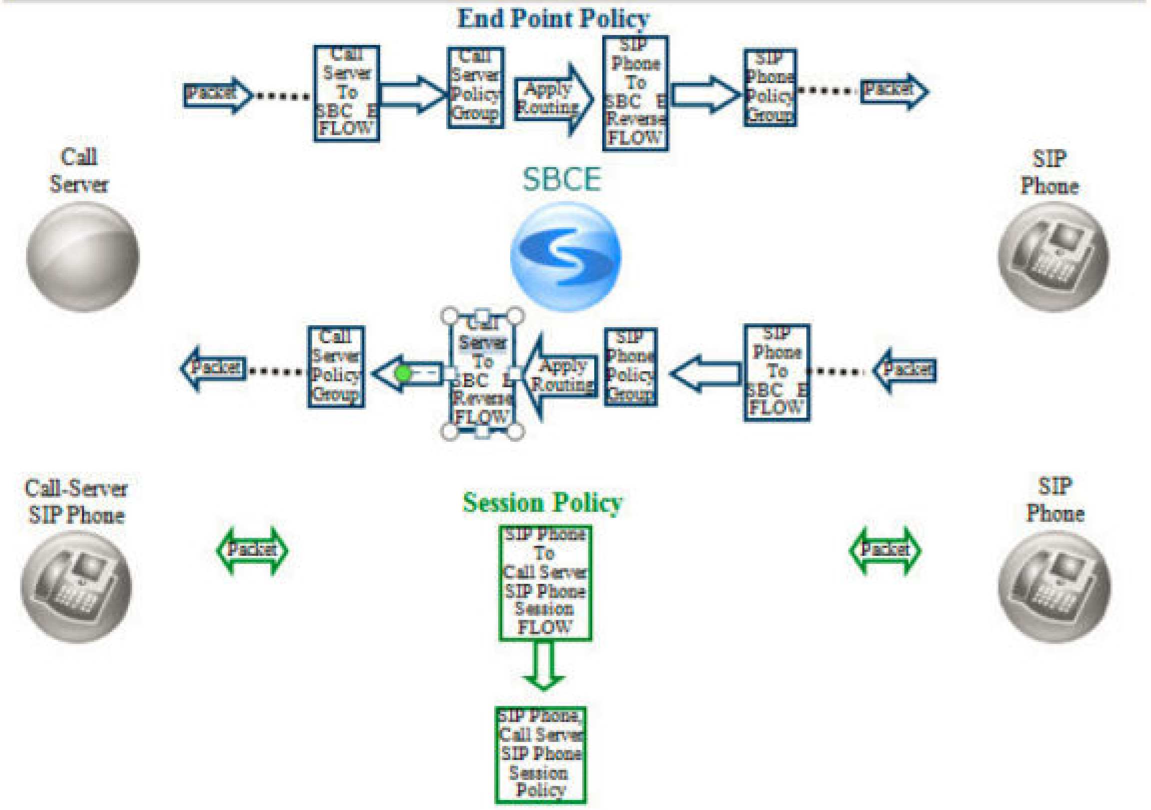
1. Packet received by Avaya SBCE
2. Avaya SBCE determines Flow.
3. SIP Phone to Avaya SBCE Flow Points to SIP Phone Policy Group; Avaya SBCE applies policy and routes packet to determined destination.
4. Call Server to Avaya SBCE REVERSE Flow points to Call Server Policy Group; Avaya SBCE applies policy.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

Session Policy

1. Packet received by Avaya SBCE.
2. Avaya SBCE determines Flow.

3. SIP Phone to Call Server SIP Phone Session Flow points to SIP Phone/Call Server SIP Phone Session Policy; SBCE applies policy.
4. Packet sent.

Example



Configuring rules and policies

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.

Note:

This section only provides a brief introduction to Rules, Profiles, and Policies. Detailed instructions for creating and editing each of the individual types of Rules, Profiles. Policies, and Policy Groups are provided in their respective sub-sections that follow later in this chapter.

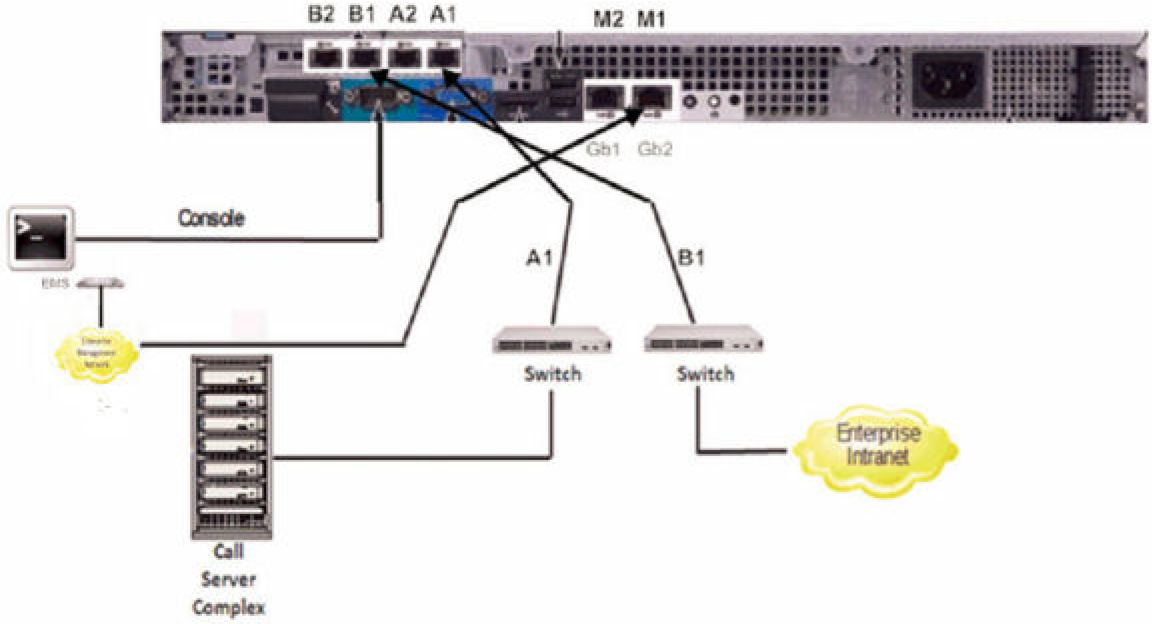
Architecture

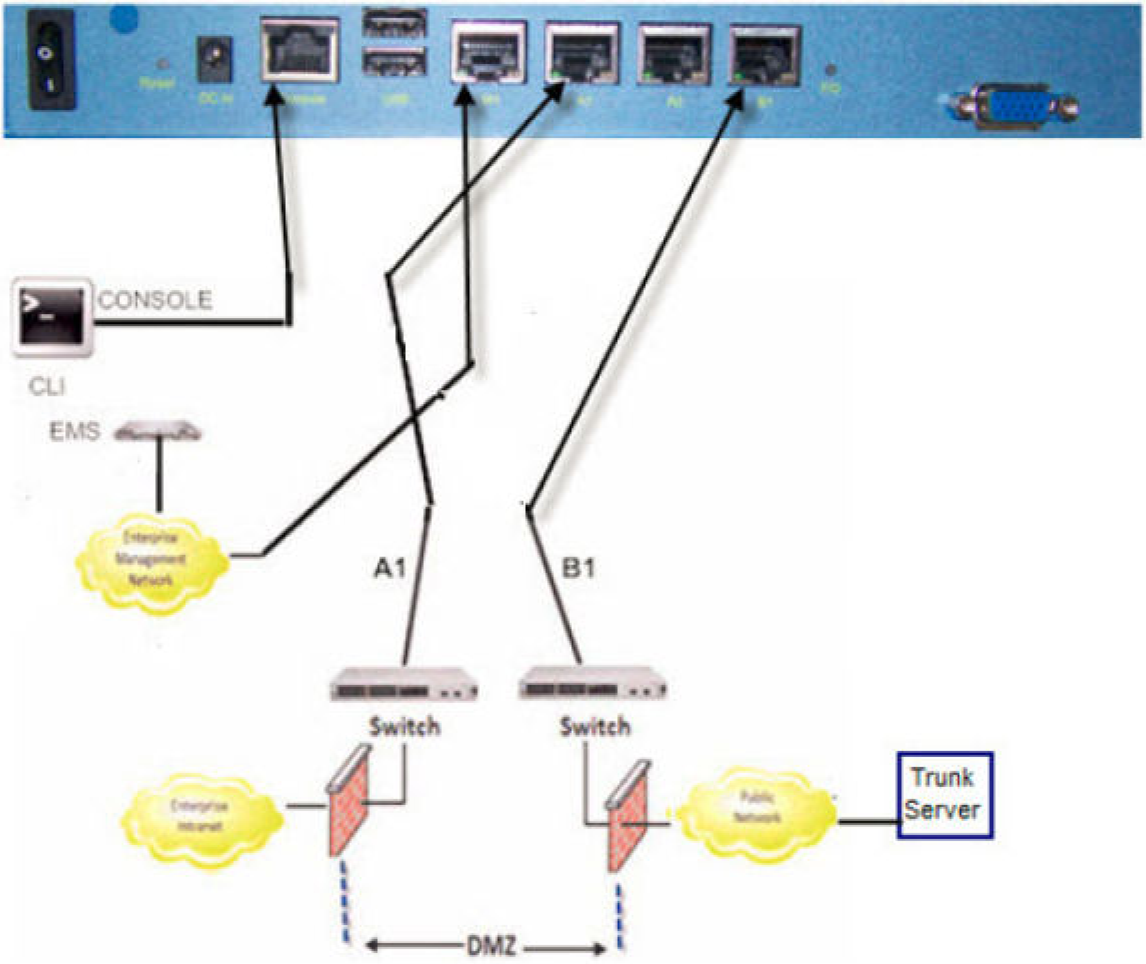
The two figures that follow provide examples ofAvaya SBCE architecture using a standard platform and a micro platform. The standard platform example is a single Avaya SBCE device deployed in the core with the call server complex and controlled by a separate EMS device. The micro platform example is a single SBCE device deployed in the enterprise DMZ and controlled by a separate EMS device.

Note:

This standard platform device and the Portwell platform device can be deployed in either of the architectures shown.

Example



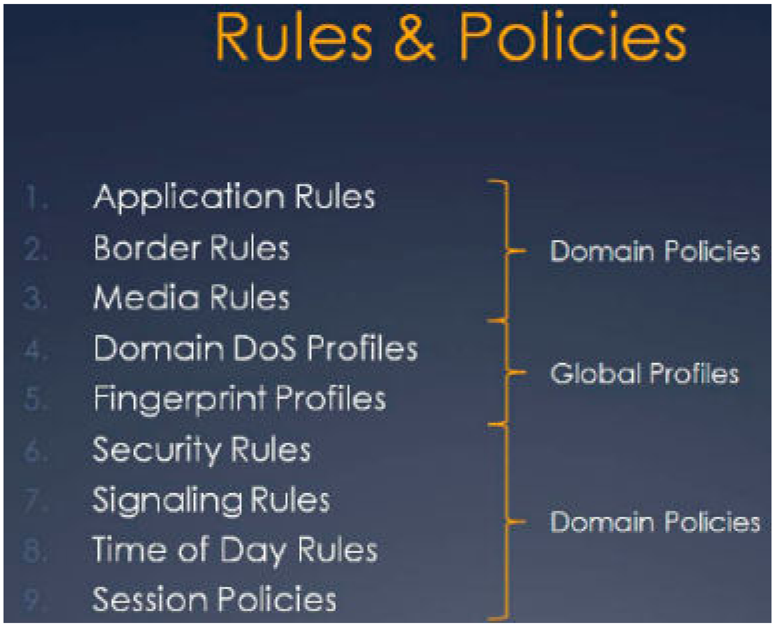


Rules and policies associations

An overview of the rules and policies associations is provided in three drawings which illustrate the following:

- List of rules with their associated policies (e.g., Application, Border, and Media Rules are associated with Domain Policies
- Types of signaling and media flows, with their associated policies and policy groups and sets and with the elements and applications they control
- Session and subscriber flows along with their associated policies

Example



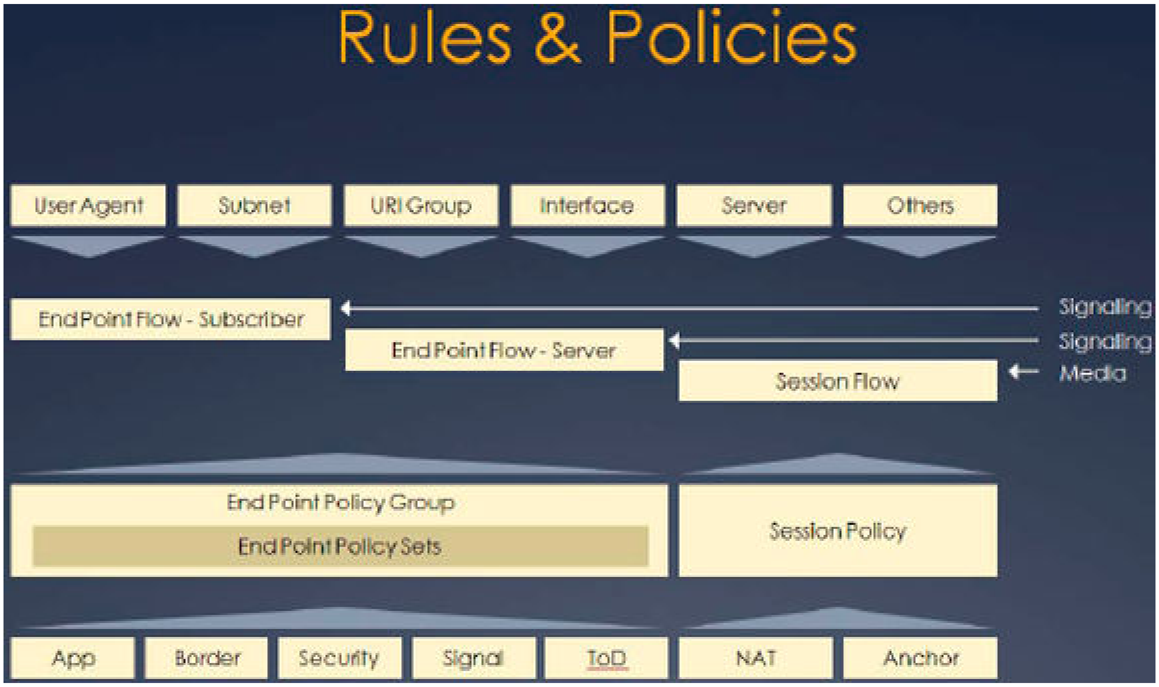
Rules & Policies

1. Application Rules
2. Border Rules
3. Media Rules
4. Domain DoS Profiles
5. Fingerprint Profiles
6. Security Rules
7. Signaling Rules
8. Time of Day Rules
9. Session Policies

Domain Policies

Global Profiles

Domain Policies



Rules & Policies

User Agent | Subnet | URI Group | Interface | Server | Others

End Point Flow - Subscriber

End Point Flow - Server

Session Flow

Signaling

Signaling

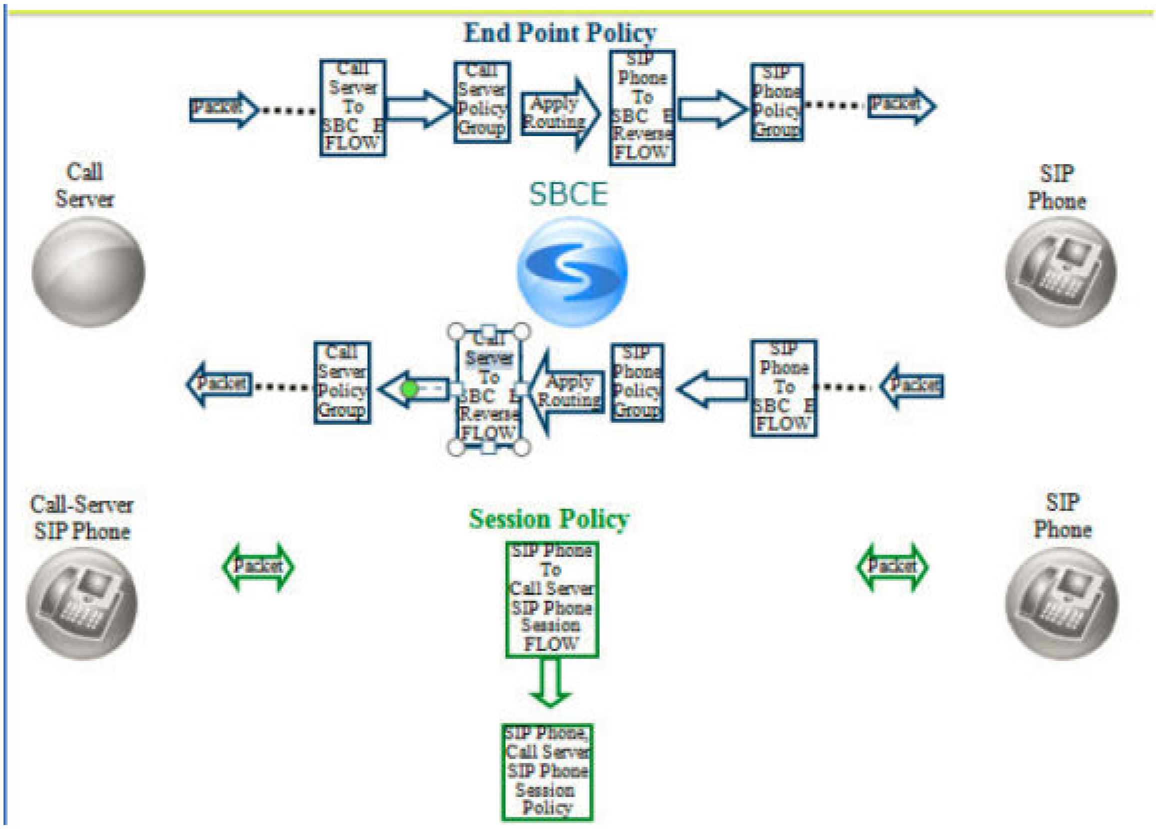
Media

End Point Policy Group

End Point Policy Sets

Session Policy

App | Border | Security | Signal | ToD | NAT | Anchor



Rules and profiles configuration steps checklists

This section provides quick-start configuration checklists for each of the the following rules and profiles:

- Application Rules
- Border Rules
- Media Rules
- Domain DoS Rules
- Fingerprint Profiles
- Security Rules
- Signaling Rules
- Time of Day Rules

Note:

This section only provides brief configuration checklists for Rules and Profiles. Detailed instructions for creating and editing each of the individual types of Rules and Profiles are provided in their respective sub-sections later in this chapter.

Application rules checklist

Application rules are used to police SIP applications and rates.

Application Rule Configuration Example

1. Select **Domain Policies > Application Rules**
2. Select **Add Rule**
3. Name = App-xxxx
4. Allow bidirectional voice, video, IM at arbitary rates
5. Finish

Border rules checklist

Border rules are used to establish NAT traversal (usually line side).

Border Rule Configuration Example

1. Select **Domain Policies > Border Rules**
2. Select **Add Rule**
3. Name = Border-xxxx
4. Enable **NAT**
5. Check **SIP** and **SDP** published IP checkboxes
6. Finish

Media rules checklist

Media rules are used to implement media-oriented security.

Media Rule Configuration Example

1. Select **Domain Policies > Media Rules**
2. Select **Add Rule**

3. Name = Media-xxxx
4. Select a media type (encrypted)
5. Select **MAD**
6. Select **Media Silencing**
7. Change Audio precedence to immediate
8. Finish

Domain DoS profiles checklist

Domain DoS profiles are used to define the server-bound DoS counters used in Security Rules.

Domain DoS Profile Configuration Example

1. Select **Global Profiles > Domain Profile**
2. Select **Add Profile**
3. Name = DoS-xxxx
4. Users = 1000
5. Client type = Other
6. Finish

Fingerprint profiles checklist

Fingerprint profiles are used to define the Fingerprint actions used in Security Rules.

Fingerprint Profile Configuration Example

1. Select **Global Profiles > Fingerprint Profiles**
2. Select **Add Profile**
3. Name = Finger-Cross
4. Finish
5. Edit **Via**
6. Action = Reauthenticate
7. Finish

Security rules checklist

Security rules are used to implement signaling-oriented security.

Security Rule Configuration Example

1. Select **Domain Policies > Security Rules**
2. Select **Add Rule**
3. Name = Secure-xxxx
4. Select **Enabled** from the drop-down list.
5. Realm = dummy.com
6. Enable Authentication Checking, REGISTER, INVITE, BYE, and REFER.
7. Select **URI** for compliance.
8. Enable Fingerprinting with Finger-Cross
9. Enable Scrubber with Package 2
10. Enable Domain DoS with DoS-xxxx
11. Finish

Signaling rules checklist

Signaling rules are used to change the behavior and QoS of SIP signaling and replies.

Signaling Rule Configuration Example

1. Select **Domain Policies > Signaling Rules**
2. Select **Add Rule**
3. Name = Signal-xxxx
4. Block Option Request Headers with 403 Forbidden
5. Finish

Time of day rules checklist

Applications rules are used to apply different rules at different times in a policy set.

Time of Day Rule Configuration Example

1. Select **Domain Policies > Time of Day Rules**
2. Select **Add Rule**
3. Name = Time-xxxx
4. Start date = Now
5. End date = Never
6. Time = All Day
7. Recurrence = Every Weekend
8. Finish

Creating a policy group checklist

The End-Point Policy Group feature allows you to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and Time of Day (ToD).

A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

✱ **Note:**

For detailed information on creating a Policy Group, refer to the section later on in this chapter titled, “End-Point Policy Groups.”

Session policies checklist

Session policies are used to prioritize media codecs, media forking, and select media anchoring.

Session Policy Configuration Example

1. Select **Domain Policies > Session Policies**
2. Name = Pol-xxxx
3. Codec Priority = (1) G.711 (2) G.722
4. Check Media Anchoring
5. Finish

✱ **Note:**

For detailed information on creating Session Policies, refer to the section later on in this chapter titled, “Session Policies.”

Points to remember

- Rules are grouped in Policy Sets
- Policy Sets are grouped in End-Point Policy Groups
- End-Point Policy Groups are assigned to End-Point Flows (subscriber and server).
- Session Policies control codec negotiation, media forking, and media anchoring.
- Session Policies are assigned to Session Flows (subscriber and server).

SIP high level message processing

This section provides an overview of SIP high level processing covering the following topics:

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

SIP registration processing

An Inbound SIP Registration from a Remote Worker could be received on a UDP/TCP/TLS socket. The SIP routing system is responsible for routing 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 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 against the provisioned IP Address field of Signaling Interface configuration to decide a match.

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 against the provisioned values of the Subscriber Flow.

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

If 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 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 Flow to take routing decisions. The SIP routing system uses the Next Hop Server1/Next Hop Server 2 fields of the Routing Profile to determine the communication addresses and transport of the SIP Server.

The Next Hop Server 1 /Next Hop Server 2 fields of the Routing Profile could be configured with an IP Address / IP Address: Port / Domain / Domain: Port. The SIP routing system initially tries to route the registration towards Next Hop Server 1, if a 408 Request Timed Out is observed the SIP routing system tries to resend the registration by selecting Next Hop Server 2 field as the target destination.

The Next Hop Server field must resolve to a valid Server Configuration for the SIP routing system to correctly route the SIP registrations. Refer to the section titled, Locating SIP Servers, for DNS NAPTR/SRV procedures followed by Avaya SBCE to resolve Next Hop Server fields.

Once the SIP server is located, the SIP routing system compares the IP address of the located SIP server 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.

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 against the provisioned IP Address field of Received Interface configuration to decide a match. If either of the URI Group or Received 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 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 a Server/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/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 towards the Call Server. The SIP responses will be properly routed by the SIP routing system using the same Subscriber / Server Flows that was matched during request processing.

Note that once the Remote Worker registers successfully to the Call Server through the Avaya SBCE, subsequent registrations reuse the same Subscriber/Server Flows that were matched during initial SIP registration for that remote worker until the Remote Worker de-Registers with the Call Server.

SIP call processing on SBCE

All the Inbound/Outbound calls from an endpoint to the Avaya SBCE are processed by the SIP routing system. An endpoint can be a SIP remote worker / Call Server / Trunk Server. The call processing happens in two stages – Inbound and Outbound.

Inbound call processing

For Inbound call, the SIP call could 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 with the IP addresses / 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 all the provisioned Server Flows associated with the Server Configuration, looking for a match. See the section “Server flow matching.”

If the SIP call is not associated with any Server Configuration the call is refused unless it matches a provisioned Subscriber flow. See the section titled, Subscriber Flow Matching.

Server flow matching (call originated from the server)

The routing system uses the URI Group, 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 against 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. Refer to the section titled, Policy Invocation and Route Resolution.

- It is possible to configure multiple Server Flows for a single Server Configuration.
- The URI Group field can be configured with the wild card entry (*) that would match against any incoming SIP request.
- The Signaling Interface configuration contains the SBC SIP communication IP Address, Port for each configured transport to receive/send SIP signaling traffic from/to the network. The SIP routing system can select a different SIP connect port listed under Advanced Options → Port Ranges for communication with external SIP entities based on configuration.
- The Received Interface field should not be confused with the Signaling interface and is not used as part of inbound call processing. Refer to the section titled, Server Flow Matching (Call towards a Server) for Received Interface field usage.

If there is no matching Server Flow the call is refused and incoming SIP request will be dropped. The SIP routing system ceases 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.

Subscriber flow matching (call originated from remote worker)

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

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

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/Subscriber Flow. An Incidence/Syslog will be raised for administrative reasons.

Policy invocation and route resolution

This section provides an overview of policy invocation and route resolution processing covering the following topics:

- Inbound policy invocation
- Route resolution (subscriber processing — call towards remote worker
- Route resolution (server processing — call towards a server)

Inbound policy invocation (call processing)

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 Route Resolution phase mentioned below.

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 (subscriber processing — call towards remote worker)

If the incoming SIP request does not contain subscriber identification parameter, the routing system proceeds with normal Route Resolution. Proceed to the section titled, Route Resolution (Server Processing).

If incoming SIP request has a subscriber identification parameter in the SIP request URI header the call is destined towards 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 SBC for each remote worker during the SIP registration process.

A sample SIP Request line containing the subscriber identification parameter is listed below for reference.

```
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 towards the SIP remote worker.

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

- Remote worker Signaling IP Address / Port (including NAT info)
- Remote Signaling Transport (UDP/TCP/TLS)
- Subscriber Flow that matched during 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 towards the remote worker. Proceed to section Outbound Call Processing.

If the SIP registration database lookup fails the call will be rejected with a SIP 403 Forbidden error response and a Syslog/Incidence will be raised. This could happen if the SIP remote worker is no longer registered through the Avaya SBCE.

Route resolution (server processing — 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 Server1/Next Hop Server 2 fields of the Routing Profile to determine the communication addresses, transport of the SIP entity for which the incoming SIP call will be re-targeted.

The Next Hop Server 1 /Next Hop Server 2 fields of the Routing Profile could be configured with an IP Address / IP Address: Port / Domain / Domain: Port. The SIP routing system initially tries to route the call towards Next Hop Server 1, if a 408 Request Timed Out is observed the SIP routing system tries to route the call by selecting Next Hop Server 2 field as the target destination.

The Next Hop Server field must resolve to a valid Server Configuration for the SIP routing system to correctly route the SIP calls. The matching of Next Hop Server to a valid Server Configuration will be discussed shortly.

Routing Profile could 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.

Once the route entry is resolved, the system proceeds with Locating SIP Servers.

Locating SIP servers

The system follows the procedures of RFC 3263 for NAPTR/SRV to correctly identify the SIP communication address (IP Address, 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. If the Next Hop Server doesn’t contain port information, the following DNS SRV procedures are employed to determine the SIP server port:

- 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 they facilitate in load balancing

Following is an explanation of the logic employed by the SIP routing system for locating SIP Server:

1. If *Next Hop Server* field contains an FQDN proceed to Step 2 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 sips scheme in the Request-URI for the following call scenarios. For both the scenarios the system selects the outbound transport as TLS.

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

   The system checks if Port information is specified as part of Next Hop Server field. If Port is not specified the system uses a default port based on the transport selected as shown in the table below else 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 DNS NAPTR Processing to determine the SIP Server Transport.

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

   a. If no NAPTR records are found the system proceeds with a 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:

      _sip._udp. prefix

      If SIP scheme is used TCP SRV record lookup is performed with:

      sips._tcp. prefix
   b. If NAPTR records are found the system proceeds with SRV lookup based on the NAPTR lookup result order and preference flags. SRV record

prefix selected is based on the current NAPTR transport selected and is listed below.

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 proceeds to Step 3.

3. The system performs DNS SRV processing to locate the SIP Server Port.

   If SRV is enabled the system continues as follows:

   If Port is not specified or DNS NAPTR is pending the system proceeds with DNS SRV lookup for the resulting FQDN from NAPTR response/configured FQDN using the SRV prefixes listed in the table above.

   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 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 perform DNS A lookup on the resulting FQDN from SRV response/ 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 no more DNS A record lookups are pending 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 as 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 Port for finding a valid Server Configuration.

   Once the SIP server is located, the SIP routing system compares the IP address of the located SIP server 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 as follows 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 (call toward a server)

The routing system uses the URI Group, 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 against the provisioned IP Address field of Received Interface configuration to decide a match. If either of the URI Group or Received 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.

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

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 as follows 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 (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 SIP REGISTER method are applied on the incoming SIP request before proceeding with Route Resolution phase.

Transmit to network (call processing)

The SIP routing system finally route the call towards the target Endpoint using the connection information determined during the routing phase.

Note that the SIP routing system retries the call to a new alternate target destination where the endpoint could be reached if SIP 408 response is received from the Transaction Layer / SIP 5xx error response is received from the Network. The alternate target destination could be an IP address from the Next Hop Server 2 field of the Routing Profile / pending DNS NAPTR/ SRV/A record entries that are yet to be tried if 3263 procedures are used.

All the messages including SIP Responses/Indialog Requests and Responses will be properly routed by the SIP routing system using the same Subscriber / Server Flows that was matched during initial INVITE call processing.

Managing domain policies

This section provides an overview of the management of domain policies covering the following topics:

- Application rules
- Border rules
- Media rules

Application rules

Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane

to define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions your network will process on order to prevent resource exhaustion.

Application Rules are part of the End-Point Policy Group configuration, which is described in the section titled “End-Point Policy Groups” in this chapter. An Application Rule or default can be selected from a list during the configuration while creating an End-Point Policy Group. In addition to selecting an Application Rule, you can also select a Border Rule, Media Rule, Security Rule, Signaling Rule, and Time of Day rule.

Creating a new application rule

About this task

Use the following procedure to create a new Application Rule.

⚠ **Caution:**

A default application 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Application Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Application Rules screen.
3. Select **Add** from the Applications pane.
   The Application Rule pop-up window is displayed.
4. Enter a name for the new Application Rule and select **Next**
   A second Application Rule pop-up window is displayed.
5. Enter the requested information into the appropriate fields while referring to the field descriptions in the table below. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Application Rule window.

Field	Description
Application Type	The type of SIP application for which this Application Rule is being configured: Voice, Video, and IM.
In	Checkbox indicating that this Application Rule will apply to traffic (Voice, Video, and/or IM) entering the enterprise network.
Out	Checkbox indicating that this Application Rule will apply to traffic (Voice, Video, and/or IM) originating from within the enterprise network.
Maximum Concurrent Sessions	The maximum number of concurrent application sessions that will be

	allowed to be active for the selected application type (Voice, Video, and IM). Additional application requests will be blocked if this threshold is exceeded.
Maximum Sessions per Endpoint	The maximum number of concurrent application sessions that will be allowed to be active for the selected application type (Voice, Video, and IM) for any single end-point. Additional application requests will be blocked if this threshold is exceeded.
Miscellaneous	
CDR Support	None: Call detail records will not be provided. Without RTP: Call detail records with change in call states will be provided. With RTP: Call detail records with call quality and call statistics will be provided in addition to change in call states.
RTCP Keep-Alive	Enables the RTCP Keep-Alive feature.

6. After entering the required information , select **Finish** to save, exit, and redisplay the Application Rules screen.

Cloning an existing application rule

About this task

Use the following procedure to clone an existing Application Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Application Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Application Rules screen.
3. In the Application Pane, Select the name of the Application Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.

The Clone Rule pop-up window is displayed.

5. Enter a name for the new Application Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Application Rules screen is redisplayed, showing the newly-cloned Application Rule.

Editing an existing application rule

About this task

Use the following procedure to edit an application border Rule.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Application Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Application Rules screen.
3. In the Application Pane, Select name of the Application Rule that you want to edit.
4. Select the **Edit** button in the lower-center section of the screen.
   The Editing Rule pop-up window is displayed.
5. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Application Rules window.
6. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Application Rules screen.
   The Application Rules screen is redisplayed, showing the newly-edited Application Rule.

Renaming an existing application rule

About this task

Use the following procedure to rename an existing Application Rule.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Application Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Application Rules screen.
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 Rename Rule pop-up window is displayed
5. Enter the new name for the Application Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Application Rules screen is redisplayed, showing the newly-renamed Application Rule.

Deleting an existing application rule

About this task

Use the following procedure to delete an existing Application Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Application Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Application Rules screen.
3. In the Application Pane, Select the name of the Application Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the Application Rule or select **Cancel** to cancel the delete operation without saving.

The Application Rules screen is redisplayed. If **OK** was selected above, the chosen Application Rule will no longer be displayed in the Application Rules screen. If **Cancel** was selected above, the chosen Application Rule will still be displayed.

Border rules

Border Rules allow you control NAT Traversal.

The NAT Traversal feature allows you to determine whether or not call flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

Creating a new border rule

About this task

Use the following procedure to create a new border Rule.

⚠ **Caution:**

A default border 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Border Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Border Rules screen.
3. Select **Add** from the Applications pane.
   The Border Rule pop-up window is displayed.
4. Enter a name for the new Border Rule and select **Next**
   A second Border Rule pop-up window is displayed.
5. Enter the requested information into the appropriate fields while referring to the field descriptions in the table below. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Border Rules window.

Field	Description
Enable Natting	Checkbox which enables the application of the Network Address Translation (NAT) feature on signaling messages. When the Enable Natting checkbox is selected, SIP signaling message contact headers and SDP connection headers will be overwritten with configured Avaya SBCE published IP/domains. **Note:** The Enable Natting checkbox should be selected for all Avaya Aura deployments.
Disable Register Proxying	Checkbox which enables the application of the Network Address Translation (NAT) feature on SIP REGISTER messages when the Enable Natting checkbox is not selected. **Note:** The Disable Register Proxying checkbox should only be selected for OCS deployments. It is not applicable for Avaya Aura deployments.
Refresh Interval	The interval, in seconds, determining the frequency with which the far-end NAT device is refreshed.
Refresh for all Clients	Checkbox which enables (checked) or disables (unchecked) refreshing of all the clients registered through Avaya SBCE.
Use SIP Published IP	Checkbox which determine whether or not the Signaling IP addresses of the enterprise call server and SIP phones as defined on the Signaling Interface tab of the Signaling Interface function (found under the Device Specific Settings feature) 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 only activated if the Use SIP Published IP is checked.

Use SDP Published IP	Checkbox which determine whether or not the Media IP addresses of the enterprise call server and SIP phones as defined on the Media Interface tab of the Media Interface function (found under the Device Specific Settings feature) are used instead of the respective SDP Published Domain. If checked, the SDP Published Domain field is inactivated and the published Media IP address is used. If unchecked, the SDP Published Domain field is activated and the published Media IP address not used; the SDP Published Domain is used.
SDP Published Domain	The domain name of the enterprise call server and SIP phones. This field is only activated if the Use SDP Published IP is checked.

6. After entering the required informaton , select **Finish** to save, exit, and redisplay the Border Rules screen.

Cloning a border rule

About this task

Use the following procedure to clone an existing Border Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Border Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Application Rule set are displayed in the Content Area of the Border Rules screen.
3. In the Application Pane, Select the name of the Border Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.
   The Clone Rule pop-up window is displayed.

5. Enter a name for the new Border Rule and select **Finish** to save your changes or select the window**Cancel** option to cancel the cloning operation and close the window without saving.
   The Border Rules screen is redisplayed, showing the newly-cloned Border Rule.

Editing an existing border rule

About this task

Use the following procedure to edit an existing border Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Border Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Border Rule set are displayed in the Content Area of the Border Rules screen.
3. In the Application Pane, Select name of the Border Rule that you want to edit.
4. Select the**Edit** button in the lower-center section of the screen.
   The Editing Rule pop-up window is displayed.
5. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Border Rules window.
6. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Border Rules screen.
   The Border Rules screen is redisplayed, showing the newly-edited Border Rule.

Renaming an existing border rule

About this task

Use the following procedure to rename an existing Border Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.

2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Border Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Border Rule set are displayed in the Content Area of the Border Rules screen.
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 Rename Rule pop-up window is displayed
5. Enter the new name for the Border Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Border Rules screen is redisplayed, showing the newly-renamed Border Rule.

Deleting an existing border rule

About this task

Use the following procedure to delete an existing Border Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Border Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Border Rule set are displayed in the Content Area of the Border Rules screen.
3. In the Application Pane, Select the name of the Border Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the Border Rule or select **Cancel** to cancel the delete operation without saving.
   The Border Rules screen is redisplayed. If **OK** was selected above, the chosen Border Rule will no longer be displayed in the Border Rules screen. If **Cancel** was selected above, the chosen Border Rule will still be displayed.

Media rules

Media Rules allow you 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 to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Creating a new media rule

About this task

Use the following procedure to create a new media Rule.

⚠ **Caution:**

A default Media 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Media Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Media Rule set are displayed in the Content Area of the Media Rules screen.
3. Select **Add** from the Applications pane.
   The Media Rule pop-up window is displayed.
4. Enter a name for the new Media Rule and select **Next**
   A second Media Rule pop-up window is displayed.
5. Enter the appropriate Media NAT enforcement strategy for RTP injection detection/prevention using one of the two checkboxes and select **Next** to save and continue. Refer to the field descriptions in Media NAT Field Descriptions on page 110. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Media Rule window.

   A third Media Rule pop-up window is displayed.
6. Enter the appropriate codec prioritization information while referring to the field descriptions in Media and Video Encryption Field Descriptions on page 111.
   A fourth Media Rule pop-up window is displayed.
7. After entering the required information in the third Media Rule pop-up screen, select **Next** to save and continue. Selecting the window cancel option cancels the

operation and closes the window without saving. Selecting **Back** redisplays the first Media Rule window.

8. In the fourth Media Rule pop-up screen, Click the checkbox to enable the Media Anomaly Detection feature. Leave blank if no Media Anomaly Detection will be used. You will select the **Enable the Media Anomaly Detection** feature checkbox in order to do the following:

   - This feature detects Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks on a RTP media stream.
   - The acceptable data rate for a given RTP stream is 20% more than the predefined bandwidth for the codec being used.
   - Whenever the incoming data rate on an RTP stream exceeds the acceptable data rate, a Media DoS attack incidence is reported.
   - If different sources are trying to send data over the RTP stream resulting in exceeding the acceptable data rate, up to five such sources are tracked and reported as a Media DDoS attack.
   - Enable RTP Injection Protection:
     - Looks for extraneous traffic being injected into the RTP stream.
     - Detects RTP Injection and generates an alert but allows the extraneous traffic to pass through without dropping any packets unless a DoS attack is detected.
     - RTP Injection is not detected for asymmetric RTP traffic and not detected in HA configurations for failed-over calls.

   All RTP traffic is limited by dropping the packets exceeding the acceptable data rate in a given second.

   Note:

   If Media Anomaly Detection is selected, choose whether or not to detect an RTP injection attack. Then designate whether or not the RTP connection is asymmetric and select an action to be taken.

   A fifth Media Rule pop-up window is displayed.

9. If, in the previous step, you clicked the checkbox to enable the Media Anomaly Detection feature, an additional option checkbox is revealed, Detect RTP Injection Attack. Click the checkbox to enable the Detect RTP Injection Attack feature or leave blank if not used, and then select **Next**.

   Note:

   The Detect RTP Injection Attack checkbox enables the detection of an RTP injection attack. Also see the Media NAT enforcement strategy settings in Step 7.

10. If, in the previous step, you clicked the checkbox to enable the Detect RTP Injection Attack feature, additional options are revealed, an Asymmetric RTP checkbox and

an Action drop-down list. Click the checkbox to enable the Asymmetric RTP feature. Leave blank if not used. If checked, select an Action and select **Next**. Media Anomaly Detection Field Descriptions on page 112

Note:

The Asymmetric RTP checkbox enables asymmetric RTP streams, where the payload type is not the same in both directions.

A fifth Media Rule pop-up window is displayed containing Media Silencing options, a checkbox to enable Media Silencing and a Timeout (seconds) edit box.

11. Enter the appropriate media silencing information while referring to the field descriptions in Media Silencing Field Descriptions on page 112. Click the checkbox to enable the Media Silencing feature. Leave blank if not used. If checked, enter a timeout value (in seconds) and select **Next**.
A sixth Media Rule pop-up window is displayed containing Media QoS Reporting and Media QoS Marking fields.

12. Enter the appropriate codec prioritization information while referring to the field descriptions in Media QoS Field Descriptions. on page 113

13. Select **Finish**
An updated Media Rules screen is displayed containing the newly-created Media Rule.

Media NAT field descriptions

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

Media NAT field descriptions

Field	Description
Media NAT	
Enforce Signaling and Media IP correlation	The Media IP and port are known.
Learn Media IP dynamically	The Media IP and port are learned dynamically.

Note:

Media NAT settings protect against RTP Injection Attacks. See the Detect RTP Injection Attack and Asymmetric RTP settings in Step-12.

Codec Priortization Field Descriptions

When creating a new Media Rule, refer to this table for information on the codec prioritizations selections in the third Media Rule pop-up window.

Media and Video Encryption Field Descriptions

Field	Description
Audio Media Encryption and Video Media Encryption	
Preferred Format #1	The most preferred encryption method for media traffic. Available selections are: 1. RTP 2. SRTP_AES_CM_128_HMAC_SHA1_32 3. SRTP_AES_CM_128_HMAC_SHA1_80 4. ERTP
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	Checkbox indicating whether or not encryption will be used for RTCP. **Note:** The Encrypted RTCP option checkbox will only be available for selection if at least one of the three Preferred Formats above it has an SRTP option selected.
Interworking	When the interworking checkbox is checked, it allows media from an encrypted media end-point flow. The reverse, unencrypted to encrypted, is also true. The interworking checkbox should be checked for the media rules in both end-point flows. Unless end-to-end encryption must be enforced, it is recommended that this checkbox be checked.

Miscellaneous	
Capacity Negotiation	Checkbox enabling compliance with SDP Capability Negotiation RFC-5939.

Media anomaly detection field descriptions

When creating a new Media Rule, refer to this table for information on the Media Anomaly checkbox selections in the sixth Media Rule pop-up window.

Media anomaly detection field descriptions

	Field	Description
	Media Anomaly	
	Media Anomaly Detection	Checkbox indicating whether or not the Media Anomaly Detection feature is to be activated.
Detect RTP Injection Attack		Checkbox indicating whether or not the Detect RTP Injection Attack feature is to be activated.
	Asymmetric RTP	The Asymmetric RTP checkbox enables asymmetric RTP streams, where the payload type is not the same in both directions. **Note:** This option is only available when the Detect RTP Injection Attack box (above) is selected.
	Action	This drop-down menu selects the action to be performed (i.e., Alert or Block) following the detection of a media anomaly.

Media silencing field descriptions

When creating a new Media Rule, refer to this table for information on the fields in the Media Silencing pop-up window.

Media silencing field descriptions

Field	Description
Media Silencing	Checkbox indicating whether or not the Media Silencing feature is to be activated. If

	the Media Silencing feature detects the absence of media packets from one leg of the call in session within the time period defined by the Timeout field, an incidence is sent to the Syslog. If media packets are not detected in either direction during the same Timeout, then the call is terminated with a BYE message. If checked, the media silencing feature is activated. If unchecked, the media silencing feature is not activated.
Timeout	The time period (in seconds) within which the media silencing feature ‘listens’ for media packets from both legs of a call. If no media packets are detected in this period, then either a Syslog entry is generated or the call is terminated.

Media QoS field descriptions

When creating a new Media Rule, refer to this table for information on the fields in the Media QoS pop-up window.

Media silencing field descriptions

Field	Description
Media QoS Reporting	
RTCP Enabled	Checkbox indicating whether or not RTCP is enabled for media QoS reports. When RTCP is enabled, RTCP statistics will be included in the Call Detail Report (CDR). If checked, RTCP is enabled. If unchecked, RTCP is disabled.
Media QoS Marking	
Enabled	Checkbox indicating whether or not Type-of-Service (ToS) quality standards will be applied to audio and video streams. If checked, the ToS quality standards will be applied and the ToS and DSCP radio buttons are activated. If unchecked, the ToS quality standards will be applied and the ToS and DSCP radio buttons are *not* activated.

ToS	A radio button indicating that ToS quality standards will be applied to audio and video streams. ToS quality standards can be applied to four (4) audio/video parameters: Audio Precedence, Audio ToS, Video Precedence, and Video ToS. Select the desired quality level from the corresponding drop-down menu. When the ToS option is selected, the DSCP quality option is disabled.
DSCP	A radio button indicating that ToS quality standards will be applied to audio and video streams. ToS quality standards can be applied to audio and video streams. Select the desired quality level from the corresponding drop-down menu. When the ToS option is selected, the DSCP quality option is disabled.

Cloning an existing media rule

About this task

Use the following procedure to clone an existing Media Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Media Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Media Rule set are displayed in the Content Area of the Media Rules screen.
3. In the Application Pane, Select the name of the Media Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.
   The Clone Rule pop-up window is displayed.
5. Enter a name for the new Media Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Media Rules screen is redisplayed, showing the newly-cloned Media Rule.

Editing an existing media rule

About this task

Use the following procedure to edit an existing Media Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Media Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Media Rule set are displayed in the Content Area of the Media Rules screen.
3. In the Application Pane, Select name of the Media Rule set that you want to edit.
   The Parameter Tabs for the selected Media Rule set will be displayed in the Content Area.
4. Select the Media Rule Parameter Tab whose values you want to edit.
   The corresponding parameters for that Media Rule Parameter Tab will be displayed in the Content Area.
5. Select the **Edit** button in the lower-center section of the screen.
   A Media Rule edit screen is displayed for the selected Parameters Tab for editing.
6. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Media Rules window.
7. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Media Rules screen.
   The Media Rules screen is redisplayed.

Renaming an existing media rule

About this task

Use the following procedure to rename an existing Media Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.

2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Media Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Media Rule set are displayed in the Content Area of the Media Rules screen.
3. In the Application Pane, Select the name of the Media Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.
   The Rename Rule pop-up window is displayed
5. Enter the new name for the Media Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Media Rules screen is redisplayed, showing the newly-renamed Media Rule.

Deleting an existing media rule

About this task

Use the following procedure to delete an existing Media Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Media Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Media Rule set are displayed in the Content Area of the Media Rules screen.
3. In the Application Pane, Select the name of the Media Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the Media Rule or select **Cancel** to cancel the delete operation without saving.
   The Media Rules screen is redisplayed. If **OK** was selected above, the chosen Media Rule will no longer be displayed in the Media Rules screen. If **Cancel** was selected above, the chosen Media Rule will still be displayed.

Security rules

Security Rules allow you to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows you to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, you can also define the security feature profile so that the feature is applied in a specific manner to a specific situation.

Note:

Scrubber Packages must be enabled in the Security Rules of Domain Policies. Only then will the Scrubber Packages take effect.

Once the Scrubber Packages are enabled in the Security Rules, a list of packages would be needed for the Security Rule.

Five security features can be controlled by enabling/disabling the Security Rules listed below:

- Authentication: Can be enabled so the users coming on a particular device can be authenticated using digest authentication.
- From URI Blacklist: Can be enabled to reject the calls from the devices configured in the Black list group.
- FingerPrint: Can be enabled to detect and drop spoofed messages.
- Scrubber: Can be enabled to detect and drop malformed messages.
- Domain Dos: Can be enabled to detect DoS attacks within a Domain policy.

Creating a new security rule

About this task

Use the following procedure to create a new Security Rule.

⚠ **Caution:**

A default Security 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane.

Existing Security Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Security Rules screen.

3. Select **Add** from the Applications pane.
   The Secirity Rule pop-up window is displayed.
4. Enter a name for the new Security Rule and select **Next**
   A second Security Rule pop-up window is displayed.
5. Select the appropriate authentication information while referring to the field descriptions in Authentication Field Descriptions on page 119, and then select **Next** to save and continue. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   A third Security Rule pop-up window is displayed.
6. In the third Security Rule pop-up window, in the drop-down list in the From/To Blacklist field, you can select a blacklist URI group to be used in checking the validity of subscribers using the network. When a blacklist URI group is selected, all calls are rejected from devices in the group.URI blacklist field descriptions on page 120

   Note:

   A blacklist is a list of callers that subscribers do not want to receive calls from. A blacklist can be created by selecting Global Profiles and then URI Groups, clicking Add, entering a blacklist name, and then enter items in the list in either plain text, a dial plan, or as one or more regular expressions.
7. Select **Next**.
   A fourth Security Rule pop-up window is displayed.
8. Select the appropriate Fingerprinting information, while referring to Fingerprint profile field descriptions on page 121.
   Another Media Rule pop-up window is displayed containing Media Silencing options, a checkbox to enable Media Silencing and a Timeout (seconds) edit box.
9. Select **Next**.
   A fifth Security Rule pop-up window is displayed.

   Note:

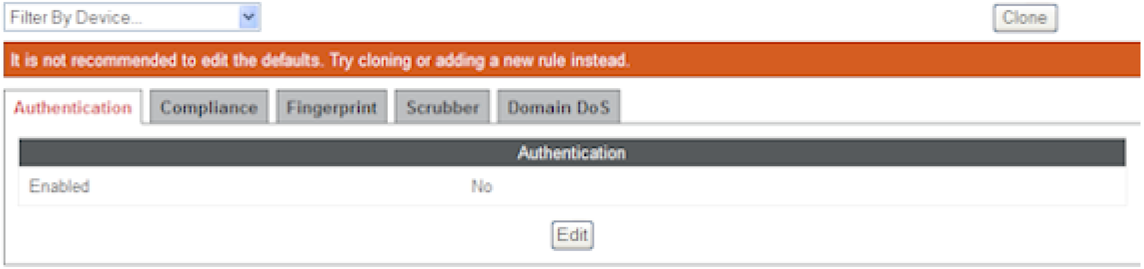
   New Scrubber Packages and VIPER signatures are added here.VIPER signatures are similar to Scrubber Packages, and are created by the VIPER team, and then packaged and released by the engineering team after testing. Refer to Updating VIPER signatures on page 62, Protocol Scrubber on page 261, and Installing a Scrubber Rules Package on page 262.

   Before adding a new scrubber package to a security rule here, you must first install the scrubber package on the SBCE/SCBE from the Scrubber feature of Global Parameters.

You can select the Scrubber function from the Global Parameters feature in the Task Pane.

10. Select the appropriate scrubber information while referring to the field descriptions in Scrubber profile field descriptions on page 121.
11. Select **Next**.
    A sixth Security Rule pop-up window is displayed.
12. Enter the appropriate codec prioritization information while referring to the field descriptions in Domain DoS Profile field descriptions on page 122.
13. Select **Finish**
    The new **Security Rule** set is added to the **Security Rule** list in the Application Pane.

Example



It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Authentication	
Enabled	No

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.

Authentication field descriptions

Field	Description
Authentication	
Enabled	A checkbox indicating whether or not SIP requests will be authenticated. If checked, SIP requests will be authenticated according to the parameters specified by the remaining fields: Authenticate, Authenticate

<table>
<tr><td></td><td>Initiating Requests Only, Authentication Timeout, and Realm. When checked, the remaining fields become active and must be defined.
If this box is not checked, then SIP requests are not authenticated and the remaining fields (Authenticate, Authenticate Initiating Requests Only, Authentication Timeout, and Realm) are inactivated.
The benefit from having Authentication enabled is that Avaya SBCE will challenge the user instead of the call server, and whenever that occurs, that user would not be challenged again by the call server. This offloads the authentication mechanism from the call server.</td></tr>
<tr><td>Authenticate</td><td>Radio buttons which allow you to determine how frequently authentication will be performed.
<table>
<tr><td>All Requests</td><td>Authenticate each SIP request.</td></tr>
<tr><td>Periodically</td><td>Only authenticate at a periodic interval, the frequency of which is determined by the Authentication Timeout field.</td></tr>
<tr><td>Once</td><td>Authenticate one time only.</td></tr>
</table>
</td></tr>
<tr><td>Authenticate Initiating Requests Only</td><td>Checkbox indicating whether or not only initiating SIP requests will be authenticated. If checked, only initiating SIP requests will be authenticated.
If this checkbox is not checked, then all SIP requests are authenticated.</td></tr>
<tr><td>Authentication Timeout</td><td>The time, in seconds, that the authentication will be maintained by the Avaya SBCE security device.
This field is only active when the Periodically radio button is checked for the Authenticate field.</td></tr>
<tr><td>Realm</td><td>The name of the authentication realm that will authenticate SIP proxy users.</td></tr>
<tr><td colspan="2">Authentication Requests</td></tr>
<tr><td>Checkboxes</td><td>When checked, indicate which SIP requests will require authentication.</td></tr>
</table>

URI blacklist field descriptions

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

Fingerprint profile field descriptions

Field	Description
From URI Blacklist	A drop-down list contains the names of pre-constructed blacklists of callers that subscribers do not want to receive calls from. **Note:** A URI blacklist can consist of plain text, a dial plan, or one or more regular expressions.

Fingerprint profile field descriptions

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

Fingerprint profile field descriptions

Field	Description
Fingerprinting	A checkbox indicating whether or not the Fingerprinting feature will be enabled. When Fingerprinting is enabled, spoofed messages will be detected and dropped. If checked, the Fingerprinting feature is enabled and the Fingerprint Profile field is activated. If unchecked, the Fingerprinting feature is not enabled and the Fingerprint Profile field is inactivated.
Fingerprint Profile	A pull-down menu from which you select the profile to be used by the Fingerprinting feature.

Scrubber profile field descriptions

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

Scrubber profile field descriptions

Field	Description
Enable Scrubber	A checkbox indicating whether or not the Scrubber feature will be enabled.

	If checked, the Scrubber feature is enabled and the Scrubber Packages field is activated. If unchecked, the Scrubber feature is not enabled and the Scrubber Packages field is inactivated.
Scrubber Packages	A collection of existing Scrubber Packages which can be selected for use by the Scrubber feature. Select one or more Scrubber Packages. Use Control-Click to select multiple packages.

Domain DoS profile field descriptions

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.

Domain DoS profile field descriptions

Field	Description
Domain DoS	A checkbox indicating whether or not the Domain DoS feature will be enabled. If checked, the Domain DoS feature is enabled and the Domain DoS Profile field is activated. If unchecked, the Domain DoS feature is not enabled and the Domain DoS Profile field is inactivated.
Domain DoS Profile	A collection of existing DoS profiles which can be selected for use by the Domain DoS feature.

Cloning an existing security rule

About this task

Use the following procedure to clone an existing Security Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Security Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Security Rules screen.

3. In the Application Pane, Select the name of the Security Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.
   The Clone Rule pop-up window is displayed.
5. Enter a name for the new Security Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Security Rules screen is redisplayed, showing the newly-cloned Security Rule.

Editing an existing security rule

About this task

Use the following procedure to edit an existing security Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Security Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Security Rules screen.
3. In the Application Pane, Select name of the Security Rule set that you want to edit.
   The Parameter Tabs for the selected Security Rule set will be displayed in the Content Area.
4. Select the Security Rule Parameter Tab whose values you want to edit.
   The corresponding parameters for that Security Rule Parameter Tab will be displayed in the Content Area.
5. Select the **Edit** button in the lower-center section of the screen.
   A Security Rule edit screen is displayed for the selected Parameters Tab for editing.
6. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Security Rules window.
7. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Security Rules screen.

The Security Rules screen is redisplayed.

Renaming an existing security rule

About this task

Use the following procedure to rename an existing Security Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Security Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Security Rules screen.
3. In the Application Pane, Select the name of the Security Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.
   The Rename Rule pop-up window is displayed
5. Enter the new name for the Security Rule and select **Finish** to save your changes or select the window**Cancel** option to cancel the cloning operation and close the window without saving.
   The Security Rules screen is redisplayed, showing the newly-renamed Security Rule.

Deleting an existing security rule

About this task

Use the following procedure to delete an existing security Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane.

Existing Security Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Security Rules screen.

3. In the Application Pane, Select the name of the Security Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the Security Rule or select **Cancel** to cancel the delete operation without saving.
   The Security Rules screen is redisplayed. If **OK** was selected above, the chosen Security Rule will no longer be displayed in the Security Rules screen. If **Cancel** was selected above, the chosen Security Rule will still be displayed.

Signaling rules

Signaling Rules allow you to define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they 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:**

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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.

3. Select **Add** from the Applications pane.
   The Signaling Rule pop-up window is displayed.
4. Enter a name for the new Signaling Rule and select **Next**
   A second Signaling Rule pop-up window is displayed.
5. Select the appropriate signaling information while referring to the field descriptions in Signaling rule field descriptions on page 129.
6. After entering the required informaton in the second Signaling Rule window,, select **Next** to save and continue. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   A third Security Rule pop-up window is displayed.
7. Select the appropriate signaling information while referring to the field descriptions in Content-Type Policy Field Descriptions on page 131.
8. After entering the required informaton in the third Signaling Rule window,, select **Next** to save and continue. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   A fourth Security Rule pop-up window is displayed.
9. Select the appropriate signaling information while referring to the field descriptions in Signaling QoS Field Descriptions on page 126.
10. Select**Finish**.
    An updated Signaling Rules screen is displayed showing the newly-created Signaling Rule.

Signaling QoS field descriptions

When creating a new Signaling Rule, refer to this table for information on the signaling QoS selections in the third Signaling Rule pop-up window.

Signaling QoS field descriptions

Field	Description
Enabled	A checkbox indicating whether or not the Signaling Quality-of-Service (QoS) feature will be enabled. Check the box to enable the Signaling QoS statistics feature or leave the box blank to disable the Signaling QoS statistics feature.

ToS	Radio button allowing you to select Type-of-Service (ToS)
DSCP	The value of the six most significant values of the Differentiated Services (DiffServ) field. These values, referred to as the Differentiated Services Point Code (DSCP), are used to provide guaranteed service to critical network traffic. Use the pull-down menu to select the desired DSCP value.

Editing an existing signaling rule

About this task

Use the following procedure to edit an existing Signaling Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Security Rule set are displayed in the Content Area of the Signaling Rules screen.
3. In the Application Pane, Select name of the Signaling Rule set that you want to edit.
   The Parameter Tabs for the selected Signaling Rule set will be displayed in the Content Area.
4. Select the Signaling Rule Parameter Tab whose values you want to edit.
   The corresponding parameters for that Signaling Rule Parameter Tab will be displayed in the Content Area.
5. Select the**Edit** button in the lower-center section of the screen.
   A Signaling Rule edit screen is displayed for the selected Parameters Tab for editing.
6. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Security Rules window.
7. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Signaling Rules screen.
   The Signaling Rules screen is redisplayed.

General parameters tab

About this task

Use the following procedure to edit the Signaling Rule General parameters tab.

⚠ **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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to edit the General parameters tab from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **General** parameters tab.
   A Signaling Rule pop-up window is displayed.
5. Select the appropriate signaling information while referring to the field descriptions in Signaling rule field descriptions on page 129.
6. After entering the required informaton in the second Signaling Rule window,, select **Next** to save and continue. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   A second Signaling Rule pop-up window is displayed.
7. Select the appropriate signaling information while referring to the field descriptions in Content-Type Policy Field Descriptions on page 131.
8. After entering the required informaton in the third Signaling Rule window,, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the previous Signaling Rule pop-up window.
   The Signaling Rule's information window is redisplayed.

Signaling rule field descriptions

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

Signaling rule field descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td colspan="2">Inbound</td></tr>
<tr><td>Requests</td><td>Drop-box allowing you to determine how incoming SIP request messages will be treated by this policy. Available options are <b>Allow</b> and <b>Block with….</b>
<table>
<tr><td>Allow</td><td>Allow all incoming SIP request messages. The corresponding fields to the right are inactivated.</td></tr>
<tr><td>Block with . . .</td><td>Block all incoming SIP request messages and return the response indicated in the corresponding fields.</td></tr>
</table></td></tr>
<tr><td>Non-2xx Final Responses</td><td>Drop-box allowing you to determine how incoming Non-2xx Final SIP response messages will be treated by this policy. Available options are <b>Allow</b> and <b>Change Response to….</b>
<table>
<tr><td>Allow</td><td>Allow all incoming Non-2xx Final Response messages. The corresponding fields to the right are inactivated.</td></tr>
<tr><td>Change Response to. . .</td><td>Block all incoming Non-2xx Final Response messages and return the response indicated in the corresponding fields.</td></tr>
</table></td></tr>
<tr><td>Optional Request Headers</td><td>Drop-box allowing you to determine how optional request headers contained in incoming SIP messages will be treated by this policy. Available options are <b>Allow</b>, <b>Remove Header</b>, and <b>Block with….</b>
<table>
<tr><td>Allow</td><td>Allow all incoming SIP messages that contain optional request headers. The corresponding fields to the right are inactivated.</td></tr>
<tr><td>Remove Header</td><td>Strip optional request headers from all incoming SIP messages and allow the message to proceed.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Block with . . .</td><td>Block all incoming SIP messages that contain an optional request header and return the response indicated in the corresponding fields.</td></tr></table></td></tr>
<tr><td>Optional Response Headers</td><td>Drop-box allowing you to determine how optional response headers contained in incoming SIP messages will be treated by this policy. Available options are <b>Allow</b>, <b>Remove Header</b>, and <b>Block with….</b><table><tr><td>Allow</td><td>Allow all incoming SIP messages that contain optional response headers. The corresponding fields to the right are inactivated.</td></tr><tr><td>Remove Header</td><td>Strip optional response headers from all incoming SIP messages and allow the message to proceed.</td></tr><tr><td>Block with . . .</td><td>Block all incoming SIP messages that contain an optional response header and return the response indicated in the corresponding fields.</td></tr></table></td></tr>
<tr><td colspan="2">Outbound</td></tr>
<tr><td>Requests</td><td>Drop-box allowing you to determine how outbound SIP request messages will be treated by this policy. Available options are <b>Allow</b> and <b>Block with….</b><table><tr><td>Allow</td><td>Allow all outbound SIP request messages. The corresponding fields to the right are inactivated.</td></tr><tr><td>Block with . . .</td><td>Block all outbound SIP request messages and return the response indicated in the corresponding fields.</td></tr></table></td></tr>
<tr><td>Non-2xx Final Responses</td><td>Drop-box allowing you to determine how outbound Non-2xx Final SIP response messages will be treated by this policy. Available options are <b>Allow</b> and <b>Change Response to….</b><table><tr><td>Allow</td><td>Allow all outbound Non-2xx Final Response messages. The corresponding fields to the right are inactivated.</td></tr><tr><td>Change Respons e to. . .</td><td>Block all outbound Non-2xx Final Response messages and return the response indicated in the corresponding fields.</td></tr></table></td></tr>
<tr><td>Optional Request Headers</td><td>Drop-box allowing you to determine how optional request headers contained in outbound SIP messages will be treated by this policy. Available options are <b>Allow</b>, <b>Remove Header</b>, and <b>Block with….</b></td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td>Allow</td><td>Allow all outbound SIP messages that contain optional request headers. The corresponding fields to the right are inactivated.</td></tr>
<tr><td>Remove Header</td><td>Strip optional request headers from all outbound SIP messages and allow the message to proceed.</td></tr>
<tr><td>Block with . . .</td><td>Block all outbound SIP messages that contain an optional request header and return the response indicated in the corresponding fields.</td></tr>
</table></td></tr>
<tr><td>Optional Response Headers</td><td>Drop-box allowing you to determine how optional response headers contained in outbound SIP messages will be treated by this policy. Available options are <b>Allow</b>, <b>Remove Header</b>, and <b>Block with….</b><table>
<tr><td>Allow</td><td>Allow all outbound SIP messages that contain optional response headers. The corresponding fields to the right are inactivated.</td></tr>
<tr><td>Remove Header</td><td>Strip optional response headers from all outbound SIP messages and allow the message to proceed.</td></tr>
<tr><td>Block with . . .</td><td>Block all outbound SIP messages that contain an optional response header and return the response indicated in the corresponding fields.</td></tr>
</table></td></tr>
</table>

Content—type policy field descriptions

When creating a new Signaling Rule, refer to this table for information on the signaling selections in the third Signaling Rule pop-up window.

Signaling content—type policy field descriptions

<table>
<tr><th colspan="2">Content—Type Policy</th></tr>
<tr><td>Action</td><td>Drop-down menu from which you choose the action to be taken by the SBCE security device when considering the content portion of SIP signaling messages. Available options are <b>Allow</b> and <b>Remove</b><table>
<tr><td>Allow</td><td>Allows the content in each SIP signaling message to pass, with the exception of those items contained in the Exceptions List which are removed.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Remove</td><td>Removes all content from each SIP signaling message, with the exception of the items contained in the Exceptions List which are allowed to pass.</td></tr></table></td></tr>
<tr><td>Exception List</td><td>The specific terms which are to be passed ort blocked, according to the action specified in the Action field.</td></tr>
<tr><td>Multipart Action</td><td>Drop-down menu from which you choose the action to be taken by the SBCE security device when considering the multi-part content portion of SIP signaling messages. <b>Allow</b> and <b>Remove</b><table><tr><td>Allow</td><td>Allows the multi-part content in each SIP signaling message to pass, with the exception of those items contained in the Exceptions List which are removed.</td></tr><tr><td>Remove</td><td>Removes all the multi-part content from each SIP signaling message, with the exception of the items contained in the Exceptions List which are allowed to pass.</td></tr></table></td></tr>
<tr><td>Exception List</td><td>The specific terms which are to be passed ort blocked, according to the action specified in the Multipart Action field.</td></tr>
</table>

Requests Parameters Tab

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

Adding Request Parameters

About this task

Use the following procedure to add In Request and Out Request parameters for a Signaling Rule (if none are already defined). In Requests refer to SIP message requests being directed to enterprise end-points. Out Requests refer to SIP message requests being directed to end-points 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to add In Request and/or Out Request parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Requests** tab.
5. Select the **Add In Header Control** button or the **Add Out Header Control** button
   The corresponding Add Request Control pop-up window is displayed.
6. Select the appropriate information while referring to the field descriptions in Request control field descriptions on page 134.
7. After selecting the required informaton in the Add Request Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Signaling Rule window.
   The selected Signaling Rule's information window is redisplayed.

Editing Request Parameters

About this task

Use the following procedure to edit In Request and Out Request parameters for a Signaling Rule (if none are already defined). In Requests refer to SIP message requests being directed to enterprise end-points. Out Requests refer to SIP message requests being directed to end-points 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.

Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.

3. Select the name of the Signaling Rule where you want to edit In Request and/or Out Request parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Requests** tab.
5. Select the **Add In Request Control** button or the **Add Out Request Control** button
   The corresponding Edit Request Control pop-up window is displayed.
6. Edit the appropriate information while referring to the field descriptions in Request control field descriptions on page 134.
7. After selecting the required information in the Edit Request Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   The selected Signaling Rule's information window is redisplayed.

Request Control Field Descriptions

When creating a new Signaling Rule, refer to this table for information on the fields in the request control pop-up window.

Request Control Field Descriptions

Field	Description
Proprietary Request	A checkbox indicating whether or not the Request being defined is a non-standard SIP request. Check the box to designate a non-standard SIP request message or leave the box blank 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. This field will be grayed-out if the Proprietary Request field is checked.
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 Response. If the Block with Response selection is made, the two fields to the right will be activated, allowing you to 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 the Block with Response selection is made, the two fields to the right will be activated, allowing you to provide the type of response to be sent.

Responses Parameters Tab

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

Adding Response Parameters

About this task

Use the following procedure to add In Response and Out Response parameters for a Signaling Rule (if none are already defined). In Response refer to SIP message responses being directed to enterprise end-points. Out Responses refer to SIP message responses being directed to end-points 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to add In Request and/or Out Request parameters from the Applications pane.
   The selected Signaling Rule’s information window is displayed.
4. Select the **Responses** tab.
5. Select the **Add In Response Control** button or the **Add Out Response Control** button
   The corresponding Add Response Control pop-up window is displayed.

6. Select the appropriate information while referring to the field descriptions in Response control field descriptions on page 137.
7. After selecting the required informaton in the Add Response Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Signaling Rule window.
   The selected Signaling Rule's information window is redisplayed.

Editing Response Parameters

About this task

Use the following procedure to edit In Response and Out Response parameters for a Signaling Rule (if none are already defined). In Responses refer to SIP message requests being directed to enterprise end-points. Out Resopnses refer to SIP message requests being directed to end-points 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to edit In Request and/or Out Request parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Responses** tab.
5. Select the **Add In Response Control** button or the **Add Out Response Control** button
   The corresponding Edit Response Control pop-up window is displayed.
6. Edit the appropriate information while referring to the field descriptions in Response control field descriptions on page 137.
7. After selecting the required informaton in the Edit Response Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the

operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
The selected Signaling Rule’s information window is redisplayed.

Response Control Field Descriptions

When creating a new Signaling Rule, refer to this table for information on the fields in the response control pop-up window.

Response Control Field Descriptions

Field	Description
Proprietary Response	A checkbox indicating whether or not the Response being defined is a non-standard SIP response. Check the box to designate a non-standard SIP response or leave the box blank 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. This field will be grayed-out if the Proprietary Request field is checked.
Method Name	The SIP message which will trigger 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 (session established). Available action options are Allow and Change Response to …. If the Change Response to … selection is made, the two fields to the right will be activated, allowing you to provide the type of response to be sent.

Request Headers Parameters Tab

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

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 none are already defined.) In Request Header Control parameters are applied to the headers of SIP messages directed to enterprise end-points. Out Request Header Control parameters are applied to the headers of SIP messages directed to end-points 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to add In Request Header and/or Out Request Header parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Request Headers** tab.
5. Select the **Add In Header Control** button or the **Add Out Header Control** button
   The corresponding Add Header Control pop-up window is displayed.
6. Select the appropriate information while referring to the field descriptions in Request header control field descriptions on page 139.
7. After selecting the required informaton in the Add Request Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Signaling Rule window.
   The selected Signaling Rule's information window is redisplayed.

Editing Request Header Parameters

About this task

Use the following procedure to edit existing Request Header parameters.

⚠ **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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to edit In Request Header and/or Out Request Header parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Request Headers** tab.
5. Select the **Add In Request Control** button or the **Add Out Request Control** button
   The corresponding Edit Request Control pop-up window is displayed.
6. Edit the appropriate information while referring to the field descriptions in Request header control field descriptions on page 139.
7. After selecting the required information in the Edit Request Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   The selected Signaling Rule's information window is redisplayed.

Request Header Control Field Descriptions

When creating a new Signaling Rule, refer to this table for information on the fields in the request header control pop-up window.

Request Header Control Field Descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Proprietary Request Header?</td><td>A checkbox indicating whether or not the header being defined is a non-standard SIP header. Check the box to designate a non-standard SIP header or leave the box blank to indicate a standard SIP header.</td></tr>
<tr><td>Header Name</td><td>The name of the proprietary SIP header. Make your selection from the corresponding drop-down list. This field will be grayed-out if the Proprietary Request Header? field is checked.</td></tr>
<tr><td>Method Name</td><td>The context or call sequence in which the header is contained.</td></tr>
<tr><td>Action</td><td>The action to be taken if the header is present in the SIP message designated in the Method Name field. Depending upon selection made in the Header Criteria field, available actions are:
<table>
<tr><td>Criteria</td><td>Action</td></tr>
<tr><td>Forbidden</td><td>1. Remove header
2. Block with . . .</td></tr>
<tr><td>Mandatory</td><td>Block with . . .</td></tr>
<tr><td>Optional</td><td>Allow</td></tr>
<tr><td colspan="2">If the Block with … Action is selected, then the two fields to the right are activated, allowing you to enter the response message to be sent in reply.</td></tr>
</table>
</td></tr>
</table>

Response Headers Parameters Tab

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

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:**
>
> 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to add In Response Header and/or Out Response Header parameters from the Applications pane.
   The selected Signaling Rule’s information window is displayed.
4. Select the **Response Headers** tab.
5. Select the **Add In Response Control** button or the **Add Out Response Control** button
   The corresponding Add Response Control pop-up window is displayed.
6. Select the appropriate information while referring to the field descriptions in Response header control field descriptions on page 142.
7. After selecting the required informaton in the Add Response Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Signaling Rule window.
   The selected Signaling Rule’s information window is redisplayed.

Editing Response Header Parameters

About this task

Use the following procedure to edit existing Response Header parameters.

> ⚠ **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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. Select the name of the Signaling Rule where you want to edit In Response Header and/or Out Response Header parameters from the Applications pane.
   The selected Signaling Rule's information window is displayed.
4. Select the **Response Headers** tab.
5. Select the **Add In Response Control** button or the **Add Out Response Control** button
   The corresponding Edit Response Control pop-up window is displayed.
6. Edit the appropriate information while referring to the field descriptions in Response header control field descriptions on page 142.
7. After selecting the required information in the Edit Response Control pop-up window, select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first Security Rule window.
   The selected Signaling Rule's information window is redisplayed.

Response Header Control Field Descriptions

When creating a new Signaling Rule, refer to this table for information on the fields in the response header control pop-up window.

Response Header Control Field Descriptions

Field	Description
Proprietary Response Header	A checkbox indicating whether or not the header being defined is a non-standard SIP response header. Check the box to designate a non-standard SIP response header or leave the box blank 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. This field will be grayed-out if the Proprietary Response Header field is checked.

<table>
<tr><td>Response Code</td><td>The code to be sent as the SIP response. Select the desired code from the drop-down box.</td></tr>
<tr><td>Method Name</td><td>SIP signaling message name (CANCEL, INVITE, PUBLISH, etc.). Make your selection from the corresponding drop-down list.</td></tr>
<tr><td>Header Criteria</td><td>Whether or not the presence of the header in the response field is Forbidden, Mandatory, or Optional.</td></tr>
<tr><td>Action</td><td>The action to be taken if the header is present in the SIP response. Available actions are:
<table>
<tr><td>Criteria</td><td>Action</td></tr>
<tr><td>Forbidden</td><td>1. Remove header
2. Change response to . . .</td></tr>
<tr><td>Mandatory</td><td>Change response to . . .</td></tr>
<tr><td>Optional</td><td>Allow</td></tr>
<tr><td colspan="2">If the Change response to … Action is selected, then the two fields to the right are activated, allowing you to enter the new response.</td></tr>
</table>
</td></tr>
</table>

Signaling QoS Parameters Tab

About this task

Use the following procedure to edit the Signaling QoS parameter set.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Siglaning Rules screen.
3. In the Application Pane, Select 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 Signaling QoS pop-up window is displayed.

5. Edit the appropriate fields while referring to Signaling QoS Field Descriptions on page 126. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Border Rules window.
6. After making the appropriate edits, select **Finish** to save, exit, and redisplay the Border Rules screen.
   The Signaling Rules screen is redisplayed.

Cloning an existing signaling rule

About this task

Use the following procedure to clone an existing Signaling Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. In the Application Pane, Select the name of the Signaling Rule that you want to clone.
4. Select **Clone** in the upper-right section of the screen.
   The Clone Rule pop-up window is displayed.
5. Enter a name for the new Signaling Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Signaling Rules screen is redisplayed, showing the newly-cloned Signaling Rule.

Renaming an existing signaling rule

About this task

Use the following procedure to rename an existing Signaling Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. In the Application Pane, Select the name of the Signaling Rule that you want to rename.
4. Select **Rename** in the upper-right section of the screen.
   The Rename Rule pop-up window is displayed
5. Enter the new name for the Signaling Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The Signaling Rules screen is redisplayed, showing the newly-renamed Signaling Rule.

Deleting an existing signaling rule

About this task

Use the following procedure to delete an existing Signaling Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Signaling Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing Signaling Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected Signaling Rule set are displayed in the Content Area of the Signaling Rules screen.
3. In the Application Pane, Select the name of the Signaling Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the Signaling Rule or select **Cancel** to cancel the delete operation without saving.

The Signaling Rules screen is redisplayed. If **OK** was selected above, the chosen Signaling Rule will no longer be displayed in the Security Rules screen. If **Cancel** was selected above, the chosen Signaling Rule will still be displayed.

Time—of—Day (ToD) rules

A Time-of-day (ToD) Rule allows you to determine when the domain policy it is assigned to will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

Creating a new ToD 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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Time-of-Day Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing ToD Rule sets are displayed in the ToD Rules section, and the parameters comprising a selected ToD Rule set are displayed in the Content Area of the Time-of-Day Rules screen.
3. Select **Add** from the Applications pane.
   The ToD Rule pop-up window is displayed.
4. Enter a name for the new ToD Rule and select **Next**
   A second ToD Rule pop-up window is displayed.
5. Enter the appropriate ToD parameters while referring to the field descriptions in Time-of-Day Field Descriptions on page 147. Select **Finish** to save and exit.
   Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first ToD Rule window.

The Time-of-Day Rules screen is redisplayed.

Time—of—Day Field Descriptions

When creating a new Time—of—Day Rule, refer to this table for information on the fields in the second ToD Rule pop-up window.

ToD Field Descriptions

Field	Description
Date	
Start Date	The day on which the ToD rule will automatically take effect. Click the Show Calendar icon to select the desired day.
Now	Indicates that the ToD rule is to take effect immediately.
End Date	The day on which the ToD rule will automatically end. Click the Show Calendar icon to select the desired day.
Never End	Indicates that the ToD rule is to remain in effect in perpetuity or until such time as an End Date is distinctly defined.
Time	
Start Time	The specific time on the designated day that the 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	The specific time on the designated day that the rule will cease being applied. Click the Show Calendar icon to select the desired ending time.
Recurrence	
Daily, Weekly, or Monthly	When the ToD rule is to automatically be placed into effect.
Daily	Allows you to determine which “daily’ cycle will be used for automatic activation: Every Day – the ToD rule will automatically take effect at the designated time on each weekday (weekends and holidays included). Every Weekday – the ToD rule will only automatically take effect on Monday through Friday.

	Every Weekend – the ToD rule will only automatically take effect on Saturday and Sunday.
Weekly	Allows you to determine which weekly cycle the ToD rule will be 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 will take effect by checking the appropriate checkbox.
Monthly	Allows you to designate the specific day of a monthly cycle that the ToD policy will take effect.

Cloning an existing ToD rule

About this task

Use the following procedure to clone an existing ToD Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Time-of-Day Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing ToD Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected ToD Rule set are displayed in the Content Area of the ToD Rules screen.
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 Clone Rule pop-up window is displayed.
5. Enter a name for the new ToD Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The ToD Rules screen is redisplayed, showing the newly-cloned ToD Rule.

Editing an existing ToD rule

About this task

Use the following procedure to edit an existing ToD Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Time—of—Day Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing ToD Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected ToD Rule set are displayed in the Content Area of the ToD Rules screen.
3. In the Application Pane, Select 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. Select the **Edit** button in the lower-center section of the screen.
   A Time of Day Rule screen is displayed.
5. Edit the appropriate fields. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original Media Rules window.
6. After making the appropriate edits, select **Finish** to save and exit.
   The ToD Rules screen is redisplayed.

Renaming an existing ToD rule

About this task

Use the following procedure to rename an existing ToD Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Time—of—Day Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing ToD Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected ToD Rule set are displayed in the Content Area of the ToD Rules screen.
3. In 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 Rename Rule pop-up window is displayed
5. Enter the new name for the ToD Rule and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.

The ToD Rules screen is redisplayed, showing the newly-renamed ToD Rule.

Deleting an existing ToD rule

About this task

Use the following procedure to delete an existing ToD Rule.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Time—of—Day Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing ToD Rule sets are displayed in the Application Pane in the Rules section, and the parameters comprising a selected ToD Rule set are displayed in the Content Area of the ToD Rules screen.
3. In the Application Pane, Select the name of the ToD Rule that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the ToD Rule or select **Cancel** to cancel the delete operation without saving.
   The ToD Rules screen is redisplayed. If **OK** was selected above, the chosen ToD Rule will no longer be displayed in the ToD Rules screen. If **Cancel** was selected above, the chosen ToD Rule will still be displayed.

End—Point policy groups

The End-Point Policy Group feature allows you to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD. (Each of which was creating using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

As various types of signaling traffic pass through the enterprise they are exhaustively inspected by the Avaya SBCE security product and ‘compared’ against the criteria defined by which ever Policy Group is active at that time, as determined by its constituent ToD policy. The specific

Policy Set the packets are compared to is determined by the order in which they are placed in the parent Policy Group; which is normally from most restrictive to least restrictive.

The packets are compared to each Policy Set in the Policy Group's prioritized list from top to bottom beginning with the most restrictive down to the least restrictive. As each individual packet's Policy Set match is found, it is further qualified by the Policy Set's Time-of-Day (ToD) rule and by the Policy Set number (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 (allow the packet to proceed to its destination without applying any security features), DENY (immediately block the packet), or APPLY (apply the security features defined by the Policy Set(s)).

Note:

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

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

Creating a new policy group

About this task

Use the following procedure to create a new policy group.

Caution:

A number of default Policy Groups whose name begins with 'default' are provided by Avaya. Editing these rule sets is not recommended, as improper configuration may cause subsequent calls to fail.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.

   Note:

   At least one Security Rule set must be defined before a Policy Group can be created. If a Security Rule does not exist, a pop-up window will be displayed telling you to create one.

3. Select **Add** from the Applications pane.
   The Policy Group pop-up screen is displayed.
4. Enter a name for the new Policy Group and select **Next**
   A second Policy Group pop-up screen is displayed.
5. Enter the requested information using the drop-down menus corresponding to each field in the screen, while referring to the parameter field descriptions in End-Point policy field descriptions on page 152. Select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first End—Point Policy Groups window.

   The End-Point Policy Groups screen is redisplayed.

End-Point Policy Field Descriptions

When creating a new Policy Group, refer to this table for information on the fields in the second Policy Group pop-up screen.

End-Point Policy Field Descriptions

Field	Description
Applicaion Rule	The name of the Application Rule that will determine which applications will have this Policy group applied.
Border Rule	The name of the Border Rule that will determine which applications will have this Policy group applied.
Media Rule	The name of the Media Rule that will be used to match media packets.
Security Rule	The name of the Security Rule that will determine which SBCE security policies will be applied when this Policy Group is activated.
Signaling Rule	The name of the Signaling Rule that will be used to match SIP signaling packets.
Time-of-Day Rule	The ToD Rule set that will be used to determine when this Policy Group will be active.

Viewing an existing policy group summary

About this task

As previously stated, end-point policy groups are comprised of a group of end-point 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 which is displayed in a separate window. Use the following procedure to view a policy group summary.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.

   > **Note:**
   >
   > In the Content Area, clicking anywhere on a specific policy group's information line will display a quick-access pop-up screen with configuration information for that policy group, with information under five tabs: Media NAT; Media Encryption; Media Anomaly, Media Silencing, and Media QoS.
3. Select **Summary** from the Applications pane.
   The End-Point Policy Group summary is displayed.
4. Use the scroll bar to view the entire report. Select **Print** to print the report or select the Windows cancel button to close the window.

Editing an existing End-Point Policy Group

Editing an End-Point Policy Group consists of: 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 an existing Policy Set; or deleting a specific Policy Set. Each of these procedures is described in the following sections.

Adding an end—point policy set

About this task

Use the following procedure to add an existing end-point policy set.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.
3. From the Application Pane, select the Policy Group to which you want to add a Policy Set
4. The Policy Sets currently assigned to the selected Policy Group are displayed in the Content Area.

   Note:

   In the Content Area, clicking anywhere on a specific policy group's information line will display a quick-access pop-up screen with configuration information for that policy group, with information under five tabs: Media NAT; Media Encryption; Media Anomaly, Media Silencing, and Media QoS.
5. Select **Add** from the Applications pane.
   The Add Policy Set pop-up screen is displayed.
6. Enter the requested information using the drop-down menus corresponding to each field in the screen, while referring to the parameter field descriptions in End-Point policy field descriptions on page 152. Select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first End—Point Policy Groups window.

   The End-Point Policy Groups screen is redisplayed.

Reordering end—point 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. As mentioned previously, The Policy Set number (priority position in the Policy Group's Policy Set list) is the deciding factor when ToD rules match on which Policy Set is applied to an incoming message.

Procedure

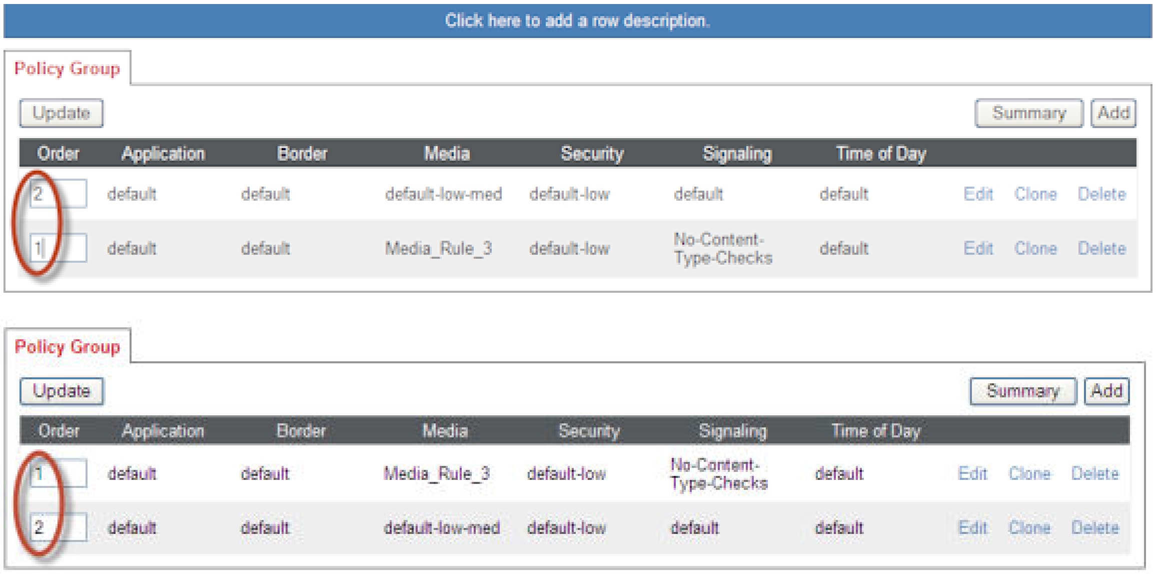
1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.

   Note:

   In the Content Area, clicking anywhere on a specific policy group's information line will display a quick-access pop-up screen with configuration information for that policy group, with information under five tabs: Media NAT; Media Encryption; Media Anomaly, Media Silencing, and Media QoS.
3. From the Application Pane, select the Policy Group whose policy sets you want to reorder.
4. The Policy Sets currently assigned to the selected Policy Group are displayed in the Content Area.
5. Change the number in the Order column to correspond to the order in which you want the Policy Sets to be executed.
6. Select **Update**

The Policy Sets are redisplayed in the Content Area to reflect the new order of precedence.

Example



Order	Application	Border	Media	Security	Signaling	Time of Day			
2	default	default	default-low-med	default-low	default	default	Edit	Clone	Delete
1	default	default	Media_Rule_3	default-low	No-Content-Type-Checks	default	Edit	Clone	Delete

Order	Application	Border	Media	Security	Signaling	Time of Day			
1	default	default	Media_Rule_3	default-low	No-Content-Type-Checks	default	Edit	Clone	Delete
2	default	default	default-low-med	default-low	default	default	Edit	Clone	Delete

Editing an end—point policy set

About this task

Use the following procedure to edit an existing end-point policy set.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.
3. From the Application Pane, select the Policy Group with the policy sets you want to edit.
4. The Policy Sets currently assigned to the selected Policy Group are displayed in the Content Area.
5. Click the **Edit** option corresponding to the policy set you want to edit.
   The Edit Policy Set pop-up screen is displayed.

6. Enter the desired fields and select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first End—Point Policy Groups window.

   The End-Point Policy Groups screen is redisplayed.

Deleting an existing end—point policy set

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.
3. From the Application Pane, select the Policy Group with the policy sets you want to delete.
4. The Policy Sets currently assigned to the selected Policy Group are displayed in the Content Area.
5. Click the **Delete** option corresponding to the policy set(s) you want to delete.
   A delete confirmation pop-up screen is displayed.
6. Select **OK** to delete the selected policy set or select **Cancel** to cancel the delete operation.

   The End-Point Policy Groups screen is redisplayed.

Deleting an existing end—point policy group

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as Admin.

2. Select the **End—Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing End-Point Policy Groups are displayed in the Applications pane. The End-Point Policy sets comprising a selected End-Point Policy Group are displayed in the Content Area of the End-Point Policy Groups screen.
3. From the Application Pane, select the Policy Group that you want to delete.
4.
5. Click the **Delete** option in the upper-right portion of the Content area.
   A delete confirmation pop-up screen is displayed.
6. Select **OK** to delete the selected policy group or select **Cancel** to cancel the delete operation.

   The End-Point Policy Groups screen is redisplayed.

Session policies

Session Policies allow you to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Creating a new session policy

About this task

Use the following procedure to create a new session policy.

⚠ **Caution:**

A default session policy named default is provided by Avaya. Editing this default session policy is not recommended, as improper configuration may cause subsequent calls to fail.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the application pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session policies screen.

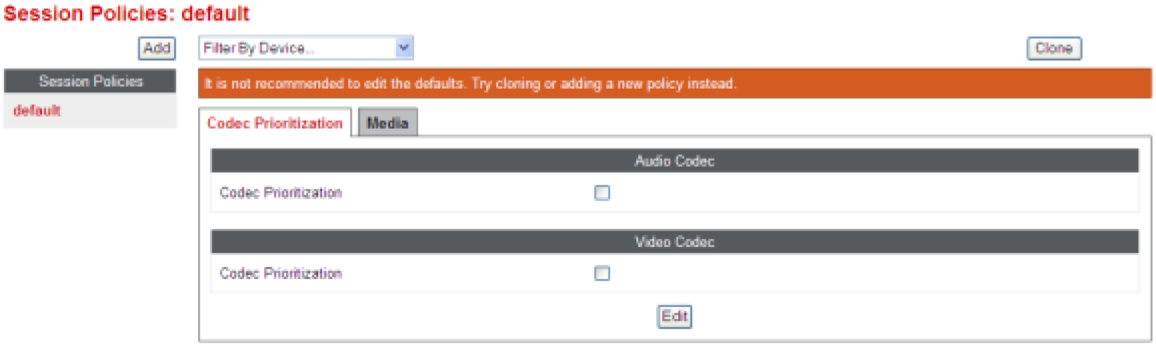
3. Select **Add** from the Applications pane.
   The Session Policy pop-up window is displayed.
4. Enter a name for the new session policy and select **Next**
   A second session policy pop-up window is displayed.
5. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows while referring to Codec prioritization field descriptions on page 161. Select **Next** to save and continue. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the first session policies window.

   A third session policy pop-up window is displayed.
6. Click the checkbox to activate Avaya SBCE Media Anchoring or leave blank to leave media anchoring disabled. Disabling Media Anchoring, as described in Chapter 1, keeps the media traffic within the Remote Branch Network if both calling parties reside inside the network.
7. Click **Next** .
   The Add Session Policy pop-up screen is displayed.
8. Select a Media Forking profile from the drop-down list. If no Media Forking profile has been created, there will be no option other than None.

   Note:

   The Media Forking feature is not available on the Portwell platform.

Example



Session Policies: default

It is not recommended to edit the defaults. Try cloning or adding a new policy instead.

Audio Codec

Codec Prioritization □

Video Codec

Codec Prioritization □

Cloning an existing session policy

About this task

Use the following procedure to clone an existing session policy.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session policies screen.
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 Clone Policy pop-up window is displayed.
5. Enter a name for the new session policy and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The session policies screen is redisplayed, showing the newly-cloned session policy.

Editing an existing session policy

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

Editing codec prioritization parameters

About this task

Use the following procedure to edit codec prioritization parameters..

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session policies screen.

3. In the Application Pane, Select name of the session policy whose codec prioritization parameters you want to edit.
   The codec prioritization parameters for the selected session policy will be displayed in the Content Area.
4. Select the **Codec Prioritization** tab.
   The codec prioritization information screen is displayed.
5. Select the **Edit** button in the lower-center section of the screen.
   The codec prioritization pop-up screen is displayed.
6. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows, while referring to Codec prioritization field descriptions on page 161. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the original session policies window.
7. After making the appropriate edits, select **Finish** to save and exit.
   The session policies screen is redisplayed.

Codec prioritization field descriptions

When creating a new session policy, refer to this table for information on the fields in the second session policy pop-up screen.

Codec prioritization field descriptions

Field	Description
Audio Codec	
Codec Prioritization	A checkbox that forces audio codecs to be matched according to the priority defined by the Preferred Codec Priority 1 through Preferred Codec Priority 5 fields.
Allow Preferred Codecs Only	A checkbox that will only match codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed will not be matched.
Preferred Codec Priority 1 through 5	Optional fields (required to be completed only if Codec Prioritization is checked) that contain the names of audio codecs you want specifically matched in a particular order.
Video Codec	
Codec Prioritization	A checkbox that forces video 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	A checkbox that will only match codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed will not be matched.
Preferred Codec Priority 1 through 5	Optional fields (required to be completed only if Codec Prioritization is checked) that contain the names of video codecs you want specifically matched in a particular order.

Editing media anchoring parameters

About this task

Use the following procedure to edit media anchoring parameters..

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session policies screen.
3. In the Application Pane, Select name of the session policy whose media anchoring parameters you want to edit.
   The session policies parameters for the selected session policy will be displayed in the Content Area.
4. Select the **Media Anchoring** tab.
   The media anchoring information screen is displayed.
5. Select the **Edit** button in the lower-center section of the screen.
   The media anchoring pop-up screen is displayed.
6. Change the state of the Media Anchoring feature by clicking the checkbox to activate the feature or by deselecting the checkbox to deactivate the feature.
7. After making the appropriate edit choice, select **Finish** to save and exit.
   The session policies screen is redisplayed.

Editing media forking parameters

About this task

Use the following procedure to edit media forking parameters..

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session policies screen.
3. In the Application Pane, Select name of the session policy whose media forking parameters you want to edit.
   The session policies parameters for the selected session policy will be displayed in the Content Area.
4. Select the **Media Forking** tab.
   The media anchoring information screen is displayed.
5. Select the **Edit** button in the lower-center section of the screen.
   The media forking pop-up screen is displayed.
6. Select a Media Forking profile from the drop-down list.
7. After selecting a Media Forking profile, click on **Finish** to save and exit.
   The session policies screen is redisplayed.

Renaming an existing session policy

About this task

Use the following procedure to rename an existing session policy.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.

Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session polices screen.

3. In the Application Pane, Select the name of the session policy that you want to rename.
4. Select **Rename** in the upper-right section of the screen.
   The Rename Policy pop-up window is displayed
5. Enter the new name for the session policy and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The session policies screen is redisplayed, showing the newly-renamed session policy.

Deleting an existing session policy

About this task

Use the following procedure to delete an existing session policy.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing session policies are displayed in the Application Pane, and the parameters comprising a selected session policy are displayed in the Content Area of the session polices screen.
3. In the Application Pane, Select the name of the session policy that you want to delete.
4. Select **Delete** in the upper-right section of the screen.
   The delete confirmation pop-up window is displayed
5. Select **OK** to delete the session policy or select **Cancel** to cancel the deletion operation and close the window without saving.
   The session policies screen is redisplayed, showing the newly-renamed session policy.

Managing end-point and session flows

The End-Point Flows and Session Flows features allow you to define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or from without. These features provide you with the complete and unparalleled flexibility to monitor, identify, and control very specific types of calls based upon these user-definable parameters. End-Point Flows, which profile SIP signaling parameters, are combined with Session Flows, which profile SDP media parameters, to completely identify and characterize a call placed through the network. Any number of End-Point and Session Flows may be defined.

There are two methods that can be used to create a new End-Point or Session Flow. The first method uses the Add Flow function of the Flows feature, wherein 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, called Cloning, allows you to copy an existing flow and only change those parameters which would make it distinct. These methods are described in the following sections.

End—Point flows

The following sections contain the procedures necessary to create, clone, view, edit, and delete End-Point Flows.

Creating a new end-point flow

End-Point Flows are of two types: Subscriber and Server. Subscriber End-Point Flows refer to the actual end-point devices (hard phones, soft phone clients, wireless handsets, etc.) from which SIP messages will originate and to which they are destined. Server End-Point Flows refer to the IP call servers which connect to SIP trunk services.

Creating a new subscriber end-point flow

About this task

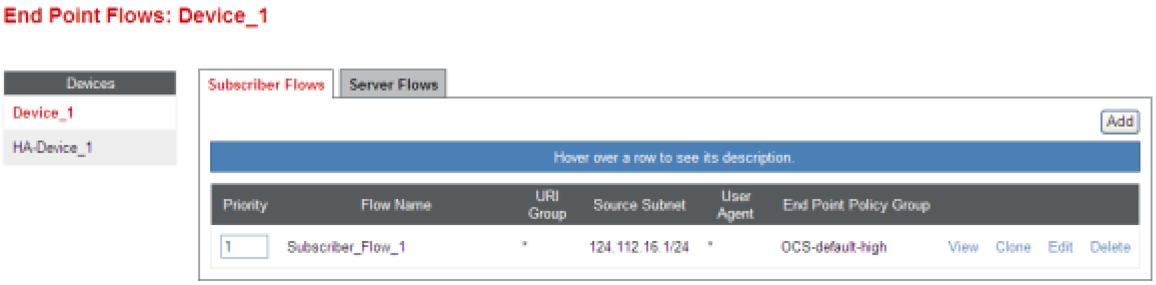
Use the following procedure to manually create a subscriber end-point flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of call flows (Subscriber or Server) for the selected Avaya SBCE security devices are displayed under the corresponding tab displays of the Content Area of the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device for which the new Subscriber End-Point Flow will be created.
   The End-Point Flows screen is displayed showing the flows that are currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Select the **Subscriber Flows** tab.
5. Select **Add** in the upper-right portion of the Content Area.
   The Add Flow pop-up window is displayed.
6. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows while referring to Add subscriber end-flow criteria field descriptions on page 171; and select **Next** to save and continue, or select the window cancel operation to cancel the add flow operation.
   A second Add Flow pop-up window is displayed.
7. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows while referring to Add subscriber end-flow profile field descriptions on page 167. Select **Finish** to save and exit. Selecting the window cancel option cancels the operation and closes the window without saving. Selecting **Back** redisplays the previous Add Flow screen.

   The End—Point Flows screen is redisplayed.

Example



End Point Flows: Device_1

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group				
1	Subscriber_Flow_1	*	124.112.16.1/24	*	OCS-default-high	View	Clone	Edit	Delete

Add Subscriber Flow Profile Field Descriptions

When creating a new end-point flow, refer to this table for information on the fields in the third Add Flow pop-up screen.

Add Subscriber Flow Profile Field Descriptions

Field	Description
Profile	
Source	Radio button allowing you to select the SIP signaling source: Subscriber or Click-to-Call client.
Methods Allowed before REGISTER	Scroll window allowing you to select the SIP signaling messages which are allowed to precede the REGISTER message.
Media Interface	Drop-down menu from which you can select the Media Interface profile to be used for RTP media traffic.
End-Point Policy Group	Drop-down menu from which you select the End-Point Policy Group to be used for this Subscriber End-Point Flow.
SIP Cluster Flow	Checkbox indicating whether or not the calls are routed by the SIP cluster. If this checkbox is selected, then the Routing Profile field is inactivated.
Routing Profile	Drop-down menu from which you select the Routing Profile to be used for this End-Point Flow. This field is only activated if the SIP Cluster Flow checkbox is not selected.
RADIUS Profile	Drop-down menu from which you select the RADIUS Profile to be used for this Subscriber End-Point Flow. **Note:** This field will only be selectable if at least one RADIUS server has been configured and the selected End-Point Policy Group’s Security Rule has Authentication enabled.
Criteria	
Topology Hiding Profile	Drop-down menu from which you select the Topology Hiding Profile to be used for this Subscriber End-Point Flow.
Phone Interworking Profile	Drop-down menu from which you select the name of a pre-configured Phone Interworking Profile.
TLS Client Profile	Drop-down menu from which you select the TLS Client Profile to be used for this Subscriber End-Point Flow.

File Transfer Profile	Drop-down menu from which you select the File Transfer Profile to be used for the selected Subscriber End-Point Flow.
Signaling Manipulation Script	Drop-down menu from which you select the Signaling Manipulation Script to be used for this Subscribe End-Point Flow.

Creating a new server end-point flow

About this task

Use the following procedure to manually create a server end-point flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of call flows (Subscriber or Server) for the selected Avaya SBCE security devices are displayed under the corresponding tab displays of the Content Area of the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device for which the new Server End-Point Flow will be created.
   The End-Point Flows screen is displayed showing the flows that are currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Select the **Server Flows** tab.
5. Select **Add** in the upper-right portion of the Content Area.
   The Add Flow pop-up window is displayed.
6. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows while referring to Add server flow profile field descriptions on page 169; and select **Finish** to save and exit, or select the window cancel operation to cancel the add flow operation.
   The End—Point Flows screen is redisplayed

Add Server Flow Profile Field Descriptions

When creating a new end-point flow, refer to this table for information on the fields in the second Add Flow pop-up screen.

Add Server Flow Profile Field Descriptions

Field	Description
Criteria	
Flow Name	The name assigned to this Subscriber End-Point Flow.
Server Configuration	Drop-down menu from which you 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	Drop-down menu from which you select the Received Interface to be used for this Server End-Point Flow.
Signaling Interface	Drop-down menu from which you select the Signaling Interface to be used for this Server End-Point Flow..
Media Interface	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.
End-Point Policy Group	Drop-down menu from which you select the End-Point Policy Group to be used for this Server End-Point Flow.

Cloning an existing end-point flow

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

Note:

An end-point 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 end—point flow

About this task

Use the following procedure to clone an existing subscriber end—point flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   Existing devices are displayed in the Application Pane, and the parameters comprising a selected device's subscriber end-point flows and server end-point flows are displayed under their respective tabs in the Content Area of the session policies screen.
3. Select the **Subscriber Flows** tab.
   The existing Subscriber end-point flows for the selected device are displayed in the Content Area.
4. Select **Clone** option corresponding to the Subscriber end-point flow that you want to clone.
   The Clone Flow: Criteria pop-up screen is displayed.
5. Enter a name for the new Subscriber flow and edit any other parameters if necessary while referring toAdd flow criteria field descriptions on page 171, and select **Finish** to save your changes or select the window**Cancel** option to cancel the cloning operation and close the window without saving.
   The end flows screen is redisplayed, showing the newly-cloned Subscriber Flow.

Cloning an existing server end—point flow

About this task

Use the following procedure to clone an existing server end—point flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   Existing devices are displayed in the Application Pane, and the parameters comprising a selected device's subscriber end-point flows and server end-point flows are displayed under their respective tabs in the Content Area of the session policies screen.
3. Select the **Server Flows** tab.
   The existing Server end-point flows for the selected device are displayed in the Content Area.
4. Select **Clone** option corresponding to the Server end-point flow that you want to clone.
   The Clone Flow: Criteria pop-up screen is displayed.
5. Enter a name for the new server flow and edit any other parameters if necessary while referring toAdd flow criteria field descriptions on page 171, and select **Finish** to save your changes or select the window **Cancel** option to cancel the cloning operation and close the window without saving.
   The end flows screen is redisplayed, showing the newly-cloned Server Flow.

Add Flow Criteria Field Descriptions

When creating a new end-point flow, refer to this table for information on the fields in the second Add Flow pop-up screen.

Add Flow Criteria Field Descriptions

Field	Description
Criteria	
Flow Name	The name assigned to this Subscriber End-Point Flow.
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 which can legitimately originate a call.
Source Subnet	The subnet address from which calls originate.
Via Host	The domain name or subnet of the SIP proxy servers through which the SIP signaling messages will be routed.

Contact Host	The domain name or subnet of the end-point originating the SIP message.
Signaling Interface	The Signaling Interface profile to be used by the SIP proxy server(s).

Editing existing end—point flows

About this task

Use the following procedure to edit existing subscriber or server end—point flows.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End—Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   Existing devices are displayed in the Application Pane, and the parameters comprising a selected device's subscriber end-point flows and server end-point flows are displayed under their respective tabs in the Content Area of the session policies screen.
3. Select either the **Subscriber Flows** tab or the **Server Flows** tab.
   The existing end-point flows for the selected device are displayed in the Content Area.
4. Select the **Edit** option corresponding to the flow that you want to edit.
   The Edit Flow: Criteria pop-up screen is displayed.
5. Make your changes to the existing fields. If you are editing a Server End-Point Flow profile, prodeed directly to Step 6 below. If you are editing a Subscriber End-Point Flow profile, select **Next** and proceed to the Edit Flow: Profile pop-up screen, where you will make your changes there before proceeding to Step 6 below.
6. Select **Finish** .
   The end flows screen is redisplayed.

Reordering the precedence of end—point flows

About this task

Use the following procedure to reorder the precedence of existing Subscriber and Server End-Point Flows.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **End—Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   Existing devices are displayed in the Application Pane, and the parameters comprising a selected device's subscriber end-point flows and server end-point flows are displayed under their respective tabs in the Content Area of the session policies screen.
3. Select either the**Subscriber Flows** tab orthe**Server Flows** tab.
   The existing end-point flows for the selected device are displayed in the Content Area.
4. Change the numbers in the Order column to the left of each flow information line to reflect the order or precedence that you want the flows to be executed in.
5. Select **Update Order** .
   The End-Point Flows are redisplayed in the Content Area to reflect the new order of precedence.

Deleting an existing end—point flow

About this task

Use the following procedure to delete an existing end—point flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   Existing devices are displayed in the Application Pane, and the parameters comprising a selected device's subscriber end-point flows and server end-point flows are displayed under their respective tabs in the Content Area of the session policies screen.
3. Select either the **Subscriber Flows** tab or the **Server Flows** tab.
4. Select the **Delete** option corresponding to the flow that you want to edit.
   A delete confirmation pop-up window is displayed
5. Select **OK** to continue with the deletion of the flowor select **Cancel** to cancel the delete operation without saving.

The end—point flows screen is redisplayed. If **OK** was selected above, the chosen flow will no longer be displayed in the end—point flows screen. If **Cancel** was selected above, the chosen flow will still be displayed.

Session flows

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

Creating a new session flow

About this task

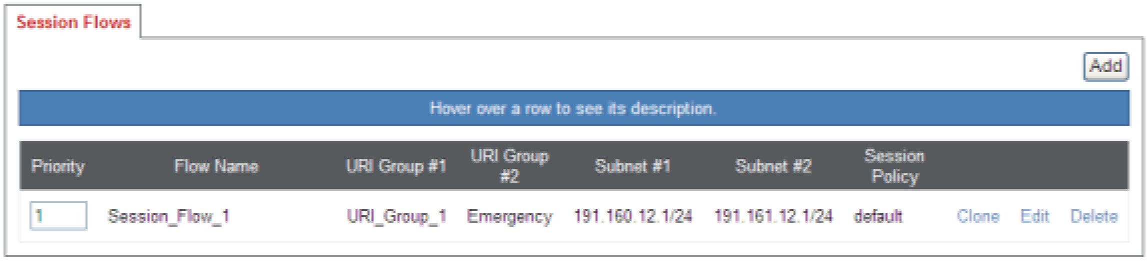
Use the following procedure to manually create a new session flow.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of Session Flows for the selected Avaya SBCE security device are displayed in the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device for which the new Session Flow will be created .
   The Session Flows currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Select **Add**.
   The Add Flow pop-up screen is displayed.
5. Provide the requested information using the field boxes, drop-down menus, and radio buttons while referring to Add session flow field descriptions on page 175 .
   Selecting the window cancel option cancels the operation and closes the window without creating a new end-point flow.
6. Select **Finish**.

The new session flow is added and displayed in the Content Area.

Example



Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy			
1	Session_Flow_1	URI_Group_1	Emergency	191.160.12.1/24	191.161.12.1/24	default	Clone	Edit	Delete

Add Session Flow Field Descriptions

When creating a new session flow, refer to this table for information on the fields in the second Add Flow pop-up screen.

Add Session Flow Field Descriptions

Field	Description
Criteria	
Flow Name	The name assigned to this Session Flow.
URI Group # 1	A drop-down list from which you select a currently defined SIP URI Group policy to identify the source of an originating call.
URI Group # 2	A drop-down list from which you select a currently defined SIP URI Group policy to identify the destination of a call.
Subnet # 1	The subnet address from which calls originate.
Subnet # 2	The subnet address to which calls are destined.
Session Policy	The Session Policy profile to be used for this Session Flow.

Cloning an existing session flow

About this task

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

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. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of Session Flows for the selected Avaya SBCE security device are displayed in the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device for which the new Session Flow will be cloned .
   The Session Flows currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Select the **Clone** option corresponding to the Session Flow that you want to clone.
   The Clone Flow pop-up screen is displayed.
5. Add a new Flow Name to identify this cloned flow and edit any other parameters as desired, using the field boxes, drop-down menus, and radio buttons while referring to Add session flow field descriptions on page 175 . Selecting the window cancel option cancels the operation and closes the window without creating a new end-point flow.
6. Select **Finish**.
   The cloned session flow is added and displayed in the Content Area.

Editing existing session flows

About this task

Use the following procedure to edit existing Session Flows.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered

list of Session Flows for the selected Avaya SBCE security device are displayed in the Avaya SBCE Control Center.

3. From the Application Pane, select the Avaya SBCE Device whose Session Flow you want to edit.
   The Session Flows currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Select the **Edit** option corresponding to the Session Flow that you want to edit.
   The Edit Flow pop-up screen is displayed.
5. Make your changes to the existing parameter fields as desired, using the field boxes, drop-down menus, and radio buttons while referring to Add session flow field descriptions on page 175 . Selecting the window cancel option cancels the operation and closes the window without creating a new end-point flow.
6. Select**Finish**.
   The edited session flow is updated, saved, and displayed in the Content Area.

Reordering the precedence of session flows

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of Session Flows for the selected Avaya SBCE security device are displayed in the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device whose Session Flows you want to reorder.
   The Session Flows currently defined for that Avaya SBCE device are displayed in the Content Area.
4. Change the number in the **Order** column to reflect the order or precedence which you want the flows to be executed.
5. Select **Update Order**.
   The Session Flows are redisplayed in the Content Area to reflect the new order of precedence.

Deleting an existing session flow

About this task

Use the following procedure to delete an existing Session Flow.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered Avaya SBCE security devices for which the new flow will be applied are listed in the Application Pane under the heading Devices. A specifically ordered list of Session Flows for the selected Avaya SBCE security device are displayed in the Avaya SBCE Control Center.
3. From the Application Pane, select the Avaya SBCE Device whose Session Flow you want to delete.
   The delete confirmation pop-up screen is displayed.
4. Click **OK**.
   The session flow is deleted..

Uniform resource identifier (URI) groups

The URI Group feature allows you to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be taken for a given call flow.

Creating a new URI group

About this task

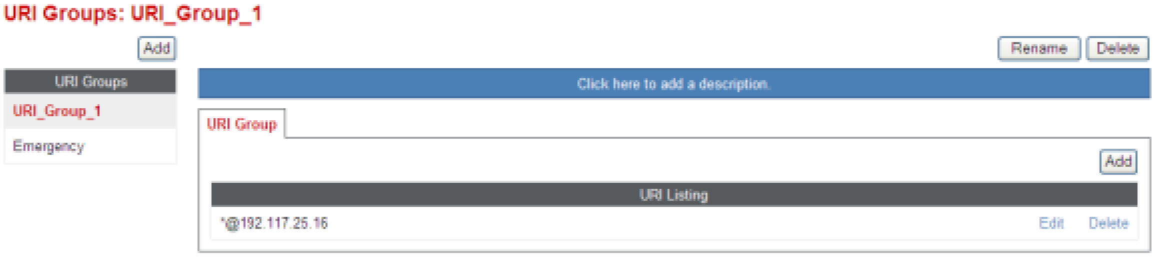
Use the following procedure to manually create a new URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.

2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   The URI Groups window is displayed.
3. In the Application Pane, select**Add**.
   The Add URI Group pop-up screen is displayed.
4. Provide a name for the new URI group, and then select **Next** to continue or select the window cancel option to cancel the operation without saving.
   Selecting Next displays a second Add URI Group pop-up screen.
5. Provide the requested information using the field boxes, drop-down menus, and radio buttons while referring toAdd URI group field descriptions on page 179 .
   Selecting the window cancel option cancels the operation and closes the window without creating a new URI group.
6. Select **Finish**.
   The new URI group is added and displayed in the Content Area.

Example



URI Groups: URI_Group_1

*@192.117.25.16

Add URI Group Field Descriptions

When creating a new URI group, refer to this table for information on the fields in the second Add URI Group pop-up screen.

Add URI Group Field Descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>URI Type</td><td>Radio button allowing you to select the type of URI expression you will enter into the URI(s) field. Available selections are:
<table>
<tr><td>Plain</td><td>Common SIP URI format:
*@192.168.15.12
*@avaya.com</td></tr>
<tr><td>Dial Plan</td><td>Valid SIP Dial Plan in the format:
9555XXXX@*</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td></td><td>9555NXXX@avaya.com
011*@*</td></tr>
<tr><td>Regular Expression</td><td>REGEX in the format:
[0-9]{3,5}\.user@domain\.com,
(simple|advanced)\-user[A-Z]{3}@.*</td></tr>
</table></td></tr>
<tr><td>URIs</td><td>A text box into which you enter the desired URI(s), using the format selected in the URI Type field.</td></tr>
</table>

Emergency Group

The Emergency URI group is an integral part of the system (not user-defined).The Emergency group is created to define special numbers that should not be restricted by any Domain Policies.

Note:

The SIP Options tab of the Advanced Options screen further defines the management of numbers contained in the Emergency URI group. Refer to Managing SIP Options on page 211.

Adding an additional URI to an existing URI group

About this task

Use the following procedure to add an additional URI to an existing URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing URI Groups are displayed in the Application Pane. The various URIs that comprise that URI Group are displayed in the Content Area.
3. In the Application Pane, select the URI group to which you want to add an additional URI.
   A list of SIP URIs currently assigned to the selected URI Group is displayed on the URI Group tab in the Content Area.
4. In the Content Area, select **Add** .
   the Add URI pop-up screen is displayed.

5. Enter the desired URI(s) into the fields.
6. Either select **Finish** to save the new information or select the window cancel option to cancel the operation and close the window without entering the information.
   If Finish is selected, the selected URI group is displayed in the Content Area with the new URI added to the group.

Editing an existing URI group

About this task

Use the following procedure to edit an existing URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing URI Groups are displayed in the Application Pane. The various URIs that comprise that URI Group are displayed in the Content Area.
3. In the Application Pane, select the URI group that you want to edit.
   A list of SIP URIs currently assigned to the selected URI Group is displayed on the URI Group tab in the Content Area.
4. In the Content Area, select **Edit** option that corresponds to the URI that you want to edit.
   the Edit URI pop-up screen is displayed.
5. Edit the URI as desired.
6. Either select **Finish** to save the newly-edited information or select the window cancel option to cancel the operation and close the window without saving the edit changes.
   If Finish is selected, the selected URI group is displayed in the Content Area with the newly—edited URI group.

Deleting a SIP URI from an existing URI group

About this task

Use the following procedure to delete a SIP URI from an existing URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing URI Groups are displayed in the Application Pane. The various URIs that comprise that URI Group are displayed in the Content Area.
3. In the Application Pane, select the URI group from which you want to delete a SIP URI.
   A list of SIP URIs currently assigned to the selected URI Group is displayed on the URI Group tab in the Content Area.
4. In the Content Area, select **Delete** option that corresponds to the URI that you want to delete.
   A delete confirmation screen is displayed.
5. Select **OK** to perform the delete operation or select**Cancel** to abort the delete operation.
   The URI Groups screen is redisplayed. If OK was selected, the SIP URI will be removed from the list of URIs comprising the selected URI Group.

Renaming an existing URI group

About this task

Use the following procedure to rename an existing URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing URI Groups are displayed in the Application Pane. The various URIs that comprise that URI Group are displayed in the Content Area.
3. In the Application Pane, select the URI Group that you want to rename.
4. In the upper-right portion of the Content Area, select **Rename**.
   A Rename Group pop-up screen is displayed.
5. Enter a new name for the existing URI Group in the New Name field.
6. Select **Finish** to save the selected URI Group with the new name or select the window cancel option to terminate the renaming process and close the window without saving.

The URI Groups screen is redisplayed. If you selected Finish, the selected URI Group is shown with the new name, otherwise its original name is shown.

Deleting an existing URI group

About this task

Use the following procedure to delete an existing URI group.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing URI Groups are displayed in the Application Pane. The various URIs that comprise that URI Group are displayed in the Content Area.
3. In the Application Pane, select the URI Group that you want to delete.
4. In the upper-right portion of the Content Area, select **Delete**.
   A delete confirmation pop-up screen is displayed.

   Note:

   If the selected URI Group is associated with a security policy or a call flow,an information pop-up screen will be displayed instead of the delete confirmation. The information screen will display a message similar to the following: “You can’t delete URI_1 because it’s used with a flow. To delete, first remove any associations.” Refer to Managing end-point and session flows on page 165.
5. Select **OK** to delete the selected URI Group or select the window cancel option to terminate the deletion process and close the window without deleting.
   The URI Groups screen is redisplayed. If you selected OK in the deletion confirmation screen, the selected URI Groups screen is shown without the deleted URI Group name in the list.

Chapter 6: System Configuration

Basic system configuration overview

The SBCE Control Center (EMS) allows you to configure and manage the following system-related security features of the Avaya SBCE security products deployed in an enterprise VoIP network:

- Backup / 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 SBCE applications
  - View, edit, and delete SBCE device configurations
- Configure Advanced Options
  - Manage Subsystem Logs
  - CDR Listing
  - Feature Control
  - SIP options
  - Signaling port ranges
- Manage Global Parameters
  - RADIUS Authentication
  - Cluster Proxy
  - SIP Clusters
  - SNMP Settings
  - Routing Profiles
  - Trace Settings
  - Syslog

  - Authorize User Agents
- Manage Device-Specific Settings
  - Signaling Interface
  - Media Interface

This section provides an overview of the overall basic configuration process, including the following:

- SBCE Architecture
- Basic Configuration Quick-Start Steps Checklists
  - Reconfigure SBCE
  - Enabling Interfaces
  - Configuring URI Groups
  - Configuring Routing Profiles
  - Configuring Interworking
  - Adding Servers
  - Adding TLS Certificates
  - Adding TLS Server Profiles
  - Adding Domain Policy Groups
  - Adding Signal Interfaces
  - Adding Media Interfaces
  - Adding Subscriber Flows
  - Adding Server Flows
  - Adding Session Flows

This section only provides brief basic configuration checklists. For detailed procedures regarding each of the topics in this overview section, refer to the appropriate sections in the chapters listed below:

- Chapter 5 — “Domain Policy Administration”
- Chapter 6 — “System Configuration” (this chapter)
- Chapter 7 — “Security Configuration”
- Chapter 8 — “Network Configuration”

Basic configuration quick-start steps

These are the overall configuration steps and where to locate them in the task pane of the GUI.

Step	Task Pane Menu Feature Selection
Reconfigure (if required)	
Enable Interfaces	Device Specific Settings
Configure URI Groups	Global Profiles
Configure Routing Profiles	Global Profiles
Interworking Profiles	Global Profiles
Add Servers (Call/Trunk)	Global Profiles
TLS Certificates	TLS Management
TLS Profiles	TLS Management
Domain Policy Group	Domain Policies
Signaling Interface	Device Specific Settings
Media Interface	Device Specific Settings
Subscriber Flow	Device Specific Settings
Server Flow	Device Specific Settings
Session Flow	Device Specific Settings

Reconfiguring SBCE checklist

About this task

SBCE reconfiguration is only required if you are going to change the management (M1) IP.

Management interfaces (i.e., M1, M2) and media interfaces (i.e., A1, A2, B1, B2) MUST NOT be configured on the same subnet.Standard platform interfaces: M1, M2, A1, A2, B1, and B2

Portwell platform interfaces: M1, A1, A2, and B1

Procedure

1. Uninstall the SBCE device from the GUI.

2. Initiate a secure shell (SSH) connection to the SBCE (ipcs/<*password*>).
3. Run the reconfigure script: /usr/local/ipcs/icu/scripts/ipcs-reconfigure
4. Reprovision the SBCE in the GUI.

Enabling interfaces checklist

About this task

Enable Interfaces by performing the following steps:

Note:

Assume IP addresses for all ports have been assigned during installation or reconfiguration.

Procedure

1. Select: Device Specific Settings > Network Management > Interface Configuration
2. Enable: A1, B1

Configuring URI groups checklist

About this task

Configure URI Groups to define dialed phone numbers for routing purposes.

Procedure

1. Select: Global Profiles > URI Groups
2. Explain existing URI Groups

Example

URI Group Configuration Example

Add Group

Name = URI-*xxxx*

Add URI Group (select Dial Plan)

9*XXXX*@.*

Finish

Configuring routing profiles checklist

About this task

Configure Routing Profiles to define the route for a particular URI.

Procedure

1. Select: Global Profiles > Routing
2. Explain existing Routes

Example

Routing Profile Configuration Example

Add Profile

Name = Route-*xxxx*

URI Group = URI-*xxxx*

Next Hop Server 1 = *xxxx*

Outgoing Transport = UDP

Configuring interworking checklist

About this task

Configure Interworking Profiles to manipulate headers, etc. for compatibility.

Procedure

1. Select: Global Profiles > Server Interworking
2. Explain existing Interworking Profiles
   SIP Trunk Interworking

Example

Interworking Configuration Example

Add Profile

Name = Interwork-*xxxx*

Describe the screens

Click all Next and Finish buttons

Adding servers checklist

About this task

Configure to add Call Servers and Trunk Servers (SIP Trunk).

Procedure

1. Select: Global Profiles > Server Configuration
2. Explain existing configurations

Example

Add Server Configuration Example

Add Profile

Name = Server-*xxxx*

Type = Call Server

Addresses = *xxxx*

Transports = TCP, UDP port 5060

Interworking Profile = Interwork-xxxx

Adding TLS certificates checklist

About this task

TLS Certificates are only needed if line side phones are encrypted.

Procedure

Select: TLS Management > Certificates

Example

TLS Certificate Configuration Example

Generate CSR

Install a Certificate

More steps involved (See details in Network Configuration chapter)

Adding TLS server profiles checklist

About this task

Create a new TLS Server Profile to allow encrypted phones to connect.

Procedure

1. Select: TLS Management > Server Profiles
2. Explain existing profile

Example

TLS Server Profile Configuration Example

Add Profile

Name = TLS-*xxxx*

Finish

Adding domain policy groups checklist

About this task

Policy Groups contain our policy sets and rules.

Procedure

1. Select: Domain Policies > End Point Policy Groups

2. Explain existing Policy Groups and Policy Sets

Example

Policy Group Configuration Example

Add Group

Name = Policy-*xxxx*

Choose default rules

Finish

Adding signal interfaces checklist

About this task

Signal Interfaces define the type of signaling on the ports.

Procedure

1. Select: Device Specific Settings > Signaling Interface
2. Explain existing Signaling Interfaces

Example

Signaling Interface Configuration Example

Refer to further details in the appropriate section later in this chapter.

Adding media interfaces checklist

About this task

Media Interfaces define the type of signaling on the ports.

Procedure

1. Select: Device Specific Settings > Media Interface

2. Explain existing Media Interfaces

Example

Media Interface Configuration Example

Refer to further details in the appropriate section later in this chapter.

Adding subscriber flows checklist

About this task

Subscriber Flows allow us to categorize line-side signaling and apply a policy.

Procedure

1. Select: Device Specific Settings > End Point Flows > Subscriber Flows
2. Explain existing flows

Example

Subscriber Flows Configuration Example

Name = Phone Flow-*xxxx*

Routing Profile = Route-*xxxx*

Finish

Adding server flows checklist

About this task

Server Flows allow us to categorize trunk-side signaling and apply a policy.

Procedure

1. Select: Device Specific Settings > End Point Flows > Server Flows
2. Explain existing flows

Example

Server Flow Configuration Example

Name = Server Flow-*xxxx*

Server = Server-*xxxx*

Finish

Adding session flows checklist

About this task

Session Flows allow us to categorize media traffic and apply a policy.

Procedure

1. Select: Device Specific Settings > Session Flows
2. Explain existing flows

Example

Session Flow Configuration Example

Session Policies (codec negotiation and media anchoring) are available by selecting: Domain Policies > Session Policies

Backup / Restore system information

The Backup/Restore feature provides the ability to backup (make a snapshot) of the EMS security configuration to a user-definable location that is secure and physically-separate from the Avaya SBCE equipment chassis for later retrieval or restoration.

> **Note:**
>
> A configuration backup can be taken manually and restored as needed. Scheduled backup operations are currently not supported.

Designating a Snapshot Server

Before the Backup/Restore feature can be used, a server must first be designated as a snapshot server to hold the backup files, from which they can be retrieved when necessary.

About this task

Use the following procedure to designate a snapshot server.

⚠ **Caution:**

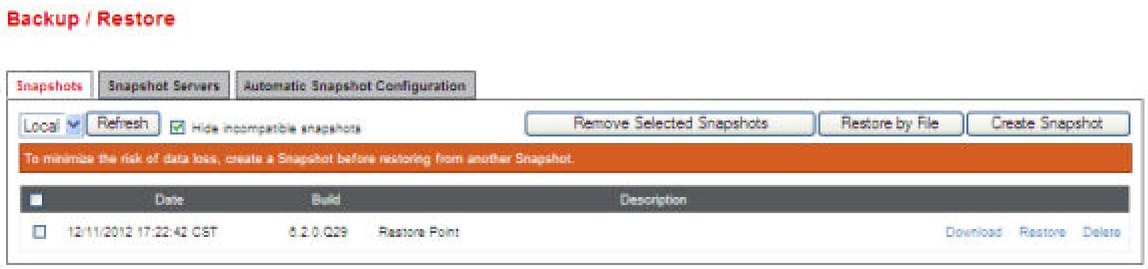
A snapshot can only be restored to the same Avaya SBCE product version on the same EMS box that the snapshot was created on. When restoring the snapshot, the EMS box must be configured with the same original management IP used when the snapshot was created. If the EMS box serial number, Avaya SBCE product version, or management IP does not match, the restore operation will fail and the system settings will revert to the prior state.

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.
3. Select the **Snapshot Servers** tab.
   The **Snapshot Servers** screen will be displayed in the Content Area.
4. Click on **Add**.
   The Add Snapshot Servers pop-up window will be displayed.
5. Add the requested information into the fields provided according to the information contained in Add Snapshot Server Pop-up Window Field Descriptions. on page 196
6. Click **Finish**.

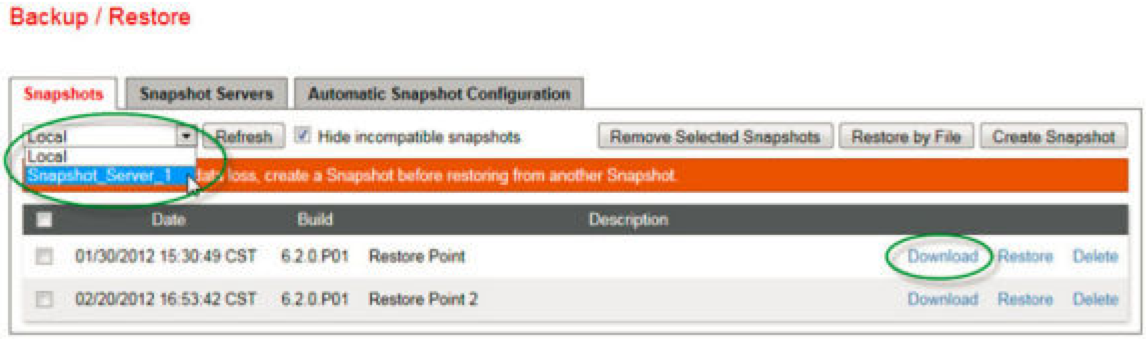
The Snapshot Server will be created and displayed in the Content Area.

Example


Backup / Restore
Snapshots
Snapshot Servers
Automatic Snapshot Configuration
Local
Refresh
Hide incompatible snapshots
Remove Selected Snapshots
Restore by File
Create Snapshot

To minimize the risk of data loss, create a Snapshot before restoring from another Snapshot.

■	Date	Build	Description			
□	12/11/2012 17:22:42 CST	6.2.0.Q29	Restore Point	Download	Restore	Delete



...data loss, create a Snapshot before restoring from another Snapshot.

■	Date	Build	Description			
□	01/30/2012 15:30:49 CST	6.2.0.P01	Restore Point	Download	Restore	Delete
□	02/20/2012 16:53:42 CST	6.2.0.P01	Restore Point 2	Download	Restore	Delete

Next steps

Making a System Snapshot on page 197

Add Snapshot Server pop-up window field descriptions

Name	Description
Profile Name	A descriptive name that will be used to refer to the snapshot server being configured.
Server Address (ip:port)	The physical IP address and port number of the snapshot server to which backup files (snapshots) will be transferred via secure FTP (SFTP).
User Name	The User Name of the administrative account which is authorized to make system backups.
Password	The password assigned to authenticate the administrative accounted identified in the previous field.
Confirm Password	Enter password again for confirmation.

Name	Description
Repository Location	The physical path (directory) on the snapshot server where the backup files will be stored to and retrieved from.

Making a system snapshot

Before you begin

Designating a Snapshot Server on page 194

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select **Backup/Restore** from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Select **Create Snapshot**.
   The Create Snapshot pop-up window will be displayed
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 will be displayed on the Create Snapshot pop-up window informing you that the snapshot has been successfully created. When the process has completed, the newly created snapshot will be displayed in the Content Area of the Snapshots screen.

Restoring a system snapshot

Two methods are provided for restoring a snapshot to the EMS server; one is manual and the other is automatic. The manual method involves two steps but gives you more control over how the snapshot files will restore the EMS while the automated method simply restores the backup files without further intervention on your part.

⚠ **Caution:**

The process of restoring a snapshot (backup) file (both manual and automatic) takes the EMS off-line while the files are being transferred and the device reconfigured.

This means that no SBCE detection or mitigation features will be available for the entire duration of the restore procedure, making your system vulnerable to intrusions and attacks.

It is strongly recommended that restoration procedures only be done during times of relative system inactivity or during normally scheduled periods of maintenance.

Manual Method

The manual method of restoring a snapshot to the EMS is a two-step process whereby the snapshot is first retrieved from the snapshot server to your local workstation and then uploaded to the EMS for re-configuration. Use the following two procedures in succession to restore an EMS to a previous snapshot configuration: Retrieving a Snapshot File on page 198 and Restoring a Snapshot File on page 199.

Automatic Method

The automatic method of restoring a snapshot to the EMS is a single-step process which restores the EMS to the previous configuration (snapshot) without further intervention on your part. See Restoring a Snapshot File Automatically on page 200 for the procedure.

Retrieving a snapshot file

Before you begin

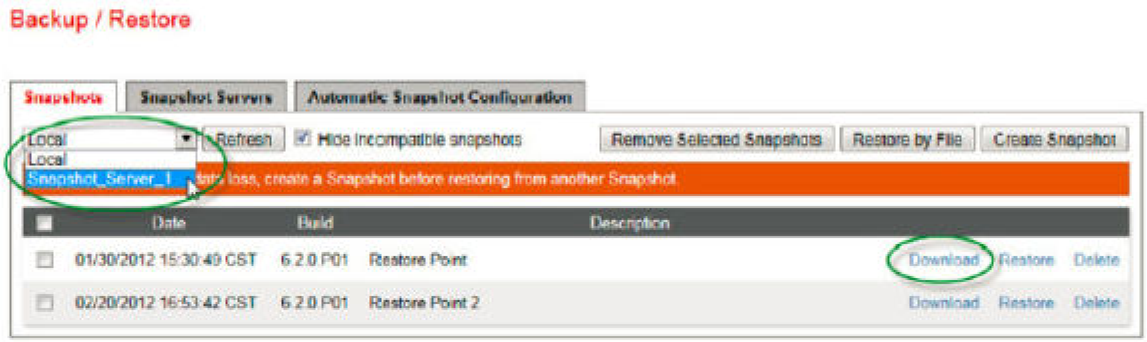
Making a System Snapshot on page 197

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select Backup/Restore from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Select the snapshot server that contains the snapshot file you want to retrieve from the drop-down menu in the Content Area.
   All the snapshot files that are contained on the selected snapshot server will be displayed in the Content Area.
4. Select the snapshot file you want to retrieve by clicking the corresponding **Download** option.
   A dialog pop-up window will be displayed.
5. Select the **Save to Disk** radio button and click OK.
   A dialog pop-up window will be displayed.
6. Designate a destination to save the snapshot file and click **Save**.

The snapshot file will be saved in the designated location.

Example



loss, create a Snapshot before restoring from another Snapshot

□	Date	Build	Description			
□	01/30/2012 15:30:40 CST	6.2.0 P01	Restore Point	Download	Restore	Delete
□	02/20/2012 16:53:42 CST	6.2.0 P01	Restore Point 2	Download	Restore	Delete

Next steps

Restoring a Snapshot File on page 199

Restoring a snapshot file

Before you begin

Retrieving a Snapshot File on page 198

About this task

Once the snapshot file has been retrieved from the snapshot server and saved on your local workstation, it may now be uploaded to the EMS server where it will be uncompressed and used to reconfigure the EMS to a previous state.

Note:

Any device whose management IP does not EXACTLY match the management IP contained in the snapshot will become inaccessible, *including the EMS*.

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

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select Backup/Restore from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Select the corresponding **Restore by File** option.
   The Restore by File pop-up window will be displayed.
4. Click **Browse**.

A dialog pop-up window will be displayed.

5. Select the desired snapshot file and select **Open**.
   The selected snapshot file is entered into the Restore Point File field of the Restore by File pop-up window.
6. Select **Finish**.
   A warning pop-up window will be displayed, asking you to confirm that you want to proceed with the restoration procedure.
7. Click **OK**.
   The EMS will be taken off-line and the snapshot file transferred to the EMS server, where it will be uncompressed and used to reconfigure the EMS software to a previous configuration.

Restoring a snapshot file automatically

Before you begin

Making a System Snapshot on page 197

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select Backup/Restore from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Using the drop-down menu in the Content Area, select the snapshot server that contains the snapshot file you want to retrieve.
   All the snapshot files that are contained on the selected snapshot server will be displayed in the Content Area.
4. Select the snapshot file you want to restore to the EMS by clicking the corresponding **Restore** option.
   A warning pop-up window will be displayed, asking you to confirm that you want to proceed with the automatic restoration procedure.
5. Click **OK**.
   The EMS will be taken off-line and reconfigured with the snapshot file.

Deleting a system snapshot

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select Backup/Restore from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Select the snapshot file you want to delete by clicking the corresponding **Delete** option.
   A pop-up window will be displayed, asking you to confirm your selection.
4. Click **OK**.
   The snapshot file is deleted.

Configuring automatic snapshots

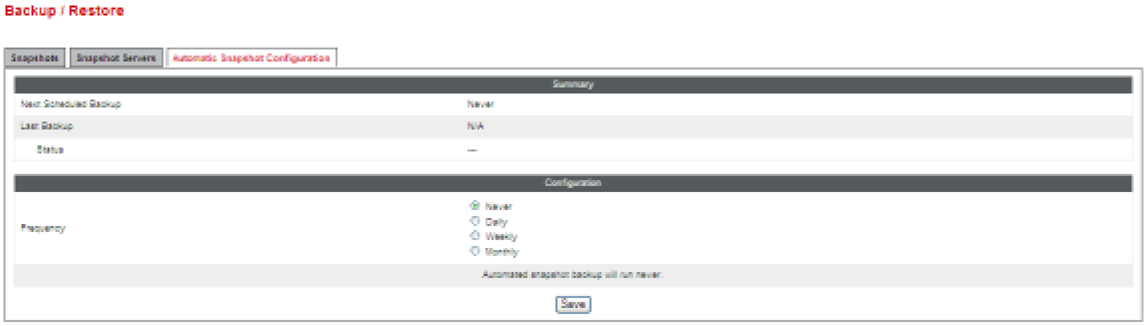
Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select Backup/Restore from the Task Pane.
   The Backup/Restore screen will be displayed in the Content Area, defaulting to the Snapshots tab display.
3. Select the Automatic Snapshot Configuration tab.
   The Automatic Snapshot Configuration screen will be displayed in the Content Area. In the Summary area of the Automatic Snapshot Configuration tab, the configuration for a previously saved backup will be displayed if one existed, otherwise the default setting of Never will be displayed.
4. Indicate the snapshot frequency desired by selecting the appropriate radio button.
   When the Weekly or Monthly Frequency option is selected, a group of Day(s) checkboxes (i.e., Su, Mo, Tu, We, Th, Fr, and Sa) is displayed.

   When the Monthly Frequency option is selected, an additional row of checkboxes is displayed for Occurrence (i.e., 1st, 2nd, 3rd, 4th, and Last).
5. Click on the small calendar icon to the right of the Time.
   An Edit Time dialog box will be displayed.
6. Enter the desired start time in the dialog box.

7. Click Save and then Close on the dialog box.
8. Click Save at the bottom of the screen.

Example



Summary	
Next Scheduled Backup	Never
Last Backup	N/A
Status	—

Configuration	
Frequency	● Never ○ Daily ○ Weekly ○ Monthly

Automated snapshot backup will run never.

Management of deployed Avaya SBCE security devices

In addition to configuring newly installed Avaya SBCE security devices (Chapter 4, Device Configuration), the System Management feature also allows you to perform a number of additional functions which help you to effectively manage your network. The additional functions that can be performed using the System Management feature are:

- Shutdown and reboot individual Avaya SBCE security devices
- Restart SBCE applications
- Swap SBCE devices
- View, edit, and delete SBCE device configurations

Shutting down an Avaya SBCE security device

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select **System Management** from the Task Pane.
   The System Management screen will be displayed in the Content Area, defaulting to the Installed tab display.
3. Click the **Shutdown** option corresponding to the Avaya SBCE security device you want to shutdown.
   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 shutdown.

Rebooting an Avaya SBCE security device

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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

About this task

Use the following procedure to restart a stopped Avaya SBCE application.

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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 Restart Application option corresponding to the Avaya SBCE security device whose application you want to restart.
   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 restarted.

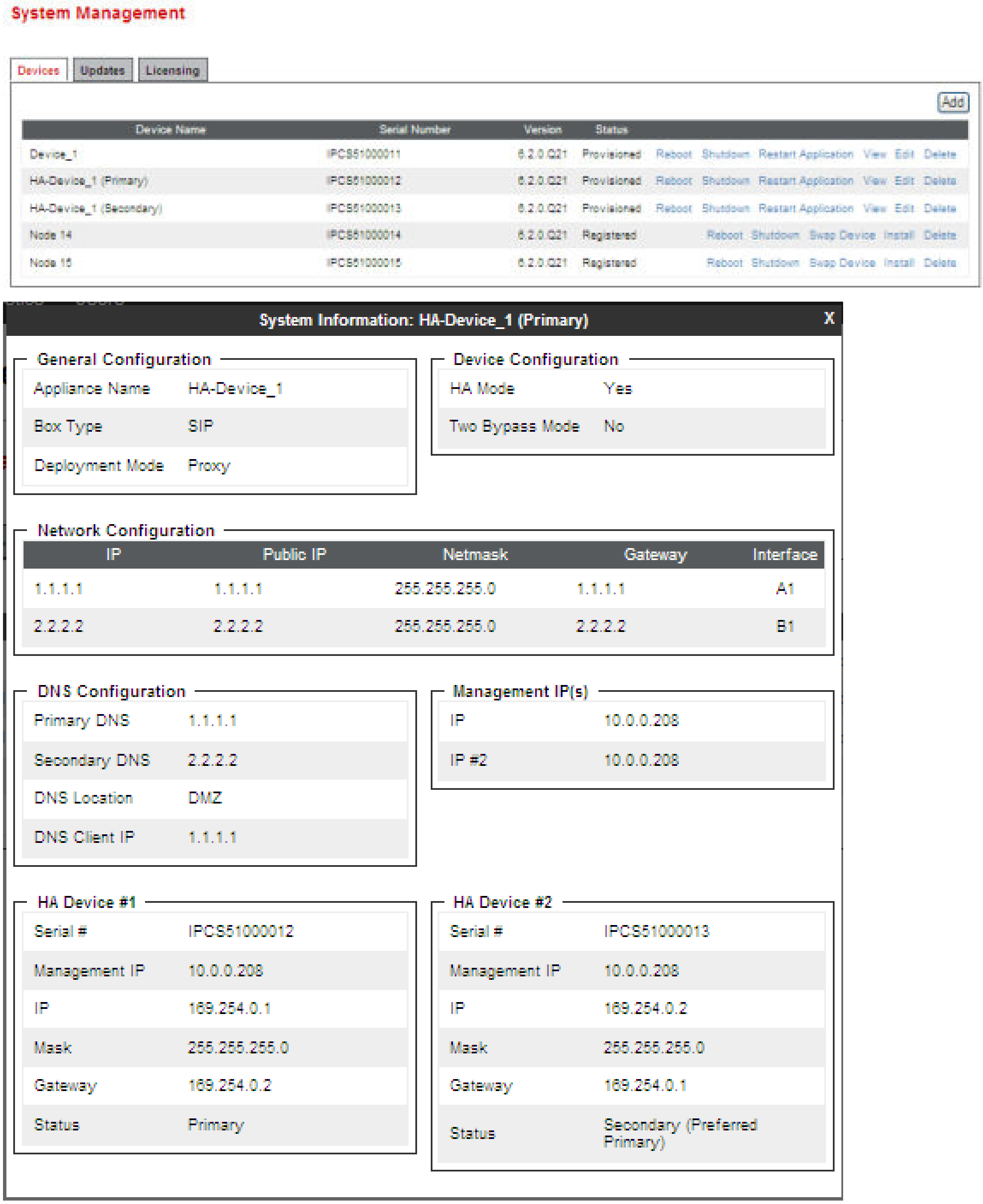
Viewing device configuration

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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 **View** option corresponding to the Avaya SBCE security device whose configuration you want to view.
   A Device Configuration pop-up window will be displayed.
4. Click the Cancel icon when you are finished viewing the configuration information.

The Device Configuration pop-up window will be closed.

Example



System Management

Device Name	Serial Number	Version	Status	
Device_1	IPCS51000011	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
HA-Device_1 (Primary)	IPCS51000012	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
HA-Device_1 (Secondary)	IPCS51000013	6.2.0.Q21	Provisioned	Reboot Shutdown Restart Application View Edit Delete
Node 14	IPCS51000014	6.2.0.Q21	Registered	Reboot Shutdown Swap Device Install Delete
Node 15	IPCS51000015	6.2.0.Q21	Registered	Reboot Shutdown Swap Device Install Delete

System Information: HA-Device_1 (Primary)

General Configuration

Appliance Name	HA-Device_1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	Yes
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
1.1.1.1	1.1.1.1	255.255.255.0	1.1.1.1	A1
2.2.2.2	2.2.2.2	255.255.255.0	2.2.2.2	B1

DNS Configuration

Primary DNS	1.1.1.1
Secondary DNS	2.2.2.2
DNS Location	DMZ
DNS Client IP	1.1.1.1

Management IP(s)

IP	10.0.0.208
IP #2	10.0.0.208

HA Device #1

Serial #	IPCS51000012
Management IP	10.0.0.208
IP	169.254.0.1
Mask	255.255.255.0
Gateway	169.254.0.2
Status	Primary

HA Device #2

Serial #	IPCS51000013
Management IP	10.0.0.208
IP	169.254.0.2
Mask	255.255.255.0
Gateway	169.254.0.1
Status	Secondary (Preferred Primary)

Editing device configuration

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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 Edit option corresponding to the Avaya SBCE security device whose configuration you want to edit.
   The Edit Device Configuration pop-up window will be displayed
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, *Network Configuration*.

Deleting device configuration

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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 **Delete** option corresponding to the Avaya SBCE security device whose configuration you want to delete.
   A confirmation pop-up window will be displayed asking you to confirm your selection.
4. Click **OK**.
   The Avaya SBCE device configuration is deleted and the System Management screen is updated and redisplayed with the deleted device removed from the list.

Upgrading system management

About this task

Note:

This is the generic upgrade procedure. For more detailed procedures see the *Updating Avaya Session Border Controller* book.

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
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 Updates tab to display the System Management Updates screen.
4. Select an upgrade package.
5. Click **Upgrade**.

Advanced option configuration

The **Advanced Options** function of the Troubleshooting feature allows you to: enable or disable Avaya SBCE subsystem execution logs; enable or disable Avaya SBCE security features; configure SIP signaling message options; and designate signaling and media port ranges. In addition, you can view system-generated Call Detail Records (CDRs).

Managing SBCE logging level

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Click on **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options**.
4. Click on **Troubleshooting**.

5. Click on **Debugging**.
   The Debugging screen defaults to the Subsystem Logs tab display. A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
6. From the Application Pane, select the Avaya SBCE device for which you want to manage log files.
7. Check or uncheck the box corresponding to the type of execution log you want to Enable (checked) or Disable (unchecked).
8. Select **Save** when you are finished.
   A message will be displayed at the top of the screen that says:
   `Configuration update successful.`

Viewing a CDR file

Procedure

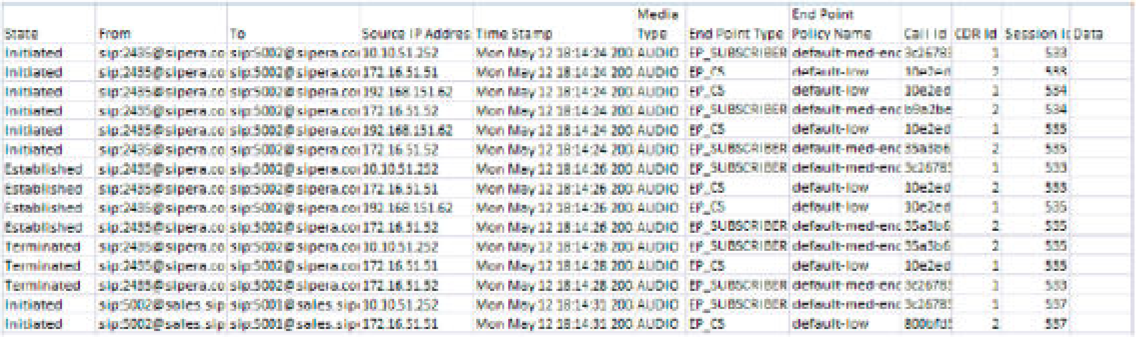
1. Log in to the Avaya SBCE Control Center as the Admin.
2. Click on **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options** in the Task Pane.
   The Advanced Options screen defaults to the CDR Listing tab display. A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
4. From the Application Pane, select the Avaya SBCE device whose CDR files you want to view.
   A list of available CDR files is displayed 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. Refer to the section titled, “Application Rules,” in Chapter 5 of this document.
5. Select the CDR file you want to view.
   A dialog box is displayed.
6. Click the **Open with** radio button and select `EXCEL.EXE` as the program to use in viewing the CDR file.
7. Click **OK**.

The CDR file is opened.

Example



				Media		End Point				
State	From	To	Source IP Addres	Time Stamp	Type	End Point Type	Policy Name	Call Id	CDR Id	Session Ic	Data
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	10.10.51.252	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c26785	1	533	
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.51	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	2	533	
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	192.168.151.62	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	1	534	
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.52	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	b9a2be	2	534	
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	192.168.151.62	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	1	535	
Initiated	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.52	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Established	sip:2435@sipera.co	sip:5002@sipera.coi	10.10.51.252	Mon May 12 18:14:26 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c26785	1	533	
Established	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.51	Mon May 12 18:14:26 200	AUDIO	EP_CS	default-low	10e2ed	2	533	
Established	sip:2435@sipera.co	sip:5002@sipera.coi	192.168.151.62	Mon May 12 18:14:26 200	AUDIO	EP_CS	default-low	10e2ed	1	535	
Established	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.52	Mon May 12 18:14:26 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Terminated	sip:2435@sipera.co	sip:5002@sipera.coi	10.10.51.252	Mon May 12 18:14:28 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Terminated	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.51	Mon May 12 18:14:28 200	AUDIO	EP_CS	default-low	10e2ed	1	533	
Terminated	sip:2435@sipera.co	sip:5002@sipera.coi	172.16.51.52	Mon May 12 18:14:28 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c26785	1	533	
Initiated	sip:5002@sales.sip	sip:5001@sales.sip	10.10.51.252	Mon May 12 18:14:31 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c26785	1	537	
Initiated	sip:5002@sales.sip	sip:5001@sales.sip	172.16.51.51	Mon May 12 18:14:31 200	AUDIO	EP_CS	default-low	800bfd	2	537	

Next steps

See CDR File Content on page 209 for more information on the CDR File.

CDR file content

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

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

Security feature control

The Feature Control tab of the Advanced Options function allows you to enable (or disable) system-wide Avaya SBCE security features. Use the following procedure to manage the activation of these features.

The SBCE-specific security features enable/disable settings described next, are accessible by selecting: Troubleshooting —> Advanced Options.

The security features enable/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 the Chapter 7 section , DoS Security Features on page 246 for more details.

Managing security features

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Click on **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options** in the Task Pane.
   The Advanced Options screen defaults to the CDR Listing tab display. A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
4. From the Application Pane, select the Avaya SBCE device whose security features you want to manage.
5. Select the **Feature Control** tab in the Content Area.
   The Feature Control screen is displayed.
6. In the Enable / Disable column, check or uncheck the box corresponding to the security feature you want to Enable (checked) or Disable (unchecked).
   Enabling a feature directs the Avaya SBCE security device to detect the indicated anomaly (DoS, DDoS, etc.) or perform the corresponding service.
7. Click **Save** when you are finished.

Managing SIP options

About this task

The Feature Control tab of the Advanced Options function allows you to enable and disable DNS caching. Use the following procedure to manage these features.

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Click on **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options** in the Task Pane.
   The Advanced Options screen defaults to the CDR Listing tab display. A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
4. From the Application Pane, select the Avaya SBCE device whose security features you want to manage.
5. Select the **Feature Control** tab in the Content Area, and make the appropriate selections..
6. Select the **SIP Options** tab.
   Make your selections based upon the information contained in Options Tab Display Field Descriptions on page 211
7. Click **Save** when you are finished.
   Your selections will be saved.

SIP options tab display field descriptions

Field	Description
DNS Caching	Checkbox enabling or disabling DNS Caching.
E911 URI Group	Selecting Emergency enables the numbers contained in the Emergency URI group to be free from any dial-out restrictions which 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

Field	Description
	numbers that should not be restricted by any Domain Policies. SBCE administrators should input all applicable emergency numbers for their country for special handling.
Maximum Concurrent Sessions	The number of allowed concurrent dial-out sessions. Entering a value of zero (0) allows unlimited sessions.

Managing port options

About this task

The Port Ranges tab of the Advanced Options function allows you to 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 Control Center as the Admin.
2. Click on **Device Specific Settings** in the Task Pane to expand the menu.
3. Select **Advanced Options** in the Task Pane.
   A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
4. From 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 Port Ranges screen is displayed.
6. Enter the beginning and ending port numbers for each of the fields listed. Port Ranges tab display field descriptions on page 212
7. Click **Save**.

Port Ranges tab display field descriptions

Note:

For SIP deployments, Internal (toward Call Server) signaling interfaces and media interfaces and External (toward Trunk Server) signaling interfaces and media interfaces are created and defined using the Signaling Interface and Media Interface functions of the Device Specific Settings feature from the Task Pane.

Note:

The fixed Ports for TCP, UDP, or TLs defined under Device Specific Settings > Signaling Interface should 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.

Field	Description
Signaling Port Range	(Direction = Away from SBCE) This port range is used by SBCE to initiate connections for outgoing SIP requests from SBCE towards a SIP Server (Call Server or Trunk Server).
Config Proxy Internal Signaling Port Range	(Direction = Away from SBCE) This port range is used by SBCE to initiate connections from SBCE toward Configuration Servers (i.e., Configuration Servers of the following types: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP).
Listen Port Range	(Direction = Toward SBCE) This port range is used in PORTID Mode (see Table 8-4 in the Chapter 8 section, "*Managing SIP Server Configurations*" SBCE listens on these ports for requests from a SIP Server (usually a Call Server) during non-persistent phone-related communications (e.g., calls, signaling) where a link does not stay up indefinitely.
HTTP Port Range	(Direction = Away from SBCE) This port range is used by Tinyproxy to initiate connections for SBCE towards the upstream server or any other http server based on the routing for non-persistent non-phone-related communications (e.g., web services, media) where a link does not stay up indefinitely.
OCS FTP Listen Port Range **OCS Alternate FTP Listen Port Range — For OCS use only**	(Direction = Toward SBCE) This port range is used for OCS FTP (See Chapter 12, "*Office Communications Server Support*." OCS clients operate with two fixed port ranges (one range with starting port 6891 and an alternate range with starting port 11175), therefore SBCE provides two separate range parameter fields (OCS FTP Listen Port Range and OCS Alternate FTP Listen Port Range) to accommodate an OCS deployment.

Enabling High Availability

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Click on **System Management** in the Task Pane.
   A list of installed Avaya SBCE security devices is displayed 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 Edit Device Configuration pop-up window will be displayed.
4. Select the High Availability (HA) checkbox.
5. Select a Device Pair from the pull-down list.
6. Click on the **Finish** button to save and exit.

Configuring HA Heartbeat Interval and Max Retries

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select **Device Specific Settings** from the Task Pane.
3. Click on **Advanced Options**.
   A list of installed Avaya SBCE security devices is displayed in the Application Pane under the heading Devices.
4. From the Application Pane, select the Avaya SBCE security device whose security features you want to manage.
   The HA Pairs tab becomes visible.
5. Select the **HA Pairs** tab in the Content Area.
6. Click **Edit**.
   The Edit HA Pairs Options window is displayed.
7. Enter the appropriate values for Interval (ms) and Max Retries.
8. Click on **Finish** to save and exit.

Global Parameters overview

The Global Parameters feature allows you to provision Simple Network Management Protocol (SNMP) parameters to enhance alarm reporting. By supporting each of the three current versions of SNMP (v1, v2, and v3), this feature allows you to take advantage of the most up-to-date security and remote configuration capabilities available to efficiently manage network events (alarms).

In addition to managing SNMP parameters, the Global Parameters feature also allows you to manage Syslog and RADIUS parameters, as well as provisioning authorized user agents (end-points).

Adding a new RADIUS server

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.
   The Radius screen is displayed.
3. Select **Add**.
   The Add Server screen is displayed.
4. Enter the requested information into the appropriate fields using the Add RADIUS Server Pop-up Window Field Descriptions on page 215 table.
5. Click **Finish**.
   The new RADIUS server is displayed in the Content Area.

Add RADIUS Server Pop-up Window Field Descriptions

Field	Description
Server Name	A descriptive name used to identify this RADIUS server.
Primary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.

Field	Description
Secondary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Retry Timeout (seconds)	The maximum amount of time (in milliseconds) allowed for a successful authentication to be completed. If no successful authentication is completed within this amount of 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 or not the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Checking this box will cause the SBC to maintain the current session upon receipt of the SESSION EXPIRE message. Leaving the box blank will cause the SBC to terminate the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method the Avaya SBCE security device will use to select which RADIUS server it will choose to 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 against which communications between the two will be encrypted.
Accounting Server	Checkbox indicating whether or not this RADIUS server is also to be designated as an Accounting Server, able to receive CDRs. Checking this box indicates this RADIUS server is also an Accounting Server and can receive CDRs. Leaving the box blank indicates this RADIUS server is *not* also an Accounting Server and will *not* receive CDRs.

Editing an Existing RADIUS Server Profile

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.
   The Radius screen is displayed.
3. Select the **Edit** button corresponding to the server profile you want to edit.
   The Edit Server pop-up window is displayed.
4. Make your changes to the existing fields using the Add RADIUS Server Pop-up Window Field Descriptions on page 215 table.
5. Click **Finish**.
   The RADIUS server configuration is updated and saved.

Deleting an Existing RADIUS Server Profile

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.
   The Radius screen is displayed.
3. Select the **Delete** button corresponding to the server profile you want to delete.
   A confirmation pop-up window will be displayed.
4. Click **OK** to confirm.
   The selected RADIUS server configuration is deleted and the RADIUS tab display is updated.

Adding a New SIP Cluster Configuration

Before you begin

The following entries need to be configured prior to creating a new SIP Cluster:

- Server Configuration —
- Signaling Interface (at least two should be created) — Adding a New Signaling Interface on page 240
- Media Interface — Adding a New Media Interface on page 242

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **Cluster Proxy** function of the **SIP Cluster** feature from the Task Pane.
   The SIP Cluster screen is displayed.
3. Click **Add** in the Application Pane.
   The Add SIP Cluster pop-up screen is displayed.
4. Enter a name for the new SIP Cluster and then click **Next**.
   A second Add SIP Cluster pop-up screen is displayed.
5. Enter the requested information into the appropriate fields using the Subsequent Add SIP Cluster Pop-up Window Field Descriptions on page 219 table.
6. Select **Next**.
   The Add Primary Device pop-up window is displayed.
7. Enter the requested information into the appropriate fields using the Add Primary Device Pop-up Window Field Descriptions on page 219 table.
8. Select **Next**.
   The Add Configuration Server pop-up window is displayed.
9. Enter the requested information into the appropriate fields using the Add Configuration Server Pop-up Window Field Descriptions on page 220 table.
10. Select **Next**
    The Add Signaling Server pop-up window is displayed
11. Enter the requested information into the appropriate fields using the Add Signaling Server Pop-up Window Field Descriptions on page 220 table.
12. Select **Finish**.
    The new SIP Cluster configuration is displayed in the Content Area.

Subsequent Add SIP Cluster Pop-up Window Field Descriptions

Field	Description
Secure Mode	Checkbox indicating whether or not communications between Avaya SBCE and endpoints are secure or not
SDP Capability Negotiation for SRTP	Check box to make SBC end-point communications compliant with RFC-5939. This option is only shown if Secure Mode is enabled.
Domain Name	The domain name assigned to this SIP cluster.
Configuration Update Interval (minutes)	The frequency with which the configuration file is updated from the file server. (Enter a value between 15 and 1440)

Add Primary Device Pop-up Window Field Descriptions

Field	Description
SBC Device Name	The name of the primary SIP call server.
SBC Device IP	The IP address of the primary SIP call server.
Configuration Server Client Address	The IP address of the configuration server.

Add Configuration Server Pop-up Window Field Descriptions

Field	Description
Server Type	The type of configuration server. Selections are: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP.
Relay	Checkbox indicating whether or not the Avaya SBCE security device will function as a relay for packets traversing the network. A checked box indicates the SBC will relay packets while an unchecked box indicates packets will not be relayed, but processed.
IPCS Port	The port number of the Avaya SBCE security device.
Real Server IP	The IP address of the actual configuration server in the cluster to which packets are routed.
Real Server Port	The port on the actual configuration server in the cluster to which packets are sent.

Add Signaling Server Pop-up Window Field Descriptions

Field	Description
Server Configuration Profile	A drop-down list from which you select the Server Configuration Profile to be used by this SIP cluster.
End-Point Signaling Interface	A drop-down list from which you select the End-Point Signaling interface to be used by this SIP cluster.
Session Policy Group	A drop-down list from which you select the Session Policy Group to be used by this SIP cluster.

Editing an Existing SIP Cluster Configuration (Advanced Services only)

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **Cluster Proxy** function of the **SIP Cluster** feature from the Task Pane.
   The SIP Cluster screen is displayed.
3. From the Application Pane, select the SIP Cluster you want to edit.
   The Content Area will default to the General tab display.
4. Select **Edit**.
   The Edit SIP Cluster pop-up window is displayed
5. Edit the fields as desired.
6. Click **Finish**.
   The changes are made and the SIP Cluster window is redisplayed.

Deleting an Existing SIP Cluster Configuration (Advanced Services only)

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **Cluster Proxy** function of the **SIP Cluster** feature from the Task Pane.
   The SIP Cluster screen is displayed.
3. From the Application Pane, select the SIP Cluster you want to delete.
   The Content Area will default to the General tab display
4. Select **Delete**.
   A confirmation screen will be displayed.
5. Click **OK** to confirm.

Signaling Forking Overview (Standard Platform Only)

The Signaling Forking feature allows the Avaya SBCE device to bifurcate signaling packets according to a designated Signaling Forking Profile (see description in this section). This solution addresses problems faced by call recorders deployed for quality assurance and compliance. The Signaling Forking feature enables, for security and compliance purposes, the monitoring and recording of calling behavior, call attempts, and other related user actions involving signaling.

Note:

The Signaling Forking and Media Forking features described in this section are not supported in the Avaya SBCE Portwell platform.

The Signaling Forking Profile sets up conditions for sending a duplicate stream of signaling packets to a call recorder.

Without the Avaya SBCE device, ports of all phones would need to be spanned to the signaling recorder. Spanning all ports becomes a tedious task. With the Avaya SBCE device in the picture, the spanning of all ports is not required.

Note:

Signaling Forking and Media Forking are two separate functions that must be configured separately. Configuring your site for Signaling Forking does not automatically configure it for Media Forking, and configuring your site for Media Forking does not automatically configure it for Signal Forking.

Adding a Signaling Forking Profile (Standard Platform only)

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **Device Specific Settings** > **Network Management** and then select the Interface Configuration tab to display the Interface Configuration screen.
3. In the Interface Configuration screen click on the Toggle State button to toggle the state to Enable the Interface that needs to fork signaling traffic.
4. Click the Add button in the upper-right portion of the Signaling Forking screen, to display the Add Forking Profile screen for configuring the appropriate settings.

5. Make all of the appropriate selections and entries using the Add Forking Profile Screen Field Descriptions on page 223 table.
6. Click **Finish**.
   A Signaling Forking Profile Information screen is displayed.

Add Forking Profile Screen Field Descriptions

Field	Description
Name	Signaling Forking Profile Name
Local IP	Select which signaling Interface IP signaling traffic needs to be mirrored
Local Port	Configure the signaling traffic local port information on which SBC handles signaling traffic
Remote IP	Configure the remote client/server IP from/to which signaling traffic needs to mirrored
Remote Port	Configure the signaling traffic Remote port information from/to which SBC handles signaling traffic
Transport	Configure the signaling traffic transport.
Interface	Select the Local Interface which is used for Spanning the Signaling Traffic
Gateway MAC Addresses	Enter the correct Destination MAC

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 (see description in this section). This solution addresses problems faced by call recorders deployed for quality assurance and compliance.

Note:

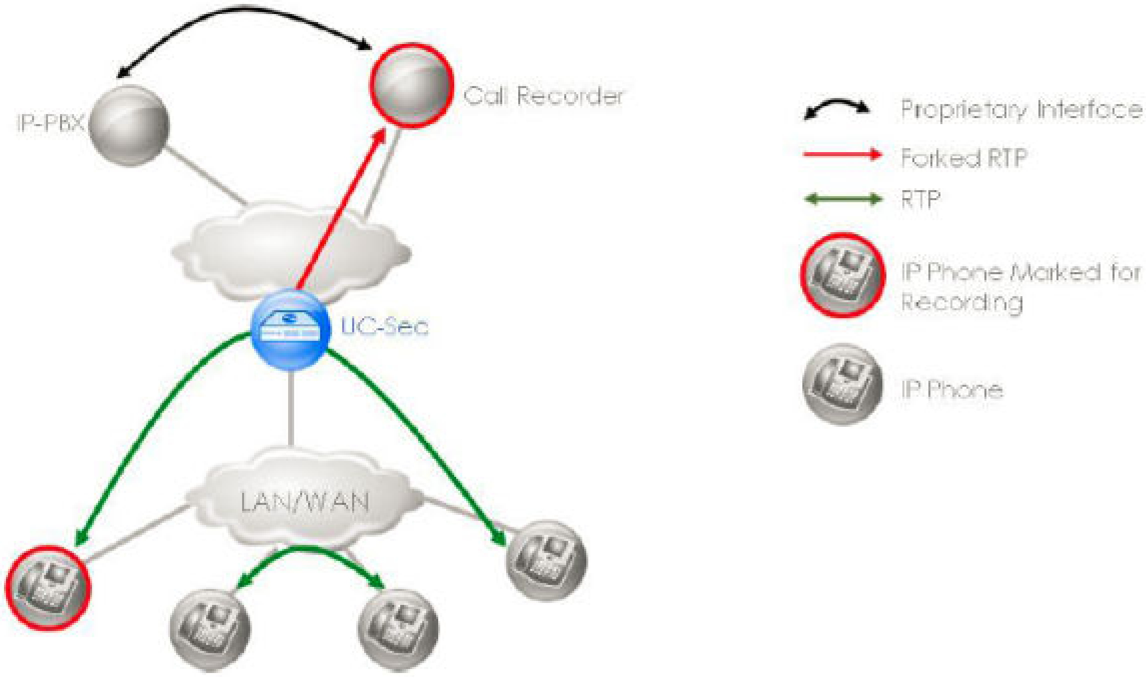
Media Forking and Signaling Forking are two separate functions that must be configured separately. Configuring your site for Media Forking does not automatically configure it for Signaling Forking, and configuring your site for Signaling Forking does not automatically configure it for Media Forking.

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 (e.g., JTAPI).

Note:

Without the SBC device, ports of all phones would need to be spanned, so that media could be established between phones. Spanning all ports becomes a tedious task. With the SBC device in the picture, the spanning of all ports is not required, as the SBC anchors the media and forks the media packets to the call recorder.

A high-level topology illustration of Media Forking is provided below.



Adding a Media Forking Profile (Standard Platform only)

Procedure

1. Log in to the Avaya SBCE Control Center as the Admin.
2. Select the **Media Forking** function of the Global Profiles feature from the task pane.
3. Enter a `profile name`, and click **Next**.
   The Add Media Forking Profile Edit screen will be displayed.

4. Make all of the appropriate selections and entries using the Add Media Forking Profile Edit Screen Field Descriptions on page 225 table.
5. Click **Finish**.
   A Media Forking Profile Information screen is displayed.

Add Media Forking Profile Edit Screen Field Descriptions

Note:

For configuring IP-PBX and the recording device, please refer to their individual manuals, as this information is not covered in this document.

Field	Description
Call Scenario	Designate the type of call to be forked: • Hairpin Calls • Non-Hairpin Calls
Media Type	Select which part of the call to mirror: • Audio Stream • Video Stream • Other Streams
Control Information	Designate whether or not to mirror the RTCP stream.
Enable VLAN Tagging?	If yes, select the checkbox, enter a VLAN ID (1-4095), and choose a protocol.
MAC Addresses	Enter the correct Destination MAC address and correct Source MAC address.

Adding Media Forking Profile to Session Policy (Standard Platform only)

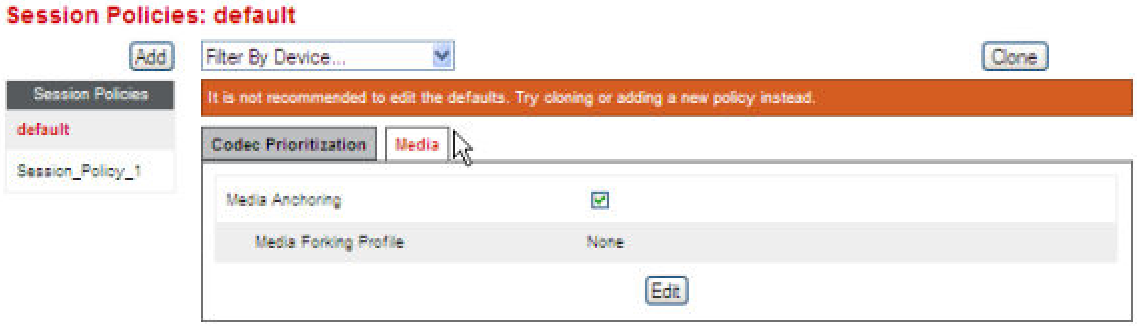
Procedure

1. In SIP deployments, in addition to adding a Media Forking Profile from the Global Profiles > Media Forking menu selection (described previously), you can also add

a Media Forking Profile via the Domain Policies > Session Policies > Media Forking tab menu selection.

2. After selecting Domain Policies > Session Policies to display Session Policies Information screen, select the name of Session Policy that you want to add a Media Forking Profile to from the Session Policies.
3. Once you have selected the appropriate Session Policy select the Media tab and click on the Edit button to display the Media Forking Edit Pop-up screen.
4. In the Media Forking Profile drop-down menu, select the Media Forking profile that you want to add to the selected Session Policy.
5. Follow the instructions in Chapter 5, “Domain Policy Administration,” and add the Session policy to the Session Flow. Make sure that the session flow matches with the required call recorders.

Example



It is not recommended to edit the defaults. Try cloning or adding a new policy instead.

Media Anchoring ☑

Media Forking Profile None

SNMP Settings

About this task

Provisioning SNMP parameters (v1/v2 and v3) is essentially comprised of granting certain users access to the SNMP information. Use the following procedure to create the access accounts.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **SNMP** function from the Device Specific Settings feature from the Task Pane.
   The SNMP screen is displayed, which defaults to showing the contents of the SNMP v1/v2 tab. The Content Area contains two user-selectable tabs (SNMP v1/v2 and SNMP v3) which provide access to global SNMP parameters.

3. Proceed to next sections for information on configuring user access.

Adding a New SNMP v1/v2 Community

About this task

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

Procedure

1. In the Application Pane in the Devices list, select the device for adding a new SNMP community (e.g., EMS).
2. In the Content Area, select the SNMP v1/v2 tab.
3. Select **Add**.
   The Add SNMP Community pop-up window is displayed
4. In the Community Name field, enter the name of the community that will have access to the SNMP v1/v2 information. This will be the SNMP user password for that account.
5. Select **Save**.
   The new community will be displayed on the SNMP v1/v2 tab.

Editing an Existing SNMP v1/v2 Community

About this task

Use the following procedure to edit an existing SNMP v1/v2 community.

Procedure

1. In the Content Area, select the SNMP v1/v2 tab.
2. Select the **Edit** option corresponding to the community you want to edit.
   The Edit SNMP Community pop-up window is displayed.
3. Edit the Community Name and Traps fields as desired (note changes above) and select Save.
   The new field values are saved and the SNMP v1/v2 tab display is updated.

Deleting an Existing SNMP v1/v2 Community

Procedure

1. In the Content Area, select the SNMP v3 tab.
2. Select the **Delete** option corresponding to the SNMP v3 account you want to delete.
   A confirmation pop-up window is displayed asking you to confirm your selection
3. Select **Yes** to delete the SNMP user.
   The selected SNMP v3 user is deleted and the SNMP v3 tab display is updated.

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 Add User pop-up window is displayed.
3. Enter the requested information into the appropriate fields using the SNMP v3 Configuration: Add User Pop-up Window Field Descriptions on page 229 table.
4. Select **Finish**.
   The SNMP v3 screen is updated to display the new SNMP v3 account.

SNMP v3 Configuration: Add User Pop-up Window Field Descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>User Name</b></td><td>The assigned name/designation of the user being granted access to SNMP v3 data.</td></tr>
<tr><td><b>Authentication Scheme</b></td><td>The scheme to be used to authenticate the user prior to granting access to SNMP data.
<table>
<tr><td>noAuthNoPriv</td><td>The user will not be authenticated and SNMP data will not be encrypted.</td></tr>
<tr><td>authNoPriv</td><td>The user will be authenticated, but SNMP data will not be encrypted.</td></tr>
</table></td></tr>
<tr><td><b>AuthPassPhrase</b></td><td>The user password for authentication.</td></tr>
<tr><td><b>Repeat AuthPassPhrase</b></td><td>The AuthPassPhrase entered again for verification.</td></tr>
<tr><td><b>Authentication Protocol</b></td><td>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 authentication protocol currently supported are:
<table>
<tr><td>MD5</td><td>Message Digest Algorithm.</td></tr>
<tr><td>SHA</td><td>Secure Hash Algorithm.</td></tr>
</table></td></tr>
<tr><td><b>Enable Traps?</b></td><td>Enable the use of unsolicited SNMP messages to signal significant system events (alarms).</td></tr>
<tr><td><b>Traps IP Config (ip:port)</b></td><td>The IP address and port on which SNMP traps will be received.</td></tr>
</table>

Editing an Existing SNMP v3 Account

About this task

Use the following procedure to edit 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 you want to edit.
   The Edit User pop-up window is displayed.
3. Edit the desired fields using the SNMP v3 Configuration: Add User Pop-up Window Field Descriptions on page 229 table.
4. Select **Finish**.

Deleting an Existing SNMP v3 Account

About this task

Use the following procedure to delete 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 you want to delete.
   A confirmation pop-up window is displayed asking you to confirm your selection.
3. Select **Yes** to delete the SNMP user.
   The selected SNMP v3 user is deleted and the SNMP v3 tab display is updated.

Adding a Management Server

Procedure

1. In the Content Area, select the Management Servers tab.

2. Click **Add**.
   The Add IP Address pop-up window is displayed
3. In the IP Address(es) field, type one or more server IP addresses separated by commas or new lines.
4. Click **Finish** to display the Management Servers tab with the new server(s) listed.

Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be 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:**

A default Routing profile named default is provided by Avaya. Editing this profile is not recommended as improper configuration may cause subsequent calls to fail.

Creating a new routing profile

About this task

Use the following procedure to create a new Routing profile.

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.
2. Select the **Routing** function from the Global Profiles feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected routing profile are displayed in the Content Area of the Avaya SBCE Control Center.
3. Click **Add** from the Applications Pane.
   The Add Routing Profile pop-up window is displayed.
4. Enter a `distinctive name` for the new Routing Profile and press Next.
   The Add Routing Profile: Next Hop Routing pop-up window is displayed.
5. Enter the requested information into the appropriate fields. Table Add Routing Profile: Next Hop Routing Pop-up Window Field Descriptions on page 232 describes each user-definable field displayed in the window.

6. Click **Finish**.
   The new Routing profile appears in the Application Pane.

Add Routing Profile: Next Hop Routing Pop-up Window Field Descriptions

Field	Description
URI Group	A drop-down menu from which you select the URI Group to which this Next Hop Routing profile will be applied.
Next Hop Server 1	The IP address or domain of the primary Next Hop server.
Next Hop Server 2	The IP address or domain of the secondary Next Hop server.
NAPTR	A checkbox that activates or deactivates the Naming Authority Pointer.
SRV	A checkbox that activates or deactivates the Service Record.
Routing Priority based on Next Hop Server	A checkbox which indicates that routing priority will be determined by the next hop server or deactivates the Service Record.
Outgoing Transport	The protocol(s) used for transporting outgoing signaling packets. Available selections are: TLS, TCP, and UDP.

Note:

The above options are given for finding the destination address. The user can choose any one of three methods for finding the destination address: (1) SRV; (2) NAPTR; and (3) Routing priority based on next hop server.

Cloning an existing routing profile

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Routing** function from the Global Profiles feature from the Task Pane. Existing Routing Profiles are displayed in the Application Pane.
3. In the Application Pane, select the routing profile that you want to clone.
4. In the Content Area, click **Clone**. The Clone Profile pop-up window will be displayed.
5. Provide a name for the cloned Routing profile.
6. Click **Finish**. The Routing profile is cloned and renamed.

Routing Rule Management

Editing a routing profile consists of managing the routing rules it contains. Routing rules within a profile can be added, edited, reordered, and deleted. These procedures are contained in the following sections.

Related topics:

Adding a Routing Rule on page 233
Editing a Routing Rule on page 234
Deleting a Routing Rule on page 234
Reordering Routing Rule Precedence on page 235

Adding a Routing Rule

About this task

Use the following procedure to add a new routing rule to an existing routing profile.

Procedure

1. Login to the Avaya SBCE Control Center as Admin.
2. Select the Routing function from the Global Profiles feature from the Task Pane. Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the Avaya SBCE Control Center.

3. From 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 Add Routing Rule pop-up window is displayed.
5. In the Add Routing Rule pop-up window, enter the desired fields and press **Finish** when done.
   The new routing rule is saved and the Add Routing Rule display is updated.

Editing a Routing Rule

About this task

Use the following procedure to edit an existing routing rule.

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.
2. Select the Routing function from the Global Profiles feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the Avaya SBCE Control Center.
3. From the Applications Pane select the routing profile to which you want to edit an existing routing rule.
4. Click the **Edit** option corresponding to the routing rule you want to edit.
   The Edit Routing Rule pop-up window is displayed.
5. Edit the desired fields.
6. Select **Finish**.
   Your changes are saved and the Routing Profile display is updated.

Deleting a Routing Rule

About this task

Use the following procedure to delete an existing routing rule.

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.

2. Select the Routing function from the Global Profiles feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the Avaya SBCE Control Center.
3. From the Applications Pane select the routing profile to which you want to delete a routing rule.
4. Click the **Delete** option corresponding to the routing rule you want to delete.
   The Delete Confirmation pop-up window is displayed
5. Click **OK**.
   The routing rule is deleted and the Routing Profile display is updated.

Reordering Routing Rule Precedence

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as the Admin.
2. Select the Routing function from the Global Profiles feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the Avaya SBCE Control Center.
3. From 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 which you want the routing rules to be executed.
5. Click the **Update Order** button.
   The routing rules are redisplayed in the Content Area to reflect the new order of precedence

Renaming an Existing Routing Profile

About this task

Use the following procedure to rename an existing Routing profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Routing** function from the Global Parameters feature from the Task Pane.
   Existing Routing Profiles are displayed in the Application Pane.
3. In the Application Pane, select the routing profile that you want to rename.
4. In the Content Area, click **Rename Profile**.
   The Rename Profile pop-up window will be displayed.
5. Enter a new name for the routing profile.
6. Click **Finish**.
   The selected routing profile is renamed and the Routing Profile screen is updated and redisplayed.

Deleting an Existing Routing Profile

About this task

Use the following procedure to delete an existing Routing profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Routing** function from the Global Profiles feature from the Task Pane.
   Existing Routing Profiles are displayed in the Application Pane.
3. In the Application Pane, select the routing profile that you want to delete.
4. Click **Delete**.
   The Delete Confirmation pop-up window is displayed
5. Click OK.

The routing profile is deleted and the Routing Profile screen updated and redisplayed.

Syslog Parameter Management

This section provides a procedure for managing syslog parameters.

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 via UDP and/or TCP. 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 it 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. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Syslog Management** function from the Troubleshooting feature from the Task Pane.
   The Syslog Management screen is displayed, defaulting to the Log Level tab view
3. From the Application Pane, select the Avaya SBCE security device for which you want to configure log level information.
4. Select the desired log collection facility from the pull-down menu for each class of logs (Platform, Trace, Security, and Protocol) and the types of information to be collected.
   The Rename Profile pop-up window will be displayed.
5. Click **Save**.
   The Log Level information is saved.

User Agents (Advanced Services Only)

The User Agents function of the Global Parameters feature allows you to manage which types of SBC end-points (user agent) are authorized to use the network. You can easily add, edit, and delete user agent types from a master global list.

Use the following procedures to manage user agents.

Viewing Authorized User Agents (Advanced Services only)

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **User Agents** function of the Global Parameters feature from the Task Pane.
   The User Agents screen is displayed.

Adding a New User Agent (Advanced Services only)

Procedure

1. Select **Add User Agent** from the User Agents display.
   The User Agents screen is displayed.
2. In the Name field, enter a name that will be displayed to identify the user agent.
3. In the Regular Expression field, you can either enter an exact match for the internal ID of the user agent phone, or you can enter a regular expression that will match multiple phones with similar IDs.
4. Click **Finish**.
   The new user agent is added to the User Agents display.

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**"

Editing an Existing User Agent (Advanced Services only)

Procedure

1. From the User Agents screen, select the **Edit** option corresponding to the user agent type you want to edit.
   The User Agents screen is displayed.
2. Edit the user agent as necessary and select **Finish**.
   The changes made to the user agent are shown in the User Agents display.

Deleting an Existing User Agent (Advanced Services only)

Procedure

1. From the User Agents display, select the **Delete** option corresponding to the particular user agent type you want to delete.
   A delete confirmation pop-up window is displayed.
2. Click **OK**.
   The user agent is deleted 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. The procedures for managing these two features are provided in the following sections.

Viewing an Existing Signaling Interface

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Signaling Interface** function of the Device Specific Settings feature from the Task Pane.
   The Signaling Interface screen is displayed.
3. From the Application Pane select the SBC device to display the Signaling Interface parameters for that device.

Adding a New Signaling Interface

Procedure

1. Select **Add**.
   The Add Signaling Interface pop-up window is displayed.
2. Enter the requested information into the appropriate fields using the Add Signaling Interface Pop-up Window Field Descriptions on page 240 table.

   Note:

   Ports configuration is the user’s choice. However, it is important that if the user has a data firewall that the ports configured in the SBCE be synchronized with the ports in the data firewall. If the user has no data firewall, no action is required.
3. Click **Finish**.
   The new configuration is displayed in the Signaling Interface display.

Add Signaling Interface Pop-up Window Field Descriptions

Field	Description
Name	The name used to refer to this profile.

Field	Description
IP Address	The IP address of the SBCE security device used by SIP signaling messages traversing the network.
TCP Port	The port the SBC security device will 'listen' to for TCP packets.
UDP Port	The port the SBC security device will 'listen' to for UDP packets.
Enable Stun	Enable STUN functionality on the SBC security device on the UDP port specified above
TLS Port	The port the SBC security device will 'listen' to for TLS packets.
TLS Profile	Add TLS certificates for TLS port specified above Checkbox is disabled when no TLS Port value is specified.
Enable Shared Control	Enable OneX Client Shared control support on the SBC security device (This should be enabled only on the Internal Side Interface of SBC (i.e. towards call server) (SBCE TLS port must be enabled before enable this check box)
Shared Control Port	The port the SBCE security device will 'listen' to for OneX shared control packets

Note:

Ports configuration is the user's choice. However, it is important that if the user has a data firewall that the ports configured in the SBC be synchronized 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. From the Signaling Interface display, select the **Edit** option corresponding to the Signaling Interface configuration you want to edit.
   The Edit Signaling Interface pop-up window is displayed.
2. Edit the configuration as necessary and select **Finish**.

The changes are saved and the Signaling Interface display is updated.

Deleting an Existing Signaling Interface

Procedure

1. From the Signaling Interface display, select the **Delete** option corresponding to the Signaling Interface configuration you want to delete.
   A delete confirmation pop-up window is displayed.
2. Click **OK**.
   The Signaling Interface configuration is deleted.

Viewing an existing media interface

About this task

Use the following procedures to view media interface parameters.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Media Interface** function of the Device Specific Settings feature from the Task Pane.
   The Media Interface screen is displayed.
3. From the Application Pane, select the SBC device for which you want to view the **Media Interface** parameters.
   The Media Interface parameters for that device are displayed.

Adding a New Media Interface

Procedure

1. Select **Add** on the Media Interface tab.
   The Add Media Interface pop-up window is displayed

2. Enter the requested information into the appropriate fields in the new information line according to the information contained in Add Media Interface Pop-up Window Field Descriptions on page 243.
3. Select **Finish**.
   The new configuration is displayed in the Media Interface display.

Add Media Interface Pop-up Window Field Descriptions

Field	Description
Name	The name used to refer to this profile.
IP Address	The IP address of the SBC security device to which media packets are sent.
Port Range	The range of ports on the SBC security device allocated for media traffic.

Note:

Ports configuration is the user’s choice. However, it is important that if the user has a data firewall that the ports configured in the SBC be synchronized with the ports in the data firewall. If the user has no data firewall, no action is required.

Editing an existing Media Interface

Procedure

1. From the Media Interface display, select the **Edit** option corresponding to the Media Interface configuration you want to edit.
   The Edit Media Interface pop-up window is displayed.
2. Edit the configuration as necessary and select **Finish**.
   The changes are saved and the Media Interface display is updated.

Deleting an Existing Media Interface

Procedure

1. From the Media Interface display, select the **Delete** option corresponding to the Media Interface configuration you want to delete.
   A Delete Confirmation pop-up window is displayed.
2. Click **OK** to confirm.
   The Media Interface configuration is deleted.

Chapter 7: Security Configuration

Overview

The Avaya SBCE Control Center allows you to view various security-related features of SBCE security products, such as:

- Configuring Denial-of-Service (DoS) Policies
    - DoS settings for SIP endpoints
    - DoS settings for aggregate domains
    - DoS activity profiling per user-definable time-period

More on DoS Configuration can be found below:

- Protocol Scrubber Rules
- Fingerprinting
- Topology Hiding

System-wide single endpoint DoS configurations

System-wide single endpoint DoS configurations are found by clicking on **DoS/DDoS** under **Global Parameters** in the Task Pane. These are used to configure DoS settings for system-wide SIP endpoints.

Domain DoS configurations

Domain DoS configurations are found by clicking on **Domain DoS** under **Global Profiles** in the Task Pane. These are used to create a DoS profile for particular aggregate domains. Once profile is created it is applied to aggregate domains using **Security Rules** found under **Domain Policies** in the Task Pane.

SIP server DoS configuration

SIP server DoS configuration are found by clicking on **Server Configuration** under **Global Profiles** in the Task Pane. These are used to configure DoS security settings for particular SIP servers. Guidance for DoS thresholds for SIP servers can be found by DoS learning:

- Found by clicking on **DoS Learning** under **Troubleshooting** in the Task Pane

  .
- Enables DoS activity profiling per user-definable time period.
- Applied to DoS configuration for SIP servers.

For more on DoS configurations, please see DoS Security Features on page 246.

DoS security features

The DoS Security feature of the Avaya SBCE Control Center allows you to view and edit a wide variety of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attack response and control parameters that can then be applied either to individual SIP endpoints or their parent domain. Additionally, the current release of the SBC supports DoS activity reporting for certain time periods. The procedures to perform these functions are contained in the following sections.

Note:

The global Dos/DDos security parameter settings described next, are accessible by selecting: **Global Parameters** → **DoS/DDoS**.

The threshold settings for each of 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/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**. Then, one at a time, select each individual SBCE device from the Application Pane and then select its **Feature Control** tab.

See “Enabling/Disabling SBCE Security Features” for more details.

Viewing DoS/DDoS settings

About this task

Use the following procedure to view DoS/DDoS settings that were previously configured using the **Security Rules** function of the Domain Policies feature.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the **Global Parameters** feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.

   DoS/DDoS Attack Type Descriptions on page 247 contains a description of the DoS/DDoS attack types referenced by the tabs.

   Select the tab containing the particular DoS/DDoS settings you want to view. The selected settings will be displayed in the Content Area.

DoS/DDoS attack type descriptions

DoS attack type	Attack type description
Single Source DoS	Any type of DoS attack that is directed against one or more enterprise endpoints that originate from a single source (normally spoofed).
Phone DoS/DDoS	A type of DoS attack that is directed against a single enterprise endpoint.
Stealth DoS/DDoS	A type of low-volume DoS attack that is directed against an endpoint where the source of the call is constantly changed.
Call Walking	A type of DoS attack whereby serial calls originating from a single source (normally spoofed) are directed against a sequential group of endpoints.

DoS attack type	Attack type description
Toll Fraud	Refers to internal or external users using the corporate phone system to place unauthorized toll calls. Toll fraud can occur with both TDM and IP-based voice systems.

Editing DoS/DDoS settings

About this task

Use the following procedure to edit DoS/DDoS settings.

Procedure

1. Login to the Avaya SBCEControl Center as the `Admin`.
2. Select the **DoS/DDoS** function of the **Global Parameters** feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Walking**, and **Toll Fraud**) in the Content Area.
3. Select the tab containing the DoS/DDoS settings you want to edit.
   The selected DoS/DDoS settings will be displayed in the Content Area.
4. Click the **Edit** icon corresponding to the specific DoS/DDoS settings you want to edit.
   An Edit Response pop-up window for Call Walking is displayed.
5. Edit the fields as desired and click **Finish** to save your changes or **Cancel** to return the fields to their previous values and close the window without saving.

Viewing toll fraud settings

About this task

Use the following procedure to view toll fraud settings.

Procedure

1. Login to the Avaya SBCEControl Center as the `Admin`.

2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab to display a toll fraud tab.

Adding a toll fraud rule

About this task

Use the following procedure to add a new toll fraud rule.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab to display a toll fraud tab display.
4. Click on the **Add** button to display an Add Toll Fraud DoS pop-up window.
5. Complete the parameter fields in the Add Toll Fraud DoS pop-up window (Add Toll Fraud DoS Parameter Descriptions on page 249).

Add toll fraud DoS parameter descriptions

Parameter	Description
Name	A name assigned to the new toll fraud DoS profile.
URI Group	Select **Emergency** (contains a default integral URI listing) or select the name of a custom URI group (contains a custom URI Group listing) from the drop-down list. See Chapter 5 “Domain Policy Administration,”

Parameter	Description
	and the sub-section, “Uniform Resource Identifier (URI) Groups.”
Whitelist URI Group	Select **None** or select the name of a custom URI group to use as a Whitelist (contains a custom URI Group listing). The URI Group listing used as a Whitelist is created in the same manner as a standard URI Group. See Chapter 5 “Domain Policy Administration,” and the sub-section, “Uniform Resource Identifier (URI) Groups.”
Call Duration	The upper limit for detecting a potential Toll Fraud call. See Example 1 in Figure 7–5 where the Call Duration value of 2 (in seconds) is entered to detect calls of 2 seconds or less.
Call Threshold	The lower limit for detecting a potential Toll Fraud call that matches the Call Duration specified above. See Example 1 in Figure 7–5 where the Call Threshold value of 10 (in number of calls) is entered to detect calls reaching a total count of 10.
Threshold Interval	The time interval or cutoff time limit for detecting and counting calls which fall within the Call Duration and Call Threshold parameters defined above. Detects potential Toll Fraud calls that match the Call Duration and Call Threshold parameters specified above. See Example 1 in Figure 7-5 where the Call Threshold value of 10 (in number of calls) is entered to detect calls reaching a total count of 10. In this example, when a Threshold Interval count of 10, the specified Action (i.e., either an Alert or Reason Phrase transmission) will be performed beginning with the 11th call.
Action	• Alert — Alert only viewable via the Incidents and Logs → System Logs buttons at the top of the screen. • Block within... — Transmits the specified Reason Phrase, in addition to sending an alert as described above for the Alert option.
Block Duration	Length of time (in minutes) that the block and response code transmission will occur, as

Parameter	Description
	specified in the two Block within . . . parameter fields.

Editing an existing toll fraud rule

About this task

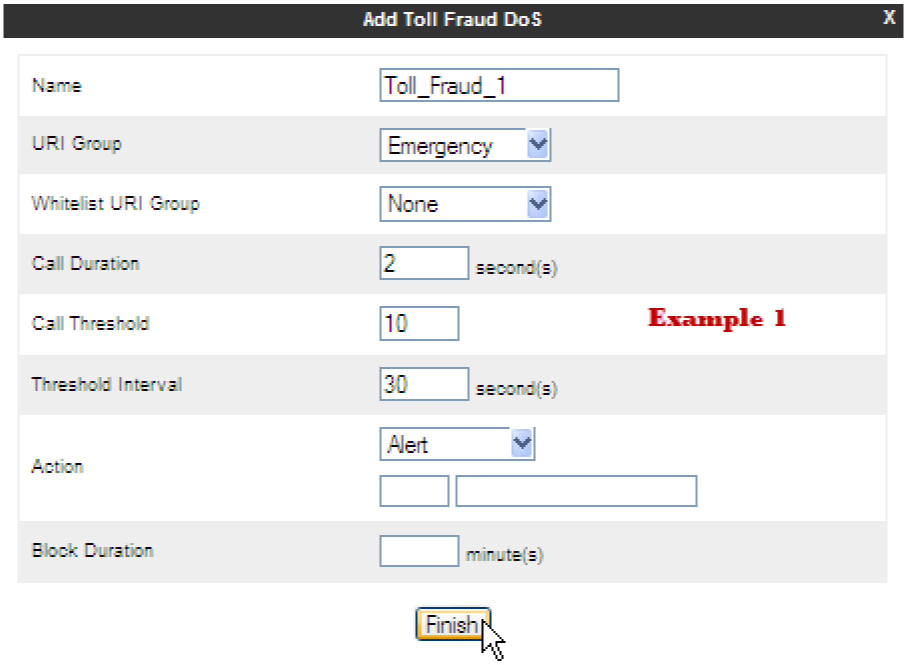
Use the following procedure to edit an existing toll fraud rule.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab.
4. Click on the **Edit** link corresponding to the toll fraud rule which you want to edit.
   An Edit Toll Fraud DoS pop-up window is displayed.
5. Edit the fields as desired and click **Finish** to save your changes or **Cancel** to return the fields to their previous values and close the window without saving.

Example

In Example 1, the Toll Fraud profile named “Toll_Fraud_1” will be activated when 10 calls (Call Threshold) are detected each having a total length of 2 seconds or less (Call Duration) within the time period of 30 seconds (Threshold Interval). In the case of the example above, when the Toll_Fraud_1 profile is activated only an Alert will be issued (Action), which is viewable via the Incidents and Logs > System Logs buttons at the top of the screen.

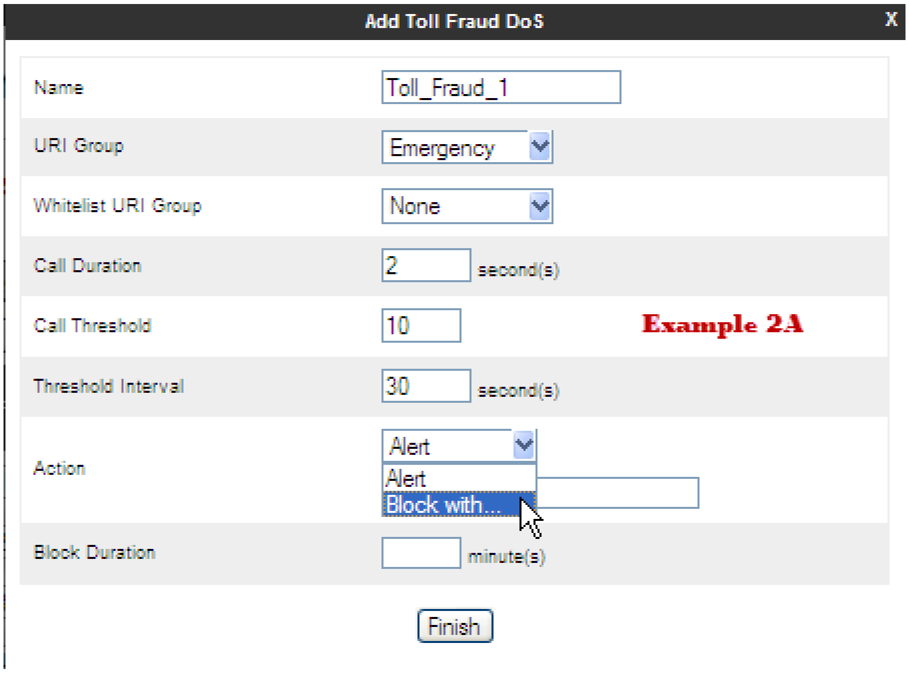


Name	Toll_Fraud_1
URI Group	Emergency
Whitelist URI Group	None
Call Duration	2 second(s)
Call Threshold	10
Threshold Interval	30 second(s)
Action	Alert
Block Duration	minute(s)

Example 1

Examples 2A and 2B illustrate the selection of an alternate Action option (Block with...) and the completion of the associated parameter fields, Action and Block Duration.

In Example 2A, selecting the **Block with...** action from the Action drop-down list activates two Action parameter fields and one Block Duration parameter field.



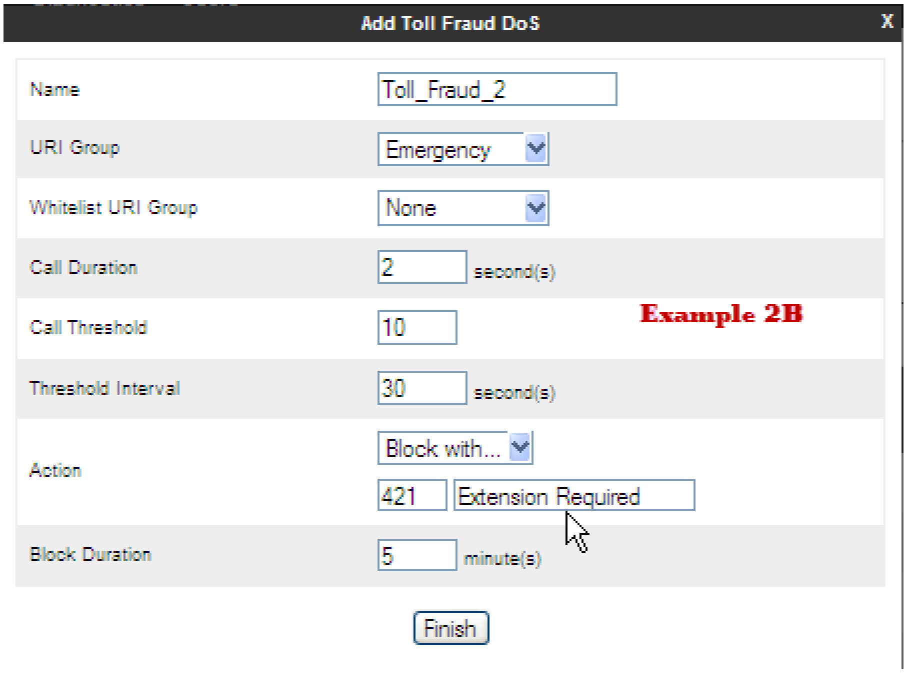
Name	Toll_Fraud_1
URI Group	Emergency
Whitelist URI Group	None
Call Duration	2 second(s)
Call Threshold	10
Threshold Interval	30 second(s)
Action	Alert
Block Duration	minute(s)

Example 2A

Entering a 3-digit SIP Client Failure Response Code (see SIP Response Codes on page 253) in the left-hand Action parameter field automatically fills in the associated character stream name in the right-hand Action parameter field.

For example, entering the numbers “421” in the left-hand field will automatically display the characters “Extension Required” in the right-hand field. In Example 2B, when the conditions occur that are defined above in the Call Duration, Call Threshold, and Threshold Interval fields, then the 421 Response Code Reason Phrase will be sent in the reply stream.

The duration of the Reason Phrase transmission is determined by the time (in minutes) entered in the Block Duration parameter field.



Add Toll Fraud DoS

Name	Toll_Fraud_2
URI Group	Emergency
Whitelist URI Group	None
Call Duration	2 second(s)
Call Threshold	10
Threshold Interval	30 second(s)
Action	Block with... 421 Extension Required
Block Duration	5 minute(s)

SIP response codes

Respose Code	Reason Phrase
400	Bad request
401	Unauthorized
402	Payment required
403	Forbidden
404	Not found
405	Method not allowed
406	Not acceptable
407	Proxy authentication required
408	Request timeout

Respose Code	Reason Phrase
410	Gone
413	Request entity too large
414	Request URI too long
415	Unsupported media type
416	Unsupported URI scheme
420	Bad extension
421	Extension required
423	Interval too brief
480	Temporarily unavailable
481	Call/transaction does not exist
482	Loop detected
483	Too many hops
484	Address incomplete
485	Ambiguous
486	Busy here
487	Request terminated
488	Not acceptable here
491	Request pending
493	Undecipherable
500	Server internal error
501	Not implemented
502	Bad gateway
503	Service unavailable
504	Server timeout
505	Version not supported
513	Message too large
600	Busy everywhere
603	Decline
604	Does not exist anywhere
606	Not acceptable

Cloning a toll fraud rule

About this task

Use the following procedure to clone a toll fraud rule.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab to display a toll fraud tab display similar to the example in Figure 7–4.
4. Click on the **Clone** link corresponding to the toll fraud rule which you want to clone.
   The Edit Toll Fraud DoS pop-up window similar to the example in Figure 7–5 is displayed.
5. Enter a new name for the cloned profile and click **Finish**.
   The cloned toll fraud rule is saved and the Toll Fraud Rules screen re-displayed.

Re-ordering toll fraud rules

About this task

Use the following procedure to update the priorities of toll fraud rules.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab to display a toll fraud tab display.

4. Enter appropriate values for the priority order for the toll fraud rules in the **Priority** text box.
5. Click on **Update Order** button in the Content Pane to save the priority order.
   The priority order is updated in ascending order and the Toll Fraud Rules screen is re-displayed.

Deleting a toll fraud rule

About this task

Use the following procedure to delete a toll fraud rule.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **DoS/DDoS** function of the Global Parameters feature from the Task Pane.
   The DoS Settings screen will be displayed, containing five tabs (**Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, **Call Waking**, and **Toll Fraud**) in the Content Area.
3. Select the **Toll Fraud** tab to display a toll fraud tab display similar to the example in Figure 7–4.
4. Click on the **Delete** link corresponding to the toll fraud rule which you want to delete.
   A confirmation pop-up window will be displayed asking you to confirm your selection.
5. Click **OK**.
   The toll fraud rule is deleted.

Domain DoS profiles

The Domain DoS profiles allow you to rate limit a number of SIP-specific services to ensure the availability of VoIP network resources. Domain DoS profiles can be viewed, added, cloned, edited, and deleted. The procedures to perform these functions are described below.

Viewing an existing Domain DoS profile

About this task

Use the following procedure to view an existing Domain DoS profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Domain DoS/DDoS** function of the **Global Profiles** feature from the Task Pane.
   The Domain DoS screen is displayed, containing a list of available Domain DoS profiles in the Application Pane and their associated rate limited SIP services and corresponding thresholds in the Content Area.
3. From the Application Pane, select the Domain DoS profile you want to view.
   The Rate Limit parameters corresponding to the selected Domain DoS profile will be displayed in the Content Area.

Adding a new Domain DoS profile

About this task

Use the following procedure to add a new Domain DoS profile.

Procedure

1. Select **Add**.
   The Add Domain DoS pop-up window is displayed (Figure 7–10).
2. Enter a name for the new profile and click **Next** (Figure 7–11).
3. Enter Number of Users on this Call Server, and choose Client Type from the dropdown menu.
   - Number of Users on this Call Server: The estimated number of users on this call server
   - Client Type: The type of phones connecting to this call server

   Note:

   These fields will also show when "Recalculate Values" is clicked on the "Rate Limit" tab after the profile has been created.

4. Click **Finish**.
   The new Domain DoS profile is saved and the Domain DoS screen (Figure 7–12) is re-displayed.

Cloning an existing Domain DoS profile

About this task

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

Procedure

1. From the Application Pane, select the Domain DoS profile you want to clone (Figure 7–9).
2. Select **Clone**.
   The Clone Domain DoS pop-up window is displayed (Figure 7–13).
3. Enter a name for the cloned profile and click **Finish**.
   The cloned Domain DoS profile is saved and the Domain DoS screen re-displayed.

Renaming an existing Domain DoS profile

About this task

Use the following procedure to rename an existing Domain DoS profile.

Procedure

1. From the Application Pane, select the Domain DoS profile you want to rename (Figure 7–9).
2. Select **Rename**.
   The Rename Domain DoS pop-up window is displayed (Figure 7–15).
3. Enter a new name for the profile and click **Finish**.
   The new name is saved and the Domain DoS screen redisplayed (Figure 7–16).

Editing an existing Domain DoS profile

About this task

Use the following procedure to edit an existing Domain DoS profile.

Procedure

1. From the Application Pane, select the Domain DoS profile you want to edit (Figure 7–9).
2. Click the **Edit** option corresponding to the SIP service or method you want to edit. An **Edit Domain DoS** pop-up window similar to the example shown in Figure 7–17 will be displayed.

   The Action parameters in the Action drop-down parameter list (Figure 7–17) are described in DoS Domain Action Parameter Descriptions on page 259.
3. Edit the fields as desired.
   Select **Finish** to save your changes or **Cancel** to return the fields to their previous values and close the window without saving.

DoS Domain action parameter descriptions

Parameter	Description
Method	
Initiated Threshold (per 5 seconds)	
Pending Threshold	
Field Threshold (per 5 seconds)	
Action	
Alert Only	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 with Response	When the specified limit is reached, block the call and send a configured response.
SIP Challenge	Initiate Authentication

Parameter	Description
Whitelist	If the call originator exists in the Whitelist, do not block the call.

Note:

When the **Enforce Limit with Response** action parameter is selected, two additional fields are displayed and enabled below the list which allow for entry of a SIP response code in the left field and the auto-completion of the associated SIP response phrase, as previously described in Editing Toll Fraud Settings on page 248 when the **Block with...** action parameter is selected, as illustrated in Figures 7–6 and 7–7.

Deleting an existing Domain DoS profile

About this task

Use the following procedure to delete an existing Domain DoS profile.

Note:

This procedure applies to DoS server profiles. Refer to Editing the DoS Protection Parameter Tab on page 288 for information on creating and editing DoS server profiles.

Procedure

1. From the Application Pane, select the Domain DoS profile you want to delete (Figure 7–9).
2. Select **Delete**.
   A confirmation pop-up window will be displayed similar to that shown in Figure 7–18 asking you to confirm your selection.
3. Select **OK**.
   The selected Domain DoS profile is deleted.

Viewing learned DoS parameters

About this task

Use the following procedure to define simple time-of-week and time-of-day parameters in which the EMS will ‘learn’ or gather, save, and report the historical traffic activity towards the server occurring at a particular SBC device deployed in the network.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **DoS Learning** function of the Troubleshooting feature from the Task Pane.
   The Learned Info screen is displayed, containing a list of installed SBC devices in the Application Pane.
3. Select the SBC security device from the Application Pane whose DoS activity you want to learn.
4. Using the pull-down menus on the **Learned Info** tab in the Content Area, select the time period for which you want to learn DoS activity.
5. Select **Update**.
   Any DoS activity detected for the specified time period will be displayed in the Content Area.

Protocol scrubber

Protocol Scrubbing is an Avaya SBCE feature that utilizes a highly sophisticated statistical mechanism to thoroughly check incoming SIP signaling messages for various types of protocol-specific events and anomalies. It verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against updatable templates received from Avaya. Typically, messages which violate the security rules dictated by the scrubber templates will be dropped while those which violate syntax rules will be repaired (either re-written, truncate, 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.

The Protocol Scrubbing feature for SIP allows you install a scrubber rules package, enable or disable the scrubber rules contained in the package, and delete the package from the system. In addition, you can 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.

Refer to Security Rules on page 117 and Updating VIPER signatures on page 62.

Viewing Scrubber rules

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Scrubber** function of the Global Parameters feature from the Task Pane.
   The Scrubber screen is displayed, containing two user-selectable tabs in the Content Area: **Packages** and **Rules**.
3. Select the **Rules** tab.
   Any installed scrubber rules (templates) will be displayed in the Content Area.

Installing a Scrubber rules package

Procedure

1. Select the **Scrubber** function of the Global Parameters feature from the Task Pane.
2. Select the **Packages** tab.
3. Click **Install Package**.
   The Install Scrubber Package pop-up window is displayed (Figure 7–23).
4. Select the **Browse** button to navigate to the directory containing the chosen scrubber package and select it.
   The scrubber package filename will be inserted in the Scrubber Package Edit window.
5. Click **Install**.
   The selected scrubber package is loaded, enabled, and listed in the **Packages** tab display.

   Note:

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

Refer to Security Rules on page 117.

Example

Next steps

Configuring Scrubber actions

Procedure

1. After installing the Scrubber rules, actions can be configured by clicking on the **Action** button located on the right-hand side of the **Rules** tab screen.
2. There are three actions allowed:
   a. BLOCK — Drops the message
   b. REJECT — Responds back to a request with a “400 Bad Request” response
   c. DROP HEADER — Drops the header that the rule mismatched to

Enabling/disabling an installed Scrubber Rules package

About this task

Note:

After installing a Scrubber Rules package, the package must be enabled, as described in this section, before the rules package takes effect.

Procedure

1. In the Content Area, click the **Toggle** button corresponding to the scrubber package you want to enable or disable.
2. The selected scrubber package is enabled (or disabled).

Deleting an existing Scrubber Rules package

Procedure

1. In the Content Area, click the **Delete** icon corresponding to the scrubber package you want to delete.
   A Delete Confirmation pop-up window similar to that shown in Figure 7–24 is displayed.
2. Click **OK**.
   The selected Scrubber package is deleted.

Fingerprinting (advanced services only)

Fingerprinting is a highly accurate mechanism used by SBCE devices to characterize and identify SIP endpoints within a network. By analyzing a number of specific characteristics, a profile of a particular endpoint is generated against which security and call-flow policies can be applied. Although default fingerprint profiles are provided, additional profiles can be added, cloned, and enabled or disabled. These procedures are provided in the following sections.

Viewing a Fingerprint profile (advanced services only)

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
   The Fingerprint Profiles screen is displayed, containing a list of the different fingerprinting criteria and their status (enabled/disabled).

   Note:

   Fingerprint profiles used for OCS configurations should have the **Header Order** criteria disabled.
3.

Adding a new Fingerprint profile (advanced services only)

About this task

Note:

Fingerprint profiles can be used in defining many Endpoint Policy Groups. Refer to the section titled “Endpoint Policy Groups” in Chapter 5.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
3. From the Application Pane, select **Add**.
   The Add Fingerprint Profile pop-up window is displayed.
4. Enter a name for the new profile and click **Finish**.
   The new Fingerprint profile is added to the Fingerprint Profiles list in the Application Pane (Figure 7–28).

Cloning a Fingerprint profile (advanced services only)

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
3. From the Application Pane, select the Fingerprint profile (Figure 7–28) that you want to clone.
4. Click **Clone**.
   The new Clone Profile pop-up window is displayed (Figure 7–29).
5. Enter a name for the clone and click **Finish**. The cloned Fingerprint profile is added to the Fingerprint Profiles list in the Application Pane.

Editing a Fingerprint profile (advanced services only)

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
3. From the Application Pane, select the Fingerprint profile (Figure 7–28) whose parameters you want to edit.
4. In the Content Area, click the **Edit** option corresponding to the specific Fingerprint characteristic you want to edit.
   The Edit Criteria pop-up window is displayed, similar to that shown in Figure 7–30.
5. Edit the fields as desired and click **Finish**.
   The new field values are saved and the Fingerprint profile re-displayed in the Content Area.

Renaming a Fingerprint profile (advanced services only)

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
3. From the Application Pane, select the Fingerprint profile (Figure 7–28) that you want to rename.
4. Click **Rename**.
   The Rename Profile pop-up window is displayed (Figure 7–31).
5. Enter a new name for the profile and click **Finish**.
   The profile is renamed.

Deleting a Fingerprint profile (advanced services only)

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Fingerprint** function of the Global Profiles feature from the Task Pane.
3. From the Application Pane, select the Fingerprint profile (Figure 7–28) that you want to delete.
4. Click **Delete**.
   The Delete Confirmation pop-up window is displayed (Figure 7–32).
5. Click **OK**.
   The profile is deleted.

Configuring Fingerprinting actions (advanced services only)

Procedure

1. In the Fingerprint Profile screen, click the **Edit** option corresponding to the criteria you want to edit.
   The Edit Criteria pop-up screen is displayed.
2. You can choose one of the following three actions allowed:
   a. ALERT — Syslog and Incidence are generated
   b. RE-AUTHENTICATE — Syslog is generated
   c. BLOCK — Syslog and Incidence are generated

Creating a new Topology Hiding profile

About this task

Use the following procedure to create a new Topology Hiding profile.

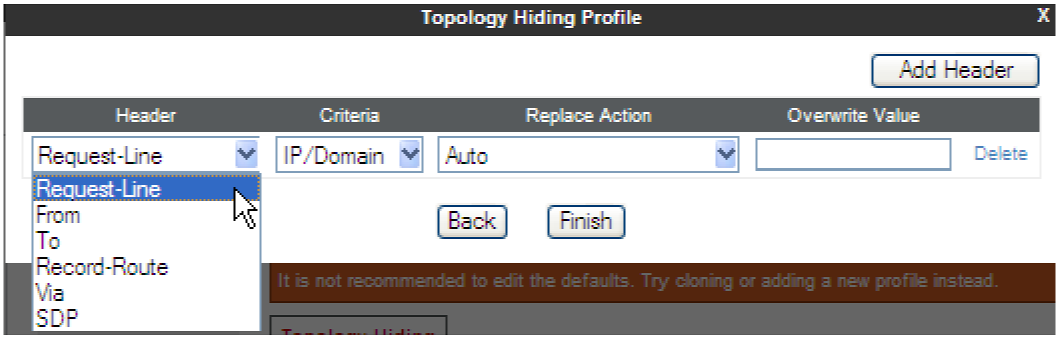
Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Topology Hiding** function from the Global Profiles feature from the Task Pane
   Existing Topology Hiding profiles are displayed in the Application Pane and their corresponding Topology Headers are displayed in the Content Area of the Avaya SBCE Control Center, which has the default profile selected.
3. From the Application Pane, click **Add**.
   The first Topology Hiding Profile pop-up screen is displayed.
4. Enter a name for the new profile and click **Next**.
   The second Topology Hiding Profile screen is displayed.
5. In the second Topology Hiding Profile screen), begin to select the chosen parameters by selecting the drop-down list of **Header** parameters to choose one of the parameters for the new profile.
6. In the second Topology Hiding Profile screen, next select the drop-down list of **Criteria** parameters to choose one of the parameters for the new profile.
7. In the second Topology Hiding Profile screen, next select the drop-down list of **Replace Action** parameters to choose one of the parameters for the new profile.

   In the drop-down list in the **Replace Action** field, shown above, if you select the action **Overwrite**, the **Overwrite Value** field to the right will accept entry of a value (i.e., an IP address).
8. After selecting the appropriate values in the Topology Hiding Profile fields, select **Finish** to save, submit, exit, and re-display the Topology Hiding Profile screen.

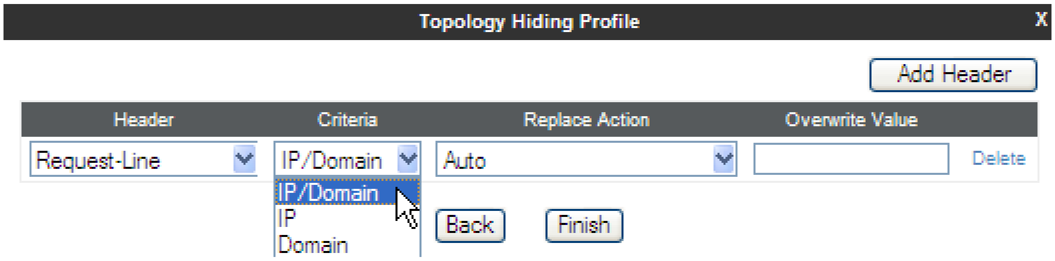
This ends the procedure for creating a new Topology Hiding Profile.

Example

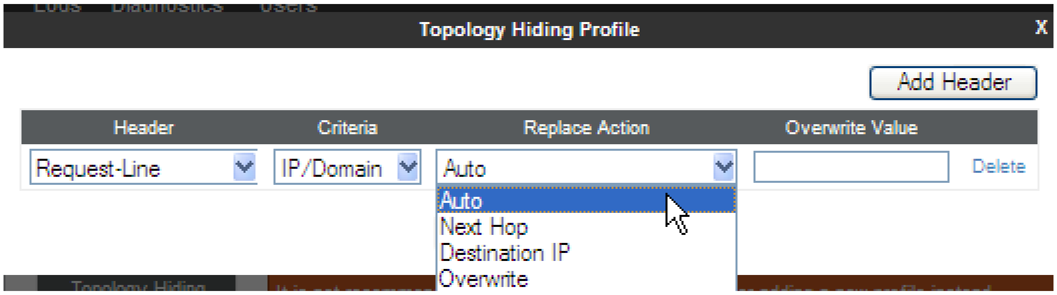


Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.



Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete



Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete

Adding a new Topology Hiding header

About this task

Use the following procedure to add a new Topology Hiding Header to an existing Topology Hiding profile.

Note:

In previous versions of Avaya SBCE prior to Release 4.0.4, this section was titled “Adding a New Topology Hiding Rule.” With Release 4.0.4, Topology Hiding rules are now replaced with and based on headers instead of based on rules and URI groups as was done previously.

Procedure

1. In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7–41) to which you want to add a new Topology Hiding Header.
2. In the Content Area, click the **Edit** button to display the Edit Topology Hiding Profile screen (Figure 7–42).
3. In the Edit Topology Hiding Profile screen (Figure 7–42), select the **Add Header** button to add an additional Header description row, as shown in the second Edit Topology Hiding Profile screen.

   Note:

   The total number of new Headers that can be added is restricted to the number of parameter names in the **Header** field drop-down list. For example, the list contains six Header parameter names, therefore you are only able to create six Headers with the names, Request-Line, From, To, Record-Route, Via, and SDP.

   When you select the **Add Header** button, a new Header description row is added below with the **Header** field containing the value of the next available Header name (e.g., “From”), which you can change by selecting a different value from the list.
4. In the drop-down list in the new **Header** field (named “From” in the example (Figure 7–43), you can use the supplied name of “From” or select another unused Header parameter name for the new Topology Hiding Header.
   For this example, the Header name of Record-Route is selected, as shown below (Figure 7–44).
5. After selecting an unused Header parameter name (e.g., Record_Route in the example) from the **Header** field drop-down list, select the remaining parameters from the **Criteria** field drop-down list, from the **Replace Action** field drop-down list, and if “Overwrite” was selected as the **Replace Action**, enter an IP address in the **Overwrite Value** field.
6. Click **Finish** to submit, save, exit, and redisplay the Topology Hiding Profile display screen, which should now contain your newly-added Header, as shown in the updated Topology Hiding Profile display screen Figure 7–45.

   Note:

   In Figure 7–45, the Topology Hiding Profile named TH_Profile_2 now has two Topology Hiding Headers defined, the original one named Request-Line and the one you just added named Record-Route.

Editing a Topology Hiding Header

About this task

Use the following procedure to edit an existing a Topology Hiding rule for a specific Topology Hiding Profile.

Procedure

1. In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7–45) containing the Topology Hiding Header you want to edit.
2. Click the **Edit** button (see Figure 7–45) at the bottom of the display an Edit Topology Hiding Profile screen (Figure 7–46), as shown in the example below.
3. In the Edit Topology Hiding Profile screen (Figure 7–46), you can edit any or all of the displayed Header rows just as described in the previous section, “Adding a New Topology Hiding Header.” Just select new choices from the drop-down lists in the **Header** column, **Criteria** column, and **Release Action** column as described previously.
   This ends the procedure for editing a Topology Hiding Header.

Deleting a Topology Hiding profile

About this task

Use the following procedures to delete an existing a Topology Hiding Profile.

Procedure

1. In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-45) that you want to delete.
2. Click the **Delete** button (see Figure 7–45) at the top right-hand portion of the display to delete the selected Topology Hiding Profile.
   This ends the procedure for deleting a Topology Profile.

Deleting a Topology Hiding header

About this task

Use the following procedures to delete an existing the headers in a Topology Hiding Profile.

Procedure

1. In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7–45) containing the Topology Hiding Header you want to delete.
2. Click the **Edit** button (see Figure 7–45) at the bottom portion of the screen to display an Edit Topology Hiding Profile screen (Figure 7–46).
3. In the Edit Topology Hiding Profile screen (Figure 7–46), select the delete option corresponding to the Topology Hiding Header you want to delete.
   This ends the procedure for deleting a Topology Hiding Header.

Cloning an existing Topology Hiding profile

About this task

Use the following procedure to clone (copy) an existing Topology Hiding Profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Topology Hiding** function from the Global Profiles feature from the Task Pane.
   Existing Topology Hiding Profiles are displayed in the Application Pane and their corresponding Topology rules are displayed in the Content Area of the Avaya SBCE Control Center.
3. In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7–45) that you want to clone.
4. In the Content Area, click **Clone**.
   The Clone Profile pop-up window will be displayed (Figure 7–47).
5. Enter a name (e.g., TH_Profile_3) for the cloned profile and click **Finish**.

The Topology Hiding Profile is cloned and re-displayed (Figure 7–48) in the Application Pane.

Renaming an existing Topology Hiding profile

About this task

Use the following procedure to rename an existing Topology Hiding Profile.

Procedure

1. In the Application Pane, select the Topology Hiding Profile (TH_Profile_3 in the Figure 7–49 example that you want to rename.
2. In the Content Area, click **Rename Profile**.
   The Rename Profile pop-up window (Figure 7–49) is displayed.
3. Enter a new name (e.g.,TH_Profile_4) for the profile and click **Finish**.
   The profile is renamed and re-displayed in the Application Pane (Figure 7–50).

Headers affected by Topology Hiding

When creating or editing Topology Hiding Profiles, there are six types of headers (i.e., **Request-Line**, **From**, **To**, **Record-Route**, **Via**, and **SDP**) available for selection in the Header drop-down list, as illustrated in below (Figure 7–51).

Note:

In addition to the six headers listed in the drop-down list, there are additional headers (not listed) that are affected when either of two types of listed headers (i.e., **To** header and **From** header) are selected in the **Header** drop-down list.

Topology Hiding Headers on page 274 lists the six headers along with all of the other affected headers in three header categories (i.e., **Source Headers**, **Destination Headers**, and **SDP Headers**).

In the table, where applicable (i.e., **To** header and **From** header), additional affected headers are noted. In Topology Hiding Settings Examples on page 274, descriptions are provided for all possible combinations of selections in the three parameter drop-down lists (i.e., **Header**, **Criteria**, and **Replace Action**), as shown in Figure 7–51 below.

Topology Hiding headers

Main Header Names	Header(s) Affected by Main Header	Header Affecting This Header
Source Headers		
Record-Route		
Route		
From	• Referred-By • PAsserted Identity	
Referred-By		From
PAsserted Identity		From
Destination Headers		
To	ReferTo	
Request Start Line		
ReferTo		To
Diversion		
SDP Headers		
Origin Header		

Topology Hiding Settings Examples

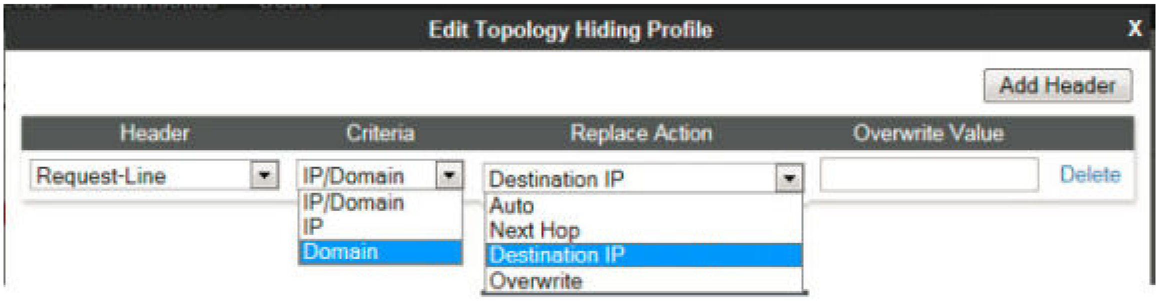
This section provides examples for all of the possible combinations of topology hiding settings listed in the **Header** drop-down list (Figure 7–51), in the order listed (i.e., **Request-Line**, **From**, **To**, **Record-Route**, **Via**, and **SDP**). Each of the **Header** types is combined with each combination of the **Criteria** types (i.e., **IP/Domain**, **IP**, and **Domain**) and **Replace Action** types (i.e., **Auto**, **Next Hop**, **Destination IP**, and **Overwrite**) along with a description of the resulting action or effect.

Topology Hiding examples for Request-Line Header

Following settings explain the Topology Hiding examples for **Request-Line** Header.

1. Topology Hiding will replace the **Request-Line** header by the next hop address/domain from the routing profile.
    - Header — Request-Line
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Auto
2. Topology Hiding will replace the **Request-Line** header by the next hop address/domain from the routing profile.
    - Header — Request-Line
    - Criteria — IP/Domain
    - Replace Action — Next Hop
3. Topology Hiding will replace the **Request-Line** header with the Destination **IP/Domain** from the SIP message.
    - Header — Request-Line
    - Criteria — IP/Domain
    - Replace Action — Destination IP
4. Topology Hiding will replace the **Request-Line** header by the **Overwrite Value**.
    - Header — Request-Line
    - Criteria — IP/Domain
    - Replace Action — Destination IP

Example



Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Destination IP	

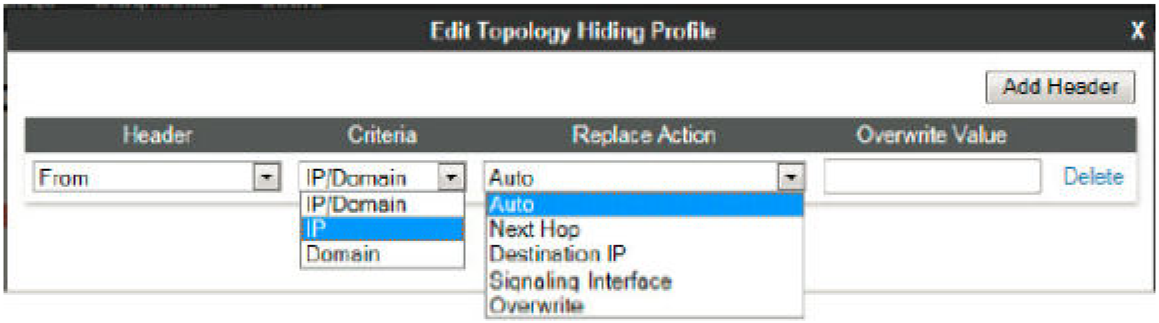
Topology Hiding examples for From header

Note:

The **From** header (and **To** header) settings also affect two other header types, the **Referred-By** header and the **P-Asserted-Identity** header. When the **From** header settings **Replace Actions** listed below are executed, automatic updates to the **Referred-By** header and **P-Asserted-Identity** header are performed as well.

1. If the SIP message is from the Subscriber side then Topology Hiding will replace the **From** Header with the next hop address/domain from the routing profile If the SIP message is from the Call Server side or Trunk Server side then Topology Hiding will replace the **From** Header with the Signaling Interface.
   - Header — From
   - Criteria — IP/Domain or IP or Domain
   - Replace Action — Auto
2. Topology Hiding will replace the **From** header with the next hop address/domain from the Routing profile.
   - Header — From
   - Criteria — IP/Domain or IP or Domain
   - Replace Action — Next Hop
3. Topology Hiding will replace the **From** header with the Destination IP from the SIP Message.
   - Header — From
   - Criteria — IP/Domain or IP or Domain
   - Replace Action — Destination IP
4. Topology Hiding will replace the **From** header with the Signaling Interface IP/Domain.
   - Header — From
   - Criteria — IP/Domain or IP or Domain
   - Replace Action — Signaling Interface
5. Topology Hiding will replace the **From** header with the Overwrite Value.
   - Header — From
   - Criteria — IP/Domain or IP or Domain
   - Replace Action — Overwrite

Example



Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Auto	

Topology Hiding examples for To header

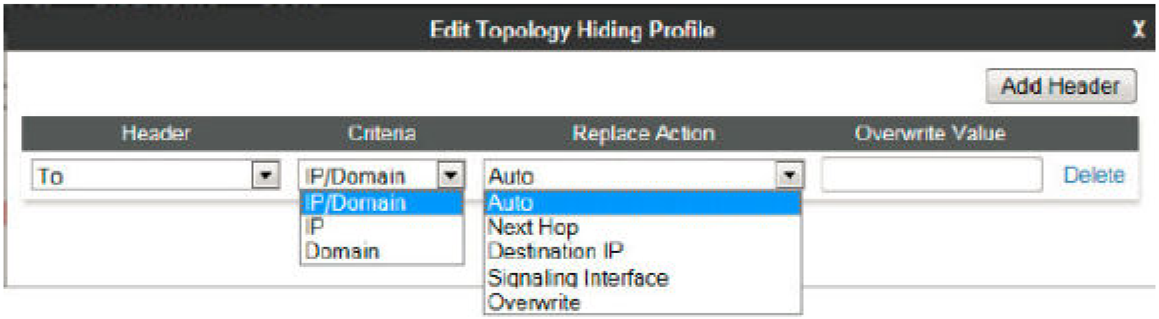
Note:

The **To** header (and **From** header) settings also affect two other header types, the **Referred-By** header and the **P-Asserted-Identity** header. When the **To** header settings **Replace Actions** listed below are executed, automatic updates to the **Referred-By** header and **P-Asserted-Identity** header are performed as well.

1. If the SIP message endpoint type is Subscriber then Topology Hiding will replace 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 will replace the **To** header with the Next Hop Address.
    - Header — To
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Auto
2. Topology Hiding will replace the **To** header with the Next Hop Address/Domain from the Routing profile.
    - Header — To
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Next Hop
3. Topology Hiding will replace the **To** header with the Destination IP from the SIP Message.
    - Header — To
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Destination IP
4. Topology Hiding will replace the **To** header with the Signaling Interface IP/Domain
    - Header — To
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Signaling Interface
5. Topology Hiding will replace the **To** header with the Overwrite Value
    - Header — To
    - Criteria — IP/Domain or IP or Domain

- Replace Action — Overwrite

Example



Edit Topology Hiding Profile

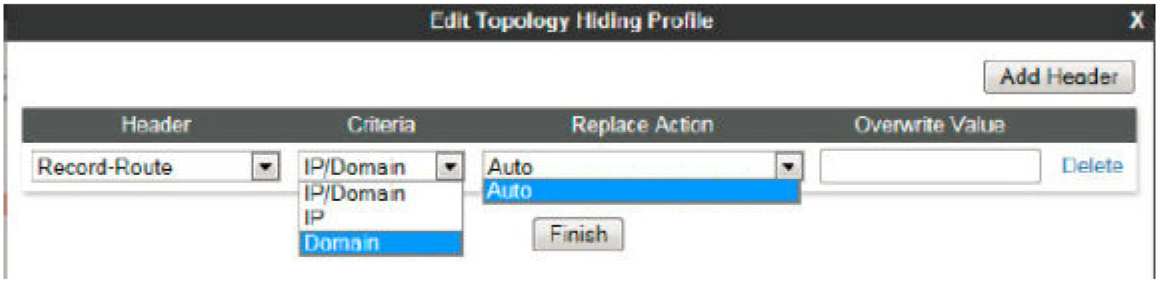
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Auto		Delete

Topology Hiding examples for Record-Route header

Topology Hiding will take and store the IP/Domain from the outbound message **Record-Route** header and then remove the **Record-Route** header from the outbound message. When the inbound message is received, Topology Hiding will put the stored IP/Domain in a **Record-Route** header and add the header to the inbound message.

- Header — Record-Route
- Criteria — IP/Domain or IP or Domain
- Replace Action — Auto

Example



Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete

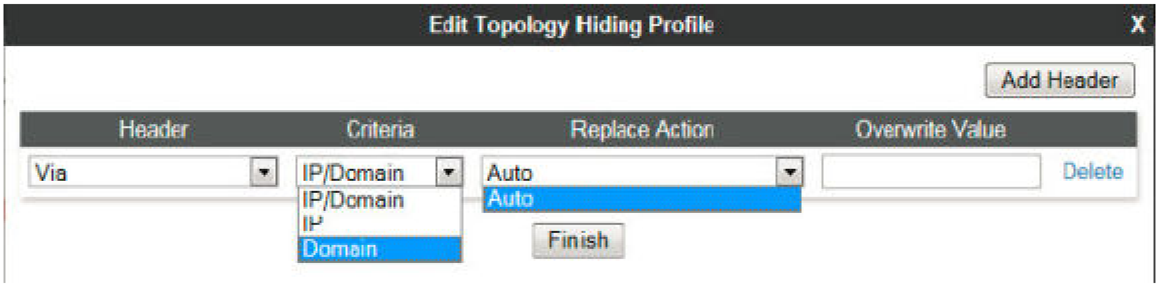
Topology Hiding examples for Via header

Topology Hiding will take and store the IP/Domain from the outbound message **Via** header and then remove the **Via** header. When the inbound message is received, Topology Hiding will put the stored IP/Domain in a **Via** header and add the header to the inbound message.

- Header — Via

- Criteria — IP/Domain or IP or Domain
- Replace Action — Auto

Example



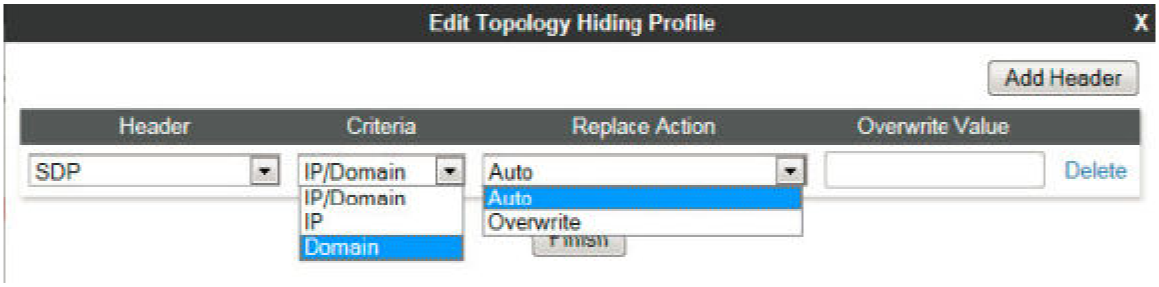
Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete

Topology Hiding examples for SDP header

1. Topology Hiding will replace the SDP message IP/Domain with the Media Interface IP/Domain.
    - Header — SDP
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Auto
2. Topology Hiding will replace the SDP message IP/Domain with the Overwrite Value.
    - Header — SDP
    - Criteria — IP/Domain or IP or Domain
    - Replace Action — Overwrite

Example



Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
SDP	IP/Domain	Auto		Delete

Chapter 8: Network Configuration

Overview

The Avaya SBCE Control Center allows you to perform a number of network-specific configuration and management functions. These include the ability to:

- Manage SIP server configurations
- Manage interworking profiles
- Manage network configurations and custom routes
- Manage Transport Layer Security (TLS) parameters

The procedures required to perform these functions are contained in the following sections.

SIP Server Configuration Management

Configurations for SIP call servers (trunk, proxy, etc.) can be centrally managed from the *Server Configuration SIP* feature of the SBCE security device. This feature allows you to define a number of different server profiles for use in a variety of deployments, security profiles, and company policies. Existing server profiles can be viewed and new policies added, cloned, edited, renamed, and deleted. The procedures for performing these operations are described in the following sections.

SIP Server Configuration Profile Management

Use the following procedures to manage SIP server configuration profiles.

Viewing a SIP Server profile

About this task

Use the following procedure to view SIP Server profiles.

Procedure

1. Login to the Avaya SBCE Control Center as the *Admin*.
2. Select the *Server Configuration* function of the *Global Profiles* feature from the Task Pane.
   The Server Configuration screen is displayed, containing a list of available Server Configuration profiles in the Application Panel.

Adding a new SIP Server profile

About this task

Use the following procedure to add a new SIP Server profile.

Procedure

1. Select **Add**.
   The Add Server Configuration Profile pop-up window (Figure 8–2) is displayed.
2. Enter a name for the new profile and click **Next**.
   The Add Server Configuration Profile – General pop-up window (Figure 8–3) is displayed.
3. In the General pop-up window (Figure 8–3), enter the requested information into the appropriate fields.
   Selecting **Cancel** clears the fields and closes the pop-up window. See the Add Server Configuration Profile General Popup Window Field Descriptions on page 283 for more information.
4. Select **Next**.
   The Add Server Configuration Profile – Authentication pop-up window (Figure 8–4) is displayed.
5. Enter the requested information into the appropriate fields.
   Selecting **Cancel** clears the fields and closes the pop-up window. See the Add Server Configuration Profile Authentication Pop-up Window Field Descriptions on page 284 for more information.
6. Select **Next**.
   The Add Server Configuration Profile – Heartbeat pop-up window (Figure 8–5) is displayed.
7. Enter the requested information into the appropriate fields.
   Selecting **Cancel** clears the fields and closes the pop-up window. See the Add Server Configuration Profile Heartbeat Pop-up Window Field Descriptions on page 284 for more information.

8. Select **Next**.
   The Add Server Configuration profile – Advanced pop-up window (Figure 8–6) is displayed.
9. Enter the requested information into the appropriate fields.
   Selecting **Cancel** clears the fields and closes the pop-up window. See the Add Server Configuration Profile Advanced Pop-up Window Field Descriptions on page 285 for more information.

   Note:

   When the Enable DoS Protection checkbox is checked in the previous screen, a second Add Server Configuration Profile – Heartbeat pop-up screen is displayed, prompting for the number of users on this Call Server.
10. Select **Next**.
    An updated Server Configuration screen (Figure 8–7) is displayed.

Add Server Configuration profile – General pop-up window field descriptions

Use these field descriptions.

Field	Description
Server Type	Pull-down menu from which you select the type of SIP server for which this profile is being defined. Available selections are: **Trunk Server**, **Call Server**, **Proxy Server**, **Registrar Server**, **MWI Server**, **Presence Server**, **Music Server**, and **Conference Server**.
IP Addresses/Supported FQDNs	The IP address or Fully-Qualified Domain Name (FQDN) of the SIP server. You can add multiple IPs and FQDNs, separated by commas.
Supported Transports	Checkboxes indicating which type(s) of transport protocols are supported by the SIP server. Available selections are: **TCP**, **UDP**, and **TLS**. Clicking the checkbox indicates that protocol is supported by the server and the corresponding port field is then activated.

Field	Description
TCP Port	The port assignment for TCP traffic.
UDP Port	The port assignment for UDP traffic.
TLS Port	The port assignment for TLS traffic.

Add Server Configuration profile – Authentication pop-up window field descriptions

Use these field descriptions.

Field	Description
Enable Authentication	Checkbox indicating whether or not the SIP server requires authentication. Checking this box indicates authentication is required and the remaining fields are activated. An empty checkbox 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	

Add Server Configuration profile – Heartbeat pop-up window field descriptions

Use these field descriptions

Field	Description
Enable Heartbeat	Checkbox indicating whether or not a synchronization signal (heartbeat) will be established between the SBCE security device and the SIP server.

Field	Description
	Checking this box indicates a heartbeat will be established and maintained and the remaining fields are activated. An empty checkbox indicates no heartbeat will be maintained and the remaining fields remain inactivated.
Method	Drop-down menu from which you determine the manner in which the heartbeat will be maintained. Available selections are: **Ping** , **Register**, and **Options**.
Frequency	The frequency with which the heartbeat signal will be sent.
From URI	The source of the heartbeat signal.
To URI	The destination of the heartbeat signal.

Add Server Configuration profile – Advanced pop-up window field descriptions

Use these field descriptions.

Field	Description
Enable DoS Protection	Checkbox indicating whether or not DoS protection will be enabled for this SIP server. Checking this box indicates DoS protection will be enabled for this server. An empty checkbox indicates no DoS protection will be enabled for this SIP server.
Enable Grooming	Checkbox indicating whether or not the same connection will be used for the same subscriber or port.
Interworking Profile	Drop-down menu from which you can select the Interworking profile to be used for this SIP server.
TLS Client Profile	Drop-down menu from which you can select the TLS Client profile to be used for this SIP server.

Field	Description
TCP Connection Type	Manner in which TCP connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**. **Note:** This field will only be displayed and configurable if a respective "TCP Port" has been configured for this SIP server.
UDP Connection Type	Manner in which UDP connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**. **Note:** This field will only be displayed and configurable if a respective "UDP Port" has been configured for this SIP server.
TLS Connection Type	Manner in which TLS connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**. **Note:** This field will only be displayed and configurable if a respective "TLS Port" has been configured for this SIP server.

Editing a SIP Server profile

About this task

Use the following procedure to edit a SIP server profile.

Note:

SIP server profiles are edited by selecting the desired parameters tab (General, Authentication, Heartbeat, and Advanced, and then changing the information contained on the screen displayed.

If the **Enable DoS Protection** checkbox, there will be two additional parameters tabs, **DoS Whitelist** and **DoS Protection**.

Procedure

1. In the Application Pane, select the server profile you want to edit.
2. In the Content Area, select the tab whose parameters you want to edit.
3. Click the **Edit** button at the bottom of the selected tab screen.

As an example, if the `Config_Server_2` profile is selected and it is **Advanced** tab is selected prior to clicking on the **Edit** button, a Server Configuration Profile – Advanced Edit pop-up window is displayed.

4. Edit the desired fields, and click **Finish**.
   Your changes are saved and the Server Configuration screen is re-displayed.

Editing the DoS Whitelist Parameter tab

Editing the **DoS Whitelist Parameter** tab entails either adding or deleting URI/Domain information to and from the DoS Whitelist. Each of these procedures is described below.

Note:

In order for the **DoS Whitelist Parameter** tab to be displayed, as described in Editing the DoS Protection Parameter Tab on page 288, the **Enable DoS Protection** checkbox (see Figure 8–6) must be checked in Step 9 of the procedure described in Adding a new SIP Server Profile on page 282.

This can also be done later by editing the **Advanced** tab, as described in Editing a SIP Server Profile on page 286 and illustrated (Figure 8–10) below.

Adding a URI or Domain to the DoS Whitelist

Procedure

1. In the Content Area, select the **DoS Whitelist Parameter** tab.
2. Click **Add**.
   The Add Whitelist URI pop-up window is displayed (Figure 8–11).
3. Enter the **URI / Domain** into the field provided as shown in the example and click **Finish**.
   The URI/Domain is added to the Whitelist (Figure 8–12).

Deleting a URI or Domain from the DoS Whitelist

Procedure

1. In the Content Area, select the **Delete** option corresponding to the URI/Domain you want to delete.
2. A Delete Confirmation pop-up window, similar to that shown in Figure 8–13 will be displayed.
3. Click **OK**.
   The URI/Domain is deleted and the **DoS Whitelist** tab is re-displayed (Figure 8–14), showing that the URI/Domain (Avaya.com) has been removed.

Editing the DoS Protection parameter tab

Editing the **DoS Protection** parameter tab only allows you to manage certain parameters for a specific set of SIP services and methods. The procedure to these parameters is contained below.

✱ **Note:**

In order for the **DoS Protection** parameter tab to be displayed, as described below, the **Enable DoS Protection** checkbox must have been checked during the procedure described in the section Adding a new SIP Server profile.

This can be done later by editing the **Advanced** tab, as described in the section Editing a SIP Server profile.

Procedure

1. In the Content Area, select the **DoS Protection** parameter tab.
2. Click the **Edit** option corresponding to the SIP service or method you want to edit.
   The corresponding Edit Server DoS pop-up window is displayed for the **Presence Updates** parameter.
3. Edit the desired fields and click **Finish**.
   Your changes are saved and the DoS Protection screen re-displayed.

Cloning an existing SIP Server profile

About this task

Use the following procedure to clone (make an exact copy of) an existing SIP Server profile.

Procedure

1. In the Application Pane, select the server profile you want to clone (Figure 8–17).
2. In the Content Area, click **Clone**.
   The Add Server Configuration Profile pop-up window is displayed (Figure 8–18).
3. Enter a new name for the cloned profile and click **Finish**.
   The profile is copied, renamed, and saved and the Server Configuration screen is re-displayed (Figure 8–19).

Renaming an existing SIP Server profile

About this task

Use the following procedure to rename an existing SIP Server profile.

Procedure

1. In the Application Pane, select the server profile you want to rename.
2. In the Content Area, click **Rename Profile**.
   The Rename Server Configuration Profile pop-up window is displayed (Figure 8–20).
3. Enter a new name for the profile and click **Finish**.
   The profile is renamed and the Server Configuration screen is re-displayed (Figure 8–21).

Deleting an existing SIP Server profile

About this task

Use the following procedure to delete an existing SIP Server profile.

Procedure

1. In the Application Pane, select the server profile you want to delete, as shown in Figure 8–22.
2. In the Content Area, click **Delete**.
   A Delete Confirmation pop-up window is displayed.
3. Click **OK**.
   The SIP Server profile is deleted and the Server Configuration screen is re-displayed

Server Interworking

The *Server Interworking* function of the Global Profiles feature allows you to set certain parameters to make the SBCE security device function in an enterprise VoIP network using different implementation of the SIP protocol.

Viewing existing Server Interworking profiles

About this task

Use the following procedure to view existing interworking profiles.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Server Interworking** function of the **Global Profiles** feature from the Task Pane.
   The Interworking screen is displayed, containing a list of available interworking profiles in the Application Pane.

Adding a new Interworking profile

About this task

Use the following procedure to add a new interworking profile.

Procedure

1. From the Application Pane, click **Add**.
   The Interworking Profile pop-up window is displayed (Figure 8–26).
2. Enter a name for the new profile and click **Next**.
   The Interworking Profile – General pop-up window is displayed (Figure 8–27).
3. Enter the requested information into the appropriate fields (Add Interworking Profile General Pop-up Window Field Descriptions on page 291).
   Selecting **Cancel** clears the fields and closes the pop-up window.
4. Select **Next**.
   The Interworking Profile – Privacy pop-window is displayed (Figure 8–28).
5. Enter the requested information into the appropriate fields (Add Interworking Profile Privacy Pop-up Window Field Descriptions on page 293).
   Selecting **Cancel** clears the fields and closes the pop-up window.
6. Select **Next**.
   The Interworking Profile – SIP Timers pop-window is displayed (Figure 8–29).
7. Enter the requested information into the appropriate fields (Add Interworking Profile SIP Timers Pop-up Window Field Descriptions on page 293).
   Selecting **Cancel** clears the fields and closes the pop-up window.
8. Select **Next**.
   The Interworking Profile advanced settings pop-window is displayed (Figure 8–30).
9. Enter the requested information into the appropriate fields (Add Interworking Profile Advanced Settings Pop-up Window Field Descriptions on page 294).
   Selecting **Cancel** clears the fields and closes the pop-up window.
10. Select **Finish**.
    The new Server Configuration profile is added and the Server Configuration screen is re-displayed. pop-window is displayed (Figure 8–31).

Add Interworking Profile – General pop-up window field descriptions

Field	Description
Hold Support	The standard to be used to provide HOLD support. Available selections are: **None**, **RFC 2543**, and **RFC 3264**.

Field	Description
180 Handling	Radio buttons allowing you to determine how 180 Ringing messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
181 Handling	Radio buttons allowing you to determine how *181 Call is being Forwarded* messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
182 Handling	Radio buttons allowing you to determine how *182 Queued* messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
183 Handling	Radio buttons allowing you to determine how *183 Session Progress* messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
Refer Handling	Checkbox indicating whether or not REFER requests will be handled by the SBCE security device.
3xx Handling	Checkbox indicating whether or not the SBCE security device will handle *3xx Redirection Response* messages.
Diversion Header Support	Checkbox indicating whether or not Diversion Headers will be supported by the SBCE security device.
Delayed SDP Handling	Checkbox indicating whether or not delayed SDP packets will be processed by the SBCE security device.
T.38 Support	Checkbox indicating whether or not the T.38 FAX Relay standard will be supported by the SBCE security device.
URI Scheme	The URI scheme to be used by the SBCE security device. Available selections are: **SIP**, **TEL**, and **ANY**.
Via Header Format	The Via Header Format to be used by the SBCE security device. Available selections are: **RFC3261** and **RFC2543**

Add Interworking Profile – Privacy pop-up window field descriptions

Field	Description
Privacy	
Privacy Enabled	Checkbox indicating whether or not privacy will be used between the SBCE security device and the SIP server.
User Name	User Name to be used for privacy authentication.
P-Asserted-Identity	Checkbox indicating that the SBCE will rewrite the FROM header in a trusted SIP message with the P-Asserted-ID. This is used for maintaining privacy for the From header. Trunk servers usually Accept SIP INVITE with P-asserted ID. For some Trunk servers, SBCE will insert this header from the From header, insert it in P-asserted ID and change From as Anonymous user, and send out the request.
P-Preferred-Identity	Checkbox indicating that the SBCE will use the P-Preferred-ID during the private sessions.
Privacy Header	The Privacy Header to be used during privacy sessions.
DTMF	
DTMF Support	Radio buttons indicating the type of DTMF support. Available selections are: **None**, **SIP NOTIFY**, and **SIP INFO**.

Add Interworking Profile – SIP Timers pop-up window field descriptions

Field	Description

SIP Timer	
Min-SE	The minimum value (in seconds) 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.
Init Timer	Initial request retransmission interval (in milliseconds). This is the initial SIP request retransmission interval. It corresponds to Timer T1 in RFC 3261.This timer is used when sending request over UDP.
Max Timer	The maximum retransmission interval for non-INVITE requests (in milliseconds). This is the maximum retransmission interval for non-INVITE requests. It corresponds to Timer T2 in RFC 3261.
Trans Expire	Value of the Transaction Expiration timer (in seconds).
Invite Expire	The transaction expiration time for an INVITE transaction after a provisional response has been received (in seconds).
Transport Timers	
TCP Inactive Timer	The maximum amount of inactivity allowed to lapse (in seconds) before the TCP connection is terminated.

Add Interworking Profile – Advanced Settings pop-up window field descriptions

Field	Description
Record Routes	Radio buttons which direct the SBCE security device to record route information. Available selections are: **None**, **Single Side**, and **Both Sides**.
Topology Hiding: Change Call-ID	Checkbox which directs the SBCE security device to change the **Call-ID** field in the SIP message header.
Call-Info NAT	Checkbox indicating that the **Call-Info** field should be changed by the SBCE security device to accommodate NAT functionality.

Field	Description
Change Max Forwards	Checkbox which directs the SBCE security device to change the Max-Forward Header field in the SIP Message header.
Include Endpoint IP for Context Lookup	Checkbox which directs the SBCE security device to use end point ip while looking for SBCE internal sip context
OCS Extensions	Checkbox which directs the SBCE security device to use OCS related functionality on OCS environment
Avaya Extensions	Checkbox which directs the SBCE security device to use Avaya related functionality on Avaya environment
Nortel Extensions	Checkbox which directs the SBCE security device to use Nortel related functionality on Nortel environment
Diversion Manipulation	Checkbox which directs the SBCE security device to copy SIP Diversion header from 3xx message to Sip Request message while 3xx handling will be enabled on SBCE security device
Diversion Header URI	Checkbox which directs the SBCE security device to add SIP Diversion header on the Sip Invite message
Metaswitch Extensions	Checkbox which directs the SBCE security device to use Metaswitch related functionality on Metaswitch environment
Reset on Talk Spurt	Checkbox which directs the SBCE security device to reset rtp flow on talk spurt
Reset SRTP Context on Session Refresh	Checkbox which directs the SBCE security device to reset media flow while session refresh scenario
Has Remote SBCE	Checkbox which directs the SBCE security device to use far-end firewall functionality
Route Response on Via Port	Checkbox which directs the SBCE security device to use SIP Via header port to route response
Cisco Extensions	Checkbox which directs the SBCE security device to use Cisco related functionality on Cisco environment

Existing Server Interworking profile settings

Interworking profiles have their parameters grouped across five tab displays: **General**, **Timers**, **URI Manipulation**, **Header Manipulation**, and **Advanced**, all of which can be selected and easily edited. Editing the contents of the **General**, **Timers**, and **Advanced** tabs is different than how the contents of the **URI Manipulation** and **Header Manipulation** tabs are edited.

Refer to the procedure Editing the General, Timers, and Advanced Parameter Tabs for editing the **General**, **Timers**, and **Advanced** tabs.

Refer to the procedure Editing the URI Manipulation and Header Manipulation Parameter Tabs for editing the **URI Manipulation** and **Header Manipulation** tabs.

Editing the General, Timers, and Advanced parameter tabs

About this task

Use the following procedure to edit the contents of the General, Timers, and Advanced parameter tabs.

Note:

For the purposes of this procedure, the General parameters tab is as an example. The editing procedure is the same for the Timers and Advanced parameter tabs.

Procedure

1. In the Application Pane, select the Interworking profile you want to edit.
2. In the Content Area, select the parameter tab you want to edit (General, Timers, or Advanced).
   The parameters for that tab are displayed in the Content Area.
3. In the Content Area, click **Edit**.
   The corresponding Editing Profile pop-up window is displayed.
4. Edit the desired fields and click **Finish**.
   Your changes are saved and the updated Interworking screen is re-displayed).

URI Manipulation and Header Manipulation parameter tabs

In addition to being added and edited, the contents of the **URI Manipulation** and **Header Manipulation** parameter tabs can also be deleted. Each of these procedures is provided in the following sections.

Adding a new Regex expression

Procedure

1. In the Content Area, click the URI Manipulation tab.
   The existing Regex entries are displayed.
2. Click **Add**.
   The Add Rule pop-up window is displayed (Figure 8–35).
3. Enter the requested information into the appropriate fields (Add Regex Expression Pop-up Window Field Descriptions on page 297).
   Selecting **Cancel** clears the fields and closes the pop-up window.
4. Click **Finish**.
   The new Regex expression is added to the Content Area and the URI Manipulation screen is re-displayed (Figure 8–36).

Add Regex expression pop-up window field descriptions

Field	Description
User Regex	The Regex rule to be used to match the **User** field in the SIP message.
Domain Regex	The Regex rule to be used to match the **Domain** field in the SIP message.
User Action	The action to be taken by the SBCE security device if a User Regex match is found. Available selections are contained in a drop-down menu.

Field	Description
User Values	The values to be used in the manner directed by the **User Action** field.
Domain Action	The action to be taken by the SBCE security device if a Domain Regex match is found. Available selections are contained in a drop-down menu.
Domain Values	The values to be used in the manner directed by the **Domain Action** field.

Editing an existing Regex expression

Procedure

1. In the Content Area, click the URI Manipulation tab.
   The existing Regex entries are displayed.
2. Click the **Edit** option corresponding to the Regex expression you want to edit.
   The Edit Regex pop-up window is displayed (Figure 8–37).
3. Edit the desired fields and click **Finish**.
   The changes to the Regex expression are saved and the URI Manipulation screen is re-displayed.

Deleting an existing Regex expression

Procedure

1. In the Content Area, click the URI Manipulation tab.
   The existing Regex entries are displayed.
2. Click the **Delete** option corresponding to the Regex expression you want to delete.
   A Delete Confirmation pop-up window is displayed (Figure 8–38).
3. Click **OK**.
   The Regex expression is deleted.

Adding new Header Manipulation parameters

Procedure

1. In the Content Area, click the Header Manipulation tab.
   The existing parameter entries are displayed.
2. Click **Add**.
   The Add Rule pop-up window is displayed (Figure 8–39).
3. Enter the requested information into the appropriate fields (Add Header Manipulation Parameter Pop-up Window Field Descriptions on page 299).
   Selecting **Cancel** clears the fields and closes the pop-up window.
4. Click **Finish**.
   The new header manipulation parameters are added to the Content Area and the Header Manipulation screen is re-displayed (Figure 8–40).

Add Header Manipulation parameter pop-up window field descriptions

Field	Description
Header	The SIP header field to be manipulated. Available selections are contained in a drop-down menu.
Action	The action to be performed. Available selections are contained in a drop-down menu.
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.

Editing Header Manipulation parameters

Procedure

1. In the Content Area, click the Header Manipulation tab.
   The existing parameter entries are displayed.
2. Click the **Edit** option corresponding to the parameters you want to edit.
   The Edit Parameter pop-up window is displayed (Figure 8–41).
3. Edit the desired fields according to the information contained in Add Header Manipulation Parameter Pop-up Window Field Descriptions on page 299 and click **Finish**.
   The changes to the **Header Manipulation** parameters are saved and the Header Manipulation screen is re-displayed (Figure 8–42).

Deleting Header Manipulation parameters

Procedure

1. In the Content Area, click the Header Manipulation tab.
   The existing parameter entries are displayed.
2. Click the **Delete** option corresponding to the parameters you want to delete.
   A Delete Confirmation pop-up window is displayed (Figure 8–43).
3. Click **OK**.
   The header manipulation parameters are deleted.

Cloning an existing Interworking profile

About this task

Use the following procedure to clone (make an exact copy of) an existing interworking profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.

2. Select the *Interworking* function of the Global Profiles feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to clone.
4. In the Content Area, click **Clone**.
   The Clone Profile pop-up window is displayed (Figure 8–44).
5. Enter a name for the cloned profile and click **Finish**.
   The profile is copied, renamed, and saved and the Interworking screen is re-displayed (Figure 8–45).

Renaming an existing Interworking profile

About this task

Use the following procedure to rename an existing interworking profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the *Interworking* function of the Global Profiles feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to rename.
4. In the Content Area, click **Rename Profile**.
   The Rename Profile pop-up window is displayed (Figure 8–46).
5. Enter a new name for profile and click **Finish**.
   The profile is renamed and the Interworking screen is re-displayed (Figure 8–46).

Deleting an existing Interworking profile

About this task

Use the following procedure to delete an existing interworking profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the *Interworking* function of the Global Profiles feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to delete.
4. In the Content Area, click **Delete**.

The Delete Confirmation pop-up window is displayed (Figure 8–48).

SBCE Network Interfaces Management

The *Network Management* function of the Device Specific Settings feature allows you to configure the network interface settings affecting the SBCE security devices deployed throughout the enterprise. Rather than following the network's interpretation of what the 'best path' to reach a destination is, source-based routing essentially follows the path specified in the IP header. One benefit of source-based routing is that it allows for multiple gateways but at the expense of not supporting custom routes.

Note:

Current SBC configuration capabilities allow for the configuration of only one input interface and one output interface.

Note:

Source-based routing essentially over-rides normal Avaya SBCE routing protocols, thus requiring an intimate knowledge of the VoIP network topology to be effective.

When an SBCE security device is installed using the System Management feature (see Chapter 4. Device Configuration), certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.

Use the following procedure to manage Avaya SBCE network interface parameters.

Viewing Network Interface Settings

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Network Management** function of the Device Specific Settings feature from the Task Pane.
   The Network Management screen is displayed.

Editing Network Management parameters

Procedure

1. Login to the SBCE Control Center as the `Admin`.
2. Select the **Network Management** function of the **Device Specific Settings** feature from the Task Pane.
3. In the Application Pane, select the SBCE security device whose network parameters you want to edit.
4. In the Content Area, select the parameter tab (**Network Configuration** or **Interface Configuration**) that you want to edit (Figure 8–50).
5. Edit the various fields using the procedures contained in the following sections.

Example

Next steps

Edit the Network Configuration tab

Use the procedures in the following sections to edit the Network Configuration tab.

Adding a New Network Interface

Procedure

1. In the Content Area on the **Network Configuration** tab, click the **Add** button (Figure 8–50).
   A blank IP address/public IP information line is added to the bottom of the IP Address display area (Figure 8–51).
2. Enter the requested information into the appropriate fields in the new information line according to the information contained in SBCE Interface Addressing Field Descriptions on page 304.

   Be sure to provide the necessary Netmask information, if the **Netmask** field is activated.

3. After entering the appropriate field information, select **Save** to save and submit the updates (Figure 8–52).

SBCE Interface Addressing field descriptions

Field	Description
Netmask	The subnet mask to which the SBCE security device is assigned.
IP Address	The IP address of the physical SBCE interface.
Public IP	The publically-reachable IP address of the physical SBCE interface.
Interface	A drop-down menu from which you select the specific physical interface of the SBCE security device being defined.

Editing an existing Network Interface

Procedure

1. While referring to the field descriptions in SBCE Interface Addressing Field Descriptions on page 304, make the desired changes in the Content Area to the existing information in the **Netmask**, **IP Address**, **Public IP** and **Interface** fields.
2. Select **Save** to save and submit the updates.
   The IP and interface information is saved and the Network Configuration screen will be re-displayed with the updated information.

Deleting an existing Network Interface

Procedure

1. In the Avaya SBCE Control Center, click the **Delete** option (located on the right-hand edge of each information row) corresponding to the SBCE interface that you want to delete.
   A Delete Confirmation pop-up window is displayed asking you to confirm your selection (Figure 8–53).
2. Click **OK**.
   The interface is deleted and the Network Management screen will be re-displayed with the selected interface information removed.
3. Select **Save** to save and submit the updates.
   The IP and interface information is saved and the Network Configuration screen will be re-displayed with the updated information.

Editing the administrative state of the Interface Configuration

About this task

The administrative state of interface configurations can either be enabled or disabled. Use the following procedure to toggle the administrative state of an interface configuration.

Procedure

On the **Interface Configuration** tab in the Content Area, click the **Toggle** button that corresponds to the physical interface on the SBCE whose state you want to enable/ disable, and the Administrative Status of the interface is changed to the opposite state.

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. It enables clients to authenticate servers or, optionally, servers to authenticate clients. Avaya SBCE security products utilize TLS primarily to facilitate secure communications with remote users.

Managing TLS parameters consists of generating and installing a Certificate Signing Request (CSR), installing a Certificate Authority (CA) certificate, and installing the Certificate Revocation List (CRL). Once these procedures are completed, you must create a client profile and a server profile. The procedures required to perform these procedures are contained in the following sections.

Certificate Signing Request Management

This section provides procedures for creating Certificate Revocation Lists (CRLs) and for installing certificates, CA certificates, and CSRs.

Pre-installed Avaya Profiles and Certificates

Configuring Avaya SBCE deployments under TLS Management is very easy because the products have pre-installed default profiles and certificates.

Note:

If your configuration will not use the default profiles and certificates, and will be using a third-party certificate, follow the procedures in the next section, Installing Non-Avaya Certificates, and the sections which follow that provide procedures for manually configuring a TLS Client profile, TLS Server profile, and HTTPS profile.

Pre-installed Client Profiles

TLS Management → Client Profiles (Screen displayed)

AvayaSBCEClient (Profile displayed in Content Area)

Pre-installed Server Profiles

TLS Management → Server Profiles (Screen displayed)

AvayaSBCEServer (Profile displayed in Content Area)

AvayaHTTPSProxy (Profile displayed in Content Area)

Pre-installed Certificates

TLS Management → Certificates (Certificate displayed)

AvayaSBC.crt (Certificate displayed in Content Area)

Pre-installed CA Certificates

TLS Management → Certificates (Screen displayed)

AvayaSBCCA.crt (Certificate displayed in Content Area)

Installing Non-Avaya Certificates

About this task

Use the following procedures to install a non-Avaya built-in certificate.

Procedure

1. Login to theAvaya SBCE Control Center as the `Admin`.
2. Select the **Certificates** function of the TLS Management feature from the Task Pane to display the TLS Management Certificates screen.
3. The TLS Management Certificates screen contains three sections described in TLS Certificates Screen Field Descriptions on page 307: *Certificates*, *CA Certificates*, and *Certificate Revocation Lists (CRLs)*.

TLS Certificates Screen Field Descriptions

Field	Description
Certificates	Certificates are some Certificate Authority (CA) signed certificate or self-signed certificate. This is a certificate that will be incorporated into a server certificate profile and sent to clients to setup a TLS connection. **Note:** All certificates, certificate authorities, and certificate revocation lists uploaded to the EMS must be a valid X.509 certificate in the PEM format. Certificates not in this format may be converted using a proper SSL tool, such as the publicly available OpenSSL tool (https://www.openssl.org/).
CA Certificates	The unsigned public key certificates from a Certificate Authority (CA), which vouches for the correctness of the data contained in a

Field	Description
	certificate, and verifies the signature of the certificate.
Certificate Revocation Lists	The Certificate Revocation Lists (CRLs) which contain the serial numbers of CSRs which have been revoked, or are no longer valid, and should not be relied upon by any system subscriber.

Installing Certificate Option

Procedure

1. Select the **Install** button located in the upper-right-hand portion of the screen. The Install Certificate pop-up screen is displayed (Figure 8–56).
2. In the Install Certificate screen (Figure 8–56), select or enter the appropriate information. Install Certificate Pop-up Screen Field Descriptions on page 308 provides descriptions of the parameter fields. There are three options for type of certificate. The screen display changes with each option selection. In the example in Figure 8–56, the first option, **Certificate**, is selected.
3. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the *Certificate File* and *Trust Chain File*.
4. Choose one of the two **Key** options: **Use Existing Key** or **Upload Key File**.
5. Click the **Upload** button.

   Upon completing the procedure detailed above, continue with the procedure steps detailed in Upload Key File Option Uploading Key File Option – SBCE and EMS in Same Server Box on page 309 and Uploading Key File Option – SBCE and EMS in Separate Server Boxes on page 310.

Certificate Pop-up Screen Field Descriptions

Field	Description
Certificate Name	The name of the certificate you want to install. This field is optional, and if not specified will default to the filename of the uploaded

Field	Description
	certificate. Additionally, specifying this to be the same name as another certificate will overwrite the existing certificate with the one being uploaded.
Certificate File	Location of the certificate on your system. Use the **Browse** feature to locate the file, if necessary.
Trust Chain File	The trust chain file used to verify the authenticity of the certificate. Use the **Browse** feature to locate the file, if necessary.
Key	The private key you want to use. You may opt to either use the existing key or select a file containing another key. Use the **Browse** feature to locate the file, if necessary.
Key File	The **Key File Browse** button is displayed when the **Upload Key File** checkbox is selected. Use the **Browse** feature to locate the file, if necessary.

Uploading Key File Option – SBCE and EMS in same server box

Procedure

1. Initiate a secure shell (SSH) connection to the box.
2. Enter the following: `sudo su`.
3. Navigate to the key directory using the cd command as follows: `cd/usr/local/ipcs/cert/key`.
4. Run the following command without quotes: `enc_key “key file name” “passphrase”`

Uploading Key File Option – SBCE and EMS in separate server boxes

Procedure

1. Initiate a secure shell (SSH) connection to each SBCE box if there are multiple Avaya SBCE servers, and then repeat Steps 2 through 5 below.
2. Enter the following: `sudo su`
3. Enter the following: `clipcs`
4. Once the CLIPCS console has started, run the command: `certsync`
5. After the above certsync command completes, enter the following command: `certinstall “certificate name”`
6. When prompted, enter the `“passphrase”` .

   where “certificate name” is the file you browsed for in the Install Certificate pop-up screen, as described in Installing Certificate Option on page 308.

   Note:

   Upon completing the procedure steps detailed above in Installing Certificate Option on page 308, Uploading Key File Option – SBC and EMS in Same Server Box on page 309, and Uploading Key File Option – SBC and EMS in Separate Server Boxes on page 310 proceed to the subsections which appear later in “Creating a New Client Profile” and “Creating a New Server Profile.”

   If you are not using the preconfigured default Avaya profiles (i.e., AvayaSBCClient, AvayaSBCServer, and AvayaHTTPSProxy), you will be required to create new profiles for TLS.

   Create a new client profile by following the procedure in “Creating a New Client Profile.”

   Create a new server profile and a new HTTPS Server profile by following the procedure in “Creating a New Server.”

Extracting certificate and key from a PFX / 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:

Note: PFX is an older term that has been in most cases superceded by PKCS#12

Note:

Upon completing the extraction procedure detailed below, continue with the procedure steps detailed in Install Certificate OptionInstalling Certificate Option on page 308, Uploading Key File Option – SBCE and EMS in Same Server Box on page 309, and Uploading Key File Option – SBCE and EMS in Separate Server Boxes on page 310.

Procedure

1. Copy the keystore file to `/home/ipcs/` directory on the SBCE and run the commands in Step 2 and Step 3 to extract the certificate and key, respectively.
2. Command to extract the certificate from the keystore file: `openssl pkcs12 -in <filename>.pfx -out <filename>.crt -nokeys –clcerts`
3. Command to extract the key from the keystore file: `openssl pkcs12 -in <filename> -out <filename>.key -nocerts`

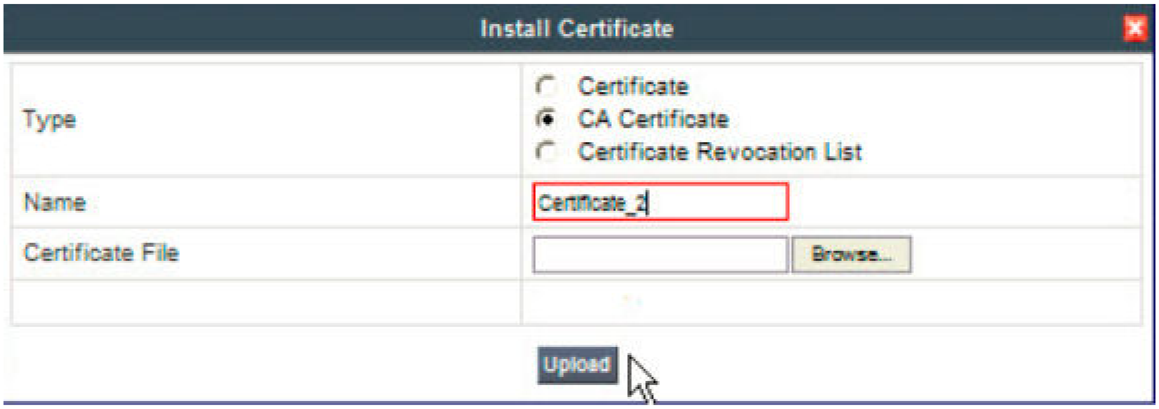
Installing CA Certificate Option

Procedure

1. In the Install Certificate screen, there are three options for type of certificate. The screen display changes with each option selection. In the example shown below, the middle option, **CA Certificate**, is selected.
2. Select or enter the appropriate information in the **Install CA Certificate** screen. The parameter field descriptions are provided in Install CA Certificate Screen Field Descriptions on page 312.
3. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the **Certificate File**.

4. Click the **Upload** button.

Example



Type: ○ Certificate ● CA Certificate ○ Certificate Revocation List

Name: Certificate_2

Certificate File:

Install CA Certificate screen field descriptions

Field	Description
Certificate Name	The name of the certificate you want to install.
Certificate File	Location of the certificate on your system. Use the **Browse** feature to locate the file, if necessary.

Installing Certificate Revocation List Option

Procedure

1. In the Install Certificate screen (Figure 8–56), there are three options for type of certificate. The screen display changes with each option selection. In the example below in Figure 8–58, the last option, **Certificate Revocation List**, is selected.
2. Select or enter the appropriate information in the Install Certificate Revocation List screen (Figure 8–58). The parameter field descriptions are provided in Install CRL Screen Field Descriptions on page 313
3. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the **Certificate File**.

4. Click the **Upload** button.

Install CRL Screen Field Descriptions

Field	Description
CRL Name	Name of the Certification Revocation List (CRL) file to be installed.
CRL File	Location on your system of the Certification Revocation List (CRL) file.

Creating a Certificate Signing Request

About this task

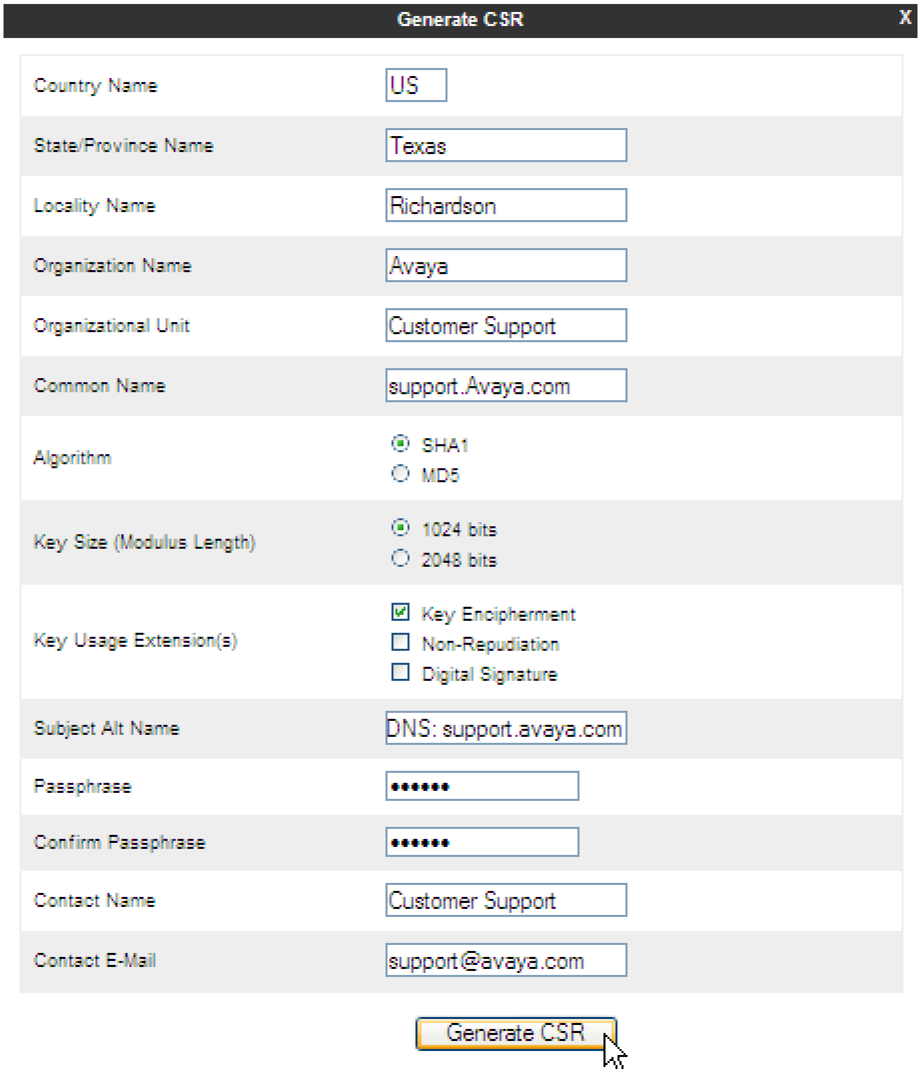
Use the following procedures to create a Certificate Signing Request (CSR).

Procedure

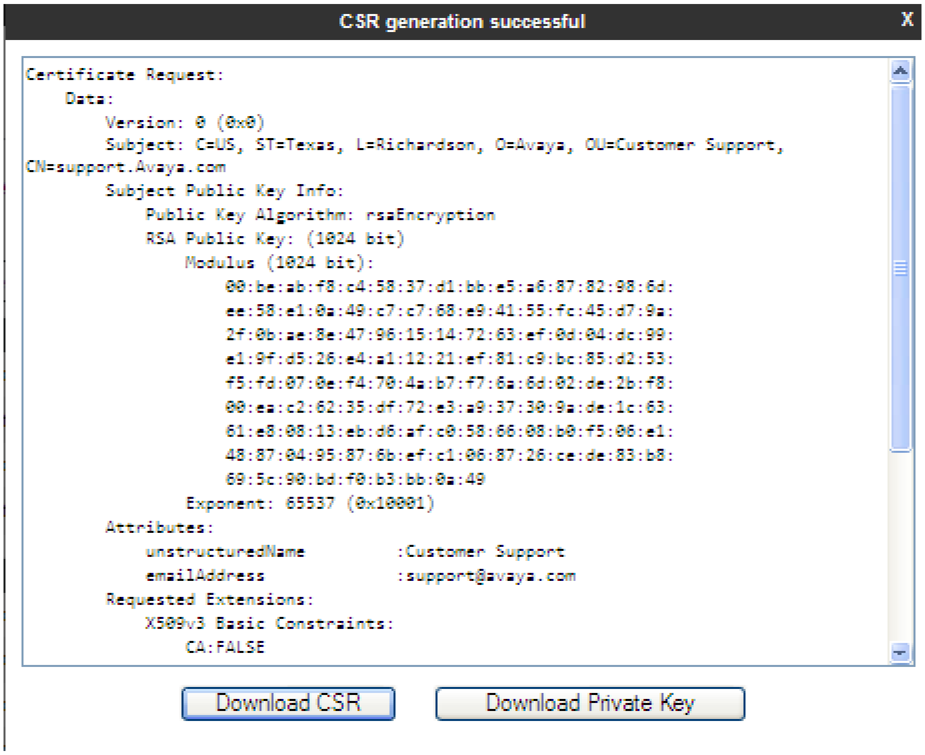
1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Certificates** function of the TLS Management feature from the Task Pane.
   The TLS Management: Certificates screen is displayed.
3. Select the **Generate CSR** button located in the upper-right-hand portion of the screen.
   The TLS Management Generate CSR pop-up screen is displayed.
4. Enter the appropriate information in the TLS Management Generate CSR screen and then click the **Generate CSR** button at the bottom of the screen to create the *Certificate Signing Request (CSR)* file. The parameter field descriptions are provided in TLS Management Generate CSR Screen Field Descriptions on page 315.

Examples are provided below of a completed TLS Management Generate CSR screen with parameters entered and the resulting display after clicking on the **Generate CSR** button.

Example



Country Name	US
State/Province Name	Texas
Locality Name	Richardson
Organization Name	Avaya
Organizational Unit	Customer Support
Common Name	support.Avaya.com
Algorithm	● SHA1 ○ MD5
Key Size (Modulus Length)	● 1024 bits ○ 2048 bits
Key Usage Extension(s)	☑ Key Encipherment □ Non-Repudiation □ Digital Signature
Subject Alt Name	DNS: support.avaya.com
Passphrase	••••••
Confirm Passphrase	••••••
Contact Name	Customer Support
Contact E-Mail	support@avaya.com



```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=Texas, L=Richardson, O=Avaya, OU=Customer Support,
CN=support.Avaya.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:be:ab:f8:c4:58:37:d1:bb:e5:a6:87:82:98:6d:
                    ee:58:e1:0a:49:c7:c7:68:e9:41:55:fc:45:d7:9a:
                    2f:0b:ae:8e:47:96:15:14:72:63:ef:0d:04:dc:99:
                    e1:9f:d5:26:e4:a1:12:21:ef:81:c9:bc:85:d2:53:
                    f5:fd:07:0e:f4:70:4a:b7:f7:6a:6d:02:de:2b:f8:
                    00:ea:c2:62:35:df:72:e3:a9:37:30:9a:de:1c:63:
                    61:e8:08:13:eb:d6:af:c0:58:66:08:b0:f5:06:e1:
                    48:87:04:95:87:6b:ef:c1:06:87:26:ce:de:83:b8:
                    69:5c:90:bd:f0:b3:bb:0a:49
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :Customer Support
            emailAddress             :support@avaya.com
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

TLS Management Generate CSR screen field descriptions

Field	Description
Country Name	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.
Algorithm	The hash algorithms (*MD5* or *SHA1*) to be used with the RSA signature algorithm.

Field	Description
	It is highly recommended that SHA1 is used over MD5.
Key Size (Modulus Length)	The certificate key length (*1024* or *2048*) in bits.
Key Usage Extension	The purpose for which the public key may be used: *Key Encipherment*, *Non-Repudiation*, *Digital Signature*.
Subject Alt Name	Optional text field which can be used to further identify this certificate.
Passphrase	Password used when encrypting the private key.
Repeat Passphrase	A verification field for the *Passphrase*.
Contact Name	Individual within the issuing organization acting as point-of-contact for issues relating to this certificate.
Contact E-mail	E-mail address of the *Contact*.

Client Profile Management

Use the following procedures to create, edit, and delete TLS client profiles.

Creating a new client profile

About this task

Use the following procedure to create a new TLS client profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Client Profiles** function of the TLS Management feature from the Task Pane.
   The Client Profiles screen is displayed.
3. Select **New Profile**.
   The **New TLS Client Profile** pop-up window is displayed.
4. Enter the requested information into the appropriate fields.

5. Select **Save**.
   The TLS client profile is installed and displayed.

TLS Client Profile pop-up screen field descriptions

Field	Description
TLS Profile	
Profile Name	Descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification Required	Checkbox indicating whether or not peer verification is required. 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	Certificates to be used for peer verification. Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. **Ctrl+Shift** will allow the user to drag to select multiple lines and **Ctrl** will allow clicking 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. Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. **Ctrl+Shift** will allow the user to drag to select multiple lines and **Ctrl** will allow clicking to toggle individual lines.
Verification Depth	Maximum depth used for the certificate chain verification.
Renegotiation Parameters	
Renegotiation Time (optional)	The amount of time after which the certificate is renegotiated.
Renegotiation Byte Count (optional)	The number of bytes after which the certificate is renegotiated.

Field	Description
Cipher Suite Options	
Cipher Suites	The level of security to be used for encrypting data. Available selections are: • All — Support all cipher suite options. • Strong Only — Encryption support that is strong enough for most business or government needs. For use within the United States only. • Export Only — The strongest level of encryption allowed by federal law for exportable products. • Null Only — Weakest level of encryption. Only used for debugging. • DH — Diffie-Hellman key exchange. • ADH — Authenticated Diffie-Hellman. • MD5 — Message Digest algorithm 5.

Editing a Client Profile

About this task

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

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Client Profiles** function of the TLS Management feature from the Task Pane.
   The Client Profiles screen is displayed (Figure 8–65).
3. From the Applications Pane, select client profile you want to edit.
   The configuration of the selected client profile is displayed in the Content Area.
4. From the Content Area, select **Edit**.
   The Edit TLS Client Profile pop-up window (Figure 8–66) is displayed.
5. Edit the desired fields and select Save to save your changes or **Cancel** to revert to the previous field values and close the window.

If necessary, refer back to TLS Client Profile Pop-up Screen Field Descriptions on page 317 for a description of the fields contained on the TLS Client Profile pop-up window.

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. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Client Profiles** function of the TLS Management feature from the Task Pane.
   The Client Profiles screen is displayed (Figure 8–65).
3. From the Applications Pane, select the client profile you want to delete.
4. From the Content Area, select **Delete**.
   A Delete Confirmation pop-up window similar to that shown in Figure 8–67 is displayed asking you to confirm your selection.
5. Select **OK**.
   The TLS client profile is deleted.

Server Profile Management

Use the following procedures to create, edit, and delete TLS server profiles.

Creating a new server profile

About this task

Use the following procedure to create a new TLS server profile.

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Server Profiles** function of the TLS Management feature from the Task Pane.
   The Server Profiles screen is displayed.
3. From the Applications Pane, select **Add**.
   The TLS Server Profile pop-up window is displayed.
4. Enter the requested information into the appropriate fields. New TLS Server Profile Pop-up Window Field Descriptions on page 320 provides a description of each of the fields.
5. Select **Save**.
   The TLS Server profile is created, installed, and listed in the Applications Pane with its configuration displayed in the Content Area.

New TLS Server Profile pop-up window field descriptions

Field	Description
TLS Profile	
Profile Name	Descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification Required	Checkbox indicating whether or not peer verification is required. If this box is checked, then peer verification is required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become active. If this box remains unchecked, then peer verification is not required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become inactive (grayed-out).

Field	Description
Peer Certificate Authorities	Certificates to be used for peer verification. Using **Ctrl+Shift**, any combination of selections can be made from this list.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. Using **Ctrl+Shift**, any combination of selections can be made from this list.
Verification Depth	Maximum depth used for the certificate chain verification.
Renegotiation Parameters	
Renegotiation Time (optional)	The amount of time after which the certificate is renegotiated.
Renegotiation Byte Count (optional)	The number of bytes after which the certificate is renegotiated.
Cipher Suite Options	
Cipher Suites	The level of security to be used for encrypting data. Available selections are: • All — Support all cipher suite options. • Strong Only — Encryption support that is strong enough for most business or government needs. For use within the United States only. • Export Only — The strongest level of encryption allowed by federal law for exportable products. • Null Only — Weakest level of encryption. Only used for debugging. • DH — Diffie-Hellman key exchange. • ADH — Authenticated Diffie-Hellman. • MD5 — Message Digest algorithm 5.

Editing a server profile

Procedure

1. Login to the Avaya SBCE Control Center as the `Admin`.

2. Select the **Server Profiles** function of the TLS Management feature from the Task Pane.
   The Server Profiles screen is displayed.
3. From the Applications Pane, select server profile you want to edit.
   The configuration of the selected server profile is displayed in the Content Area.
4. From the Content Area, select **Edit**.
   The Edit TLS Server Profile pop-up window (Figure 8–66) is displayed.
5. Edit the desired fields and select **Save** to save your changes or **Cancel** to revert to the previous field values and close the window.

   If necessary, refer back to New TLS Server Profile Pop-up Window Field Descriptions on page 320 for a description of the fields contained on the TLS Server Profile pop-up window.

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

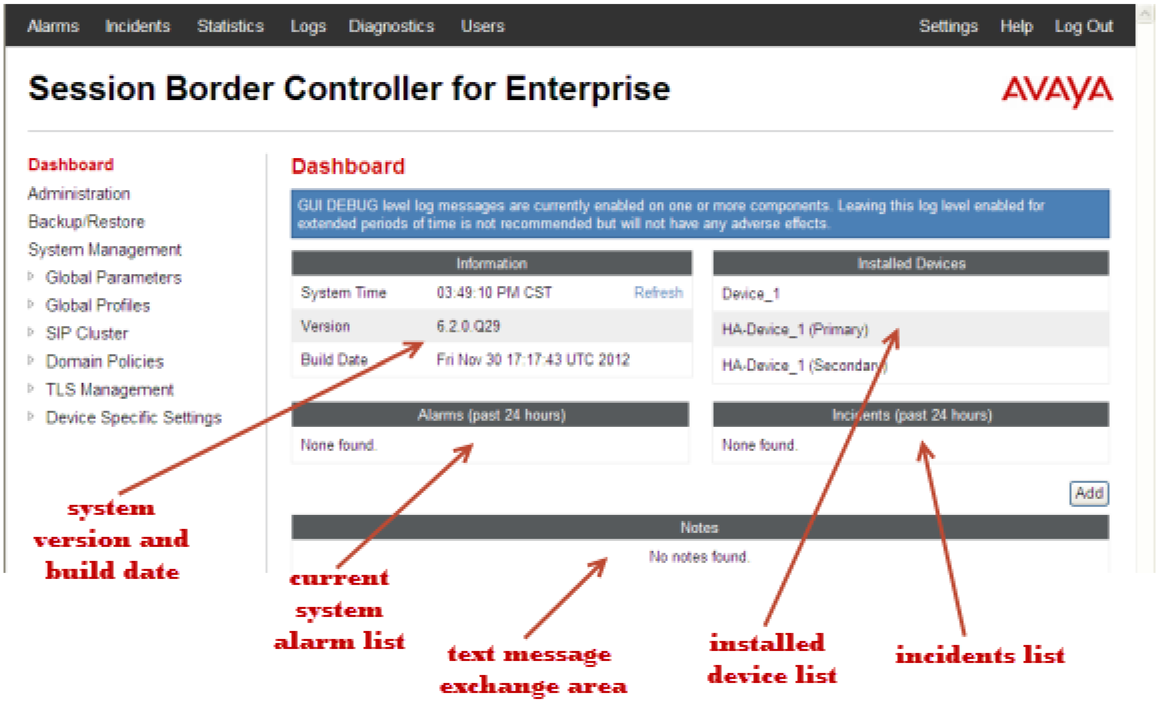
1. Login to the Avaya SBCE Control Center as the `Admin`.
2. Select the **Server Profiles** function of the TLS Management feature from the Task Pane.
   The Server Profiles screen is displayed.
3. From the Applications Pane, select the server profile you want to delete.
4. From the Content Area, select **Delete**.
   A Delete Confirmation pop-up window similar to that shown in Figure 8–71 is displayed asking you to confirm your selection.
5. Select **OK**.
   The TLS server profile is deleted.

Chapter 9: System Monitoring

Dashboard screen

The Dashboard screen is the top-level display screen which provides direct access to all the features, functions, and information available on the current release of the Avaya SBCE security system. From this screen you can display additional, separate, summary windows (Alarms, Incidents, Statistics, Logs, Diagnostics, and Users) which contain active, up-to-the-minute alarms, incident, statistical, log, diagnostic, and user information as well as review and exchange textual messages with other administrative user accounts.

The Content Area of the Dashboard screen contains various summary areas which display top-level, system-wide information such as which alarms and incidents are currently active, links to available Quick Links, a list of installed Avaya SBCE security devices, Avaya SBCE device deployment information, and an area for viewing and exchanging text messages with other administrators.



Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

Information		
System Time	03:49:10 PM CST	Refresh
Version	6.2.0.Q29	
Build Date	Fri Nov 30 17:17:43 UTC 2012	

Installed Devices
Device_1
HA-Device_1 (Primary)
HA-Device_1 (Secondary)

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Notes

No notes found.

system version and build date

current system alarm list

text message exchange area

installed device list

incidents list

Dashboard alarm and event reporting component descriptions on page 324

Dashboard Alarm and Event Reporting Component Descriptions

When creating a new session flow, refer to this table for information on the fields in the second Add Flow pop-up screen.

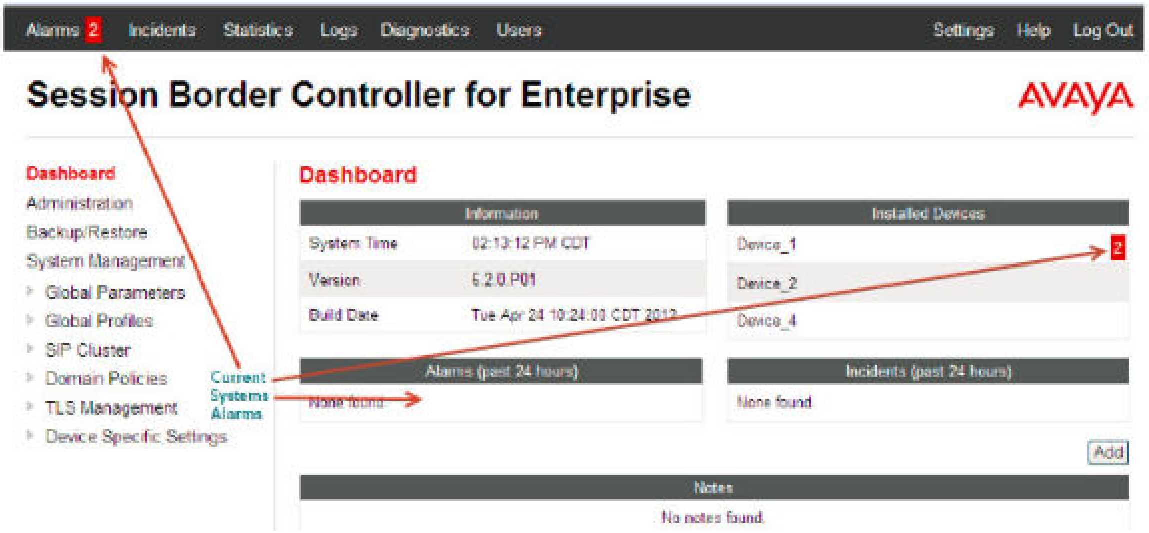
Dashboard Alarm and Event Reporting Component Descriptions

Component	Description
Dashboard	Provides a snapshot view of the Avaya SBCE Control Center and system status information.
Version	System software version.
Build Date	System software build date.
Installed Avaya SBCE Security Device List	A list of all Avaya SBCE security devices currently deployed throughout the network.
Text Message Exchange Area	User-editable text message exchange area.
Current Incidents List	A list of current incidents reported by the Avaya SBCE security devices to the Avaya SBCE Control Center (EMS).
Current System Alarm List	A list of current alarms reported by the Avaya SBCE security devices to the Avaya SBCE Control Center (EMS).

Managing system alarms

Current system alarms are reported to the Avaya SBCE Control Center and immediately displayed in two places: as a blinking red indicator on left side of the Tool Bar and as a corresponding text message in the Latest Alarms section.

These notifications provide the information necessary to clear the condition causing the alarm notification, after which time the alarm can be cleared from the display.



Information	
System Time	02:13:12 PM CDT
Version	5.2.0.P01
Build Date	Tue Apr 24 10:24:00 CDT 2012

Installed Devices	
Device_1	2
Device_2	
Device_4	

Alarms (past 24 hours)
None found

Incidents (past 24 hours)
None found

Notes
No notes found.

Viewing current system alarms

About this task

The Alarms screen provides a summary display of all currently active system alarms. If no alarms are active, this display screen is blank. The Alarms screen is normally only accessed 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Alarms** option from the Toolbar or click on the specific alarm you want to view from the **Latest Alarms** section of the dashboard screen..
   The alarms viewer screen is displayed.
3. Select the Avaya SBCE device for which you want alarms displayed.
   All currently active alarms for selected Avaya SBCE security device are displayed in the Content Area. For a brief description of each of the security reporting components of the Alarms screen, refer to Current alarms screen field descriptions on page 326.
4. Clear the alarm using the appropriate clearing event from the corresponding appendix located at the back of this manual:
5. Delete the cleared alarm using the procedure described in Deleting current system alarms on page 326.

Current alarms screen field descriptions

When creating a new session flow, refer to this table for information on the fields in the second Add Flow pop-up screen.

Current alarms screen field descriptions

Field	Description
Alarm Details	The specific / descriptive name of the active alarm.
State	Current state of the alarm: ON (The State field for any displayed alarm is always: ON)
Time	Date and time the alarm was generated.
Device	The Avaya SBCE device which generated the alarm.
Alarm ID	Sequential, numerical identifier of the alarm being reported.

Deleting current system alarms

About this task

Use the following procedure to delete current system alarms.

Note:

	Note: Alarms should only be deleted from the Alarms display after the condition which originally caused the alarm has been properly cleared by qualified personnel. Alarms can be cleared through two processes: 1. Once the failure condition is solved, an operator clears the alarm display manually depending on the alarm. 2. Once the failure condition is solved, no operator intervention is expected, and the alarm display clears automatically depending on the alarm.

Procedure

1. From the Alarms screen, select the **Clear** option corresponding to the alarm notification you want to delete.
   A delete confirmation pop-up screen is displayed.

2. Select**OK**.
   The alarm display is cleared.

Viewing current system incidents

About this task

In addition to viewing system alarms, you can view a complete descriptive list of all system incidents which have occurred since the last viewing period using the Incident screen. It shows the last five incidents at any point of time. This feature allows you to view system-wide incidents according to category (DoS, Policy, Scrubbing, etc.). When the Incident screen is open, all of the latest incident information will be available, and the operator can scroll through the incidents list while displaying 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Incidents** option from the Toolbar or click on the specific alarm you want to view from the **Latest Incidents** section of the dashboard screen..
   The incidents viewer screen is displayed.
3. Using the Avaya SBCE Device and Category fields located at the top of the Incidents screen, define a search filter to find and display the particular incidents you want to view. The Incident display will change to reflect the search criteria as soon as a selection has been made. Periodically select Refresh to refresh the display as ensure all the desired incidents are displayed. Select Clear Filters to set the Avaya SBCE Device and Category fields to All. This will cause all current Incidents to be displayed.

   Incidents category selections include:

   - All
   - Authentication
   - Black White List
   - DoS
   - High Availability
   - Media Anomaly Detection
   - Policy
   - Protocol Discrepancy

- RSA Authentication
- Scrubbing
- Spam
- TLS Certificate

Viewing system statistics

About this task

The Statistics screen provides a snap-shot display of certain cumulative, system-wide generic and SIP-specific operational information.

The various Statistics tabs (Calls, Policy, and Protocol) can be displayed whenever up-to-date statistical information is required.

Note:

Statistics information can only be viewed; they cannot be edited or deleted.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Statistics** option from the Toolbar.
   The statistics screen is displayed.
3. See the specific statistics tab you want to view. The contents of each of the selected tabs will be displayed.

Viewing system logs

About this task

The 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. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Logs** option from the Toolbar and select the System Logs menu option to display the Syslog Viewer.

The Syslog Viewer screen is displayed.

3. In the Query Options Start Date field and End Date field, You can 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 for 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/Time entry is not required when you enter a Start Date/Time.

4. In the Query Options Keyword field in the top-left portion of the Syslog Viewer, enter one or more words to define the limits of the log report and click on the Search button on the right-hand portion of the viewer.
   The report is run and a report output is displayed.

   Note:

   Keyword searches are case-insensitive and tokenized (each keyword term entered in the Keyword field will be searched for separately), but all keyword terms that are entered in the Keyword field must be found in a log line in order for the log line to be included and displayed within a report.

Viewing diagnostics results

About this task

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

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Diagnostics** option from the Toolbar.
   The diagnostics screen is displayed.
3. Click the **Full Diagnostics** tab.
4. Click the **Start Diagnostic**.
   The tests listed in the Task Description portion 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 particular test, the diagnostic will terminate and display the reason for the termination in the Status column.

5. Click one of the tabs to run and/or rerun a specific individual diagnostic test (i.e., Ping Test, Application, Protocol, Octeon PCF, Octeon TCP, Octeon TLS, Octeon Memory, or Octeon Ethernet) and view the results in the Content Area.

Viewing administrative users

About this task

The Users screen provides a summary of all active system administrative accounts currently logged into the Avaya SBCE Control Center.

Note:

Logged-in Users account information can only be viewed; it cannot be modified in any way. Use the following procedure to view which system administrative accounts are currently logged into the Avaya SBCE Control Center.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Users** option from the Toolbar.
   The users screen is displayed.

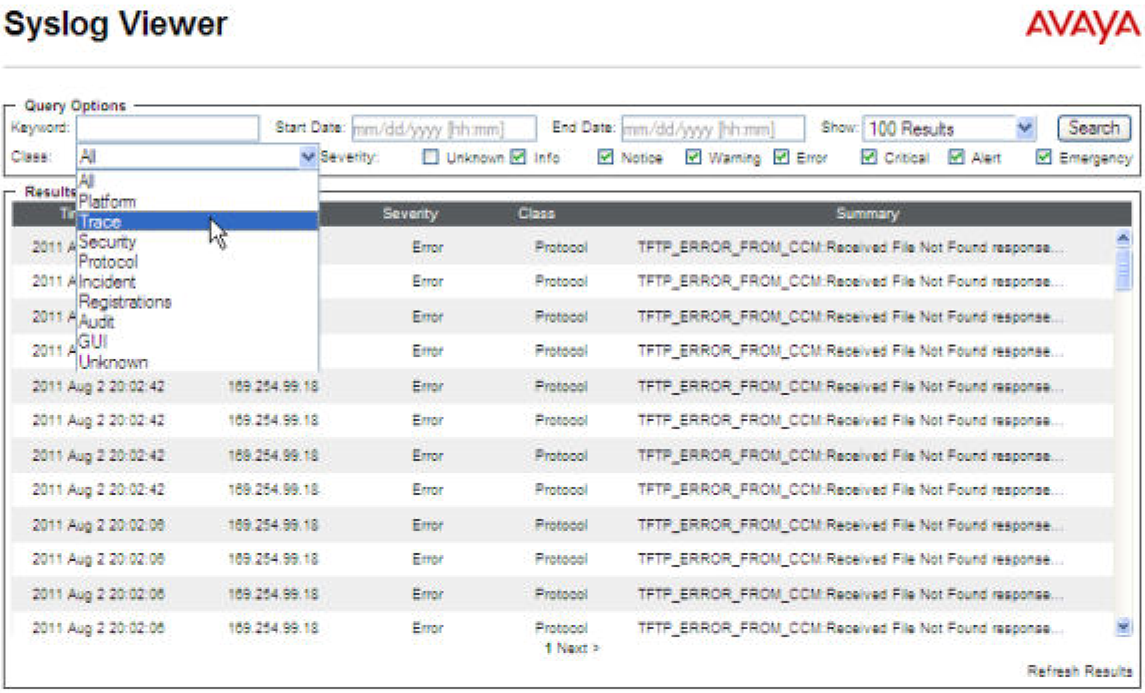
Trace

The Trace function allows you to trace an individual packet or group of packets comprising a call through the Avaya SBCE. The information gathered shows how the call traversed the Avaya SBCE-secured network.

Call trace

The Call Trace is a signaling level trace for a given URI and direction (From/To/Any) that displays SIP message flow information sent in syslog messages. The syslog messages containing Call Trace information can be seen with the log viewer function that is activated by clicking on the Logs toolbar selection at the top of the Avaya SBCE GUI screen.

In the Logs drop-dowm menu, select the System Logs option to display the Syslog Viewer screen, and then select the Trace option from the Class drop-down list of viewer options.



Syslog Viewer

Query Options

Keyword:

Start Date: mm/dd/yyyy [hh:mm]

End Date: mm/dd/yyyy [hh:mm]

Show: 100 Results

Class: All

Severity: □ Unknown ☑ Info ☑ Notice ☑ Warning ☑ Error ☑ Critical ☑ Alert ☑ Emergency

Results

Ti		Severity	Class	Summary
2011 A		Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 A		Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 A		Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 A		Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:42	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:42	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:42	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:42	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:06	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:06	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:06	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...
2011 Aug 2 20:02:06	169.254.99.18	Error	Protocol	TFTP_ERROR_FROM_CCM:Received File Not Found response...

To manage Call Trace profiles, follow the procedures detailed in the sections that follow on adding, editing, deleting, and viewing Call Trace profiles and data.

Note:

In the Logs Viewer screen, select the Trace option from the Class drop-down list to view Call Trace information. Select additional options in the Logs Viewer screen to limit the Call Trace information that is displayed.

Clicking on an item in the Call Trace Logs Viewer display will provide additional information in a Call Trace Details pop-up screen.

Adding a new call trace profile

About this task

Use the following procedure to add a new call trace profile.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the**Device Specific Settings** feature from the Task Pane, select the **Troubleshooting** sub-feature, and select the **Trace** function.
3. From the Application Pane, select the Avaya SBCE device to which you want to add a new call trace profile.
   The screen defaults to the Call Trace tab display.

4. Select the **Add** button in the upper-right portion of the screen.
   The Add Capture Profile pop-up screen is displayed.
5. Provide the requested information using the edit field, radio buttons, and checkbox while referring to Add capture profile field descriptions on page 332. Selecting the window cancel option cancels the operation and closes the window without creating a new capture profile.
6. Select**Finish**.
   The new call trace is added and displayed in the Content Area.

Add capture profile field descriptions

When adding a new call trace profile, refer to this table for information on the fields in the Add Capture Profile pop-up screen.

Add capture profile field descriptions

Field	Description
URI	The Uniform Resource Locator (URI) of the call.
Type	The type of call to capture: To, From, and Any.
Capture	Checkbox indicating whether or not the path of the call through the SBC system is to be captured.

Editing an existing call trace profile

About this task

Use the following procedure to edit an existing call trace profile.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the**Device Specific Settings** feature from the Task Pane, select the **Troubleshooting** sub-feature, and select the **Trace** function.
3. From the Application Pane, select the Avaya SBCE device to which you want to edit an existing call trace profile.
   The screen defaults to the Call Trace tab display.

4. Select the **Edit** option on the right-hand portion of the selected call trace profile line.
   The Edit Trace pop-up screen is displayed.
5. Edit the desired information using the edit field, radio buttons, and checkbox while referring to Add capture profile field descriptions on page 332. Selecting the window cancel option cancels the operation and closes the window without creating a new capture profile.
6. Select**Finish**.
   The edited call trace is saved and re-displayed in the Content Area.

Deleting an existing call trace profile

About this task

Use the following procedure to delete an existing call trace profile.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the**Device Specific Settings** feature from the Task Pane, select the **Troubleshooting** sub-feature, and select the **Trace** function.
3. From the Application Pane, select the Avaya SBCE device to which you want to edit an existing call trace profile.
   The screen defaults to the Call Trace tab display.
4. Select the **Delete** option on the right-hand portion of the selected call trace profile line.
   The delete confirmation pop-up screen is displayed.
5. Select **OK**.
   The selected Call Trace profile is deleted.

Viewing call trace data

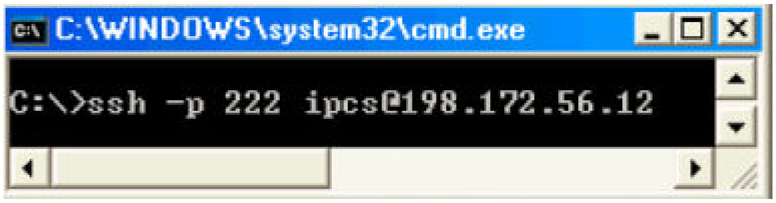
About this task

Call trace information is directed to the Avaya management interface device into the following file path: /archive/syslog/ipcs/octeon.log

Use the following procedure to view call trace information.

Procedure

1. Using a Secure Shell (SSH) Client (such as PuTTY), connect to the Avaya management interface device. A sample SSH command string is shown below.

   ```
   C:\>ssh -p 222 ipcs@198.172.56.12
   ```

   Note:

   To determine the Management IP address to use in the SSH command string, select the System Management feature from the Task Pane, and then select the View button for a specific device to display a System Information. A list of Management IP addresses will be displayed in the lower-right portion of the screen.

2. Once connected, from the prompt (login as:) enter the account name (e.g.,"ipcs") and then enter the password when prompted for it to display the Avaya SBCE Dashboard screen.
   The Dashboard screen is displayed.
3. From the dollar sign prompt ($), enter "sudo su" and then from the pound sign prompt (#) that appears enter the change directory (cd) command to navigate to the /archive/syslog/ipcs directory.
4. The log file (octeon.log) is contained in the /archive/syslog/ipcs directory.From this directory from the pound sign (#) prompt, you can use the VI editor to view this file by entering the command as follows: # vi octeon.log
   The Call Trace filtered information set up previously in the Call Trace profiles will be contained in the octeon.log log file and viewable in a vi editor screen.

Packet capture

About this task

Use the following procedure to display a Packet Capture Configuration pop-up screen containing filtering options for configuring a packet capture.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the**Device Specific Settings** feature from the Task Pane, select the **Troubleshooting** sub-feature, and select the **Trace** function.

3. From the Application Pane, select the Avaya SBCE device to which you want to edit an existing call trace profile.
   The screen defaults to the Call Trace tab display.
4. Select the **Packet Capture** tab.
   The Packet Capture tab screen is displayed.
5. In the Packet Capture Configuration screen, enter the appropriate capture information and then click on the **Start Capture** button to start the capture.
   The Packet Capture information pop-up screen is displayed.
6. In the Packet Capture information screen, select the file name of the capture.
   The File Download pop-up screen is displayed.
7. In the File Download pop-up screen, click on the **Save** button.
   The Save As pop-up screen is displayed.

   Note:

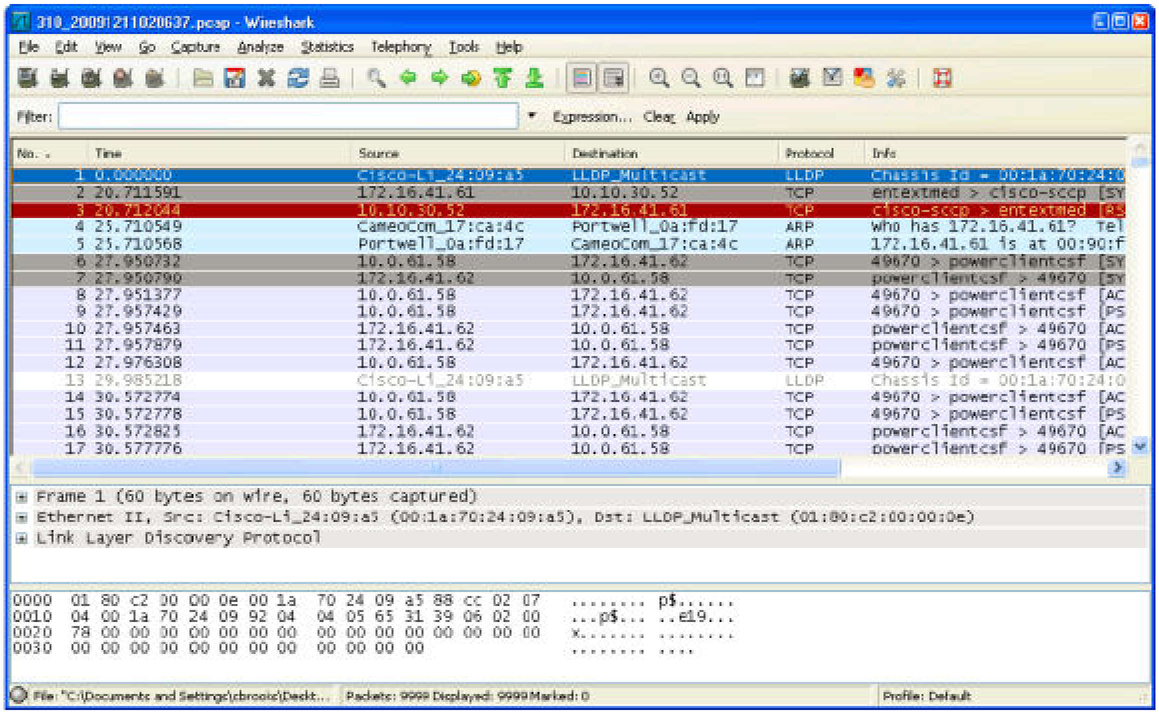
   The Packet Capture feature saves captures in the pcap format that is viewable using Wireshark (originally named Ethereal), a free and open-source packet analyzer application used for network troubleshooting, analysis, and software protocol development.
8. In the Save As pop-up screen, use the Save In drop-down list to navigate to a directory for saving the Packet Capture (pcap) file and click on the **Save** button to save the file to the new directory.

   Note:

   You will need to download and install Wireshark, or a similar network analyzer program, in order to view the Packet Capture (pcap) file.
9. In the save directory, use Wireshark or a similar application to open up the Packet Capture (pcap) file. If Wireshark is already running, you can double-click on the file to open it with Wireshark. Otherwise, you will need to start Wireshark first and then either open the file from within the Wireshark application or double-click on the Packet Capture file in the save directory.

A Capture File information screen is displayed similar to the example below.

Example



310_20091211020637.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco-Li_24:09:a5	LLDP_Multicast	LLDP	Chassis Id = 00:1a:70:24:0
2	20.711591	172.16.41.61	10.10.30.52	TCP	entextmed > cisco-sccp [SY
3	20.712044	10.10.30.52	172.16.41.61	TCP	cisco-sccp > entextmed [RS
4	25.710549	CameoCom_17:ca:4c	Portwell_0a:fd:17	ARP	who has 172.16.41.61? Tel
5	25.710568	Portwell_0a:fd:17	CameoCom_17:ca:4c	ARP	172.16.41.61 is at 00:90:f
6	27.950732	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [SY
7	27.950790	172.16.41.62	10.0.61.58	TCP	powerclientcsf > 49670 [SY
8	27.951377	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [AC
9	27.957429	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [PS
10	27.957463	172.16.41.62	10.0.61.58	TCP	powerclientcsf > 49670 [AC
11	27.957879	172.16.41.62	10.0.61.58	TCP	powerclientcsf > 49670 [PS
12	27.976308	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [AC
13	29.985218	Cisco-Li_24:09:a5	LLDP_Multicast	LLDP	Chassis Id = 00:1a:70:24:0
14	30.572774	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [AC
15	30.572778	10.0.61.58	172.16.41.62	TCP	49670 > powerclientcsf [PS
16	30.572825	172.16.41.62	10.0.61.58	TCP	powerclientcsf > 49670 [AC
17	30.577776	172.16.41.62	10.0.61.58	TCP	powerclientcsf > 49670 [PS

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_24:09:a5 (00:1a:70:24:09:a5), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
⊞ Link Layer Discovery Protocol
```

```
0000  01 80 c2 00 00 0e 00 1a  70 24 09 a5 88 cc 02 07   ........ p$......
0010  04 00 1a 70 24 09 92 04  04 05 65 31 39 06 02 00   ...p$... ..e19...
0020  78 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   x....... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\Documents and Settings\cbrooiz\Deskt... Packets: 9999 Displayed: 9999 Marked: 0 Profile: Default

Audit logs

About this task

The Audit Log Viewer displays the contents of the audit log, which contains a record of security related events, such as logins, session starts, session ends, new user additions, password attempts/retries/changes, etc. Use the following procedure to display the Audit Log Viewer information.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Logs** option from the Tool Bar and select the **Audit Logs** menu option.
   The Audit Log Viewer is displayed.
3. In the Query Options Start Date field and End Date field in the Audit Log Viewer you can filter the results displayed in a search report to fall within starting and ending dates and times.

4. In the Query Options Keyword field in the top-left portion of the Audit Log Viewer, enter one or more words to define the limits of the log report and click on the Search button on the right-hand portion of the viewer.
   The report is run and a report output is displayed.
5. To see additional details about a particular log line in a report, select the log line.
   The Audit Log Details screen is displayed.

   Note:

   The Log Level rules for the Audit Log and other logs are set from the Task Pane by selecting **Device Specific Settings** and then selecting **Syslog Management**.

   Audit Logging is enabled in the Log Level row for:Class: AuditFacility: LOG_LOCAL6

   The Log Level Facility name LOG_LOCAL6 is reserved for Audit Loggingand cannot be changed. The LOG_LOCAL6 file path destination cannot be changed either.

Chapter 10: Command Line Interface

Command line interface overview

The Command Line Interface (CLI) is a high-speed serial management interface that provides direct (local or remote) access to the Avaya SBCE security device for performing various administrative and operational tasks. These tasks are executed using a robust assortment of commands entered via a terminal emulator such as Telnet or another commonly available serial application like HyperTerminal.

The CLI for Avaya SBCE (hereafter referred to as clipcs) interface is available whenever the Avaya SBCE chassis is running. Security is provided through a combination of account login and user access privileges.

Command structure

Three new GUI command-line features are: (1) gui-user; (2) gui-snapshot-create; and (3) gui-snapshot-restore. These commands (described below in the next section titled, “Root-Level Console Commands”) are executed at the root level from the root pound-sign (#) prompt.

A second set of command-line features (described later on in this chapter in the subsection titled, “CLIPCS Console Commands.”) are executed one level down from the root level, and are accessible by first entering **clipcs** at the root (#) prompt.

Root—level console commands

The three new root-level console commands, described in subsections which follow, and are entered directly from the root prompt as shown below:

```
# gui-user

# gui-snapshot-create

# gui-snapshot-restore
```

Console Command - gui-user

The gui-user console command allows the user to manipulate GUI users from the command line. The general structure of the command is:

gui-user <action> [options]

<action>

Should be one of the following:

- -a / --add – Add mode, used for configuring a new user.

  When using the –a option, the following options are also required:

  - -n / --name (see description below)
  - -p / --password (see description below)
  - -r / --role (see description below)

- -e / --edit=<username> – Edit mode, used for changing parameter fields for an existing user. This also allows for changing of the username.

  Note:

  <username> is required and should be the username of an existing user.

- -d / --delete=<username> – Delete mode, used for deleting a user.

  Note:

  <username> is required and should be the username of an existing user.Any specified options (with the exception of debug and quiet will be ignored.

- - --version – Displays the command version. Will be equal to whatever the GUI version is (which usually will match ipcs-version).
- - --help – Displays detailed information about the command and possible arguments. Also displays a few examples.

[options]

Can be any combination of the following:

- n / --name – Specifies the user name to set. Required when using –a (add) option.
- -p / --password – Specifies the password to set. Required when adding a user with the –a (add) option or editing using the –e (edit) option, or when using the -n (name) or –t (type) flags are specified (when type is not radius).
- -c / --contact-info – Specifies the contact info to set.
- -N / --real-name – Specifies the real name to set.

- -r / --role – Specifies the user role to set. Can be admin, manager, or supervisor. Required when using –a (add) option.
- -t / --type – Specifies the user type to set. Can be legacy, local, or radius.
- -s / --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 will take precedence.

When the command finishes executing, an exit code will be returned. Any relevant details for a failure will be passed to stderr. A list of possible returned exit codes follows:

- -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 usually happens 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 user name 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]

Below, are a few sample commands with descriptions:

```
gui-user --add --name test-user --password "hello, world" --type
manager
```

password and real-name support spaces in the values as long as the input is double quoted. This will exit with code 0.

Both password and real-name support spaces in the values as long as the input is double quoted.

This will exit with code 0.

```
gui-user --edit test-user --status disabled
```

Edits an existing user named test-user and disables the user. This will exit 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 will exit with 0.

```
gui-user –d test-user
```

Deletes a user named test-user using shorthand options.

While this command is syntactically correct, if we follow the progression from the previous examples, it will fail because there is no user named test-user (we renamed it to fred). Therefore, it would fail with code 3.

Console Command - gui-snapshot-create

The gui-snapshot—create console command allows the user to create a snapshot from the command line. The general structure of the command is:

gui-snapshot-create [options] [description]

[description]

[description] - Can be any string value and does not need to be quoted. If not specified, it will default to "Restore Point via CLI".

[options]

Can be any of the following:

- --version – Displays the command version. Will be equal to whatever the GUI version is (which usually will match ipcs-version).
- --help – Displays detailed information about the command and possible arguments. Also displays a few examples.
- --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 will take precedence.

When the command finishes executing, an exit code will be returned. Any relevant details for a failure will be passed to stderr. A list of possible returned exit codes follows:

- 0 – Completed successfully.
- 1 – Invalid command syntax.
- 2 – Snapshot creation partially successful. This usually occurs when a snapshot was created succesfully, but could not be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This usually occurs if the snapshot creation itself failed.
- 1000 – An unknown error has occurred.

[Examples]

Below, are a few sample commands with descriptions:

```
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.”Nothing will be output to stdout or stderr.

Console Command - gui-snapshot-restore

The gui-snapshot—restore console command allows the user to restore a snapshot from the command line. The general structure of the command is:

gui-snapshot-restore [options] <file>

<file>

<file> must point to a valid snapshot file and can be an absolute or relative path.

[options]

Can be any of the following:

- --version – Displays the command version. Will be equal to whatever the GUI version is (which usually will match ipcs-version).
- --help – Displays detailed information about the command and possible arguments. Also displays a few examples.
- --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 will take precedence.

When the command finishes executing, an exit code will be returned. Any relevant details for a failure will be passed to stderr. A list of possible returned exit codes follows:

- 0 – Completed successfully.
- 1 – Invalid command syntax.
- 2 – Snapshot creation partially successful. This usually occurs when a snapshot was created succesfully, but could not be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This usually occurs if the snapshot creation itself failed.
- 1000 – An unknown error has occurred.

[Examples]

Below, are a few sample commands with descriptions:

```
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 parent directory's sibling named snapshots.

clipcs console commands

About this task

clipcs console commands are executed one level down from the root level, and are accessible by first entering “clipcs” at the root prompt. The “clipcs” commands are used to display certain basic information about Avaya SBCE system configuration and status.

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 system-wide commands can be executed. The instance mode is the next level of administrative control which provides direct access to a particular Avaya SBCE functional node (signaling, media, or intelligence).

Use the following procedure to use the clipcs console commands. Refer to clipcs commands descriptions on page 344.

Note:

All clipcs commands and arguments (including user passwords) are case sensitive.

Procedure

1. Display the list of available clipcs commands by entering the clipcs (in lowercase) command to start the Avaya SBCE console and then entering the help command, as shown below:

   SS310 [root@pts/3] / # clipcs

   Starting SBC Console…Please wait.

   SBC Version n.n.n (C) Avaya Systems Inc.

   SBC# help

2. Enter the clipcs commands from the root level prompt (#).

clipcs commands descriptions

This table contains a list of clipcs commands and descriptions of commands available at the console prompt (#)>

clipcs commands descriptions

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>clear</td><td>Clears the display screen.</td></tr>
<tr><td>clock</td><td>Displays, sets, and clears the internal system clock.</td></tr>
<tr><td>exit</td><td>Moves command level from instance mode to console mode.</td></tr>
<tr><td>help</td><td>Displays a list of available commands and their descriptions.</td></tr>
<tr><td>refresh</td><td>Displays the current refresh interval.</td></tr>
<tr><td>spool</td><td>Directs output to a file or device.</td></tr>
<tr><td>status</td><td>If entered in the Console mode, it displays the status of SBC nodes; if entered from the Instance mode, it displays the detailed operational status of the node being accessed.</td></tr>
<tr><td>select</td><td>Selects a particular SBC node for access and activated the instance mode.</td></tr>
<tr><td>show</td><td>A command used in combination with those shown below to display certain system-, node-, or operational-specific information.
<table>
<tr><th>SHOW Command</th><th>Description</th></tr>
<tr><td>certinstall</td><td>Installs certificates.</td></tr>
<tr><td>certsync</td><td>Synchronizes certificates.</td></tr>
<tr><td>certupdate</td><td>Updates the certificate key.</td></tr>
<tr><td>ip interface all</td><td>Displays IP-related information about physical SBC system interfaces.</td></tr>
<tr><td>ip route</td><td>Displays SBC routing information.</td></tr>
<tr><td>Flow dynamic</td><td>The show flow dynamic command displays the media Relay Information for the given active session phone IP.(See the section below titled, “Show Flow Dynamic.”</td></tr>
<tr><td>SBC cpu</td><td>Displays CPU-specific information.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>SBC global cluster</td><td>Displays SBC global cluster information.</td></tr>
<tr><td>SBC interface status</td><td>Displays the status of physical SBC system interfaces.</td></tr>
<tr><td>SBC memory</td><td>Displays memory usage statistics for all SBC processes.</td></tr>
<tr><td>SBC processes</td><td>Displays all currently running processes.</td></tr>
<tr><td>iptables version</td><td>Displays the version of the IP tables.</td></tr>
<tr><td>linux version</td><td>Displays the version of Linux.</td></tr>
<tr><td>octeon status</td><td>Displays the status of the executables running on the Octeon processor</td></tr>
<tr><td>Uptime</td><td>Displays the amount of time the system has been in operation since last power-up.</td></tr>
</table>
</td></tr>
<tr><td>quit</td><td>Terminates the current CLI session.</td></tr>
<tr><td>version</td><td>Displays the current version of the CLI server.</td></tr>
</table>

Show flow dynamic

About this task

The “flow dynamic”option for the Avaya SBCE CLI show command is useful for debugging network problems in an active session where media is only received in one direction or where media is not received in either direction.

Procedure

1. Display the list of available clipcs commands by entering the clipcs (in lowercase) command to start the Avaya SBCE console and then entering the help command, as shown below:

   ```
   SS310 [root@pts/3] / # clipcs
   
   Starting SBC Console…Please wait.
   ```

SBC Version n.n.n (C) Avaya Systems Inc.

SBC# help

2. Enter the clipcs Show Flow Dynamic command from the root level prompt (#) The media Relay Information for the given active session phone IP is displayed..
3. Use the following syntax for entering the Show Flow Dynamic command.

   Command Syntax:

   show flow dynamic [x.x.x.x (ip addr) || x.x.x.x:y (ip addr:port)] [RTP/RTCP/SRTP/SRTCP]

   Note:

   If a port number is specified in the command line, then a protocol entry at the end of the command line will not be considered.

Instance commands

Instance commands, also referred to as top commands, are two levels deep and are used to display detailed information about a specific Avaya SBCE node in the network and EMS node with multiple Avaya SBCE nodes or information about an instance (i.e., “ems” or “ss” running on a single platform for EMS or SBCE, respectively).

Refer to CLI (top) commands available from the instance mode on page 347 for a summary list of the top (or instance) commands, which currently only contains a single command, “top.” Instance commands are only available within the instance mode, which is enabled whenever the clipcs select command has been invoked to select a node or application instance. Instance or top commands communicate directly with the active (selected) SBC node or communicate with the selected “ems” or “ss” application instance running on a single platorm and provide output from that node or instance only.

Screen displays presented instance commands are automatically refreshed at a rate determined by the refresh command (default: 5 seconds).

CLI (top) commands available from the instance mode

Instance (or top) commands are only available within the instance mode, which is enabled whenever the clipcs select command has been invoked to select a node or application instance.

CLI (top) commands available from the instance mode

Command	Description

top	Displays a detailed functional status of the selected SBC node. The display is automatically refreshed every 5 seconds.

Accessing the CLI

There are three methods for accessing the clipcs Command Line Interface (CLI), remote, local, and GUI.

- To go to a remote SSH session, refer to the section,

  To establish a local SSH session, refer to the section,

  to establish an SSH session using the EMS GUI, refer to the section,

Remote clipcs access

About this task

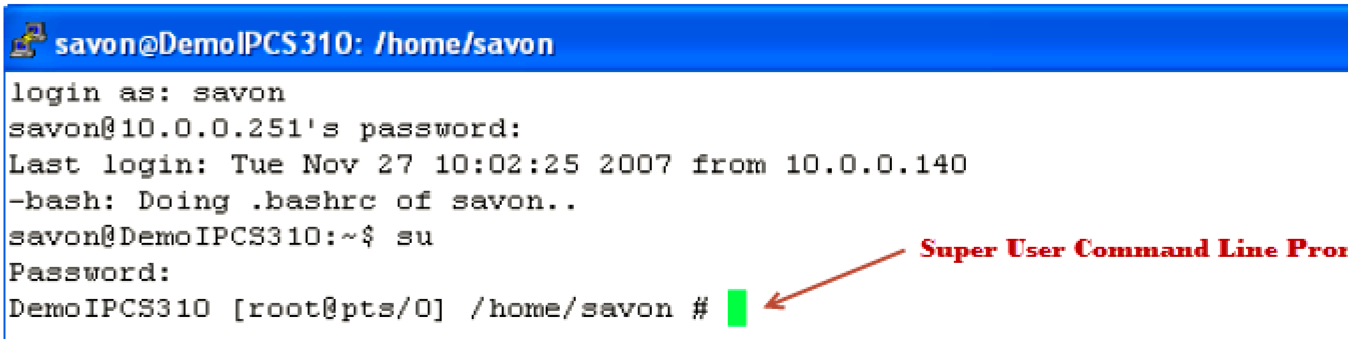
The clipcs command line interface can be accessed remotely with any SSH client using the following procedure.

Procedure

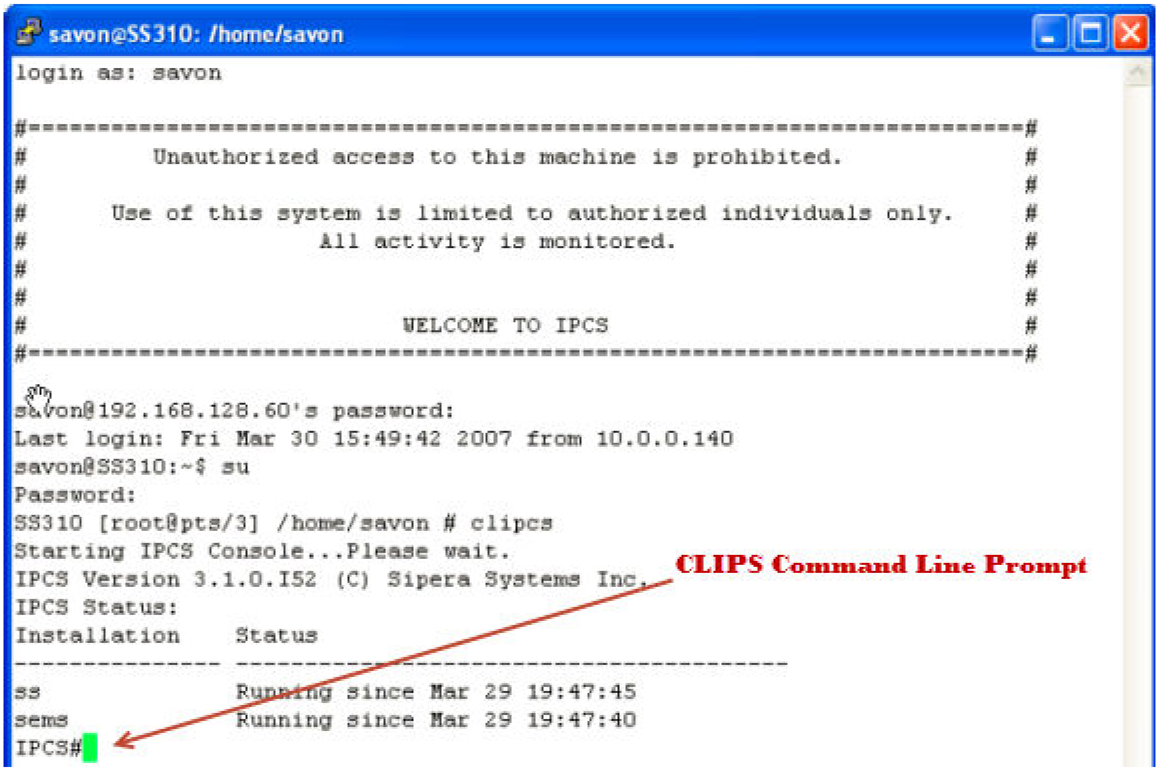
1. Start the SSH client and enter the information in the table below to establish a secure connection with the Avaya SBCE node.(Remote clipcs access information on page 349
   The session is established and the login prompt (i.e., **login as:**) is displayed.
2. Login as `savon` and press **Enter**.
   The password prompt (e.g., `savon@10.0.0.251’s password:`) is displayed.
3. Enter the password provided by Avaya and press **Enter**.
   The top-level clipcs prompt ($) is displayed.
4. Enter the `su` command to access super user privileges and press **Enter**.
   The super user password prompt (e.g., `Password:`) is displayed.
5. Enter the super user password and press **Enter**.
   The super user command line prompt (#) is displayed.
6. Start clipcs by entering the clipcs command and pressing **Enter**.

clipcs is started and the clipcs command line prompt (#) is displayed.

Example



```
login as: savon
savon@10.0.0.251's password:
Last login: Tue Nov 27 10:02:25 2007 from 10.0.0.140
-bash: Doing .bashrc of savon..
savon@DemoIPCS310:~$ su
Password:
DemoIPCS310 [root@pts/0] /home/savon #
```



```
login as: savon

#=========================================================================#
#          Unauthorized access to this machine is prohibited.            #
#                                                                         #
#      Use of this system is limited to authorized individuals only.     #
#                         All activity is monitored.                     #
#                                                                         #
#                                                                         #
#                              WELCOME TO IPCS                           #
#=========================================================================#

savon@192.168.128.60's password:
Last login: Fri Mar 30 15:49:42 2007 from 10.0.0.140
savon@SS310:~$ su
Password:
SS310 [root@pts/3] /home/savon # clipcs
Starting IPCS Console...Please wait.
IPCS Version 3.1.0.I52 (C) Sipera Systems Inc.
IPCS Status:
Installation    Status
--------------- ----------------------------------------
ss              Running since Mar 29 19:47:45
sems            Running since Mar 29 19:47:40
IPCS#
```

remote clipcs access information

To access the clipcs command line interface, enter the following information to start an SSH client session.

Remote clipcs access information

Parameter	Value
IP Address	The IPaddress of the SBC equipment node to which you want to establish a secure connection.
Port	222
Protocol	SSH

Local clipcs access

About this task

The clipcs command line interface can be accessed locally by connecting directly to an Avaya SBCE chassis with any SSH client using the following procedure.

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. Login to the command shell.

Connecting a terminal device to the SBC equipment chassis

About this task

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

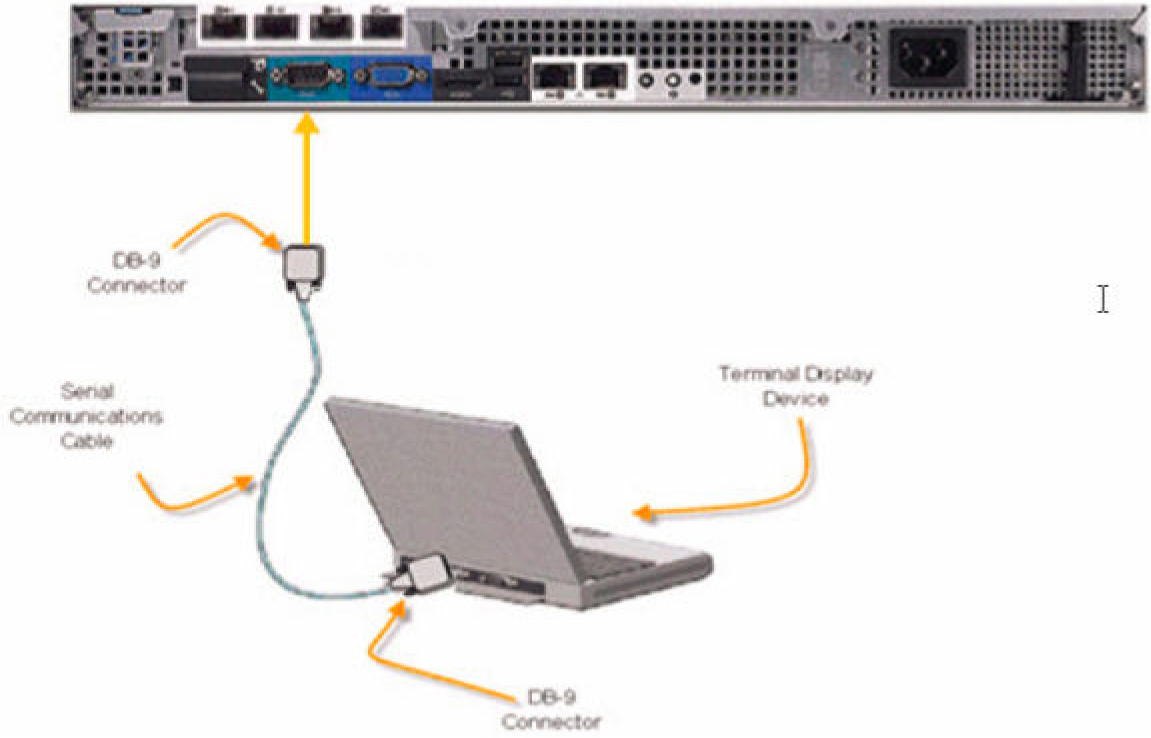
Procedure

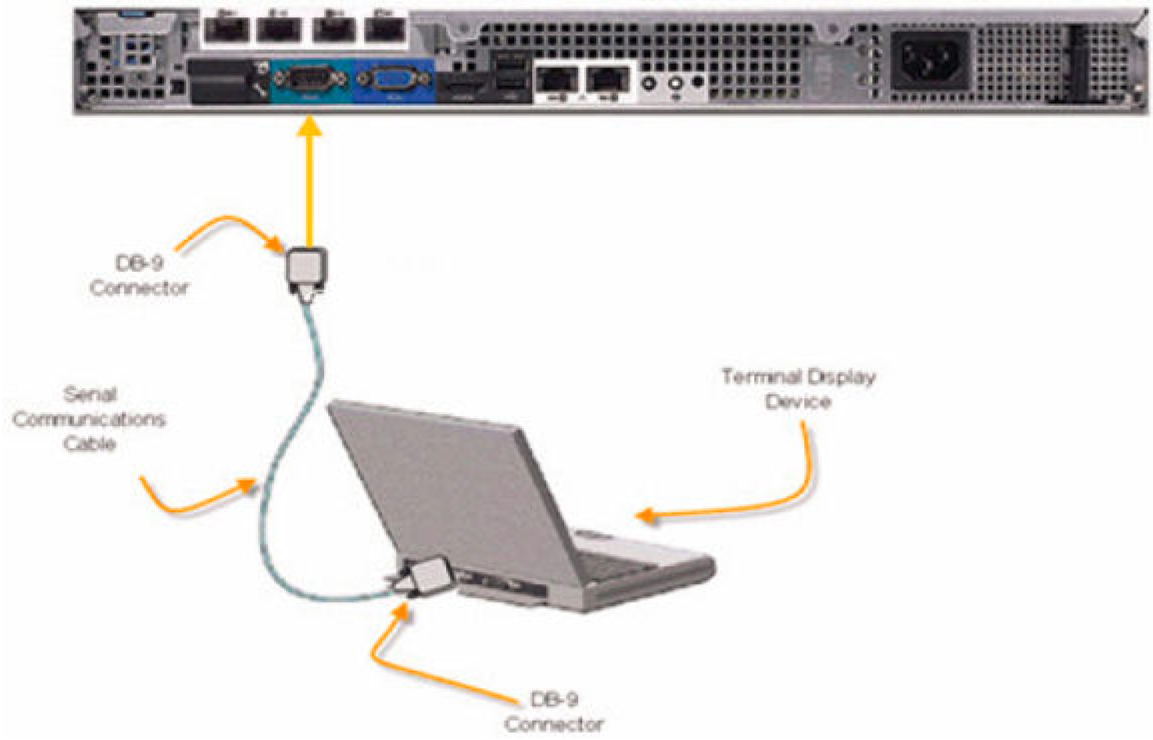
1. Locate the Console port on the SBC equipment chassis or, in the case of the Element Management System (EMS), the UART (serial COM) port. The UART port for the EMS is located on the back panel of the equipment chassis (See the document Installing Avaya Session Border Controller for more information). The Console port for the SBC equipment chassis is located on the front panel. (See the

document, “Installing Avaya Session Border Controller Enterprise (SBC),” for more information).

2. Connect an RJ45-terminated serial communications cable or a DB-9 cable (depending on the chassis model) from the terminal device to the Console or UART port as shown in the following figures.

Example





Establishing a communications session

About this task

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

Procedure

1. Configure the communications parameters of your terminal program to the settings contained in the following table. Console port communications settings on page 353
2. Press **Enter** to establish the communications session.
   A prompt for your user name and password will be displayed.

Console port communications settings

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

Console port communications settings

Parameter	Value
Baud Rate	19200
Parity	None
Data Bits	8
Stop Bits	1
Connection Setting	Direct to Com1

Logging in to the command shell

About this task

Use the following procedure to log in to the Avaya SBCE command shell to begin a CLI session.

Procedure

1. Logon to the command shell using Administrator’s user name and password. The command shell prompt will be displayed.

   [savon@localhost bin]

2. Enter `clipcs` as shown below:

   [savon@localhost bin] $ clipcs

   The CLI prompt (#) will be displayed.

   The CLI is now ready for use.

Chapter 11: Configuration Workflows for SIP Trunking

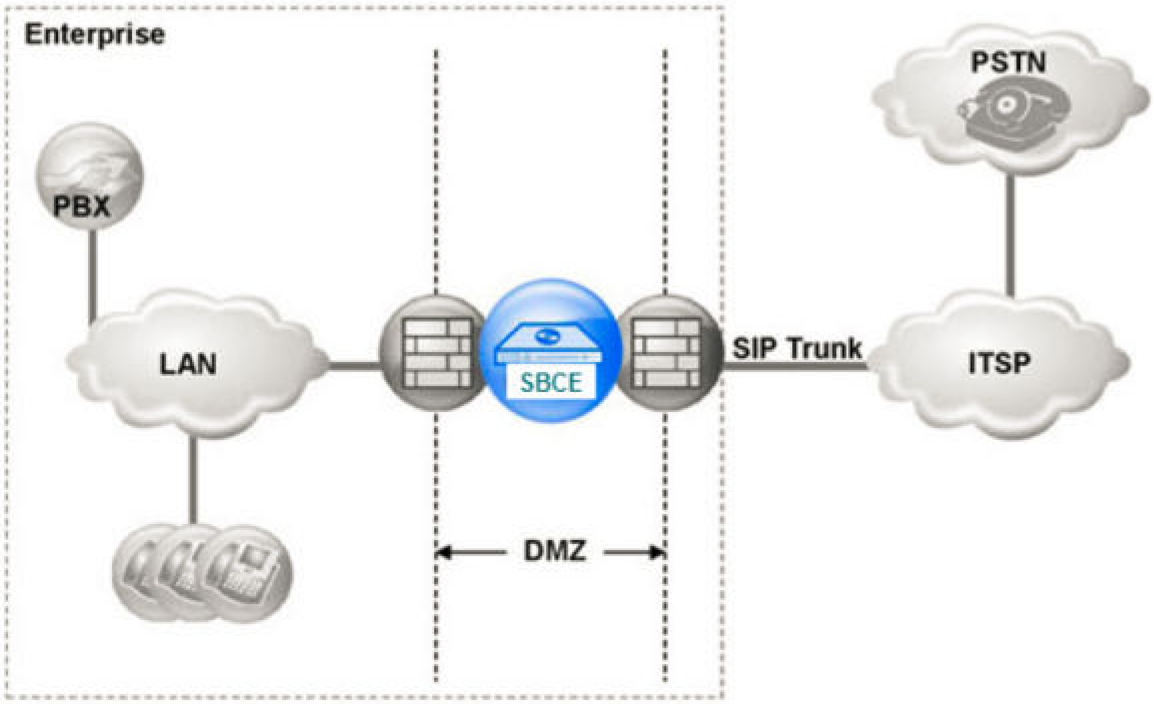
SIP Trunking overview

The SIP Trunking feature of SBCE security devices allow SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet via 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, the SIP Trunking feature in SBCE allows an enterprise to maintain granular control through well-defined domain policies securing customers' SIP implementations/servers from known SIP and Media vulnerabilities.

Because the 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 (Figure 11–1). If the signaling traffic is encrypted, the SBCE device decrypts all TLS encrypted traffic and looks for anomalous behavior before forwarding the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

Example



Configuration for generic SIP trunk (Asterisk)

About this task

This section details the procedure for configuring a generic SBCE SIP trunk with the Asterisk PBXi telephony engine. The generic SIP trunk configuration consists of the following steps:

Procedure

1. Create Routing profiles
   a. Creating Routing Profile for Call Server on page 358
   b. Creating Routing Profile for Trunk Server on page 357
2. Create Topology Hiding profiles
   a. Creating Topology Hiding Profile for Call Server on page 359
   b. Creating Topology Hiding Profile for Trunk Server on page 360
3. Creating Interworking Profiles on page 361
4. Create Server profiles
   a. Creating Server Profile for Call Server on page 361

   b. Creating Server Profile for Trunk Server on page 363

5. Create Signalling interfaces
   a. Creating External Signaling Interface toward Trunk Server on page 364
   b. Creating Internal Signaling Interface Toward Call Server on page 364
6. Create Media interfaces
   a. Creating External Media Interface toward Trunk Server on page 365
   b. Creating Internal Media Interface Toward Call Server on page 366
7. Create Server Flows
   a. Creating Flow toward Call Server on page 366
   b. Creating Flow toward Trunk Server on page 367
8. Server-specific configuration for SIP Trunking
   a. Configuring SBC for Avaya Trunk on page 368
   b. SBCE Configuration for Other Trunks on page 369

Creating Routing Profile for Trunk Server

About this task

This procedure will create a routing profile with next hop as a Trunk side Server IP address.

Note:

Use the following profile name: `Route_to_Trunk_Svr`.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Routing** function of the Global Profiles feature from the Task Pane (Figure 11–2).
3. In the Routing Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Routing Profile pop-up screen similar to the example in Figure 11–6.
4. In the **Profile Name** field, type the profile name: `Route_to_Trunk_Svr`.
5. Click **Next** to display a second Add Routing Profile screen similar to the one shown below in Figure 11–7.
6. In the second Add Routing Profile screen, in the **Next Hop Server 1** field, enter either the Domain Name of the Line server or enter the IP address and port number separated by a colon, as shown in the example above.

7. Select the checkbox labeled **Routing Priority** based on Next Hop Server.

   If the Call server domain is to be selected from the DNS server either by NAPTR or SRV, select the appropriate checkbox. If you want to use next hop instead of route header for routing in-dialog and/or out-of-dialog messages, check the appropriate checkbox.

8. Select the transport type (i.e., TLS, TCP, or UDP).

9. Click **Finish** to save the configuration and exit.
   This displays the Routing Profile screen, similar to the example in Figure 11–8, showing the newly created `Route_to_Trunk_Svr` Routing Profile along with the `Route_to_Call_Svr` Routing Profile created by the procedure described in Creating Routing Profile for Call Server on page 358.

Creating Routing Profile for Call Server

About this task

This procedure will create a routing profile with next hop as a call server address

Note:

Use the following profile name: `Route_to_Call_Svr`

Procedure

1. Login to the SBC Control Center as the `Admin`.

2. Select the **Routing** function of the Global Profiles feature from the Task Pane

3. In the Routing Profile screen that is displayed, click on the **Add Profile** button, which displays the **Add Routing Profile** pop-up screen.

4. In the **Profile Name** field, type the profile name: `Route_to_LineServer`

5. Click **Next** to display a second Add Routing Profile screen.

6. In the second Add Routing Profile screen, in the **Next Hop Server 1** field, enter either the Domain Name of the Call Server, IP Address, or enter the IP address and port number separated by a colon.

7. Select the checkbox labeled **Routing Priority** based on Next Hop Server.

   If the Call server domain is to be selected from the DNS server either by NAPTR or SRV, select the appropriate checkbox. If you want to use next hop instead of route header for routing in-dialog and/or out-of-dialog messages, check the appropriate checkbox.

8. Select the transport type (i.e., TLS, TCP, or UDP).

9. Click **Finish** to save the configuration and exit.
   This displays the Routing Profile screen showing the newly created Route_to_Call_Svr Routing Profile.

Creating Topology Hiding profile for Call Server

About this task

This procedure will create a routing profile with next hop as a call server address

Note:

Refer to Chapter 7, “Security Configuration,” and Topology Hiding Settings Examples on page 274for descriptions of the various Topology Hiding parameters combinations and their resulting actions.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Topology Hiding** function of the Global Profiles feature from the Task Pane (Figure 11–9).
3. In the Topology Hiding Profile screen that is displayed, click on the **Add Profile** button, which displays the **Add Topology Hiding Profile** pop-up screen similar to the example shown in Figure 11–10 below.
4. In the **Profile Name** field, type the profile name: `SBCE_to _Call_Svr`
5. Click **Next** to display a second Add Topology Hiding Profile screen similar to the one shown in Figure 11–11.
6. In the second Topology Hiding Profile screen, begin to select the chosen parameters by selecting the drop-down list of Header parameters to choose one of the parameters for the new profile as shown in Figure 11–12.
7. In the second Topology Hiding Profile screen (Figure 11–11), next select the drop-down list of **Criteria** parameters to choose one of the parameters for the new profile as shown in Figure 11–13.
8. In the second Topology Hiding Profile screen (Figure 11–11), next select the drop-down list of **Replace Action** parameters to choose one of the parameters for the new profile as shown in Figure 11–14.

   In the drop-down list in the **Replace Action** field, shown in Figure 11–14, if you select the action, **Overwrite**, the **Overwrite Value** field to the right will accept entry of a value (i.e., an IP address).

9. After selecting the appropriate values in the **Topology Profile** fields, select **Finish** to save, submit, and exit.

Creating Topology Hiding profile for Trunk Server

About this task

This procedure will create a routing profile with next hop as a call server address

Note:

Refer to Chapter 7, “Security Configuration,” and Topology Hiding Settings Examples on page 274for descriptions of the various Topology Hiding parameters combinations and their resulting actions.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Topology Hiding** function of the Global Profiles feature from the Task Pane (Figure 11–15).
3. In the Topology Hiding Profile screen that is displayed, click on the **Add Profile** button, which displays the **Add Topology Hiding Profile** pop-up screen similar to the example shown in Figure 11–16 below.
4. In the **Profile Name** field, type the profile name: `SBCE_to _Trunk_Svr`
5. Click **Next** to display a second Add Topology Hiding Profile screen similar to the one shown in Figure 11–17.
6. In the second Topology Hiding Profile screen, begin to select the chosen parameters by selecting the drop-down list of **Header** parameters to choose one of the parameters for the new profile as shown in Figure 11–18.
7. In the second Topology Hiding Profile screen (Figure 11–17), next select the drop-down list of **Criteria** parameters to choose one of the parameters for the new profile as shown in Figure 11–19.
8. In the second Topology Hiding Profile screen (Figure 11–17), next select the drop-down list of **Replace Action** parameters to choose one of the parameters for the new profile as shown in Figure 11–20.

   In the drop-down list in the **Replace Action** field, shown in Figure 11–20, if you select the action, **Overwrite**, the **Overwrite Value** field to the right will accept entry of a value (i.e., an IP address).

9. After selecting the appropriate values in the **Topology Hiding Profile** fields, select **Finish** to save, submit, and exit.

Creating Interworking Profiles

About this task

Interworking Profile features are configured based on different Trunk Servers (e.g., Avaya, Nortel, etc.). There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

✪ **Note:**

The procedures before and after this section provide generic instructions for SIP trunking configuration that apply to all implementations. Specific instructions are included in a section located at the end of this chapter titled, “Step-8 Server-Specific Configuration for SIP Trunking.” Refer to that section for specific instructions applicable to the Trunk Server used in your network.

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Server Interworking** function of the Global Profiles feature from the Task Pane.
3. The default Trunk Server profiles can be used as is or modified or a new Trunk Server Profile can be created beginning by clicking on the **Add Profile** button and editing a series of five pop-up edit screens followed by editing another edit pop-up screen that is accessible on the **Advance** tab of the Global Profiles Server Interworking screen.

   For details on creating Interworking Profiles see Adding a New Server Interworking Profile on page 290.

Example

Next steps

Creating Server Profile for Call Server

Procedure

1. Login to the SBC Control Center as the `Admin`.

2. Select the **Server Configuration** function of the Global Profiles feature from the Task Pane (Figure 11–23).
3. In the Server Configuration Profile screen that is displayed, click on the **Add** button, which displays the Add Server Configuration Profile pop-up screen similar to the example shown below in Figure 11–24.
4. In the Add Server Configuration Profile pop-up screen, enter a server name (e.g., Call_Server_1) in the **Profile Name** field, as shown in the example above, and click **Next** to display a second Add Server Configuration Profile pop-up screen, similar to the example in Figure 11–25.
5. In the second Add Server Configuration Profile pop-up screen, in the **Server Type** field drop-down menu, select **Call Server**.
6. In the **IP Addresses / Supported FQDNs** edit field, enter the IP address of the call server or its FQDN.
7. In the **Supported Transports** fields, select the checkboxes for both **TCP** and **UDP**.
8. In the **TCP Port** field enter `5060` and in the **UDP Port** field enter `5060`. Leave the **TLS Port** field blank. Click **Next** to display the Add Server Configuration Profile – Authentication screen shown in Figure 11–26.

   Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.
9. Completion of the Add Server Configuration Profile – Authentication screen is optional. If you are using server authentication, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Heartbeat pop-up screen shown in Figure 11–27 below.
10. Completion of the first Add Server Configuration Profile – Heartbeat screen (Figure 11–27) is optional. If you are using the heartbeat feature, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Advanced pop-up screen.

    For more information about DoS protection, see Chapter 7, “Security Configuration.”

    For more information about Signaling Manipulation, see Chapter 13, “Signaling Manipulation.”
11. In the **Add Server Configuration Profile – Advanced** screen (Figure 11–28), in the **Interworking Profile** drop-down menu, select the profile name (either the name of a default interworking profile or newly-created interworking profile) for your type of call server. In the example shown below, the default interworking profile of **avaya-ru** is selected (Figure 11–29).
12. Click the **Finish** button to display an updated Server Configuration Profile information screen, similar to the example in Figure 11–30.

Creating Server Profile for Trunk-side Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Server Configuration** function of the Global Profiles feature from the Task Pane.
3. In the Server Configuration Profile screen that is displayed, click on the **Add** button, which displays the Add Server Configuration Profile pop-up screen.
4. In the Add Server Configuration Profile pop-up screen, enter a server name (e.g., Trunk_Server_1) in the **Profile Name** field, as shown in the example above, and click **Next** to display a second Add Server Configuration Profile pop-up screen.
5. In the second Add Server Configuration Profile pop-up screen, in the **Server Type** field drop-down menu, select **Trunk Server**.
6. In the **IP Addresses / Supported FQDNs** edit field, enter the IP address of the trunk-side server or its FQDN.
7. In the **Supported Transports** fields, select the checkboxes for both **TCP** and **UDP**.
8. In the **TCP Port** field enter `5060` and in the **UDP Port** field enter `5060`. Leave the **TLS Port** field blank. Click **Next** to display the Add Server Configuration Profile – Authentication screen.

   Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.
9. Completion of the Add Server Configuration Profile – Authentication screen is optional. If you are using server authentication, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Heartbeat pop-up screen.
10. Completion of the first Add Server Configuration Profile – Heartbeat screen is optional. If you are using the heartbeat feature, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Advanced pop-up screen.

    For more information about DoS protection, see Chapter 7, “Security Configuration.”

    For more information about Signaling Manipulation, see Chapter 13, “Signaling Manipulation.”
11. In the **Add Server Configuration Profile – Advanced** screen (Figure 11–36), in the **Interworking Profile** drop-down menu, select the profile name (either the name of a default interworking profile or newly-created interworking profile) for your type

of call server. In the example shown below, the default interworking profile of **avaya-ru** is selected.

12. Click the **Finish** button to display an updated Server Configuration Profile information screen.

Creating External Signaling Interface toward Trunk-side Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Signaling Interface** function of the Device Specific Settings feature from the Task Pane (Figure 11–38).
3. In the Signaling Interface screen that is displayed, click on the **Add** button on the right-hand side of the screen to display the first Add Signaling Interface pop-up screen similar to the example shown in Figure 11–39.
4. In the first Add Signaling Interface pop-up screen, in the **Name** edit field, enter a descriptive name for the external signaling interface toward the trunk server.
5. In the **IP Address** edit field drop-down menu, select the IP address of the external signaling interface.
6. In the **TCP Port** field enter `5060` and in the **UDP Port** field enter `5060`. Leave the **TLS Port** field blank. Click **Next** to save and exit.

   Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.

Creating Internal Signaling Interface toward Call Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Signaling Interface** function of the Device Specific Settings feature from the Task Pane.

3. In the Signaling Interface screen that is displayed, click on the **Add** button on the right-hand side of the screen to display the first Add Signaling Interface pop-up screen.
4. In the first Add Signaling Interface pop-up screen, in the **Name** edit field, enter a descriptive name for the external signaling interface toward the call server.
5. In the **IP Address** edit field drop-down menu, select the IP address of the internal signaling interface.
6. In the **TCP Port** field enter `5060` and in the **UDP Port** field enter `5060`. Leave the **TLS Port** field blank. Click **Next** to save, exit, and display the Signaling Interface screen, showing the newly-created internal and external signaling interfaces.

   Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.

Creating Internal Media Interface toward Trunk Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Media Interface** function of the Device Specific Settings feature from the Task Pane (Figure 11–42).
3. In the Media Interface screen that is displayed, click on the **Add** button on the right-hand side of the screen to display the first Add Media Interface pop-up screen similar to the example shown in Figure 11–43 below.
4. In the first Add Media Interface pop-up screen, similar to the example in Figure 11–43 above, in the **Name** edit field, enter a descriptive name for the external media interface toward the trunk server.
5. In the **IP Address** edit field drop-down menu, select the IP address of the external media interface.
6. In the **Port Range** fields enter starting and ending port range numbers.
7. Click **Finish** to save and exit.

Creating Internal Media Interface toward Call Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **Media Interface** function of the Device Specific Settings feature from the Task Pane.
3. In the Media Interface screen that is displayed, click on the **Add** button on the right-hand side of the screen to display the first Add Media Interface pop-up screen.
4. In the first Add Media Interface pop-up screen in the **Name** edit field, enter a descriptive name for the internal media interface toward the call server.
5. In the **IP Address** edit field drop-down menu, select the IP address of the internal media interface.
6. In the **Port Range** fields enter starting and ending port range numbers.
7. Click **Finish** to save, exit, and display the Media Interface screen showing the newly-created internal and external media interfaces.

Creating Flow toward Call Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **End Point Flows** function of the Device Specific Settings feature from the Task Pane to display the End Point Flows screen.
3. In the End Point Flows screen that is displayed with the default **Subscriber Flows** tab selected, click on the **Server Flows** tab to display the Server Flows information screen.
4. Click on the **Add** button on the right-hand side of the screen to display the Add Flow pop-up screen.
5. In the Add Flow Criteria pop-up screen, in the **Flow Name** field, enter the Flow name as: `Call_Server_Flow_1`.
6. In the **Server Configuration** field drop-down menu, select the profile name (e.g., Call_Server_1) of the call (line side) server profile..

7. Leave the **From URI Group**, **Transport**, and **Remote Subnet** fields set to the default (*).

   The fields are changed based on customer requirements.
8. In the **Received Interface** field drop-down menu, select the name (e.g., Ext_Sig_Intf_to_Trk_Svr) of the interface pointing toward the phone network, as shown in Figure 11–48.
9. In the **Signaling Interface** field drop-down menu, select the name (e.g., Sig_Intf_Int_to_Call_Server) of the interface pointing toward the call server, as shown in Figure 11–48.
10. In the **Media Interface** field drop-down menu, select the name of the interface (e.g., Int_Med_Intf_to_Call_Svr) pointing toward the call server, as shown in Figure 11–48.
11. Leave the **End Point Policy Group** field set to the default (i.e., default-low). The fields are changed based on customer requirements.
12. In the **Routing Profile** field drop-down menu, select the name of your previously created Routing Profile.
13. In the **Topology Hiding Profile** field drop-down menu, select the name of your previously created Topology Hiding Profile or select the default (i.e., None).
14. Leave the **File Transfer Profile** field set to the default (i.e., None).
15. Click **Finish** to save, exit, and re-display the Server Flows information screen showing the newly-created server flow.

Creating Flow toward Trunk Server

Procedure

1. Login to the SBC Control Center as the `Admin`.
2. Select the **End Point Flows** function of the Device Specific Settings feature from the Task Pane (Figure 11–46) to display the End Point Flows screen.
3. In the End Point Flows screen that is displayed with the default **Subscriber Flows** tab selected, click on the **Server Flows** tab to display the Server Flows information screen.
4. Click on the **Add** button on the right-hand side of the screen to display the Add Flow pop-up screen.
5. In the Add Flow Criteria pop-up screen, in the **Flow Name** field, enter the Flow name as: `Trunk_Server_Flow_1`.

6. In the **Server Configuration** field drop-down menu, select the profile name (e.g., Trunk_Server_1) of the call (line side) server profile, as shown in the example in Figure 11–50.
7. Leave the **From URI Group**, **Transport**, and **Remote Subnet** fields set to the default (*).

   The fields are changed based on customer requirements.
8. In the **Received Interface** field drop-down menu, select the name (e.g., Int_Sig_Intf_to_Call_Svr) of the interface pointing toward the phone network, as shown in Figure 11–50.
9. In the **Signaling Interface** field drop-down menu, select the name (e.g., Ext_Sig_Intf_to_Trk_Svr) of the interface pointing toward the call server, as shown in Figure 11–50.
10. In the **Media Interface** field drop-down menu, select the name of the interface (e.g., Ext_Med_Intf_to_Trk_Svr) pointing toward the call server, as shown in Figure 11–50.
11. Leave the **End Point Policy Group** field set to the default (i.e., default-low). The fields are changed based on customer requirements.
12. In the **Routing Profile** field drop-down menu, select the name of your previously created Routing Profile.
13. In the **Topology Hiding Profile** field drop-down menu, select the name of your previously created Topology Hiding Profile or select the default (i.e., None).
14. Leave the **File Transfer Profile** field set to the default (i.e., None).
15. Click **Finish** to save, exit, and re-display the Server Flows information screen showing the newly-created server flow, similar to the example in Figure 11–51 below.

Configuring SBC for Avaya Trunk

Procedure

1. Perform all of the previous steps (i.e., Step-1 through Step-7), needed for all trunk configurations, including a SIP trunk with Avaya. One particular parameter setting (i.e., Interworking Profile) must be specifically selected, as detailed below.
2. Login to the SBC Control Center as the `Admin`.
3. Select the Server Configuration function of the Global Profiles feature from the Task Pane.

4. Server Configuration screen that is displayed with the default **General** tab selected, in the profile list, select the trunk server name (e.g., Trunk_Server_1) of the server previously created in part two of Step-4.
5. Click on the **Advanced** tab to display the trunk server information screen.

   In the Server Configuration screen example below, the **Interworking Profile** field already has the correct profile (e.g., avaya-ru) selected for the Avaya server. If the correct profile is not selected for Avaya, continue with the remaining steps on the next page.
6. If the correct **Interworking Profile** name for Avaya is not selected in the **Advanced** tab screen, click the **Edit** button to display the Advanced Edit pop-up screen, and select the profile name for the Avaya Interworking Profile.
7. Click **Finish** to save and exit.
8. Select the **Server Interworking** function of the Global Profiles feature from the Task Pane.
9. Select the `avaya-ru` default Interworking Profile from the **Interworking Profiles** list on the left and select the **Advanced** tab in the Server Interworking screen.
10. Click the **Edit** button at the bottom of the screen to display the Advanced Edit window.
11. De-select the **Avaya Extensions** checkbox.
12. Click **Finish** to save and exit.
13. Select the **General** tab in the Server Interworking screen.
14. Click the **Edit** button at the bottom of the screen to display the General Edit window.
15. In the **Hold Support** parameter field, select the **RFC2453** checkbox.
16. Click **Next** in this screen and click **Finish** in the next screen to save and exit.

SBCE Configuration for other trunks

Perform all of the previous steps (i.e., Step-1 through Step-7), needed for all trunk configurations, including parameter settings that are specific to the type of trunk server being configured.

Different server interworking features will need to be enabled for different trunk servers based on customer requirements. If a default Interworking Profile is not available, then a new one must be configured by following the instructions in Adding a New Server Interworking Profile on page 290.

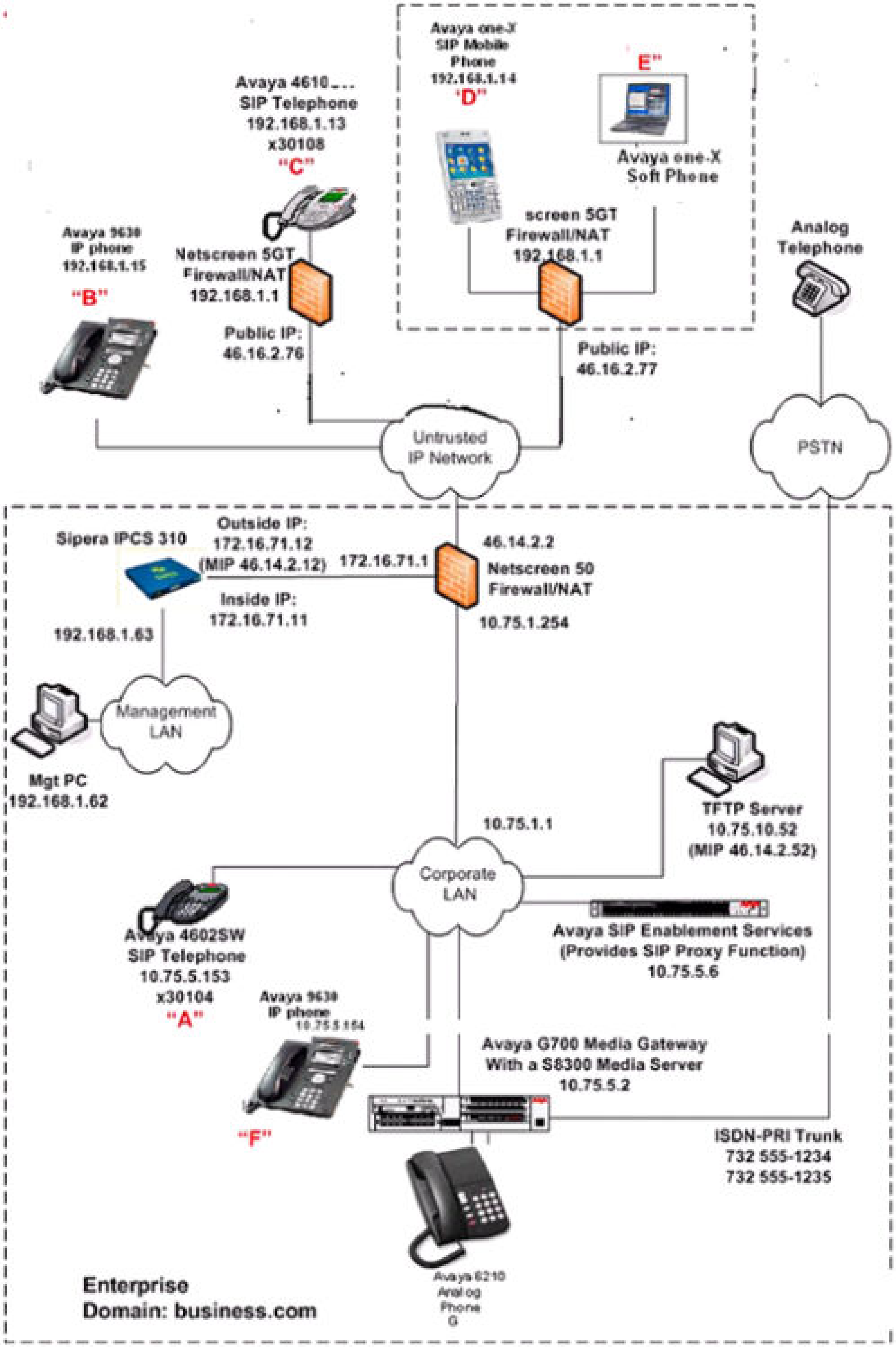
Chapter 12: Configuration Workflows for Mobile Workspace

Avaya configuration workflow for mobile workspace

This section provides a configuration workflow for Avaya Mobile Workspace

Mobile workspace for Avaya topology (Advanced Services only)

The figure below contains a topology diagram for Avaya mobile workspace.


Avaya one-X
SIP Mobile
Phone
192.168.1.14
'D"
E"
Avaya one-X
Soft Phone
Avaya 4610...
SIP Telephone
192.168.1.13
x30108
"C"
screen 5GT
Firewall/NAT
192.168.1.1
Avaya 9630
IP phone
192.168.1.15
"B"
Netscreen 5GT
Firewall/NAT
192.168.1.1
Analog
Telephone
Public IP:
46.16.2.76
Public IP:
46.16.2.77
Untrusted
IP Network
PSTN
Outside IP:
172.16.71.12
(MIP 46.14.2.12)
Sipera IPCS 310
172.16.71.1
46.14.2.2
Netscreen 50
Firewall/NAT
Inside IP:
172.16.71.11
192.168.1.63
10.75.1.254
Management
LAN
Mgt PC
192.168.1.62
TFTP Server
10.75.10.52
(MIP 46.14.2.52)
10.75.1.1
Corporate
LAN
Avaya SIP Enablement Services
(Provides SIP Proxy Function)
10.75.5.6
Avaya 4602SW
SIP Telephone
10.75.5.153
x30104
"A"
Avaya 9630
IP phone
10.75.5.104
Avaya G700 Media Gateway
With a S8300 Media Server
10.75.5.2
"F"
ISDN-PRI Trunk
732 555-1234
732 555-1235
Enterprise
Domain: business.com
Avaya 6210
Analog
Phone
G

Configuring an Avaya Cluster (Advanced Services only)

About this task

This section details the procedure for Avaya SBCE configuration for an Avaya cluster in either Secure Mode (Step 4-a) or Non-Secure Mode (Step 4-b).

Procedure

1. Create Avaya call server profile.
   - Create server profile for Avaya call server.
2. Create signaling interfaces.
   - Create external signaling interface toward phone network.
   - Create internal signaling interface toward Avaya call server.
3. Create media interfaces.
   - Create external media interface toward phone network.
   - Create internal media interface toward Avaya call server.
4. Create Avaya cluster.
   - EITHER create Avaya cluster (in Secure Mode).
   - OR create Avaya cluster (in Non-Secure Mode).
5. Create different configuration servers for different phone feature sets.
6. Create server flow.
7. Create routing profile toward Avaya call server.
8. Create subscriber flow.

Step-1 Create Avaya Call Server Profile (Advanced Services only)

About this task

Use the following procedure to create an Avaya call server profile.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.

2. Select the **Server Configuration** function from the **Global Profiles** feature from the Task Pane.
3. Select **Add** from the Applications pane.
   The Add Server Configuration Profile pop-up screen is displayed.
4. Enter a name for the server profile and select **Next**
   A second Add Server Configuration Profile pop-up screen is displayed.
5. In the second Add Server Configuration Profile pop-up screen, in the Server Type field drop-down menu, select **Call Server**.
6. In the second Add Server Configuration Profile pop-up screen, in the IP Addresses / Supported FQDNs edit fieldfield, enter the IP address of the Avaya server or its FQDN.
7. In the second Add Server Configuration Profile pop-up screen, in the Supported Transports fields, select the checkboxes for both TCP and UDP.
8. In the second Add Server Configuration Profile pop-up screen, in the TCP Port field, enter `5060`.
9. In the second Add Server Configuration Profile pop-up screen, in the UDP Port field, enter `5060`.

   Note:

   Port number 5060 is the default port number that is used for both TCP and UDP. If your Call Server uses a different port, enter that value in the Port fields for TCP and UDP.
10. In the second Add Server Configuration Profile pop-up screen, in the TLS Port field, leave this field blank and click **Next**.
    The Add Server Configuration Profile – Authentication screen is displayed.
11. Completion of the Add Server Configuration Profile – Authentication screen is optional. If you are using server authentication, enter the related information in this screen. Otherwise, click on **Next** to skip this screen.
    The Add Sever Configuration Profile – Heartbeat pop-up screen is displayed.
12. Completion of the Add Server Configuration Profile – Heartbeat screen is optional. If you are using the heartbeat feature, enter the related information in this screen. Otherwise, click on **Next** to skip this screen.
    The Add Sever Configuration Profile – Advanced pop-up screen is displayed.
13. In the Add Server Configuration Profile – Advanced screen, in the Interworking Profile field drop-down menu, select the default Avaya server profile name (e.g., avaya-ru).

    Note:

    Leave the other parameters in the Add Server Configuration Profile – Advanced screen set to their default values.

14. Select **Finish** to save and exit.

Step-2 Create Signaling Interfaces (Advanced Services only)

This section provides procedures for creating external and internal signaling interfaces.

Create external signaling interface toward phone network

About this task

Use the following procedure to create an external signaling interface toward the phone network.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Interface** function from the **Device Specific Settings** feature from the Task Pane.
   The signaling interface screen is displayed.
3. Select **Add** from the Applications pane.
   The Add Signaling Interface pop-up screen is displayed.
4. In the Add Signaling Interface pop-up screen, in the Name edit field, enter a descriptive name for the external signaling interface toward the phone network.
5. In the Add Signaling Interface pop-up screen, in the IP Address drop-down menu, select the IP address of the external signaling interface.
6. In the Add Signaling Interface pop-up screen, in the TCP Port field, enter `5060`.
7. In the Add Signaling Interface pop-up screen, in the UDP Port field, enter `5060`.

   Note:

   Port number 5060 is the default port number that is used for both TCP and UDP. If your Call Server uses a different port, enter that value in the Port fields for TCP and UDP.
8. In the Add Signaling Interface pop-up screen, in the TLS Port field, enter `5065`.
9. Do not select the Cluster TLS checkbox.
10. Do not select the Enable Stun checkbox.

11. In the TLS Profile drop-down menu, select the profile name for TLS.
12. Select **Next** to save and exit.

Create internal signaling interface toward Avaya call server

About this task

Use the following procedure to create an internal signaling interface toward the Avaya call server.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Interface** function from the **Device Specific Settings** feature from the Task Pane.
   The signaling interface screen is displayed.
3. Select **Add** from the Applications pane.
   The Add Signaling Interface pop-up screen is displayed.
4. In the Add Signaling Interface pop-up screen, in the Name edit field, enter a descriptive name for the internal signaling interface toward the Avaya call server.
5. In the Add Signaling Interface pop-up screen, in the IP Address drop-down menu, select the IP address of the internal signaling interface.
6. In the Add Signaling Interface pop-up screen, in the TCP Port field, enter `5060`.
7. In the Add Signaling Interface pop-up screen, in the UDP Port field, enter `5060`.

   Note:

   Port number 5060 is the default port number that is used for both TCP and UDP. If your Call Server uses a different port, enter that value in the Port fields for TCP and UDP.
8. In the Add Signaling Interface pop-up screen, in the TLS Port field, enter `5065`.
9. Do not select the Cluster TLS checkbox.
10. Do not select the Enable Stun checkbox.
11. In the TLS Profile drop-down menu, select the profile name for TLS.
12. Select **Finish** to save, exit, and display the newly-created external and internal signaling interfaces.

Step-3 Create Media Interfaces (Advanced Services only)

This section provides procedures for creating external and internal media interfaces.

Create external media interface toward phone network

About this task

Use the following procedure to create an external media interface toward the phone network.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Media Interface** function from the **Device Specific Settings** feature from the Task Pane.
   The media interface screen is displayed.
3. Select **Add** from the Applications pane.
   The Add Media Interface pop-up screen is displayed.
4. In the Add Media Interface pop-up screen, in the Name edit field, enter a descriptive name for the external media interface toward the phone network.
5. In the Add Media Interface pop-up screen, in the IP Address drop-down menu, select the IP address of the external media interface.
6. In the Add Media Interface pop-up screen, in the Port Range fields, enter the starting and ending port range numbers.
7. Select **Finish** to save and exit.

Create internal media interface toward Avaya call server

About this task

Use the following procedure to create an internal media interface toward the Avaya call server.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Signaling Interface** function from the **Device Specific Settings** feature from the Task Pane.
   The media interface screen is displayed.
3. Select **Add** from the Applications pane.
   The Add Media Interface pop-up screen is displayed.
4. In the Add Media Interface pop-up screen, in the Name edit field, enter a descriptive name for the internal media interface toward the Avaya call server.
5. In the Add Media Interface pop-up screen, in the IP Address drop-down menu, select the IP address of the internal media interface.
6. In the Port Ranges fields, enter the starting and ending port range numbers.
7. Select **Finish** to save, exit, and display the newly-created external and internal media interfaces.

Step-4 Create Avaya Cluster (Advanced Services only)

This section provides procedures for creating an Avaya cluster.

Step-4A Create Avaya Cluster in Secure Mode

About this task

Use the following procedure to create an Avaya cluster in secure mode.

Note:

Secure mode is useful when external users want to:

- Use TLS for SIP
- Use https for the phone configuration file download

You will have to create a TLS Server Profile to be used for the https traffic.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.

The SIP cluster screen is displayed.

3. Select **Add** from the Applications pane.
   The Add SIP cluster pop-up screen is displayed.
4. In the Add SIP cluster pop-up screen, in the Name edit field, enter a descriptive name for the new SIP cluster.
5. In the Add SIP cluster pop-up screen, in the Call Server Type drop-down menu, select **Avaya**.
6. Select **Next** to save and continue.
   A second Add SIP cluster pop-up screen is displayed.
7. In the second Add SIP cluster pop-up screen, enter the requested information into the appropriate fields. Ensure that the Secure Mode field Enabled checkbox is selected.

   Note:

   For more information on creating SIP clusters, see the section titled, "Managing SIP Clusters," in Chapter 6.
8. In the second Add SIP cluster pop-up screen, select the SDP Capability Negotiation for SRTP field Enabled checkbox to ensure that SBC communications with end-points is compliant with RFC 5939, if required.
9. In the Domain Name field, enter the domain name for the Avaya call server.
10. In the Configuration Update Interval field, enter the interval value, which is usually 15 minutes.
11. Select **Next** to save and continue.
    The Add Primary Device pop-up screen is displayed.
12. In the Add Primary Device pop-up screen, in the Avaya SBCE Device Name field drop-down menu, select the name of the applicable Avaya SBCE device (e.g., "Device_1").
13. In the Add Primary Device pop-up screen, in the Avaya SBCE Device IP field drop-down menu, select the IP address of the applicable Avaya SBCE device.
14. In the Add Primary Device pop-up screen, in the Configuration Server Client Address field drop-down menu, select the IP address where the Avaya SBCE sends traffic toward the configuration file server.

    Note:

    The configuration server client IP address usually resides in the same Avaya SBCE device that is selected in the Device Name field above.
15. Select **Next** to save and continue.
    The Add Configuration Server pop-up screen is displayed.
16. In the Add Configuration Server pop-up screen, in the Server Type field drop-down menu, select **HTTPS**.

17. In the Add Configuration Server pop-up screen, In the SBCE Port field, enter the SBCE receiving port. The default is 443.
18. In the Add Configuration Server pop-up screen, In the Real Server IP field, enter the IP address of the configuration file server. This is the same address that you entered in the Configuration Server Client Address field.
19. In the Add Configuration Server pop-up screen, In the Real Server Port field, enter `80`.
20. In the Add Configuration Server pop-up screen, In the Server TLS Profile field drop-down menu, select the name of the Profile that is configured to receive https traffic.
21. In the Add Configuration Server pop-up screen, select **Next**.
    The Add Signaling Server pop-up screen is displayed.
22. In the Add Signaling Server pop-up screen, in the Server Configuration Profile field drop-down menu, select the name of the profile (e.g., “Call_Server_1”) that you may have created previously that was referred to in the note at the beginning of this section (i.e., “You will have to create a TLS Server Profile to be used for the https traffic.”).
23. In the End Point Signaling Interface field drop-down menu, select the interface where the Avaya SBCE is to receive signaling traffic (e.g., callserver).
24. In the Session Policy Group field drop-down menu, select default.
25. Select **Finish** to save and exit.

    Note:

    Your cluster is now configured for downloading phone configuration files via https in secure mode

Step-4B Create Avaya Cluster in Non-Secure Mode

About this task

Use the following procedure to create an Avaya cluster in non-secure mode.

Note:

The procedure in Step-4B for creating a cluster in non-secure mode is almost identical to the 23 steps performed previously in Step-4A for creating a cluster in secure mode, with the exception of changes in three of the procedure steps:

- In Step 7, the Secure Mode – Enabled checkbox should NOT be selected.
- In Step 16, select **HTTP** instead of **HTTPS**.
- In Step 17, select **80** instead of **443**.

When configuring for non-secure mode, it will not be necessary to create a TLS Server Profile since the HTTP server type is used instead of the HTTPS server type that is used for secure https traffic.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
3. Select **Add** from the Applications pane.
   The Add SIP cluster pop-up screen is displayed.
4. In the Add SIP cluster pop-up screen, in the Name edit field, enter a descriptive name for the new SIP cluster.
5. In the Add SIP cluster pop-up screen, in the Call Server Type drop-down menu, select **Avaya**.
6. Select **Next** to save and continue.
   A second Add SIP cluster pop-up screen is displayed.
7. In the second Add SIP cluster pop-up screen, enter the requested information into the appropriate fields. Ensure that the Secure Mode field Enabled checkbox is NOT selected.

   Note:

   For more information on creating SIP clusters, see the section titled, “Managing SIP Clusters,” in Chapter 6.
8. In the second Add SIP cluster pop-up screen, select the SDP Capability Negotiation for SRTP field Enabled checkbox to ensure compliance with RFC 5939, if required.
9. In the Domain Name field, enter the domain name for the Avaya call server.
10. In the Configuration Update Interval field, enter the interval value, which is usually 15 minutes.
11. Select **Next** to save and continue.
    The Add Primary Device pop-up screen is displayed.
12. In the Add Primary Device pop-up screen, in the Avaya SBCE Device Name field drop-down menu, select the name of the applicable Avaya SBCE device (e.g., “Device_1”).
13. In the Add Primary Device pop-up screen, in the Avaya SBCE Device IP field drop-down menu, select the IP address of the applicable Avaya SBCE device.
14. In the Add Primary Device pop-up screen, in the Configuration Server Client Address field drop-down menu, select the IP address where the Avaya SBCE sends traffic toward the configuration file server.

Note:

The configuration server client IP address usually resides in the same Avaya SBCE device that is selected in the Device Name field above.

15. Select **Next** to save and continue.
    The Add Configuration Server pop-up screen is displayed.
16. In the Add Configuration Server pop-up screen, in the Server Type field drop-down menu, select **HTTP** for non-secure mode. (Note that **HTTPS** would be entered here for secure mode.)
17. In the Add Configuration Server pop-up screen, In the Port field, enter the SBC receiving port number of **80** for the HTTP server for non-secure mode. (Note that the default value of **443** would be entered here for the HTTPS server for secure mode.)
18. In the Add Configuration Server pop-up screen, In the Real Server IP field, enter the IP address of the configuration file server. This is the same address that you entered in the Configuration Server Client Address field.
19. In the Add Configuration Server pop-up screen, In the Real Server Port field, enter `80`.
20. Skip this step. (Note that Step 20 is eliminated when configuring for non-secure Mode.)
21. In the Add Configuration Server pop-up screen, select **Next**.
    The Add Signaling Server pop-up screen is displayed.
22. In the Add Signaling Server pop-up screen, in the Server Configuration Profile field drop-down menu, select the name of the profile (e.g., “Call_Server_1”) that you may have created previously that was referred to in the note at the beginning of this section (i.e., “You will have to create a TLS Server Profile to be used for the https traffic.”).
23. In the End Point Signaling Interface field drop-down menu, select the interface where the Avaya SBCE is to receive signaling traffic (e.g., callserver).
24. In the Session Policy Group field drop-down menu, select default.
25. Select **Finish** to save and exit.

Note:

Your cluster is now configured for downloading phone configuration files via http in non-secure mode..

Step-5 Create Different Configuration Servers for Different Phone Set Features (Advanced Services only)

The Primary Tab on the SIP Cluster information screen, accessible by selecting the Cluster Proxy function of the SIP Cluster feature in the Task Pane, is the area where you go to create different configuration servers for each new phone set feature and service. The following sections provide procedure examples for creating configuration servers for several different services.

Example 1 — WML Services

About this task

Use the following procedure to create a configuration server for WML services.

Note:

Wireless Markup Language (WML) , based on XML, is a markup language intended for devices that implement the Wireless Application Protocol (WAP) specification, such as mobile phones.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
3. Select the Primary Tab.
   The SIP Cluster Primary Tab Information screen is displayed.
4. In the SIP Cluster Primary Tab Information screen, in the Configuration Servers section, click on the **Add** button.
   The Add Configuration Server Pop-up screen is displayed.
5. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **HTTP Proxy**.
6. In the Add Configuration Server Pop-up screen, in the Port field, leave the default value of 8080.

   Note:

   The default SBC Port number is 8080. If your SBC uses a different port, enter that value in the Port field.

7. In the Add Configuration Server Pop-up screen, in the Real Server IP field, enter the IP address of the WML server.
8. In the Add Configuration Server Pop-up screen, in the Real Server Port field, leave the default value of 8080.
9. In the Add Configuration Server Pop-up screen, select **Finish** to save, exit, and redisplay the Primary Tab information screen containing the newly-added configuration server.

Example 2 — LDAP Services

About this task

Use the following procedure to create a configuration server for LDAP services.

Note:

The Lightweight Directory Access Protocol (LDAP) is a client-server protocol for querying and modifying a directory service and often is adopted on an LDAP server to authenticate users.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
3. Select the Primary Tab.
   The SIP Cluster Primary Tab Information screen is displayed.
4. In the SIP Cluster Primary Tab Information screen, in the Configuration Servers section, click on the **Add** button.
   The Add Configuration Server Pop-up screen is displayed.
5. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **LDAP**.
6. In the Add Configuration Server Pop-up screen, in the Port field, enter **389**.
7. In the Add Configuration Server Pop-up screen, in the Real Server IP field, enter the IP address of the LDAP server.
8. In the Add Configuration Server Pop-up screen, in the Real Server Port field, enter the LDAP server port number.

9. In the Add Configuration Server Pop-up screen, select **Finish** to save, exit, and redisplay the Primary Tab information screen containing the newly-added configuration server.

Example 3 — SCEP Services

About this task

Use the following procedure to create a configuration server for SCEP services.

Note:

The Simple Certificate Enrollment Protocol (SCEP) is being referenced by several manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users.

The protocol is designed to make the issuing and revocation of digital certificates as scalable as possible. The idea is that any standard network user should be able to request their digital certificate electronically and as simply as possible.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
3. Select the Primary Tab.
   The SIP Cluster Primary Tab Information screen is displayed.
4. In the SIP Cluster Primary Tab Information screen, in the Configuration Servers section, click on the **Add** button.
   The Add Configuration Server Pop-up screen is displayed.
5. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **SCEP**.
6. In the Add Configuration Server Pop-up screen, in the Port field, enter the SCEP port value.
7. In the Add Configuration Server Pop-up screen, in the Real Server IP field, enter the IP address of the SCEP server.
8. In the Add Configuration Server Pop-up screen, in the Real Server Port field, enter the SCEP server port number.

9. In the Add Configuration Server Pop-up screen, select **Finish** to save, exit, and redisplay the Primary Tab information screen containing the newly-added configuration server.

Example 4 — HTTP Services

About this task

Use the following procedure to create a configuration server for HTTP services.

Procedure

1. Avaya 46xx or 96xx Phones

   Note:

   The 46xx and 96xx phones use http as configuration server in the Avaya SBCE. Add a configuration server for http.
2. Login to the Avaya SBCEControl Center as Admin.
3. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
4. Select the Primary Tab.
   The SIP Cluster Primary Tab Information screen is displayed.
5. In the SIP Cluster Primary Tab Information screen, in the Configuration Servers section, click on the **Add** button.
   The Add Configuration Server Pop-up screen is displayed.
6. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **HTTP**.
7. In the Add Configuration Server Pop-up screen, in the Port field, enter **80**.
8. In the Add Configuration Server Pop-up screen, in the Real Server IP field, enter the IP address of the HTTP server.
9. In the Add Configuration Server Pop-up screen, in the Real Server Port field, enter the HTTP server port number.
10. In the Add Configuration Server Pop-up screen, select **Finish** to save, exit, and redisplay the Primary Tab information screen containing the newly-added configuration server.
11. Avaya Soft Phones

Note:

The Avaya soft phones require the Relay Services for the Personal Profile Manager (PPM) download. Add a configuration server for http.

12. Login to the Avaya SBCEControl Center as Admin.
13. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
    The SIP cluster screen is displayed.
14. Select the Primary Tab.
    The SIP Cluster Primary Tab Information screen is displayed.
15. In the SIP Cluster Primary Tab Information screen, in the Configuration Servers section, click on the **Add** button.
    The Add Configuration Server Pop-up screen is displayed.
16. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **HTTP**.
17. Select the Relay Services checkbox in the Options fields area located immediately below the Server Type field area.
18. In the Add Configuration Server Pop-up screen, in the Port field, enter **80**.
19. In the Add Configuration Server Pop-up screen, in the Real Server IP field, enter the IP address of the Avaya call server or the IP address of the PPM server.
20. In the Add Configuration Server Pop-up screen, in the Real Server Port field, enter either the Avaya call server port number or the PPM server port number.
21. In the Add Configuration Server Pop-up screen, select **Finish** to save, exit, and redisplay the Primary Tab information screen containing the newly-added configuration server.

Example 5 — Third Party or Non-Colocated PPM Server

About this task

Use the following procedure to create a configuration server for a third party server or a non-colocated PPM server.

Before beginning the procedure for creating a PPM Server, ensure that you have at least one HTTP server or HTTPS server created first (see requirements note below). If not, create an HTTP or HTTPS server first before beginning this procedure.

Note:

This configuration example applies to the use of a third-party Personal Profile Manager (PPM) server or to the use of an Avaya SIP PPM server that is not collocated within the Avaya SIP Enablement Service (SES).

The conditional requirements for this configuration are:

- Avaya Cluster
- At least one HTTP or HTTPS server

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Cluster Proxy** function from the **SIP Cluster** feature from the Task Pane.
   The SIP cluster screen is displayed.
3. In the SIP Cluster Proxy screen, in the Application Pane, select the **Add** button.
   The Add SIP Cluster pop-up screen. is displayed.
4. In the Add SIP Cluster pop-up screen, enter a name in the Cluster Name field.
5. In the Add SIP Cluster pop-up screen, select **Avaya** in the Callserver Type field pull-down menu.
6. Select **Next**.
   The second Add SIP Cluster pop-up screen. is displayed.
7. In the second Add SIP Cluster pop-up screen, enter the appropriate information and select **Next**.

   Note:

   In the Miscellaneous Information fields, the Configuration Update Interval is a required field, and should contain a value between 15 minutes and 1440 minutes (1 day).

   The Add Primary Device pop-up screen is displayed.
8. In the Add Primary Device pop-up screen, enter the appropriate information and select **Next**.
   The Add Configuration Server pop-up screen is displayed.
9. In the Add Configuration Server Pop-up screen, in the Server Type field drop-down menu, select **PPM** .
10. In the Add Configuration Server Pop-up screen, enter any other applicable information and then select **Finish** to save, exit, and redisplay the updated SIP Cluster Proxy screen showing the newly-added cluster.

Step-6 Create Server Flow (Advanced Services only)

About this task

Use the following procedure to create a subscriber flow or server flow.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **End Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The End Point Flows Flows Subscriber/Server screen is displayed.
3. In the End Point Flows Subscriber/Server screen, in the Content Area, select the Server Flows tab.
   The Server Flows tab screen. is displayed.
4. In the Server Flows tab screen, select the **Add** button in the upper-right portion of the screen.
   The Add Flow pop-up screen is displayed.
5. In the Add Flow pop-up screen, in the Flow Name field, enter a meaningful name (e.g., “Line Side Server”).
6. In the Add Flow pop-up screen, in the Server Configuration field drop-down menu, select the name (e.g., Config_Server_1) of the call (line side) server profile.
7. In the Add Flow pop-up screen, leave the following fields set to the default value (*): URI Group, Transport, and Remote Subnet
8. In the Add Flow pop-up screen, in the Received Interface field drop-down menu, select the name (e.g., Sig_Intf_Ext_to_Phone_Net) of the interface pointing toward the phone network.
9. In the Add Flow pop-up screen, in the Signaling Interface field drop-down menu, select the name (e.g., Sig_Intf_Int_to_Call_Server) of the interface pointing toward the Avaya call server.
10. In the Add Flow pop-up screen, in the Media Interface field drop-down menu, select the name (e.g., Med_Intf_1) of the interface pointing toward the phone network.
11. In the Add Flow pop-up screen, leave the End Point Policy Group field set to the default (i.e., default-low).
12. In the Add Flow pop-up screen, leave the Routing Profile field set to the default (i.e., default).
13. In the Add Flow pop-up screen, leave the Topology Hiding Profile field set to the default (i.e., None).

14. Select **Finish** to save, exit, and display the server flows information screen showing the newly-created server flow.

Step-7 Create Routing Profile toward Avaya Call Server (Advanced Services only)

About this task

Use the following procedure to create a routing profile toward the call server.

Note:

This example procedure creates a routing profile that will be named Route_to_Avaya_Server, which will hae the next hop configured as the Avaya call server address.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane.
   The Routing Profiles information screen is displayed.
3. In the Routing Profiles information screen, at the top of the Application Pane, select the **Add** button.
   The Routing Profile pop-up screen is displayed.
4. In the Routing Profile pop-up screen, in the Profile Name field, enter the name as “Route_to_Avaya_Server.”
5. In the Routing Profile pop-up screen, select **Next**
   A second Routing Profile pop-up screen is displayed
6. In the second Routing Profile pop-up screen, in the Next Hop Server 1 field, enter the IP address of the next hop server (i.e., the IP address of the Avaya call server).
7. In the second Routing Profile pop-up screen, select the checkbox for “Routing Priority based on Next Hop Server.”
8. In the second Routing Profile pop-up screen, select one of the Outgoing Transport modes (i.e., TLS, TCP, or UDP).
9. In the second Routing Profile pop-up screen, select **Finish** to save, exit, and redisplay the Routing Profile information screen showing the newly-created Routing Profile.

Step-8 Create Subscriber Flow (Advanced Services only)

About this task

Use the following procedure to create a subscriber flow.

Note:

This example procedure creates a subscriber flow that will be named Subscriber_Flow_1.

Procedure

1. Login to the Avaya SBCEControl Center as Admin.
2. Select the **End Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The Subscriber Flows information screen is displayed.
3. In the Subscriber Flows information screen, at the top right-hand portion of the Content Area, select the **Add** button.
   The Add Flow pop-up screen is displayed.
4. In the Add Flow pop-up screen, in the Flow Name field, enter the name as “Subscriber_Flow_1.”
5. In the Add Flow pop-up screen, leave the default (*) value in the following fields: URI Group, User Agent, Source Subnet, Via Host, and Contact Host.
6. In the Add Flow pop-up screen, in the Signaling Interface field drop-down menu, select the name (i.e., Sig_Intf_1) of the interface that receives all of the SIP traffic from the phone network.
7. In the Add Flow pop-up screen,, select **Next**.
   A second Add Flow pop-up screen is displayed.
8. In the second Add Flow pop-up screen, in the Profile section in the Source field, select the **Subscriber** button.
9. In the second Add Flow pop-up screen, select one of the Outgoing Transport modes (i.e., TLS, TCP, or UDP).
10. In the second Add Flow pop-up screen, in the Methods Allowed Before REGISTER field scroll list, select one or more methods that are to be allowed before registering. You can select multiple methods with Control-Clicks or with Click and Shift-Click to select a range.
11. In the second Add Flow pop-up screen, In the Media Interface field drop-down menu, select the name (e.g., Med_Intf_Ext_to_Phone_Net) of the interface that receives all the media traffic from the phone network.
12. In the second Add Flow pop-up screen, Leave the End Point Policy Group field set to default-low.

Note:

If the phones use TLS/SRTP, select the appropriate end policy group from the End Point Policy Group field drop-down menu.

13. In the second Add Flow pop-up screen, Do not select the SIP Cluster Flow checkbox.
14. In the second Add Flow pop-up screen, In the Routing Profile field drop-down menu, select the name (e.g., Route_to_Avaya_Server) of the routing profile that points toward the Avaya call server.
15. In the second Add Flow pop-up screen, Leave the Topology Hiding Profile set to None.
16. In the second Add Flow pop-up screen, In the Phone Interworking Profile field drop-down list, select the Avaya_Ru profile name.
17. In the second Add Flow pop-up screen, Leave the setting of None in the following fields: TLS Client Profile and File Transfer Profile.
18. In the second Add Flow pop-up screen, select **Finish** to save, exit, and redisplay the updated Subscriber Flows screen containing the newly-created Subscriber Flow

Chapter 13: Signaling Manipulation

Signaling manipulation

This application note provides an overview of Avaya's SIP signaling header manipulation feature for the Avaya SBCE product. This feature adds the ability to add, change and delete any of the headers and other information in a SIP message. The feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language that will be presented in sections that follow.

This application note describes Avaya's SIP signaling header manipulation feature as follows:

- SigMa Scripting Language ─ The proprietary scripting language developed by Avaya to define any SIP message manipulation that will be performed by SBC.
- 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 is provided through the standard Avaya SBCE Configuration/ Management Graphical User Interface.

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 SBC appliance then interprets this script at the given "hook point." (See the section titled, "Hook Points.")

SigMa primer

A SigMa script consists of one or more "Within Session" statements. Each of these statements 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.

Session statement

This section describes the three parts of the session statement, which are Method, Where Clause, and Code Block.

Session Statement

- Method — The Method statement is where you specify the SIP request method that initiates the session.
- Where Clause — The Where Clause statement is used to specify the Session selection criteria on top of the Method for which the *Code Block* needs to 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 below:Where Clause Variables on page 394
- Code Block — The Code Block is where the operations are written and encapsulated with a set of braces {}. The operations may include further selection criteria and actual operations on headers themselves.

  There are three different statements that 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:

There can be as many of the above statements written in a given session code block, as needed for a given script.

Where clause variables

Variable	Description
%INITIAL_REQUEST	This is 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 the Session's Where Clause, several Session Variables can be checked against to specify the matching criteria. The Session Variables that are valid in this clause are given in the table below.

A list of session variables with descriptions is provided in the table below.Session variables on page 395

Session variables

Variable	Description	Applicable For
%DIRECTION	This value can be "INBOUND" for incoming messages or "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 These values are explained in a separate section below.	act on message act on request act on response
%METHOD	Values can be: • INVITE • REGISTER • ACK • PRACK • BYE • CANCEL, and • etc The method name could be any method either already part of standards or proprietary.	%METHOD

Variable	Description	Applicable For
%IN_DIALOG	This is a Boolean variable. Takes either “TRUE” or “FALSE”. This indicates if the given message is a in-dialog message or a dialog creating message.	act on request
%RESP_CODE	Represents a valid SIP response code. Any value between [100, 600] is a valid one.	act on response
%REQ_METHOD	Same as METHOD. But it represents for which method the given response corresponds to.	act on response

Code blocks

The code blocks for the act on statements will contain the code necessary to carry out actions. There are four kinds of statements that can go into the code block: Assignment Statement, Conditional Statement, Function Call, and Print Statement.

Code Blocks

A list of the 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. This statement takes the following form:

```
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. A function call is usually called on a built-in function. They are the following:
  - remove(): to remove a header
  - append(): to append string to a header
  - regex_replace(): to replace text within a header using a regular expression.
- Print Statement. A Print statement prints the parameters given into the log file of the process as an INFO level log. The parameters need to be separated by commas and can be any of – free string in quotes, variables or any of the built-in variables.
  - print "foo", "bar";
  - print "Body(1) is – ", %BODY[1];

Built—in variables and arrays

There are several built-in variables and arrays in SigMa, 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. They also have a built-in hierarchy to represent the various elements within headers and SDP specification.

Built—In Variables and Arrays

Lists of built-in variables and arrays, with their valid forms, descriptions, and illustrations are provided in the following tables and figures.

HEADERS Variable on page 398

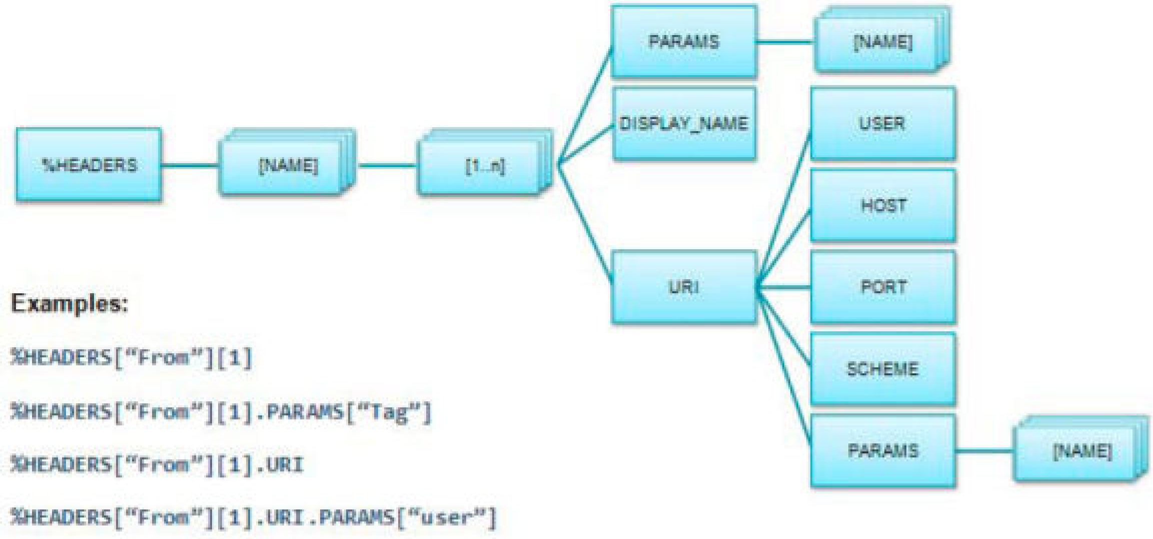
SDP Variable on page 399

Other Variables on page 400

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 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”]	Refer to various elements within a URI.

Example



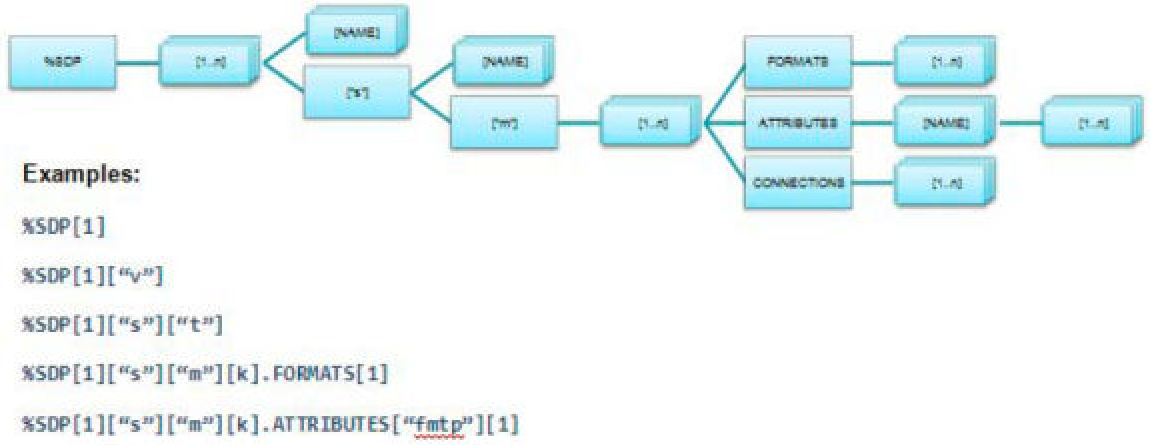
Examples:

```
%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]	Refer to nth media format specification.
	%SDP[j][“s”][“m”][k].ATTRIBUTES[“Name”][n]	Refer to nth instance of “Name” attribute in the kth media specification.
	%SDP[m][“s”][“m”][n].CONNECTIONS[k]n]	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]
```

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

There are several built-in functions available mostly for doing regular expression operations. These functions are explained in the table below.

Built—In Functions

A list of built-in functions, with their valid forms and descriptions is provided in the following table.

Built-In Functions Table on page 400

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”])	

Variable	Valid Forms	Description
regex_match()	%HEADERS[“Header”].regex_match(“regex”)	Returns “TRUE” or “FALSE” based on 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 empty string if no match was found.
	%HEADERS[“Header”].PARAMS[“Param”].regex_get(“regex”)	
regex_replace()	HEADERS[“Header”].regex_replace(“regex”, “string”)	Replaces a given match with the provide 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 can be used within assignment and conditional statements. All of the user defined variables are of string type. The variables names must all start with a ‘%’ sign and can have alpha numeric characters in their names. The only other valid extra character allowed within the variable name is the ‘_’ (underscore).

Hook points

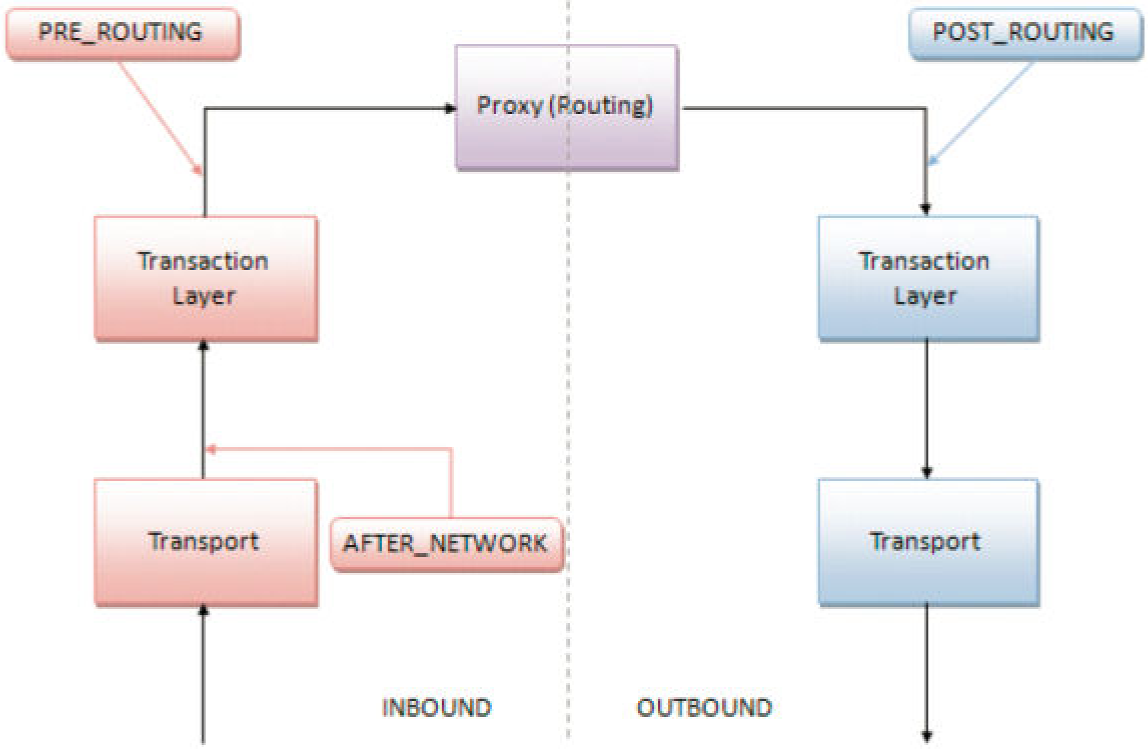
There are several hook points that are illustrated and described in the figure and table which follow.

Hook points are points within the SBC processing where given actions can be executed. These hook points can be specified by using the `%ENTRY_POINT` built-in variable within a where clause.

Hook Point	Description
AFTER_NETWORK	This is a point in packet path soon after the packet is received from network.

PRE_ROUTING	After the transaction layer, before target destination for the packet is determined.
POST_ROUTING	After target destination is determined, before the transaction layer.

Example



SigMa Scripting Examples

The SigMa scripting language is best demonstrated using some examples. This table provides some examples that explain some use cases and how they can be represented in a SigMa script.

Description	Scripting Example

Reverting From and To tags in all responses to REGISTER method.	`within session "REGISTER"`
	`{`
	`act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"`
	`    {`
	`        %from_tag = %HEADERS["From"][1].PARAMS["Tag"];`
	`        %HEADERS["From"][1].PARAMS["Tag"] = %HEADERS["To"][1].PARAMS["Tag"];`
	`        %HEADERS["To"][1].PARAMS["Tag"] = %from_tag;`

<table>
<tr>
<td></td>
<td>

```
    }
}
```

</td>
</tr>
<tr>
<td>Updating p-asserted-identity field with the value of From header if P-Asserted-Identity field value is anonymous</td>
<td>

```
within session "ALL"
{
act on message where %DIRECTION=”OUTBOUND” and
%ENTRY_POINT=”POST_ROUTING”
    {
        if (%HEADERS[“P-Asserted-Identity”]
[1].URI.USER = “anonymous”) then
        {
            %aor = %HEADERS[“From”][1].URI;
           %HEADERS[“P-Asserted-Identity”][1] = %aor;
        }
    }
}
```

</td>
</tr>
<tr>
<td>Adding a media attribute in SDP</td>
<td>

```
within session "ALL"
{
    act on message where %DIRECTION=”OUTBOUND” and
%ENTRY_POINT=”POST_ROUTING”
    {
       %SDP[1][“s”][“m”][1].ATTRIBUTES[“fmtp”] = “101
0-16”;
    }
}
```

</td>
</tr>
<tr>
<td>Adding a header</td>
<td>

```
within session "ALL"
{
    act on message where %DIRECTION=”OUTBOUND” and
%ENTRY_POINT=”POST_ROUTING”
    {
        %HEADERS[“SLiC-Version”][1] = “3.2.2”;
    }
}
```

</td>
</tr>
<tr>
<td>Trunking: Removing phone_context param from Request Uri, To and From headers</td>
<td>

```
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”]);
    }
}
```

</td>
</tr>
<tr>
<td>Learn P-Asserted-Identity from INVITE and use this value to replace From URI in every Request</td>
<td>

```
within session "INVITE"
{
act on request where %DIRECTION=”OUTBOUND” and
%ENTRY_POINT=”POST_ROUTING”
    {
        If (%INITIAL_REQUEST = ”TRUE”) then
        {
            %passert_val = %HEADERS[“P-Asserted-
Identity”][1].URI;
        }
        else
        {
            %HEADERS[“From”][1].URI = %passert_val;
```

</td>
</tr>
</table>

	`}` `}` `}`

Trunking: For all new calls, add diversion header if it doesn't 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);`
	`}`
	`}`
	`}`

SigMa Scripting Tutorial

The following section includes 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 it may not contain the actual identity. It usually 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 there is no P-Asserted-Identity header field present, a proxy MAY 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. It is a request message
2. The message is coming to the SBC

If both the above conditions are successful, as soon as the message comes from the wire, (and after the basic sanity checks and DoS checks are performed on the message), the action is performed. The script checks to see if a “P-Asserted-Identity” header exists. If it does, it removes it, else it adds the header.

Limitations

If you would like to remove all the P-Asserted-Identity headers, it is assumed that you know the maximum number of headers that would be present in the messages. You do not need to know the exact number of headers that come in because if you perform an operation on a header that does not exist, it is simply 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 it is not present in the message, `%HEADERS[“<Header-Name>”][<Header Position>] = <VAL>` will add the header to the message.

Test Case 2 - Adding a Media Attribute in SDP

Use Case

It might be required to add/modify SDP attributes or 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 looks into 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

We would need to know the number of codecs (number of formats in format-list parameter and attributes), or we would end up replacing an existing format-type.

Test Case 3 - Changing Calling Party Presentation to Restricted

Use Case

Same.

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

Same.

Limitations

None.

Test Case 4 - Replace “From” Header For a Set of Users

Use Case

In an organization, there could be several phones used by the employees and each of them might have a unique “From URI” associated with them. It may be required that all calls going out from the organization 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 above 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, i.e., `regex_match(<regular expression>)`, can be any valid Perl regular expression. However, the “$” symbol can’t be used in the regular expression.

Test Case 5 - Editing the “Allow” Header

Use Case

The Allow header is used to indicate the methods supported by the user agent. Eg: 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 may 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 can come in handy while operating on headers such as Allow, Supported, Content-Type etc, whose values can’t be extracted individually as compared to headers like “From”, “To”, or “Contact”.

Limitations

The regular expression in `regex_replace` can’t have the $ symbol.

Test Case 6 - Prefix Stripping

Use Case

Phone numbers may come in with a prefix. Sometimes, this needs to be stripped off before the call is routed. This is useful in scenarios where a call transfer is made and the number to which the call has to 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

The messages which have the “Refer-To” method are checked if the URI contains a prefix. If so, it is stripped before sending it out.

Limitations

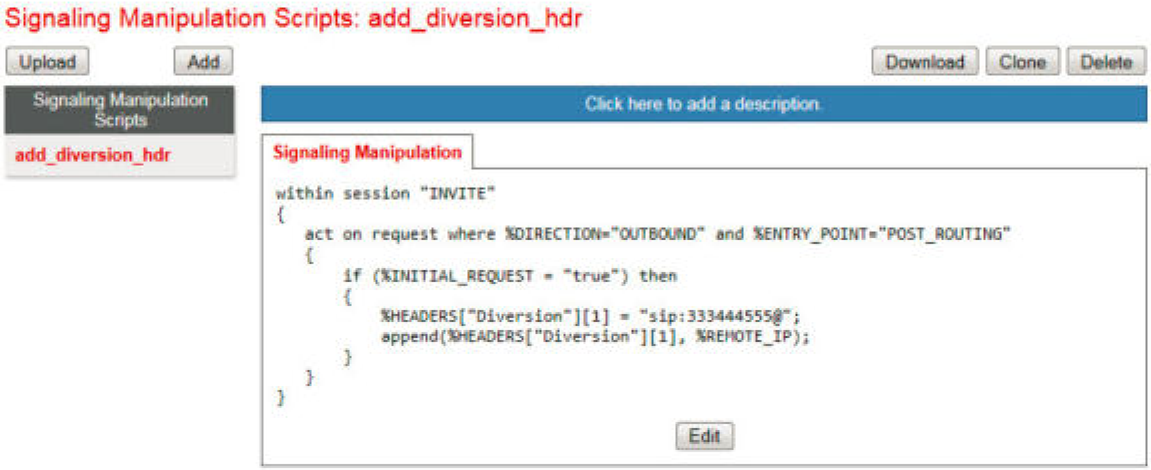
The regular expression in `regex_replace` can’t have the $ symbol.

SBC GUI SigMa Editor

The Signaling Manipulation SigMa Editor screen is accessed by selecting the Signaling Manipulation function from the Global Profiles feature in the Task Pane. This screen contains a full set of controls for managing all of your Signaling Manipulation scripts, including the following:

Interface	Description
Signaling Manipulation Scripts Pane	Lists all of the 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.

Interface	Description
	Note: By consecutively clicking on additional script names in the list, you can open up multiple SigMa Editor screens at one time.
Edit Button	Inside each SigMa Editor window at the bottom is an Edit button. Clicking on this button allows you to make modifications to the existing script.
Save Button	Once the Edit button is clicked and modifications are made to an existing script, you can click on a Save button to save the changes to the script. **Note:** Once the Save button is clicked, the script will be transparently submitted to the backend and validated before it is saved to the disk. If it fails validation, error messages will be displayed to the user to help them correct any syntax errors in the script.
Add Script Button	Located above the scripts pane, is an Add Script button which allows you to create a new script by opening up a blank SigMa Editing window to the right.
Upload Script Button	Allows you to upload the selected script to a remote location.
Download Script Button	Allows you to download a script to the device from a remote location.
Clone Script Button	Allows you to copy the selected script to a new script name for the purposes of modifying the newly named script for different functionality.
Delete Script Button	Allows you to delete the selected script



Signaling Manipulation Scripts: add_diversion_hdr
Upload
Add
Download
Clone
Delete
Signaling Manipulation Scripts
add_diversion_hdr
Click here to add a description.
Signaling Manipulation
Edit

```
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);
        }
    }
}
```

Sigma Design Overview

A Sigma Process Flowchart is provided below.

Note:

Once you have created a SigMa script, you will have to specify it in a Server Configuration before you can execute it.

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:

The procedure below assumes that no Server Configurations have been created yet. If you are specifying a SigMa script in a Server Configuration that already exists, proceed to Step 9 of this procedure.

Procedure

1. Login to the SBC Control Center as the Admin.
2. Select the Server Configuration function from the Global Profiles feature from the Task Pane.
   The Server Configuration screen is displayed.
3. In the Server Configuration screen, select the **Add** button.

The first Add Server Configuration screen is displayed.

4. In the first Add Server Configuration Profile screen, enter a name in the Profile Name field and select Next.
   The second Add Server Configuration Profile General screen is displayed.
5. In the second Add Server Configuration General screen, enter the appropriate information, and then select **Next**.
   The third Add Server Configuration Profile Authentication screen is displayed.
6. In the third Add Server Configuration Authentication screen, enter the appropriate information, and then select **Next**.
   The fourth Add Server Configuration Profile Heartbeat screen is displayed.
7. In the fourth Add Server Configuration Heartbeat screen, enter the appropriate information, and then select **Next**.
   The fifth Add Server Configuration Profile Advanced screen is displayed.
8. In the fifth Add Server Configuration Advanced screen, enter the appropriate information, and then select **Finish**.
   Configuration is saved, and the updated Server Configuration screen is refreshed showing the newly-added profile.
9. In the Server Configuration screen, select the profile name and then click the Advanced tab button.
10. In the Server Configuration Advanced Tab screen, select the Edit button to display the Edit Server Configuration Profile – Advanced screen.
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** to submit, save, and exit.

Chapter 14: Remote Access

Remote access

Secure Access Link

Secure Access Link (SAL) is used for remote access for SBCE's in non-IP Office environments. The SBC needs to be registered for remote access with the customer SAL.

SSL VPN

Remote access to the SBC when sold with IP Office is to SSL VPN into IP Office and then hop to the SBC. IP Office and SBC need to be registered together and some configuration needs to be done. For details on this please 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:

SSL VPN configured in the SBC is not currently used or supported in 6.2

Appendix A: Alarm List

System alarms list

Related topics:

CPU alarms on page 417
Memory alarms (including Swap Space) on page 418
Disk partition space alarms on page 419
Hard disk failure alarm on page 419
Link failure alarm on page 420
Process failure alarm on page 421
Database failure alarm on page 421
Component failure alarm on page 422

CPU alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
CPU	CPU utilization is over 80%	CPU utilization is betwee	No	Alarm	Minor	CPU utilization is betwee	CPU utilization goes below	No

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
		n 80%-89%.				n 80%-89%.	80% or above 89%.	
CPU	CPU utilization is over 90%	CPU utilization is between 90%-99%.	No	Alarm	Major	CPU utilization is between 90%-99%.	CPU utilization goes below 90% or becomes 100%.	No
CPU	CPU utilization is 100%	CPU utilization is 100%.	Yes	Alarm	Critical	CPU utilization is 100%.	CPU utilization becomes 100%.	No

Memory alarms (including Swap Space)

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Memory	Memory utilization is over 80%	Memory utilization is between 80%-89%.	No	Alarm	Minor	Memory utilization is between 80%-89%.	Memory utilization goes below 80% or above 89%.	No
Memory	Memory utilization is over 90%	Memory utilization is between 90%-99%.	Yes	Alarm	Major	Memory utilization is between 90%-99%.	Memory utilization goes below 90% or becomes 100%.	No
Memory	Memory utilization is 100%	Memory utilization is 100%.	Yes	Alarm	Critical	Memory utilization is 100%.	Memory utilization becomes 100%.	No

Disk partition space alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Disk partition <partition_name> utilization is over 80%	Disk partition utilization is between 80%-89%.	No	Alarm	Minor	Disk partition utilization is between 80%-89%.	Disk partition utilization goes below 80% or above 89%.	No
Disk partition space	Disk partition <partition_name> utilization is over 90%	Disk partition utilization is between 90%-99%.	Yes	Alarm	Major	Disk partition utilization is between 90%-99%.	Disk partition utilization goes below 90% or becomes 100%.	No
Disk partition space	Disk partition <partition_name> utilization is 100%	Disk partition utilization is 100%.	Yes	Alarm	Critical	Disk partition utilization is 100%.	Disk partition utilization becomes 100%.	No

Hard disk failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Hard disk failure	Hard disk <disk_id> failure	Hard disk failure	Yes	Alarm	Critical	The hard disk drive has	The alarm is cleared only when	Yes. Hard disk drive must be

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
						failed and cannot be used.	the kernel detects no failures when testing the hard disk drive. This will only happen when the hard disk drive is replaced.	replaced.

Link failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Link failure	Network link failure <interface>	Network link goes down on the given interface.	Yes. No traffic can be sent or received on the failed link.	Alarm	Critical	A link on a particular interface in down and cannot be used.	Network connection is restored and alarm manually cleared by user.	Yes. User needs to manually restore the link.

Process failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Process failure	Application failure	One or more system processes failed to send a heartbeat ping.	Yes. Port By-pass is automatically enabled.	Alarm	Critical	One or more system processes is malfunctioning	Malfunctioning process is restarted either automatically by the system or manually by the Security Administrator and the alarm cleared.	Yes. Required if automatic self-start is not successful.

Database failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database failure	Database failure	Connectivity to the database has been lost.	Yes. Port By-pass is automatically enabled after multiple failed restarts.	Alarm	Critical	Either the database is down or connectivity to the database has been lost.	The database failure being cleared either automatically by the system or manuall	Yes. Required if automatic self-start is not successful.

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
							y by the Security Administrator.	

Component failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Component failure	Component failure	One or more elements (signaling, media, intelligence, or EMS) in a multi-component configuration has failed to send a heartbeat ping.	Yes	Alarm	Critical	One or more SBCE server elements (signaling, media, intelligence, or EMS) is malfunctioning.	The malfunctioning elements could be restarted manually and the alarm cleared manually.	Required if self restart in not successful.

GUI and console alarm list

- New User Added Alarms on page 423
- New Administrator Added Alarms on page 423
- User Privilege Change Alarms on page 424

- User Deleted Alarms on page 424
- Login Failure Alarms on page 425

Related topics:

New user-added alarm on page 423
New Administrator-added alarm on page 423
User privilege change alarm on page 424
User deleted alarms on page 424
Login failure alarm on page 425

New user-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New User Added	New User Added: <username>	A new GUI/ System user was added.	No	Alarm	Informational	A new user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

New Administrator-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New Admin-added	Admin User Added: <username>	A new GUI/ System admin user was added.	No	Alarm	Informational	A new admin user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

User privilege change alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Privilege Change	User Privilege Changed: <username>	A user's access privilege was changed (either from admin to normal or from normal to admin).	No	Alarm	Informational	A user's access privilege was changed (either from admin to normal or from normal to admin).	Alarm either cleared by the administrator or it times-out.	No

User deleted alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Deleted	User deleted: <username>	A new GUI/ System admin user was deleted.	No	Alarm	Informational	A user was deleted from the system.	Alarm either cleared by the administrator or it times-out.	No

Login failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Login failure	User login failure: <username>	A user had multiple consecutive login failures.	No	Alarm	Warning	A user had more than a certain number of consecutive login failures.	Alarm either cleared by the administrator or it times-out.	No

Appendix B: SBC SNMP Details

SNMP MIB overview

This appendix provides SNMP details on the Avaya SBCE. Standard Management Information Bases (MIBs) are defined in RFC-1213. Avaya SBCE supports rfc1213.mib.

MIB-II support

The Avaya SBCEsupports MIB-II (RFC1213) for the SBC data interfaces. UDP port 8001 is used for MIB-II support.

- SBC listens on Port 161 for Avaya-mib
- Port 8001 is used for MIB-II

SBC OID Descriptions

This section describes the key Object Identifiers (OIDs).

Private Enterprise OIDS support

Avaya SBCE supports the following private enterprise OIDS.

ipcs stats sip calls: .1.3.6.1.4.1.25257.1.4.1	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipcalls
ipcs stats sip protocol: .1.3.6.1.4.1.25257.1.4.3	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipprotocol
Ipcsincidenceinfo: .1.3.6.1.4.1.25257.2	.iso.org.dod.internet.private.enterprises.Avaya.ipcsincidencesinfo
Ipcsalarmainfo: .1.3.6.1.4.1.25257.4	.iso.org.dod.internet.private.enterprises.Avaya.ipcsalarmsinfo

MIB tree structure

Avaya SBCE private enterprise OIDS MIB tree structure

FIGURE E-1 MIB Tree Structure

Key OIDS

Ipcsstatssipcalls

ipcssipcTotalRegistrationRequests	Number of Registration Requests received at node. This does not include the registration triggered by node for keeping the pinhole open.
ipcssipcTotalRegistrationsChallenged	Number of Registrations Challenged by node and also includes the number of challenges from the Call Server. The number of registrations challenged by IPCS node includes the SIP 401/407 based Radius Authentication Responses (AAA feature) and SIP 407 based SIV Authentication Responses (DOS feature).
ipcssipcTotalRegistrationsRejected	Number of Registrations Rejected by the node and also includes the failed registration responses observed from the call server at the node. Failed registration responses include the SIP 4xx-7xx class responses excluding SIP 400, SIP 401/407 Responses. The registrations are rejected by node due to failed registration challenges, failed registration processing and registrations blocked due to security features.
ipcssipcTotalCallsReceived	Total Number of SIP Calls received at the node. This one equals Calls Blocked + Calls Allowed.
ipcssipcTotalCallsBlocked	Number of SIP calls Blocked by the node due to SIP Parse errors, failed AAA challenges and calls blocked due to security features.
ipcssipcTotalCallsAllowed	Number of SIP calls classified by the node as Legitimate.

Classification of Requests/Responses matching a particular Domain Policy Group at the node

ipcsTotalINVITES	Number of SIP INVITE messages
ipcsTotalINVITERetransmits	Number of SIP INVITE Retransmits
ipcsTotalINVITE100Responses	Number of SIP INVITE 100 Responses
ipcsTotalINVITE1XXResponses	Number of SIP INVITE 1XX class Responses excluding SIP 100 Response.
ipcsTotalINVITE200Responses	Number of SIP INVITE 200 Responses
ipcsTotalINVITE200ResponseRetransmits	Number of SIP INVITE 200 Response Retransmits
ipcsTotalINVITE4XX6XXResponses	Number of SIP INVITE 4XX 6XX Responses
ipcsTotalINVITE4XX6XXResponseRetransmits	Number of SIP INVITE 4XX 6XX Response Retransmits
ipcsTotalBYESent	Number of SIP BYE requests
ipcsTotalBYERetransmits	Number of SIP BYE Retransmits
ipcsTotalBYE200Responses	Number of SIP BYE 200 Responses
ipcsTotalCANCELSent	Number of SIP CANCEL requests
ipcsTotalCANCEL200Responses	Number of SIP CANCEL 200 Responses
ipcsTotalACK200Responses	Number of SIP ACK requests for INVITE 200 OK Response
ipcsTotalACK4XX6XXResponses	Number of SIP ACK requests for INVITE 4xx-6xx class Responses
ipcsTotalACKTimeOuts	Number of SIP ACK timeouts ie. Number of ACK requests missing for the INVITE 200 OK/4xx-6xx class responses
ipcsTotalNonInviteRequests	Number of NonInvite Requests
ipcsTotalNonInvite1xxResponses	Number of NonInvite 1xx Responses
ipcsTotalNonInvite2xxResponses	Number of NonInvite 2xx Responses. Also includes the 200 OK responses for BYE and CANCEL requests

Out of Dialog Requests dropped

ipcsTotalOutOfDialogReferMesFromNW	Number of Out of Dialog REFER requests dropped at the node
IpcsTotalAckMessageOutOfDialogue	Number of Out of Dialog ACK requests dropped at the node
IpcsTotalByeMessageOutOfDialogue	Number of Out of Dialog BYE requests dropped at the node
IpcsTotalCancelMessageOutOfDialogue	Number of Out of Dialog CANCEL requests dropped at the node
IpcsTotalNotifyMessageOutOfDialogue	Number of Out of Dialog NOTIFY requests dropped at the node
ipcsTotalReinviteMessageOutOfDialogue	Number of Out of Dialog RE-INVITE requests dropped at the node

Out of Dialog Responses dropped

ipcsTotal1XXMessageOutOfDialogue	Number of Out of Dialog 1XX class responses dropped by the node
ipcsTotal2XXMessageOutOfDialogue	Number of Out of Dialog 2XX class responses dropped by the node
ipcsTotal3XXMessageOutOfDialogue	Number of Out of Dialog 3XX class responses dropped by the node
ipcsTotal4XXMessageOutOfDialogue	Number of Out of Dialog 4XX class responses dropped by the node
ipcsTotal5XXMessageOutOfDialogue	Number of Out of Dialog 5XX class responses dropped by the node
ipcsTotal6XXMessageOutOfDialogue	Number of Out of Dialog 6XX class responses dropped by the node

Out of Transaction Responses dropped

ipcsTotal1XXMessageOutOfTransaction	Number of 1XX Messages received out of transaction dropped by the node

ipcsTotal2XXMessageOutOfTransaction	Number of 2XX Messages received out of transaction dropped by the node
ipcsTotal3XXMessageOutOfTransaction	Number of 3XX Messages received out of transaction dropped by the node
ipcsTotal4XXMessageOutOfTransaction	Number of 4XX Messages received out of transaction dropped by the node
ipcsTotal5XXMessageOutOfTransaction	Number of 5XX Messages received out of transaction dropped by the node
ipcsTotal6XXMessageOutOfTransaction	Number of 6XX Messages received out of transaction dropped by the node
ipcsTotalCancelMessageOutOfTransaction	Number of CANCEL requests received out of transaction dropped by the node

Statistics details with examples

One external-external call through IPCS between two external phones

In the following scenario, a call is made from A to B.

1. No of Registrations in Statistics: Counter increments by 2

   One registration per phone, so in total 2 registrations from both A and B .

2. No of Invites in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives an INVITE

   First INVITE from phone A towards IPCS which is sent to call server.

   Second INVITE from Call Server towards IPCS which is sent to phone B

3. No of Invites 200 Responses in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives a 200 Ok for INVITE sent

   First 200 ok response from phone B towards IPCS which is sent to call server.

   Second 200 ok response from Call Server towards IPCS which is sent to phone A

4. No of Bye in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives a Bye

   First Bye from phone A towards IPCS which is sent to call server.

   Second Bye from Call Server towards IPCS which is sent to phone B

One external-internal call through IPCS between external phone A and internal phone C

In the following scenario, a call is made from A to C and the call is disconnected at A.

1. No of Registrations in Statistics: Counter increments by 1

   One registration per phone, so in total 1 registration
   Phone C registration will not be seen by IPCS as it is internal phone
2. No of Invites in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives an INVITE
   INVITE from phone A towards IPCS which is sent to call server
3. No of Invites 200 Responses in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives a 200 Ok for INVITE sent
   200 ok response from phone C towards IPCS which is sent to phone A
4. No of Bye in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives a Bye
   Bye from phone A towards IPCS which is sent to call server

SBC MIB

The following is the Avaya SBCE MIB.

```
-- File Name : AVAYA_IPCS_MIB(4).mib
-- Date      : Mon Dec 09 10:16:55 IST 2009
-- Author    : AdventNet Agent Toolkit C Edition - MibEditor 6

AVAYA-IPCS-MIB DEFINITIONS ::= BEGIN
    IMPORTS
         DisplayString, RowStatus, DateAndTime
                 FROM SNMPv2-TC
         DisplayString
                 FROM RFC1213-MIB
         enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32, Gauge32,
 Counter32, NOTIFICATION-TYPE, Counter64, IpAddress
                 FROM SNMPv2-SMI;

        moduleIdentity MODULE-IDENTITY
             LAST-UPDATED "200610030823Z"
             ORGANIZATION "Avaya "
             CONTACT-INFO ""
             DESCRIPTION  ""
             REVISION  "200610030823Z"
             DESCRIPTION  ""
             ::=  {  enterprises  1  }
```

```
       org OBJECT IDENTIFIER
           ::=  {  iso  3  }

       dod OBJECT IDENTIFIER
           ::=  {  org  6  }

       internet OBJECT IDENTIFIER
           ::=  {  dod  1  }

        private OBJECT IDENTIFIER
            ::=  {  internet  4  }

        enterprises OBJECT IDENTIFIER
            ::=  {  private  1  }

        Avaya OBJECT IDENTIFIER
            ::=  {  enterprises  25257  }

         ipcsstatisticsinfo OBJECT IDENTIFIER
            ::=  {  Avaya  1  }

         ipcsincidencesinfo OBJECT IDENTIFIER
            ::=  {  Avaya  2  }

      notifications  OBJECT IDENTIFIER
         ::=  { Avaya 3}

         ipcsalarmsinfo OBJECT IDENTIFIER
            ::=  {  Avaya  4  }

         ipcsstatssip OBJECT IDENTIFIER
            ::=  {  ipcsstatisticsinfo  4  }

         ipcsincidencesTable OBJECT-TYPE
            SYNTAX  SEQUENCE  OF  IpcsincidencesEntry
            MAX-ACCESS not-accessible
            STATUS  current
            DESCRIPTION "Table for Incidences."
            ::=  { ipcsincidencesinfo  1 }

         ipcsincidencesEntry OBJECT-TYPE
            SYNTAX  IpcsincidencesEntry
            MAX-ACCESS not-accessible
            STATUS  current
            DESCRIPTION "Row for each incidence entry."
            INDEX  {  ipcsincidenceId  }
            ::=  { ipcsincidencesTable 1 }

         IpcsincidencesEntry  ::=  SEQUENCE {
            ipcsincidenceName  OCTET STRING,
            ipcsincidenceId  Integer32,
            ipcsincidenceCategory  OCTET STRING,
            ipcsincidenceCause  OCTET STRING,
            ipcsincidenceTimeStamp  DateAndTime,
            ipcsincidenceIpcsId  OCTET STRING,
            ipcsincidencesRowStatus  RowStatus
            }

         ipcsincidenceName OBJECT-TYPE
            SYNTAX   OCTET STRING
            MAX-ACCESS  read-write
            STATUS   current
            DESCRIPTION  "Name of the incidence raised."
            :=  {  ipcsincidencesEntry  1  }
         ipcsincidenceId OBJECT-TYPE
```

```
            SYNTAX   Integer32
            MAX-ACCESS  not-accessible
            STATUS   current
            DESCRIPTION  "Unique incidence Identity."
            ::=  {  ipcsincidencesEntry  2  }

        ipcsincidenceCategory OBJECT-TYPE
           SYNTAX   OCTET STRING
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "Catagory of the incidence raised.Different categories
include DOS, FINGER_PRINT, POLICY, ROUTE, MEDIA_ANOMALY, SIP_2FA."
           ::=  {  ipcsincidencesEntry  3  }

        ipcsincidenceCause OBJECT-TYPE
           SYNTAX   OCTET STRING
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "Cause for the incidence raised."
           ::=  {  ipcsincidencesEntry  4  }

        ipcsincidenceTimeStamp OBJECT-TYPE
           SYNTAX   DateAndTime
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "Time stamp when the incidence was raised."
           ::=  {  ipcsincidencesEntry  5  }

        ipcsincidenceIpcsId OBJECT-TYPE
           SYNTAX   OCTET STRING
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "ID of the SBCE on which this incidence was raised."
           ::=  {  ipcsincidencesEntry  6  }

        ipcsincidencesRowStatus OBJECT-TYPE
           SYNTAX   RowStatus
           MAX-ACCESS  read-create
           STATUS   current
           DESCRIPTION  "RowStatus of this incidence entry."
           ::=  {  ipcsincidencesEntry  7  }

        ipcsalarmsTable OBJECT-TYPE
           SYNTAX  SEQUENCE  OF  IpcsalarmsEntry
           MAX-ACCESS not-accessible
           STATUS  current
           DESCRIPTION "Table for Alarms."
           ::=  { ipcsalarmsinfo  1 }

        ipcsalarmsEntry OBJECT-TYPE
           SYNTAX  IpcsalarmsEntry
           MAX-ACCESS not-accessible
           STATUS  current
           DESCRIPTION "Row for each Alarm entry."
           INDEX  { ipcsalarmsId  }
           ::=  { ipcsalarmsTable 1 }

        IpcsalarmsEntry  ::=  SEQUENCE {
           ipcsalarmsName  DisplayString,
           ipcsalarmsId  Integer32,
           ipcsalarmsMessage  DisplayString,
           ipcsalarmsSequenceNumber  Counter64,
           ipcsalarmsSystemType  DisplayString,
           ipcsalarmsRowStatus  RowStatus
           }
        ipcsalarmsName OBJECT-TYPE
           SYNTAX   DisplayString
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "Name of the alarm raised (Refer to the SBCE manual for the
different alarms)."
           ::=  {  ipcsalarmsEntry  1  }

        ipcsalarmsId OBJECT-TYPE
           SYNTAX   Integer32
           MAX-ACCESS  not-accessible
           STATUS   current
           DESCRIPTION  "ID of the alarm raised. Each alarm type/alarm name will
have a unique id."
           ::=  {  ipcsalarmsEntry  2  }

        ipcsalarmsMessage OBJECT-TYPE
           SYNTAX   DisplayString
           MAX-ACCESS  read-write
           STATUS   current
           DESCRIPTION  "Detailed message relating to the alarm raised."
           ::=  {  ipcsalarmsEntry  3  }

        ipcsalarmsSequenceNumber OBJECT-TYPE
           SYNTAX   Counter64
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Sequence number of the alarm raised. This is the unique id
for each alarm."
           ::=  {  ipcsalarmsEntry  4  }

        ipcsalarmsTimestamp OBJECT-TYPE
           SYNTAX   DateAndTime
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Time stamp when the alarm was raised."
           ::=  {  ipcsalarmsEntry  5  }

        ipcsalarmsSystemType OBJECT-TYPE
           SYNTAX   DisplayString
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "ID of the SBCE on which this alarm was raised."
           ::=  {  ipcsalarmsEntry  6  }

        ipcsalarmsRowStatus OBJECT-TYPE
           SYNTAX   RowStatus
           MAX-ACCESS  read-create
           STATUS   current
           DESCRIPTION  "RowStatus of the alarm raised."
           ::=  {  ipcsalarmsEntry  7  }

        ipcsincidenceNotification NOTIFICATION-TYPE
           OBJECTS   {ipcsincidenceCategory, ipcsincidenceCause, ipcsincidenceId,
ipcsincidenceIpcsId, ipcsincidenceName, ipcsincidenceTimeStamp }
           STATUS   current
           DESCRIPTION  "Notification for the incidence."
           ::=  {  notifications  1  }

        ipcsalarmsNotification NOTIFICATION-TYPE
           OBJECTS   {ipcsalarmsId, ipcsalarmsMessage, ipcsalarmsName,
ipcsalarmsSequenceNumber, ipcsalarmsSystemType, ipcsalarmsTimestamp }
           STATUS   current
           DESCRIPTION  "Notification for the alarm."
           ::=  {  notifications  2  }

        ipcsstatssipcalls OBJECT IDENTIFIER
           ::=  {  ipcsstatssip  1  }

        ipcsstatssipprotocol OBJECT IDENTIFIER
           ::=  {  ipcsstatssip  3  }

        ipcssipcTotalRegistrationRequests OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Registration Requests received. This does not
include the registration triggered by IPCS for keeping the pinhole open."
           ::=  {  ipcsstatssipcalls  1  }

        ipcssipcTotalRegistrationsChallenged OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Registrations Challanged by the node"
           ::=  {  ipcsstatssipcalls  2  }

        ipcssipcTotalRegistrationsRejected OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Registrations Rejected by the node due to failed
registration challenges."
           ::=  {  ipcsstatssipcalls  3  }

        ipcssipcTotalCallsReceived OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Total Number of SIP Calls received at the node. This one
equals .Calls Blocked + Calls Allowed."
           ::=  {  ipcsstatssipcalls  4  }

        ipcssipcTotalCallsWithAnomalyDetected OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
         DESCRIPTION  "Total Number of SIP Calls detected with anomaly at the node. "
           ::=  {  ipcsstatssipcalls  5  }

        ipcssipcTotalCallsBlocked OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP calls Blocked by the node. This one is Less
than or equal to Calls With Anomaly Detected."
           ::=  {  ipcsstatssipcalls  6  }

        ipcssipcTotalCallsAllowed OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP calls classified by the node as Legitimate."
           ::=  {  ipcsstatssipcalls  7  }

        ipcssipcTotalMessagesExchanged OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP messages exchanged between the node and the
network."
           ::=  {  ipcsstatssipcalls  8  }

        ipcssipcTotalActiveRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active registrations."
           ::=  {  ipcsstatssipcalls  9  }

        ipcssipcTotalActiveCalls OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active calls."
           ::=  {  ipcsstatssipcalls  10  }

        ipcssipcTotalActiveTCPRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active TCP registrations."
           ::=  {  ipcsstatssipcalls  11  }

        ipcssipcTotalActiveUDPRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active UDP registrations."
           ::=  {  ipcsstatssipcalls  12  }

        ipcssipcTotalActiveTLSRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active TLS registrations."
           ::=  {  ipcsstatssipcalls  13  }

        ipcssipcTotalActiveSRTPCalls OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP active SRTP calls."
           ::=  {  ipcsstatssipcalls  14  }

        ipcssipcTotalRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total registrations."
           ::=  {  ipcsstatssipcalls  15  }

        ipcssipcTotalTCPRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total TCP registrations."
           ::=  {  ipcsstatssipcalls  16  }

        ipcssipcTotalUDPRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total UDP registrations."
           ::=  {  ipcsstatssipcalls  17  }

        ipcssipcTotalTLSRegistrations OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total TLS registrations."
           ::=  {  ipcsstatssipcalls  18  }

        ipcssipcTotalCalls OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total calls."
           ::=  {  ipcsstatssipcalls  19  }

        ipcssipcTotalCallsFailed OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total calls failed."
           ::=  {  ipcsstatssipcalls  20  }

        ipcssipcTotalRegistrationsDroppedByMissingPolicy OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
          DESCRIPTION  "Number of SIP total registrations dropped by missing policy."
           ::=  {  ipcsstatssipcalls  21  }

        ipcssipcTotalInvitesDroppedByMissingPolicy OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP total invites dropped by missing policy."
           ::=  {  ipcsstatssipcalls  22  }

        ipcssipTtlCallsDeniedDueToPolicy OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
          DESCRIPTION  "Number of SIP total calls rejected due to Policy Violation."
           ::=  {  ipcsstatssipcalls  23  }

        ipcssipTtlSessDroppedDueToMaxNumofConcSessExc OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP sessions dropped due to Max no of concurrent
sessions exceed."
           ::=  {  ipcsstatssipcalls  24  }

        ipcsTotalINVITES OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP INVITE messages"
           ::=  {  ipcsstatssipprotocol  1  }

        ipcsTotalINVITERetransmits OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP INVITE Retransmits"
           ::=  {  ipcsstatssipprotocol  2  }
```

```
   ipcsTotalINVITE100Responses OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 100 Responses"
      ::=  {  ipcsstatssipprotocol  3  }

   ipcsTotalINVITE1XXResponses OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 1XX Responses"
      ::=  {  ipcsstatssipprotocol  4  }

   ipcsTotalINVITE200Responses OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 200 Responses"
      ::=  {  ipcsstatssipprotocol  5  }

   ipcsTotalINVITE200ResponseRetransmits OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 200 Response Retransmits"
      ::=  {  ipcsstatssipprotocol  6  }

   ipcsTotalINVITE4XX6XXResponses OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 4XX 6XX Responses"
      ::=  {  ipcsstatssipprotocol  7  }

   ipcsTotalINVITE4XX6XXResponseRetransmits OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP INVITE 4XX 6XX Response Retransmits"
      ::=  {  ipcsstatssipprotocol  8  }

   ipcsTotalBYESent OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP BYE"
      ::=  {  ipcsstatssipprotocol  9  }

   ipcsTotalBYERetransmits OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP BYE Retransmits"
      ::=  {  ipcsstatssipprotocol  10  }

   ipcsTotalBYE200Responses OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of SIP BYE 200 Responses"
      ::=  {  ipcsstatssipprotocol  11  }

   ipcsTotalCANCELSent OBJECT-TYPE
```

```
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP CANCEL"
           ::=  {  ipcsstatssipprotocol  12  }

        ipcsTotalCANCEL200Responses OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP CANCEL 200 Responses"
           ::=  {  ipcsstatssipprotocol  13  }

        ipcsTotalCANCELRetransmits OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP CANCEL Retransmits"
           ::=  {  ipcsstatssipprotocol  14  }

        ipcsTotalACK200Responses OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP ACK 200 Responses"
           ::=  {  ipcsstatssipprotocol  15  }

        ipcsTotalACK4XX6XXResponses OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of SIP ACK 4XX 6XX Responses"
           ::=  {  ipcsstatssipprotocol  16  }

        ipcsTotalACKTimeOuts OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of ACK Time outs"
           ::=  {  ipcsstatssipprotocol  17  }

        ipcsTotalNonInviteRequests OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of NonInvite Requests"
           ::=  {  ipcsstatssipprotocol  18  }

        ipcsTotalNonInvite1xxResponses OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of NonInvite 1xx Responses"
           ::=  {  ipcsstatssipprotocol  19  }

        ipcsTotalNonInvite2xxResponses OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of NonInvite 2xx Responses"
           ::=  {  ipcsstatssipprotocol  20  }

        ipcsTotalFromAndToHeaderMatchFailure OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
```

```
      STATUS   current
      DESCRIPTION  "Number of From And To Header Match Failure"
      ::=  {  ipcsstatssipprotocol  21  }

   ipcsTotalRegMesWithMoreContacts OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Registration Message With More Contacts"
      ::=  {  ipcsstatssipprotocol  22  }

   ipcsTotalMesWithAddrIncomplete OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Message With Address Incomplete"
      ::=  {  ipcsstatssipprotocol  23  }

   ipcsTotalAuthHeaderMatchFailure OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Auth Header Match Failure"
      ::=  {  ipcsstatssipprotocol  24  }

   ipcsTotalContactSrcAddrMatchFailure OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Contact Srource Addr Match Failure"
      ::=  {  ipcsstatssipprotocol  25  }

   ipcsTotalViaMatchFailure OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Via Match Failure"
      ::=  {  ipcsstatssipprotocol  26  }

   ipcsTotal3XXMesFromNW OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of 3XX Message From Network"
      ::=  {  ipcsstatssipprotocol  27  }

   ipcsTotalOutOfDialogReferMesFromNW OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Out Of Dialog Refer Message From Network"
      ::=  {  ipcsstatssipprotocol  28  }

   ipcsTotalRegistrationMatchFailure OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Registration Match Failure"
      ::=  {  ipcsstatssipprotocol  29  }

   ipcsTotalContactSDPConnMatchFailure OBJECT-TYPE
      SYNTAX   Gauge32
      MAX-ACCESS  read-only
      STATUS   current
      DESCRIPTION  "Number of Contact SDP Match Failure"
```

```
           ::=  {  ipcsstatssipprotocol  30  }

        ipcsTotalSpoofedSipBye OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed Sip Bye"
           ::=  {  ipcsstatssipprotocol  31  }

        ipcsTotalSpoofedReinvite OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed Reinvite"
           ::=  {  ipcsstatssipprotocol  32  }

        ipcsTotalSpoofedCancel OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed Cancel"
           ::=  {  ipcsstatssipprotocol  33  }

        ipcsTotalSpoofedCancelToRemote OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed Cancel To Remote"
           ::=  {  ipcsstatssipprotocol  34  }

        ipcsTotalSpoofed200 OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed 200"
           ::=  {  ipcsstatssipprotocol  35  }

        ipcsTotalSpoofedErrorResp OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Spoofed Error Response"
           ::=  {  ipcsstatssipprotocol  36  }

        ipcsTotalRegistrationFailed OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Registration Failed"
           ::=  {  ipcsstatssipprotocol  37  }

        ipcsTotalAckMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Ack Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  38  }

        ipcsTotalByeMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Bye Message out of Dialogue"
           ::=  {  ipcsstatssipprotocol  39  }
        ipcsTotalCancelMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Cancel Message out of Dialogue"
           ::=  {  ipcsstatssipprotocol  40  }

        ipcsTotalNotifyMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Notify Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  41  }

        ipcsTotal1XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 1XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  42  }

        ipcsTotal2XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 2XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  43  }

        ipcsTotal3XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 3XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  44  }

        ipcsTotal4XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 4XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  45  }

        ipcsTotal5XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 5XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  46  }

        ipcsTotal6XXMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 6XX Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  47  }

        ipcsTotalReinviteMessageOutOfDialogue OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Reinvite Message received out of Dialogue"
           ::=  {  ipcsstatssipprotocol  48  }

        ipcsTotal1XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 1XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  49  }

        ipcsTotal2XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 2XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  50  }

        ipcsTotal3XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 3XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  51  }

        ipcsTotal4XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 4XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  52  }

        ipcsTotal5XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 5XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  53  }

        ipcsTotal6XXMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of 6XX Message received out of Transaction"
           ::=  {  ipcsstatssipprotocol  54  }

        ipcsTotalCancelMessageOutOfTransaction OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Cancel Message received out of transaction"
           ::=  {  ipcsstatssipprotocol  55  }

        ipcsTotalContactMismatchBetweenRegistrationAndInviteMessage OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of Contact Mismatch Between Registration And Invite
Message"
           ::=  {  ipcsstatssipprotocol  56  }

        ipcsTotalFailureToRoute OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Total Number of times Failure to Route has occurred."
           ::=  {  ipcsstatssipprotocol  57  }

        ipcsTotalFailureToRouteCauseDNS OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of times Failure to Route has occurred due to DNS 
look-up failure."
           ::=  {  ipcsstatssipprotocol  58  }

        ipcsTotalFailureToRouteCauseENUM OBJECT-TYPE
           SYNTAX   Gauge32
           MAX-ACCESS  read-only
           STATUS   current
           DESCRIPTION  "Number of times Failure to Route has occurred due to ENUM 
look-up failure."
           ::=  {  ipcsstatssipprotocol  59  }

END
```

Glossary

AAA
Authentication, Authorization, and Accounting

Anti-tromboning
The capability of allowing media traffic to flow directly between two end-points that are located in the same private network, instead of having to traverse the access network before reaching its destination. Also referred to as *Media Release*. See *Tromboning*.

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 SBCAE feature which allows two SBCAE 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 Stand-by. Connected by a heartbeat signal and shared database, the two SBCAE security devices provide fail-over protection in the event one of the devices malfunctions.
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer 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

Packet Spoofing Impersonating a legitimate user transmitting data.

PAP Protected Authentication 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.

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)*.

Tromboning The situation where RTP media traffic originates at a certain point within a network and follows a path out of that network into another network (the access network, for example) and back again to a destination close to where it originated. See *Anti-Tromboning*.

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