# Working with Avaya Session Border Controller and Microsoft® Teams

Release 10.1.x
Issue 6
February 2024

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

**Licenses**

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

**License type(s)**

**Copyright**

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

**Virtualization**

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

**Third Party Components**

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Service Provider**

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

**Compliance with Laws**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

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

**Security Vulnerabilities**

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

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

**Trademarks**

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

# Contents

# Chapter 1: Introduction

## Purpose

This document contains information about installing, configuring, administering, maintaining, troubleshooting, and using Avaya Session Border Controller (Avaya SBC) when integrated with the Microsoft® Teams product.

Implementation engineers, administrators, and support personnel will find this document useful. Usage information will be useful for end users.

## Change history

| Issue | Date | Summary of changes |
|---|---|---|
| 6 | February 2024 | Updated the topic: Configuring Microsoft Teams options required for integration with Avaya SBC on page 53. |
| 5 | June 2023 | Product name changed to Avaya SBC. |
| 4 | August 2021 | Updated the following items:<br>• About licensing requirements on page 85<br>• Avaya SBC licensed features on page 86 |
| 3 | May 2021 | Updated the following sections:<br>• About Avaya SBC and Microsoft Teams on page 9<br>• Configuring Microsoft Teams options required for integration with Avaya SBC on page 53 |

*Table continues…*

| Issue | Date | Summary of changes |
|---|---|---|
| 2 | December 2020 | Updated the following items:<br>• Added information about new Release 8.1.2 enhancements in About Avaya SBC and Microsoft Teams on page 9.<br>• Added information about new media rules options that support new Microsoft Teams enhancements in Media rules field descriptions on page 37.<br>• Added a new procedure for Configuring certificates on page 52.<br>• Added information about new required Microsoft Teams configuration in Configuring Microsoft Teams options required for integration with Avaya SBC on page 53.<br>• Added two procedures for configuring number manipulation with Creating a new signaling rule on page 67 and Adding a URI Manipulation rule on page 75.<br>• Added new information about signaling manipulation in About configuring signaling manipulation for Microsoft Teams on page 77. |

# Chapter 2: Overview

## About Avaya SBC and Microsoft Teams

### General overview

Avaya SBC provides direct SIP and media connectivity between your existing enterprise voice infrastructure (for example, Avaya Aura®), the Public Switched Telephone Network (PSTN) SIP trunking services, and the Direct Routing features of Microsoft® Teams (Teams). Avaya SBC is certified to operate for incoming and outgoing calls using Teams, and provides complete coverage of customer needs with extensive scalability, interoperability, and reliability.

Calls can be made from PSTN or Avaya Aura® to Microsoft® Teams and also from Microsoft® Teams to PSTN or Avaya Aura®.

The support for Avaya SBC integration with Teams is available on Avaya SBC Release 8.1.1 and later.

Avaya SBC provides integration with the Direct Routing features of Teams so that Teams users can make voice calls, in addition to features you already use with Teams, such as video conferencing, file sharing, and chat. Phone System Direct Routing is the service inside of Teams that allows you to connect external phone lines and use Teams as an office phone system. Avaya SBC provides the Microsoft-certified SBC required to connect Teams to a private telecommunications system (PBX), such as Avaya Aura®, and to the PSTN using SIP trunking. Avaya SBC secures these connections and assures interoperability so you can select from hundreds of service providers across the globe.

Teams users can place outgoing calls to and receive incoming calls from users on an Avaya Aura® system. Incoming calls can be directed to Teams users using the Call Coverage or EC500 features of Avaya Aura®. Avaya Aura®, in turn, uses Avaya SBC and the Direct Routing features of Teams to direct calls to or from Teams users. Also, if redirection features for an Avaya Aura® user are exhausted, Avaya SBC can use LDAP routing to send the call to Teams users sequentially. For customers that have Teams users and Avaya Aura® users, the Avaya SBC can be used for both incoming and outgoing calls between Teams users and Avaya Aura® users.

For detailed information about configuring Teams when using the Direct Routing features of Avaya SBC, see the following Teams website:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page

### Microsoft® Teams enhancements

Enhancements are added to Avaya SBC Release 8.1.2 to support the following features for connectivity with Microsoft® Teams:

- Media Bypass for Direct Routing using IETF Interactive Connectivity Establishment (ICE)

- Local Media Optimization for Direct Routing

Media Bypass

Media Bypass enables you to shorten the path of media traffic and reduce the number of hops in transit for better performance. With Media Bypass, media is kept between Avaya SBC and the client instead of sending it via the Microsoft Phone System. To configure media bypass, Avaya SBC and the client must be reachable by each other.

Interactive Connectivity Establishment (ICE)

ICE is defined in RFC 5245. Avaya SBC supports an “ICE Lite” implementation, always as a peer with Microsoft® Teams. The Offer or Answer Session Description Protocol (SDP) is independent of call direction – Avaya SBC always sends an ICE Lite SDP. However, the far end Microsoft® Teams peer operates with a full ICE implementation. The far end Microsoft® Teams gathers different ICE candidates, acts as a controlling agent, and negotiates a candidate pair for the media stream.

In addition, the Far End Turn feature of the Microsoft® phone system environment is supported. Near End Turn is not supported. Avaya SBC does not gather candidates, but provides a host candidate. The host candidate is publicly reachable, but is masked with a firewall address. Avaya SBC acts as a controlled agent and does not initiate on connectivity check, but responds to a connectivity check using STUN.

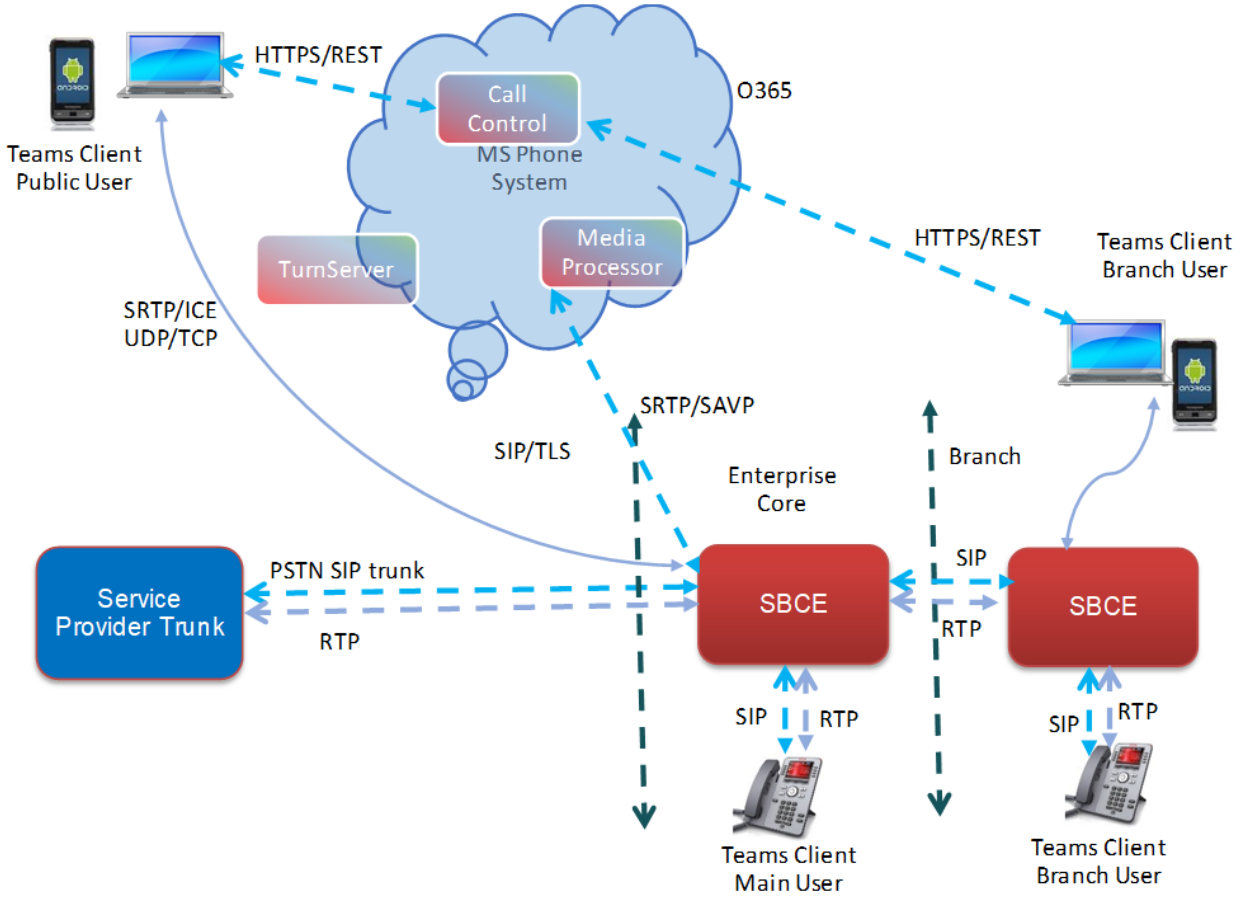
Avaya SBC uses the Radvision ICE stack, which is programmed in ICE Lite mode. For Local Media Optimization, Avaya SBC reads X-MS headers in SIP. If the X-MS header is internal; the core SBC relays ICE candidates, but does not provide ICE termination or negotiation. The branch SBC acts like an ICE termination/negotiation point.

Local Media Optimization

Local Media Optimization for Direct Routing manages voice quality by:

- Controlling how media traffic flows between the Microsoft® Teams clients and the Avaya SBC.
- Keeping media local within the boundaries of corporate network subnets.
- Allowing media streams between the Microsoft® Teams clients and Avaya SBC, even if Avaya SBC is behind corporate firewalls with private IPs and are not visible to Microsoft directly.

The following diagram illustrates the connectivity when using these new features:




With Media Bypass for Direct Routing using ICE:

- The Media Processor within the Microsoft® Phone System data center is not used.
- The Microsoft® Teams Client sets up a direct media path with Avaya SBC using ICE.
- ICE is terminated at the Avaya SBC, and standard SIP SDP procedures are followed for calls towards Avaya Aura® or the PSTN.

With Local Media Optimization for Direct Routing:

- Local Media Optimization uses a proprietary header X-MS to understand the client location.
- If the location is within an Avaya SBC branch, the core Avaya SBC passes the call through ICE.
- ICE call termination and handling happens in the branch Avaya SBC.

Local Media Optimization Use Case

As an example, you have salespeople who work at the main sales office, one of your many branch offices, and visit customers who might be at any location. Avaya SBC and Teams can be administered to handle calls efficiently for the salespeople no matter where they are located, using the call processing facilities that are local to them. For example:

- When sales people are in the main sales office, calls placed or received are administered to use the main, or core, Avaya SBC system configured for the main sales office.

- When the salespeople are working at the branch sales office, calls placed or received are administered to use the branch Avaya SBC system configured for the branch sales office.
- When the salespeople are on the road visiting customers, calls placed or received using their mobile devices are administered to use the PSTN.

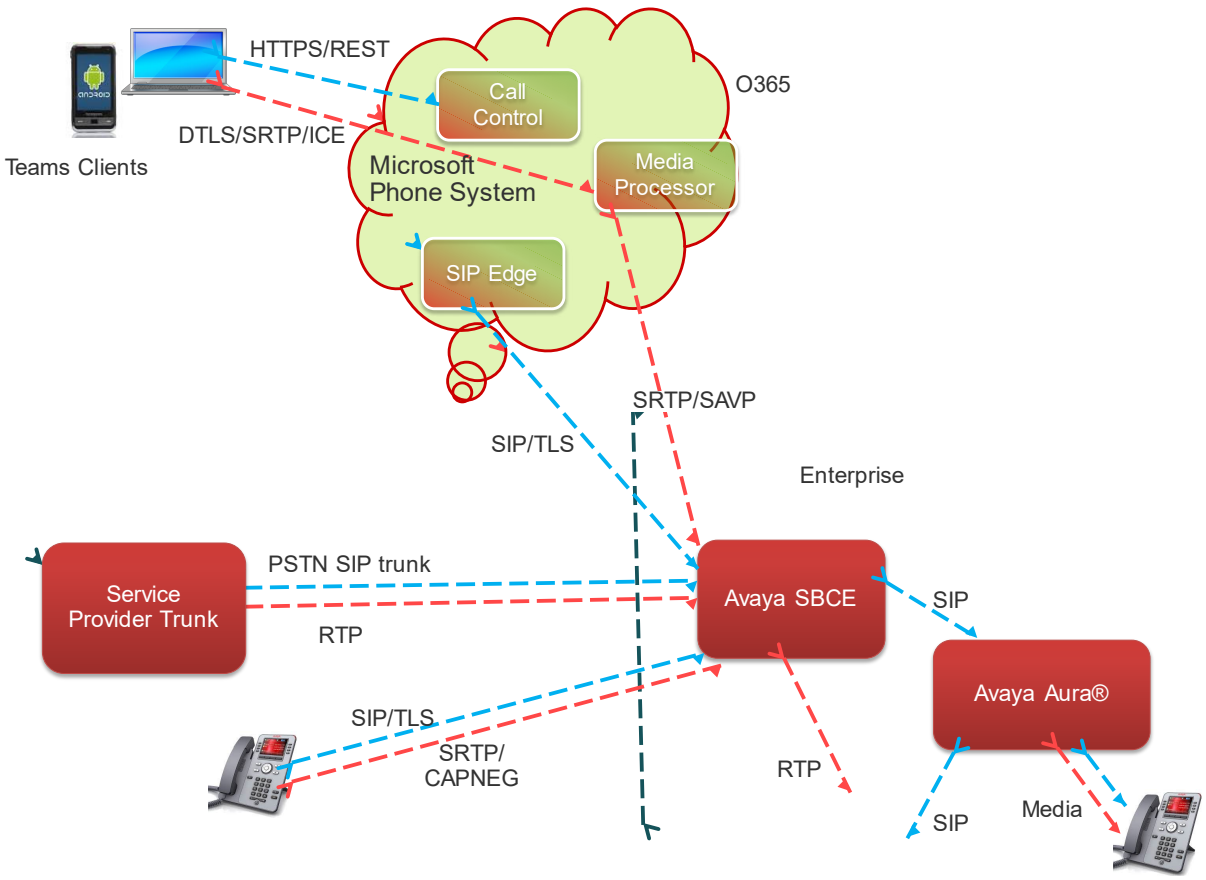
# Network diagrams

## Teams-specific deployment diagrams

### Teams Integration with Avaya SBC

The following diagram illustrates some typical use cases for Teams users that place or receive calls that integrate with Avaya SBC:

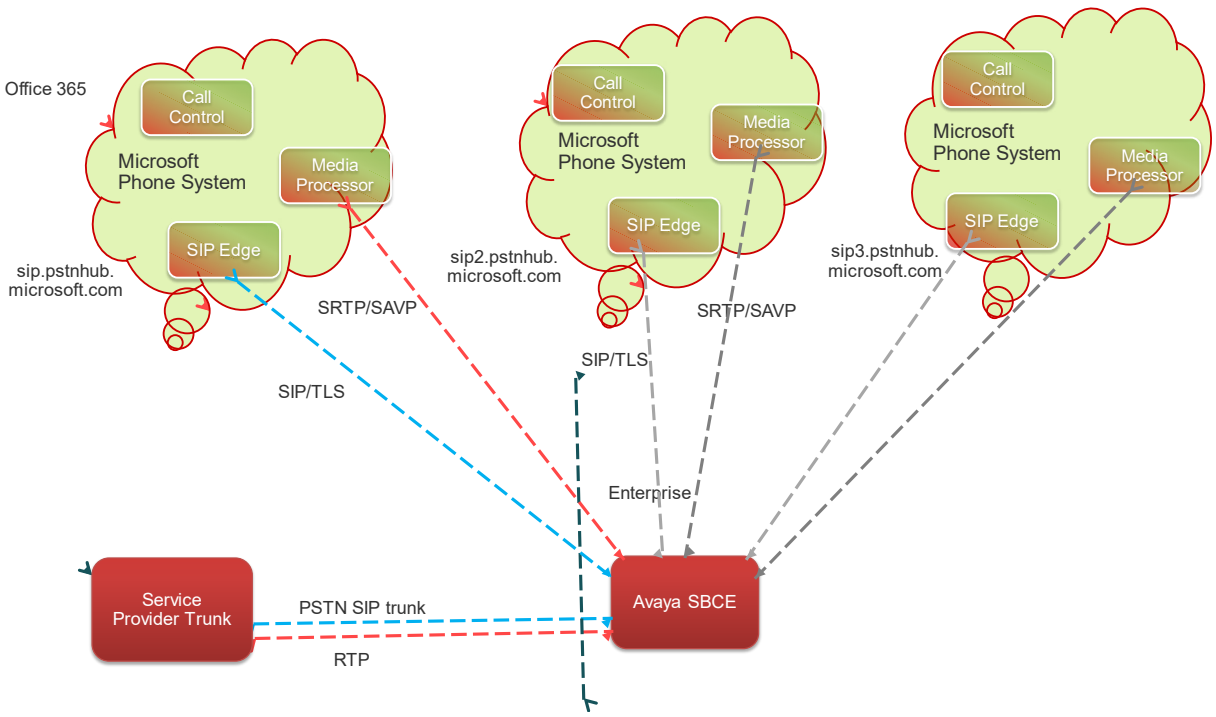
- An incoming PSTN call directly routed to the Teams user.
- An outgoing call from a Teams user routed through Avaya SBC to an Avaya Aura® user.
- An incoming PSTN call arriving at Avaya Aura® from Avaya SBC. Avaya Aura® uses EC500 and Call Coverage to forward the call a Teams user, and connects using the Avaya SBC direct routing capability.
- A PSTN call routed to an Avaya Aura® user; the Avaya Aura® user does not accept the call; Avaya SBC redirects the call to a Teams user; mapping of the Avaya Aura® user to the Teams user is fetched from the organization’s LDAP Active Directory.




## Signaling FQDN and Failover Mechanisms

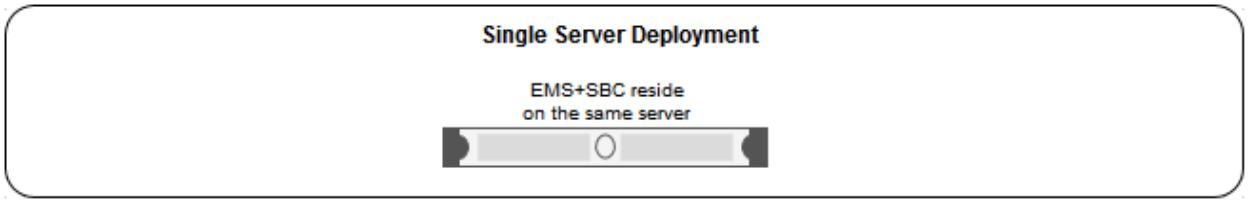
The following diagram illustrates the FQDN and failover mechanisms used with Avaya SBC and Teams:

- All SIP signaling elements like R-URI, Via, Route, R-R and Contact have FQDNs.
- The Microsoft Phone System provides three FQDNs – primary, secondary and tertiary across three regions.
- The Avaya SBC for a specific location reaches out to the location-specific DNS server and the FQDN resolves to the primary Microsoft Phone System of the location.
- DNS-SRV returns A-records and resolves into the address of the primary, secondary, and tertiary Microsoft Phone Systems.
- Avaya SBC REGISTERS to the primary Microsoft Phone System or next available healthy Microsoft Phone System and maintains the heartbeat using OPTIONS.
- If the primary Microsoft Phone System is not in good operating condition or does not respond, Avaya SBC moves new calls to the next available Microsoft Phone System, and treats it as primary.




## Single server non-HA deployment

In a single server non-HA deployment, the Element Management System (EMS) and SBC software are installed on a single server. Use this deployment scenario when you want to deploy Avaya SBC in a basic mode.




**Important:**

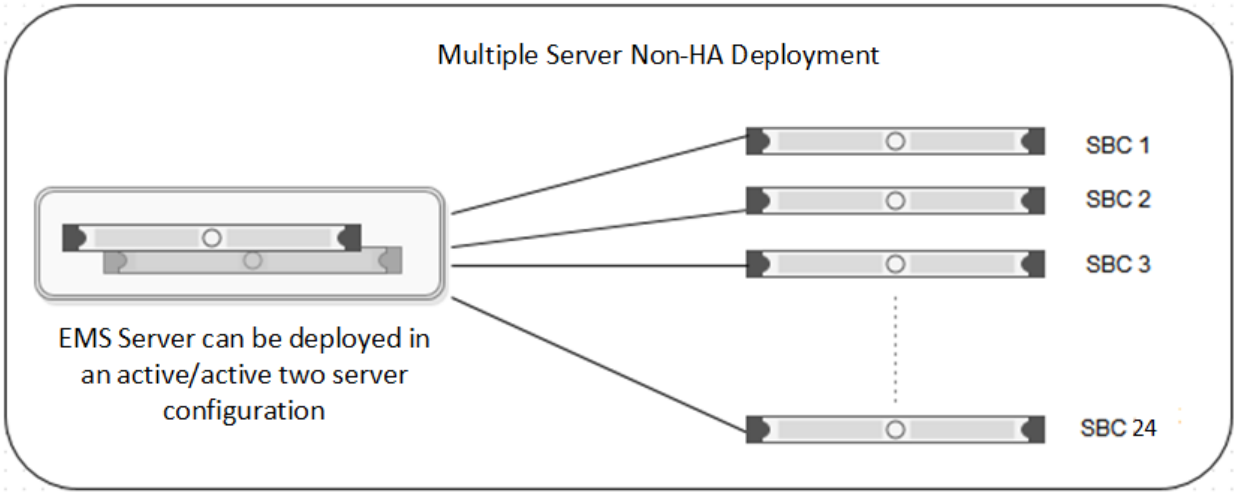
All hardware server types, virtualized environment platforms, and cloud platforms support the single-server non-HA deployment type.

## Multiple server non-HA deployment

In a multiple server deployment, the EMS and SBC software are installed on separate servers.

In a non-HA multiple server deployment, you can have one or more SBC servers controlled by a single EMS server or a replicated EMS HA pair. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. When using a single EMS server, the EMS server is configured as Primary.

You can have up to 24 individual Avaya SBC servers in this type of configuration.




If you start with a non-HA deployment and want to later move to an HA deployment, you must completely reconfigure the deployment.

**Important:**

All hardware server types, virtualized environment platforms, and cloud platforms support the multi-server non-HA deployment type.

## Multiple server HA deployment

In a multiple server deployment, the EMS and SBC software are installed on separate servers.

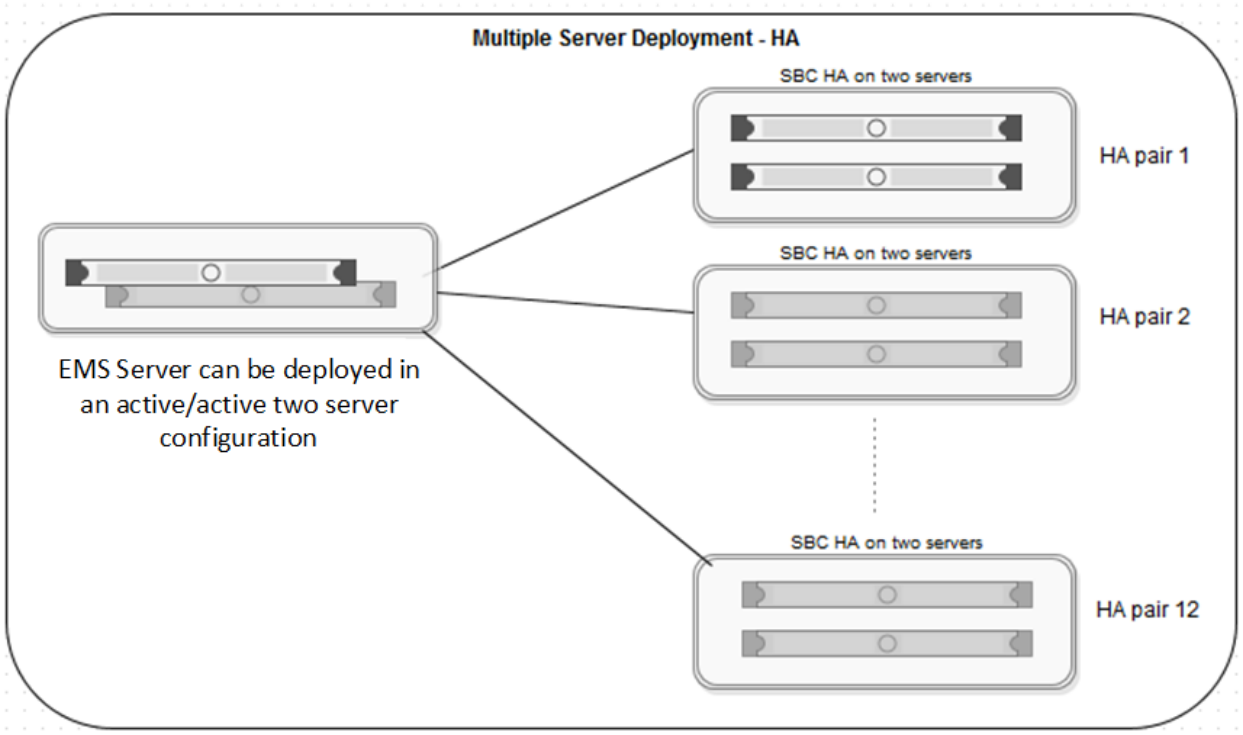
In an HA deployment, SBC servers are deployed in pairs. Each pair has one SBC server configured as Primary while the other is configured as Secondary.

Optionally, the EMS software can be replicated in an active/active HA pair deployment. In an active/active deployment, the EMS software is installed on two servers. One EMS server is configured as Primary and the other is configured as Secondary. An EMS HA pair must be reachable to each other and with the SBC servers, and can be in different geographical locations.

One EMS server or an active/active pair of EMS servers can control up to 12 separate pairs of SBC servers.

**Note:**

When deploying an HA configuration on Amazon Web Services, you only have to configure the SBC software on the primary device




**Important:**

All hardware server types, virtualized environment platforms, and cloud platforms support the multi-server HA deployment type.

Although the HA pairs and non-HA deployments are shown separately in this figure, EMS can control both an SBC HA server pair as well as a single SBC server.

SBC HA server pairs must adhere to the following requirements:

- You can enable and use the HA deployment feature only if the license file contains an HA license.
- The HA pair servers must reachable by the EMS or EMS HA pair servers over the Management Plane (M1).
- The HA pair servers must be reachable between the devices over the Management link (M1) .
- The HA pair servers must have the HA link (M2) reachable between the HA pair servers.
- The HA pair servers must set up to have all the data interfaces between the servers replicated so that the servers are connected in same subnets. For example, the A1 data interface in one SBC server should be in the same subnet as the A1 data interface of the paired SBC server. This allows you to meet the requirement that failover be functional in an active/standby mode.
- In a multiple server HA virtualized deployment, when there are multiple HA pairs and automatic IP addressing is being used on the HA link (M2), every HA pair should either have their own isolated vSwitch or each HA pair should use different IP addresses reachable with their HA pairs as stated previously for M2 connectivity.

# Interoperability

Avaya SBC Release 8.1.1 and later supports integration with Microsoft® Teams (Teams). You can use any deployment type (hardware, VMware, virtualized, Microsoft® Azure, or Amazon Web Services) as long as it supports Avaya SBC Release 8.1.1 and later.

Avaya SBC must include Avaya Aura® Release 8.x or later as part of the deployment with Teams.

Avaya SBC supports the following interoperability features:

- SIP signaling for UDP on PSTN.
- The Teams SIP signaling is set up to use TLS port 5061. For security reasons, the TLS version must be TLS 1.2.
- SRTP interworking with RTP/RTCP on the PSTN side, and SRTP/SRTCP with lifetime for the following cryptography suites:
  - AES_CM_128_HMAC_SHA1_80
  - AES_CM_128_HMAC_SHA1_32
  - AES_CM_256_HMAC_SHA1_80
  - AES_CM_256_HMAC_SHA1_32
- Refer interworking by handling REFER.
- Hold/Resume interworking since Teams has its way of handling hold, unhold, and music on hold (MOH).
- Handling of FQDN and DNS.
- Number plan manipulation.
- Teams-specific header injection to assist Teams on failover.
- RTCP generation in a scenario when legacy SIP PSTN trunks do not send RTCP.
- Transcoding support for G711u, G711a, G722, G729, and OPUS codecs. The SILK codec is not supported.

# Avaya SBC features not supported in a Teams deployment

The following Avaya SBC features are not supported when deployed in a Teams environment:

- RTCP Mux
- Comfort Noise
- Ring tone generation at Blind Transfer

For Teams users, the telephony-based features they normally use are all supported if they use their Teams devices. For example:

- Hold
- Music on hold
- Call transfer variants
- Conference
- Forwarding
- Voice mail
- Caller ID
- Auto attendant and queues
- Call pickup and call park
- Shared line appearance
- Call block

When a Teams user is on a call with non-Teams users, and the non-Teams user initiates one of these features, the feature operates based on the system where the feature was initiated. This may cause interactions with how the Teams user expects the feature to operate.

# Security requirements

The Teams SIP signaling is set up to use TLS port 5061. For security reasons, the TLS version must be TLS 1.2.

Teams requires the use of the following ECC ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Avaya SBC, working with Teams, supports SRTP interworking with RTP/RTCP on the PSTN side and SRTP/SRTCP with a lifetime for the following cryptography suites:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- AES_CM_256_HMAC_SHA1_80
- AES_CM_256_HMAC_SHA1_32

# Chapter 3: Summary configuration checklists

## Summary configuration checklists

This section provides a summary of the configuration checklists used to configure Avaya SBC for Microsoft® Teams (Teams).

### Initial setup of Avaya SBC

| Task | Reference | ✔ |
|---|---|---|
| Administer the SIP trunking server flows. | Start with About configuring server flows for SIP trunking with Microsoft Teams on page 21, read About SIP trunking on page 22, then do the procedures listed in SIP trunk configuration checklist on page 23. | |
| Administer media rules. | Media rules on page 36 | |
| Administer a SIP server profile. | About SIP server configuration profile management on page 44 | |
| Configure certificates | Configuring certificates on page 52 | |

### SIP trunk configuration

| Task | Reference | ✔ |
|---|---|---|
| Create interworking profiles. | Creating Interworking Profiles on page 24. | |
| Create server profiles for call server and trunk server. | Creating Server Profile for Call Server on page 24 and Creating Server Profile for Trunk Server on page 26. | |
| Create routing profile for call server and trunk server. | Creating Routing Profile for Call Server on page 27 and Creating a Routing Profile for a Call Server on page 27. | |
| Create Topology Hiding Profile. | Creating a Topology Hiding profile on page 30 | |
| Create signaling interfaces. | Creating External Signaling Interface toward Trunk Server on page 30 and Creating Internal Signaling Interface Toward Call Server on page 31. | |
| Create media interfaces. | Creating External Media Interface toward Trunk Server on page 32 and Creating Internal Media Interface Toward Call Server on page 33. | |

*Table continues…*

| Task | Reference | ✔ |
|---|---|---|
| Create server flows. | Creating call server flow on page 33 and Creating a trunk server flow on page 34. | |
| Perform server-specific configuration for trunking. | Configuring Avaya SBC for SIP Trunk on page 35 and Configuring Avaya SBC for other trunks on page 36. | |

### Teams configuration

See Configuring Microsoft Teams options required for integration with Avaya SBC on page 53.

### Configuration of Avaya SBC

| Task | Reference | ✔ |
|---|---|---|
| Configure server interworking. | Add server interworking profiles as described in About configuring server interworking for Microsoft Teams on page 56 and Adding a server interworking profile on page 57. | |
| Configure Session Manager adaptations for number manipulation. | Creating a new signaling rule on page 67<br>Adding a URI Manipulation rule on page 75<br>For more information about configuring these rules, see *Administering Avaya Session Border Controller*. | |
| Configure topology hiding. | About configuring topology hiding for Microsoft Teams on page 75 | |
| Configure signaling manipulation (SigMa). | About configuring signaling manipulation for Microsoft Teams on page 77 | |
| Configure transcoding. | About configuring Avaya SBC for transcoding and transrating on page 79 | |
| Configure RTCP generation. | RTCP monitoring generation support on page 83 | |

### Transcoding

| Task | Description | ✔ |
|---|---|---|
| Enable the transcoding and tranrating features. | Enabling transcoding and transrating on page 81 | |
| Administer codec prioritization. | Configuring codec prioritization on page 81 | |
| Add the media rule, which has transcoding enabled, to an endpoint policy group. | Configuring endpoint policy group on page 82 | |
| Add the endpoint policy group to a server flow. | Configuring a server flow for transcoding on page 82 | |

# Chapter 4: Initial setup of Avaya SBC

## Initial setup checklist

| Task | Reference | ✔ |
|---|---|---|
| Administer the SIP trunking server flows. | Start with About configuring server flows for SIP trunking with Microsoft Teams on page 21, read About SIP trunking on page 22, then do the procedures listed in SIP trunk configuration checklist on page 23. | |
| Administer media rules. | Media rules on page 36 | |
| Administer a SIP server profile. | About SIP server configuration profile management on page 44 | |
| Configure certificates | Configuring certificates on page 52 | |

## About configuring server flows for SIP trunking with Microsoft Teams

When configuring server flows for SIP trunking in a Microsoft Teams deployment, you must configure trunks for the PSTN and server flows for the Microsoft Teams SIP proxy. By configuring the SIP trunks and server flows, you create routing paths between the PSTN and the Microsoft Teams SIP proxy.

For Microsoft Teams to route across multiple Microsoft Teams servers, the call servers must be configured with the following FQDN names and have priority load balancing set:

- sip.pstnhub.microsoft.com
- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

Add the FQDNs of the three call servers as priority 1, 2, and 3, with the appropriate SIP server profile type corresponding to Microsoft Teams. The priority one Microsoft Teams SIP server, sip.pstnhub.microsoft.com, is always tried first. If the priority one server is not in good health due to heartbeat failure in Options, the priority two Microsoft Teams server, sip2.pstnhub.microsoft.com is tried next. If that server is not in good health, the priority three Microsoft Teams server,

sip3.pstnhub.microsoft.com, is tried next. This mechanism provides in Microsoft Teams failover and geo-redundancy.

By default, the URI group is defined as “*”, but it can be defined with any other value as required by a Microsoft Teams specific URI group profile if a specific number pattern is allowed for Direct Routing.

# Configuration of server flows for SIP trunking

## About SIP trunking

With the SIP Trunking feature of Avaya SBC security devices, SIP trunk-enabled enterprises can completely secure SIP connectivity over the Internet. This security is achieved through SIP trunking services obtained through an Internet Telephony Service Provider (ITSP).

SIP trunking ensures the privacy of all calls traversing the enterprise network, while maintaining a well-defined demarcation point between the core and access network. In addition, with the SIP Trunking feature in Avaya SBC, an enterprise can maintain granular control through well-defined domain policies. These domain policies secure SIP implementations or servers of customers from known SIP and Media vulnerabilities.

Because the Avaya SBC security device is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the SBC device for processing. See Figure 1: Avaya SBC deployed in the enterprise DMZ on page 23. If the signaling traffic is encrypted, the Avaya SBC device decrypts all TLS encrypted traffic and looks for anomalous behavior. Then, Avaya SBC forwards the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

**Example**

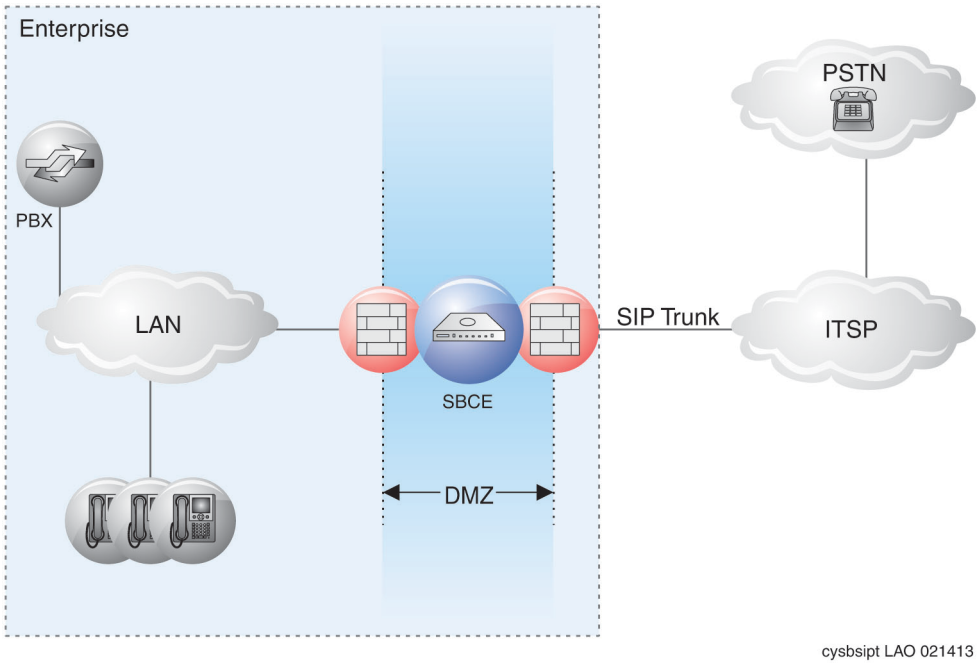



**Figure 1: Avaya SBC deployed in the enterprise DMZ**

# SIP trunk configuration checklist

Use this checklist while configuring a generic Avaya SBC SIP trunk with the generic call server or trunk server. Based on the call server options, configure the signaling manipulation and interworking. For more information about signaling manipulation, see specific call server or trunk server Application Notes.

| Task | Reference | ✔ |
|---|---|---|
| Create interworking profiles. | Creating Interworking Profiles on page 24. | |
| Create server profiles for call server and trunk server. | Creating Server Profile for Call Server on page 24 and Creating Server Profile for Trunk Server on page 26. | |
| Create routing profile for call server and trunk server. | Creating Routing Profile for Call Server on page 27 and Creating a Routing Profile for a Call Server on page 27. | |
| Create Topology Hiding Profile. | Creating a Topology Hiding profile on page 30 | |
| Create signaling interfaces. | Creating External Signaling Interface toward Trunk Server on page 30 and Creating Internal Signaling Interface Toward Call Server on page 31. | |
| Create media interfaces. | Creating External Media Interface toward Trunk Server on page 32 and Creating Internal Media Interface Toward Call Server on page 33. | |

*Table continues…*

| Task | Reference | ✔ |
|---|---|---|
| Create server flows. | Creating call server flow on page 33 and Creating a trunk server flow on page 34. | |
| Perform server-specific configuration for trunking. | Configuring Avaya SBC for SIP Trunk on page 35 and Configuring Avaya SBC for other trunks on page 36. | |

# Creating Interworking Profiles

## About this task

Interworking Profile features are configured based on different Trunk Servers, for example, Avaya and Nortel. You can use the available default profiles as is or after modification, or configure new profiles.

**Note:**

The procedures before and after this section provide generic instructions for SIP trunking configuration that apply to all implementations.

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.

   The existing interworking profiles are displayed. You can use a default Trunk Server Profile, modify the default Trunk Server Profile, or create a new Trunk Server Profile.
4. Click **Add**.
5. In the **Profile Name** field, type a name for the new profile.
6. Enter required information in the Interworking profile screens, and click **Finish**.

   The system displays the newly created interworking profile.
7. Click the **Advanced** tab, and click **Edit**.
8. Select appropriate fields on the Editing Profile screen, and click **Finish**.

## Next steps

To configure trunks servers used in your network, see Configuring Avaya SBC for SIP Trunk on page 35 and Configuring Avaya SBC for SIP Trunk on page 35.

# Creating Server Profile for Call Server

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.

The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.

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

   The system displays the Add Server Configuration Profile window.

5. In the **Profile Name** field, type a call server name and click **Next**.

   The system displays the second Server Configuration Profile window.

6. In the **Server Type** field, click **Call Server**.
7. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or of the FQDN.
8. In the **Transport** field, select the transport protocol that you want to use.

   For integration with Teams, you must select **TLS**.

9. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.

   For integration with Teams, you must select `5061` when using TLS.

10. Click **Next**.

    The system displays the Add Server Configuration Profile – Authentication screen.

11. **(Optional)** If you use server authentication, type the related information on this screen.
12. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.

13. **(Optional)** If you use the heartbeat feature, select the **Enable Heartbeat** check box and type relevant details in the **Method**, **Frequency**, **From URI**, and **To URI** fields.

    If you enable the heartbeat, a message is sent periodically to the server to help monitor the connectivity status of the server. When a primary and secondary server are available in the network, this server status is useful to determine which server is active.

14. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.

15. **(Optional)** If the Call Server is Session Manager, select the **Enable Grooming** check box.

    With Grooming enabled, the system can reuse the same connections for the same subscriber or port.

16. In the **Interworking Profile** field, select the profile name for the type of call server.

    For the Avaya Call Server Profile, you can clone the default `avaya-ru` profile. You can use the cloned profile to make any changes in the interworking profile.

17. In the **TLS Client Profile** field, select the client profile to be used for the server.
18. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.

19. In the **Connection Type** field, click a connection type.
20. Click **Finish**.

# Creating Server Profile for Trunk-side server

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The left Application pane displays the server profiles, and the Content pane displays the parameters of the selected server profile.
4. In the Application pane, click **Add**.

   The system displays the Add Server Configuration Profile window.
5. In the **Profile Name** field, type a trunk server name and click **Next**.

   The system displays the second Server Configuration Profile window.
6. In the **Server Type** field, click **Trunk Server**.
7. In the **IP Addresses / Supported FQDN** field, type the IP address of the call server or its FQDN.
8. In the **Transport** field, select the transport protocol that you want to use.
9. In the **Port** field, type `5060` or `5061`, depending on the selected transport protocol.
10. Click **Next**.

    The system displays the Add Server Configuration Profile – Authentication screen.
11. **(Optional)** If you use server authentication, type the related information on this screen.
12. Click **Next**.

    The system displays the Add Server Configuration Profile – Heartbeat screen.
13. **(Optional)** If you use the heartbeat feature, select the **Enable Heartbeat** check box and type relevant details in the **Method**, **Frequency**, **From URI**, and **To URI** fields.

    If you enable the heartbeat, a message is sent periodically to the server to help monitor the connectivity status of the server. When a primary and secondary server are available in the network, this server status is useful to determine which server is active.
14. Click **Next**.

    The system displays the Add Server Configuration Profile – Advanced window.
15. **(Optional)** If you use the TCP or TLS transport protocol, select the **Enable Grooming** check box.

    With Grooming enabled, the system can reuse the same connections for the same subscriber or port.

16. In the **Interworking Profile** field, select the profile name for the type of trunk server.

    For the Avaya Call Server Profile, you can clone the default `avaya-ru` profile. You can use the cloned profile to make any changes in the interworking profile.
17. In the **TLS Client Profile** field, select the client profile to be used for the server.
18. **(Optional)** In the **Signaling Manipulation Script** field, click a signaling manipulation script for the server.
19. In the **Connection Type** field, click a connection type.
20. Click **Finish**.

# Creating a Routing Profile for a Call Server

## About this task

Use this procedure to create a routing profile with the next hop as a call server address.

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Configuration Profiles** > **Routing**.
4. In the application pane, click **Add**.

   The application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.
5. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.
6. Click **Next**.

   The system displays the second Routing Profile window.
7. **(Optional)** In the **URI Group** field, select the URI group of the routing profile. For example, if you have a routing profile *Test1* and URI Group *user 1234@test.com*, any request message to user 1234@test.com will resolve profile Test1.
8. **(Optional)** In the **Time of Day** field, enter the time-of-day profile.

   Remote users must not use the time-of-day profile for the routing profile.
9. In the **Load Balancing** field, enter one of the following options. You can configure up to five next hop addresses with the available load balancing.
   - Priority: From the list of next-hop addresses, request messages take first priority. If a request message fails to reach the first next-hop address, the request message takes the second priority.
   - Round Robin: Request messages are delivered to the next-hop address on a round-robin basis. Any request message is processed sequentially, beginning again with the first next-hop address, in a circular manner.

**Note:**

You must create another routing profile for the next hop as a SIP trunk address.

- Weighted Round Robin: Each configured next-hop address is assigned a weight. The request messages routes to the next-hop address on the basis of the assigned weight.
- DNS/SRV: Multiple domain names can be configured. If selected, you can enable or disable NAPTR. Avaya SBC uses DNS priority to route the message. If you disable NAPTR, specify the transport type.

10. In the **Transport** field, enter **TCP** or **TLS**.

    If you define the transport type here, the system deactivates the common **Transport Type** field.

11. Select the **Next Hop Priority** check box.

    If you enable this setting, Avaya SBC processes the configured next-hop address when routing fails.

12. Select **Call Server** from **Server Configuration**.
13. Click **Add** to configure the next-hop address.
14. Click **Finish**.

# Creating Routing Profile for Trunk Server

## About this task

This procedure will create a routing profile with next hop as a Trunk side Server IP address.

**Note:**

Use the following profile name: `Route_to_Trunk_Svr`.

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Configuration Profiles** > **Routing**.
4. In the Application pane, click **Add**.

   The Application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.

5. In the **Profile Name** field, type the profile name in the `Route_to_Trunk_Svr` format.
6. Click **Next**.

   The system displays the second Routing Profile window.

7. Log in to the EMS web interface with administrator credentials.
8. In the navigation pane, click **Configuration Profiles** > **Routing**.

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

   The Application pane displays the existing routing profiles, and the Content pane displays the parameters of the selected routing profile.

10. In the **Profile Name** field, type the routing profile name in the `Route_to_Avaya_Server` format.

11. Click **Next**.

    The system displays the second Routing Profile window.

12. **(Optional)** In the **URI Group** field, select the URI group of the routing profile. For example, if you have a routing profile *Test1* and URI Group *user 1234@test.com*, any request message to user 1234@test.com will resolve profile Test1.

13. **(Optional)** In the **Time of Day** field, enter the time-of-day profile.

    **Note:**

    Remote users must not use the time-of-day profile for the routing profile.

14. In the **Load Balancing** field, enter one of the options. You can configure up to five next hop addresses with the available load balancing.

    - Priority: From the list of next-hop addresses, request messages take the first priority. If a request message fails to reach the first next-hop address, the request message takes the second priority.
    - Round Robin: Request messages are delivered to the next-hop address on a round-robin basis. Any request message is processed sequentially, beginning again with the first next-hop address, in a circular manner.

      **Note:**

      You must create another routing profile for next hop as a SIP trunk address.
    - Weighted Round Robin: Each configured next-hop address is assigned a weight. The request messages routes to the next-hop address on the basis of the assigned weight.
    - DNS/SRV: Multiple domain names can be configured. If selected, you can enable or disable NAPTR. Avaya SBC uses DNS priority to route the message. If you disable NAPTR, specify the transport type.

15. In the **Transport** field, enter **TCP** or **TLS**. If you define the transport type here, the system deactivates the common **Transport Type** field.

16. Select the **Next Hop Priority** check box. If you enable this setting, Avaya SBC processes the configured next-hop address in the event of failure routing.

17. Select **Trunk Server** from **Server Configuration**.

18. Click **Add** to configure the next-hop address.

19. Click **Finish** to save the configuration and exit.

    This displays the Routing Profile screen, showing the newly created `Route_to_Trunk_Svr` Routing Profile along with the `Route_to_Call_Svr` Routing

Profile created by the procedure described in Creating Routing Profile for Call Server on page 27.

20. For a failover trunking configuration, select the Next Hop priority checkbox.
21. Specify the priorities for the configured trunking servers.
    - Priority 1: the primary server
    - Subsequent priorities: secondary server(s)

    The following are the ways in which Avaya SBC can failover from one trunking server to the next. The ways in which Avaya SBC detects whether the server is reachable.

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

# Creating a Topology Hiding profile

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Configuration Profiles** > **Topology Hiding**.

   The left Application pane displays the Topology Hiding profiles, and the Content pane displays the parameters of the selected profile.
3. In the Application pane, click the default profile.
4. In the Content pane, click **Clone**.

   The system displays the Clone Profile window.
5. In the **Clone Name** field, type the name in the `SBCE_to _Call_Svr` format and click **Finish**.

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

# Creating external signaling interface toward Trunk-side server

## Procedure

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

3. In the left navigation pane, click **Network & Flows** > **Signaling Interface**.

   The left Application pane displays the list of signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.

4. In the upper-right corner of the Content pane, click **Add**.

   The system displays the Add Signaling Interface window.

5. In the **Name** field, type a descriptive name for the external signaling interface for the phone network.
6. In the **IP Address** field, select the IP address of the external signaling interface.
7. Depending on the transport protocol you are using for your network, do the following:
   - If you use TCP, in the **TCP Port** field, type the TCP port number. The default TCP port number is 5060.
   - If you use UDP, in the **UDP Port** field, type the UDP port number. The default UDP port number is 5060.
   - If you use TLS, in the **TLS Port** field, type the TLS port number. The default TLS port number is 5061.

   When you specify the TLS port, the system enables the **TLS Profile** and **Enable Shared Control** fields.

   **Note:**

   - TLS is a secure protocol. To use TLS, you must have advanced session licenses and encryption licenses.
   - Use the B1 interface as the external signaling interface.
   - Enable only the transport protocols that you want to use.

8. From the **TLS Profile** field, select the appropriate Avaya SBC TLS profile name.

   You can also use third-party certificates.

   If you specify the TLS port number, then you must select a TLS profile. Otherwise, leave this field blank.

9. Click **Finish**.

   **Note:**

   To configure multiple Session Managers, repeat this task to add the second signaling interface.

# Creating Internal Signaling Interface toward Call Server

## Procedure

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

3. In the left navigation pane, click **Network & Flows** > **Signaling Interface**.

   The left Application pane displays any existing signaling interfaces, and the Content pane displays the parameters of the selected signaling interface.
4. In the right-corner of the Content pane, click **Add**.
5. In the Add Signaling Interface window, add the following parameters:
   a. In the **Name** field, type a name for the internal signaling interface for the Avaya call server.
   b. From the **IP Address** field, select the IP address of the internal signaling interface.
   c. Configure the transport that you want to use.

      **Note:**

      - TLS is a secure protocol. To use TLS, you must have advanced session licenses and encryption licenses. In the **TLS Port** field, type the port number `5061`.
      - If your call server uses a different protocol, type the appropriate port numbers in the **TCP Port** or **UDP Port** fields, as applicable.
      - The default port number for TCP and UDP is 5060.
      - Do not select the **Enable Stun** check box.

   d. **(Optional)** From the **TLS Profile** field, select the profile name for TLS.

      You can select a TLS profile only when you add a TLS port. If the **TLS Port** field is empty, the **TLS Profile** field is unavailable.
   e. Click **Finish** to save and exit.

      The system displays the new internal signaling interface.

# Creating External Media Interface toward Trunk Server

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.
4. In the upper-right corner of the Application pane, click **Add**.

   The system displays the Add Media Interface window.
5. In the **Name** field, enter a descriptive name for the external media interface toward the phone network.
6. In the **IP Address** field, click the IP address of the external media interface.

7. In the **Port Range** fields, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.

8. Click **Finish**.

# Creating Internal Media Interface toward call server

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Media Interface**.

   The left Application pane displays the existing media interface, and the Content pane displays the parameters of the selected media interface.

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

   The system displays the Add Media Interface window.

5. In the **Name** field, type a descriptive name for the internal media interface of the Avaya call server.
6. In the **IP Address** field, click the IP address of the internal media interface.
7. In the **Port Range** field, type the starting and ending port range numbers.

   The port range is from 35000 through 40000.

8. Click **Finish**.

# Creating call server flow

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **End Point Flows**.

   The left Application pane displays the list of existing devices, and the Content pane provides the subscriber flow and server flow information about the selected device.

4. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow window.

5. In the **Flow Name** field, enter a flow name.
6. In the **Server Configuration** field, click the name of the Avaya call server profile.
7. Keep the default value for the **URI Group**, **Transport**, and **Remote Subnet** fields.
8. In the **Received Interface** field, click the name of the interface pointing toward the SIP trunk, for example, Sig_Intf_Ext_to_Trunk_Net.

9. In the **Signaling Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Sig_Intf_Int_to_Call_Server.
10. In the **Media Interface** field, click the name of the interface pointing toward the Avaya call server, for example, Med_Intf_1.
11. In the **End Point Policy Group** field, click the created endpoint policy.
12. In the **Routing Profile** field, choose the routing profile towards SIP trunk.
13. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
14. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.
15. In the **Remote Branch Office** field, keep the default value **Any** or select another remote branch office.
16. Click **Finish** to save and exit.

# Creating a trunk server flow

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.

   The system displays the End Point Flows page.
4. In the **Server Flows** tab, click **Add**.

   The system displays the Add Flow page.
5. In the **Flow Name** field, type a name for the server flow.
6. Unless the customer has special requirements, use the default (*) values for the **URI Group**, **Transport**, and **Remote Subnet** options.
7. In the **Signaling Interface** field, click the name of the interface that receives all of the SIP traffic from the trunk server.
8. In the **Media Interface** field, select the name of the interface that receives all media traffic from the trunk.
9. In the **End Point Policy Group** field, use the default value: default-low.

   **Note:**

   If the phones use TLS/SRTP, select the appropriate end policy group.
10. In the **Routing Profile** field, click the name of the routing profile that points toward the trunk server.

11. In the **Topology Hiding Profile** field, keep the default value or select the appropriate topology hiding profile.
12. In the **Signaling Manipulation Script** field, select the signaling manipulation script to be used for the server flow.
13. In the **Remote Branch Office** field, keep the default value **Any** or select another remote branch office.

    The **Remote Branch Office** field lists all servers configured for remote branch office.
14. Enable the **Link Monitoring from Peer** option to enable handling of incoming SIP OPTIONS messages.

    The **Link Monitoring from Peer** option is used to support the Avaya Aura® SIP Resiliency feature. Avaya SBC must support the SIP Resiliency feature in the OPTIONS response Contact header. Session Manager should know the SIP Resiliency supported for neighboring elements to change the call/message sequence behavior for the Session Manager failover/failback scenarios.

    When **Link Monitoring from Peer** is enabled, Avaya SBC sends a success (200OK) response if the OPTIONS request is matched to that server flow.

    When **Link Monitoring from Peer** is disabled, the OPTIONS request is relayed to the destination server.
15. Click **Finish**.

# Configuring Avaya SBC for SIP Trunk

## Before you begin

Perform all the steps needed for trunk configurations, including configuration of a SIP trunk with Avaya.

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Services** > **SIP Servers**.

   The system displays the Server Configuration screen.
4. In the **General** tab, ensure that you see the servers created in earlier steps.
5. Click the **Advanced** tab, and ensure that the **Interworking Profile** field displays the correct profile selected for the Avaya server.
6. **(Optional)** If the correct **Interworking Profile** name for Avaya is not selected in the **Advanced** tab screen, click the **Edit** button to display the Advanced Edit pop-up screen, and select the profile name for the Avaya Interworking Profile.
7. Click **Finish** to save and exit.
8. In the left navigation pane, click **Configuration Profiles** > **Server Interworking**.

9. In the **Interworking Profiles** list, click an Interworking profile.

   You can clone the default `avaya-ru` profile, or create a new interworking profile.
10. Click the **Advanced** tab.
11. Click the **Edit** button at the bottom of the screen.

    The system displays the Advanced Edit window.
12. In the **Extensions** field, select **None**.
13. Click **Finish** to save and exit.
14. In the Server Interworking screen, click the **General** tab.
15. In the lower-center section of the screen, click the **Edit** button.
16. In the **Hold Support** field, click **RFC2543**.
17. Click **Next**, and then click **Finish** to save and exit.

## Configuring Avaya SBC for other trunks

### Before you begin

Perform all steps needed for all trunk configurations, including parameter settings that are specific to the type of trunk server being configured.

### Procedure

1. Enable server interworking features for different trunk servers, based on the customer requirements.
2. If a default interworking profile is unavailable, then create a new profile.

   Refer Application Notes on https://support.avaya.com for specific interworking configuration.

# Media rules

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

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

# Creating a media rule

## About this task

**Caution:**

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

## Procedure

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

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

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

   The EMS server displays the second Media Rule window.
6. Administer the media rule options as described in Media rules field descriptions on page 37.
7. Click **Finish**.

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

# Media rules field descriptions

## Encryption tab

| Name | Description |
|---|---|
| Audio or Video Encryption | |

*Table continues…*

| Name | Description |
|---|---|
| **Preferred Format #1** | The most preferred encryption method for media traffic. Available selections are:<br>• RTP<br>• SRTP_AES_CM_128_HMAC_SHA1_32<br>• SRTP_AES_CM_128_HMAC_SHA1_80<br>• SRTP_AES_192_CM_HMAC_SHA1_32<br>• SRTP_AES_192_CM_HMAC_SHA1_80<br>• SRTP_AES_256_CM_HMAC_SHA1_32<br>• SRTP_AES_256_CM_HMAC_SHA1_80<br>**Note:**<br>If you select one of the SRTP options, you can encrypt RTCP signaling. The system keeps the RTCP check box active for selection. |
| **Preferred Format #2** | The second most preferred encryption method for media traffic. Available selections are the same as those in **Preferred Format #1**. |
| **Preferred Format #3** | The third most preferred encryption method for media traffic. Available selections are the same as those shown in **Preferred Format #1**. |
| **Encrypted RTCP** | Indicates whether RTCP uses encryption.<br>**Note:**<br>This check box is active for selection if at least one of the three preferred encryption formats include SRTP. |
| **MKI** | MKI is the Master Key Identifier. Specifies the master key of the SRTP session and is stored in the SRTP context. You can derive other session keys from this master key after the lifetime expires. |
| **Lifetime** | Specifies the time interval after which session keys are generated. These keys are not passed in signaling. Session keys are based on MKI. Currently, Avaya SBC does not support the interworking of different lifetime values.<br>You can leave this field blank to match any value. |
| **Interworking** | Indicates whether media from encrypted endpoints can flow to unencrypted endpoints and vice versa. Select this check box for media rules in both the endpoint flows. Enable this setting unless you want to enforce end-to-end encryption. |
| **Symmetric Context Reset** | There are two types of SRTP context reset: Symmetric and Asymmetric. For Symmetric, both the Tx and Rx context are set while sending the new offer. For Asymmetric, only Tx is set while sending the new Offer. Avaya media servers support Asymmetric SRTP context reset. However, some Avaya endpoints such as H.323, 96xx, and Avaya Workplace Client do not support Asymmetric SRTP context reset.<br>By default, this option is enabled. |

*Table continues…*

| Name | Description |
|---|---|
| **Key Change in New Offer** | Use this option to control whether a new cryptography key is generated when a new OFFER message is received. A new OFFER message is defined by a change in any of the following scenarios:<br>• Media direction, such as hold/unhold or video mute/unmute<br>• SDP version change<br>• Delayed offer<br>By default, this option is disabled. |
| Miscellaneous | |
| **Capability Negotiation** | Enables SIP and SDP signaling compliant to the RFC-5939 specification. Select this check box only if the Remote Worker supports SDP Capability Negotiation. |

## Codec Prioritization tab

| Name | Description |
|---|---|
| Audio Codec | |
| **Codec Prioritization** | Force audio codecs to be matched according to the priority defined by the Preferred Codec Priority 1 through Preferred Codec Priority 5 fields. |
| **Allow Preferred Codecs Only** | Matches only the codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed are not matched. |
| **Transcode** | Specifies that the media matched by this media rule must transcode traffic when possible. When you select this option, the system displays [Transcodable] next to the codecs that can be transcoded. |
| **Transrating** | Specifies that the media matched by this media rule must use transrating to reduce the bit rate of the media. |
| **Preferred Codecs** | Names of audio codecs that you want matched in a particular order. These are optional fields to be completed only if Codec Prioritization is selected.<br>The **Available** column lists all the available codecs. You can select a single codec, or hold down the `Ctrl` key and click to select multiple codecs simultaneously. Click **>** to move the codecs to the **Selected** column. Click **^** or **v** to change the order of the codecs in the **Selected** column.<br>The **P-Time** column lists the available packetization times. When you select a codec and a p-time, and click **>** to move the codecs to the **Selected** column, the **Selected** column displays the codecs with the p-time next to the codec name. This means the system applies transrating at the selected p-time for the preferred codecs. |
| Video Codec | |
| **Codec Prioritization** | Forces audio codecs to be matched according to the priority defined by the Preferred Codec Priority 1 through Preferred Codec Priority 5 fields. |
| **Allow Preferred Codecs Only** | Matches only the codecs listed in the previous Preferred Codec Priority fields. Audio codecs not listed are not matched. |

*Table continues…*

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

## Advanced tab

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

*Table continues…*

| Name | Description |
|---|---|
| **RTT Enabled** | Real Time Text (RTT) defines a payload type in the SDP offer answer for carrying a text conversation in real time sessions in RTP packets. The text conversation is used along with voice, video and other multimedia conversations. RTT is used with the NG911 feature of Avaya SBC to facilitate sending real time text messages to an emergency PSAP. It can also be used if any other application that requires RTT.<br><br>When the **RTT Enabled** option is enabled, Avaya SBC relays RTT (media type = text) in SDP. Avaya SBC invokes NAT for the addresses on SDP and at Media Plane while relaying the RTT in SDP. Avaya SBC does not filter or modify the parameters in SDP in case of RTT.<br><br>An SDP with RTT enabled looks similar to the following example:<br><br>`m=text 11000 RTP/AVP 100 98`<br>`a=rtpmap:98 t140/1000`<br>`a=rtpmap:100 red/1000`<br>`a=fmtp:100 98/98/98`<br><br>When the **RTT Enabled** option is disabled, Avaya SBC responds with Port 0. The default setting for **RTT Enabled** is disabled. |
| **ANAT Enabled** | Specifies whether Alternate Network Address Types (ANAT) semantics are enabled for SDP to permit alternate network addresses for media streams. ANAT semantics are useful in environments with IPv4 and IPv6 hosts. |
| **Local Preference** | Specifies the order of preference for the Alternate Network Address Types IPv4 and Dual Stack IPv6. |
| **Use Remote Preference** | Specifies that the remote party must be given ANAT preference to answer the 200 OK response offer, irrespective of the ANAT preference configured on Avaya SBC. |
| **Media Line Compliance Enabled** | Use this field to maintain compliance between the media lines especially for transfer. For example, if the transferee supports audio and video lines and the transfer target supports only audio and if this field is enabled, Avaya SBC maintains audio lines towards the transfer target and audio and video lines towards the transferee.<br><br>As per RFC 3264 compliance media lines should match in offer and answer. In case of there are devices on either side of Avaya SBC where media lines are different, Avaya SBC interworking maintains parity of media lines on both sides of Avaya SBC. |
| **ICE Gateway Support** | Enables support for Interactive Connectivity Establishment (ICE) used when connecting with Microsoft Teams. When enabled, you can administer the **Local Media Optimization** options. |

*Table continues…*

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

*Table continues…*

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

## QoS tab

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

*Table continues…*

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

### SDP capability negotiation

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

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

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

## About SIP server configuration profile management

Configurations for SIP call servers (trunk, proxy) can be centrally managed from the Server Configuration SIP feature of the Avaya SBC security device. You can use this feature to define a number of different server profiles for use in a variety of deployments, security profiles, and company policies. You can add new profiles or clone, edit, rename, view, and delete existing server profiles.

When deploying Avaya SBC with Microsoft Teams, you must configure Avaya SBC with the SIP server heartbeat options to track the status of the Microsoft Teams SIP proxy.

# Adding a new SIP server profile

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click **Add**.

   The EMS server displays the Add Server Configuration Profile page.
5. In the **Profile Name** field, type a name for the new server profile, and click **Next**.
6. On the Edit SIP Server Profile - General window, administer the options as described in Server configuration profile field descriptions on page 45 and click **Next**.
7. On the Edit SIP Server Profile - Authentication window, administer the options as described in Server configuration profile field descriptions on page 45 and click **Next**.
8. On the Edit SIP Server Profile - Heartbeat window, administer the options as described in Server configuration profile field descriptions on page 45 and click **Next**.
9. On the Edit SIP Server Profile - Registration window, administer the options as described in Server configuration profile field descriptions on page 45 and click **Next**.

   **Note:**

   The EMS server does not display the Edit SIP Server Profile - Heartbeat window and Edit SIP Server Profile - Registration window for Remote Branch Office servers.
10. On the Edit SIP Server Profile - Ping page, enter the requested information in the appropriate fields and click **Next**.
11. On the Add Server Configuration Profile - Advanced window, administer the options as described in Server configuration profile field descriptions on page 45.
12. Click **Finish** to save the changes.

# Server configuration profile field descriptions

## General options

**Note:**

The **Registration** tab and **Heartbeat** tab are not available when the **Server type** is administered as **Remote Branch Office**.

| Name | Description |
|---|---|
| **Server Type** | The type of SIP server for which this profile is being defined. The options are:<br>• **Trunk Server**: To configure a trunk server.<br>• **Call Server**: To configure a call server.<br>• **Media Server**: To configure a media server.<br>• **Remote Branch Office**: To configure a branch office in a remote site that connects to the enterprise through Avaya SBC.<br>• **Recording Server**: To configure a Recording Server to record SIP sessions. |
| **SIP Domain** | The SIP domain that validates the host name in a certificate.<br>You must specify a SIP Domain when:<br>• You have enabled extended host name validation.<br>• Custom host name is blank in the client TLS profile associated in the server configuration.<br>To validate the extended host name, Avaya SBC first looks for custom host names configured in the TLS profile. If the custom host name is blank, Avaya SBC then looks for the SIP Domain specified in the server configuration. |
| **DNS Query Type** | The DNS query type that Avaya SBC sends to the DNS server. The options are:<br>• **None/A**: Used when IP address or FQDN of A-query is configured in the EMS server. You must configure **IP Address/FQDN**, **Port**, and **Transport** fields to save any changes for the **None/A** type DNS query for the new SIP server profile.<br>• **SRV**: Used when Avaya SBC sends the SRV type query to the DNS server. Use this setting when using the DNS SRV for trunk registration feature. You must configure FQDN in the **IP Address/FQDN** and **Transport** fields to save any changes for the **SRV** type DNS query for the new SIP server profile.<br>• **NAPTR**: Used when Avaya SBC sends the NAPTR type query to the DNS server. You must configure FQDN in the **IP Address/FQDN** field to save any changes for the **NAPTR** type DNS query for the new SIP server profile.<br>**Note:**<br>• Avaya SBC does not support AAAA-query for FQDN.<br>• You can select **DNS Query Type** for **Server Type** as **Trunk Server** only. |
| **TLS Client Profile** | The TLS Client profile to be used for the SIP server. The **TLS Client Profile** option is activated only when **DNS Query Type** is set to **NAPTR**. |

*Table continues…*

| Name | Description |
|---|---|
| **IP Address/FQDN** | The IP address or Fully Qualified Domain Name (FQDN) of the SIP server.<br>You can add multiple IP addresses or FQDNs.<br>While configuring a Remote Branch Office server, if the Remote Branch Office is:<br>• Behind a NAT router, enter the IP address or FQDN of the public interface of the router.<br>• Not behind a NAT router, enter the IP address or FQDN of the IPO that is used to connect to the Avaya SBC. |
| **IP Address / FQDN / CIDR Range** | The EMS server displays this field when the **Server Type** is **Trunk Server**.<br>The IP address, Fully Qualified Domain Name (FQDN) or CIDR range of the SIP server.<br>You can add multiple IP addresses, FQDNs or CIDR ranges.<br>When you configure CIDR range in the SIP Server by default CIDRs will be configured as whitelist entries. So Avaya SBC enables inbound calls from all IP addresses within the CIDR range. However, the CIDR will not be used for routing outbound calls. For example, in the case of Microsoft Direct Routing, inbound calls to the Avaya SBC can originate from any of the IP addresses within the CIDR blocks 52.112.0.0/14 and 52.120.0.0/14. By configuring these CIDRs along with the Direct Routing Server FQDNs, the Avaya SBC will no longer reject inbound calls from any IP address within the CIDR block. Outbound calls will still route to the resolved FQDN addresses. |
| **Verify TLS Common Name** | The EMS server displays this field when the **Server Type** is **Remote Branch Office**.<br>The option for specifying whether the TLS common name must be verified during the TLS handshake. |
| **TLS Common Name** | The string used to verify whether the TLS connection from the IPO is valid. If the TLS Common Name configured in the server configuration does not match the TLS Common Name provided by the IPO, Avaya SBC rejects the TLS connection. Use one of the following values for the **TLS Common Name** field:<br>• **FQDN**<br>• **IP Address**<br>• **Name**<br>• **Domain beginning with a wild card (*)**<br>The EMS server displays this field only when the **Server Type** is **Remote Branch Office**. |
| **Port** | The port number.<br>The **Port** field is not active when the **Server Type** is **Remote Branch Office**. |

*Table continues…*

| Name | Description |
|---|---|
| **Transport** | The type of transport protocols for the SIP server. The options are:<br>• **TCP**<br>• **UDP**<br>• **TLS**<br>The **Transport** field is set to **TLS** when the **Server Type** is **Remote Branch Office**. |
| **Whitelist** | The call is not blocked if the call originator exists in the Whitelist. |

## Authentication options

| Name | Description |
|---|---|
| **Enable Authentication** | The field to indicate whether the SIP server requires authentication.<br>If selected, authentication is required and the remaining fields are activated.<br>If cleared, authentication is not required and the remaining fields remain inactivate. |
| **User Name** | The user name required for authentication. |
| **Realm** | The realm from which the legitimate authentication request is made. |
| **Password** | The password required for authentication. |
| **Confirm Password** | The password entered in the **Password** field. |

## Heartbeat options

| Name | Description |
|---|---|
| **Enable Heartbeat** | Indicates whether a synchronization signal (heartbeat) is established between the Avaya SBC security device and the SIP server.<br>Select this check box to indicate that a heartbeat is established and maintained and the remaining fields are activated.<br>Clear the check box to indicate that no heartbeat is maintained and the remaining fields remain inactivated. |
| **Method** | Specifies the method by which the heartbeat is maintained. The options are:<br>• **OPTIONS**<br>• **PING** |
| **Frequency** | Specifies the frequency of sending the heartbeat signal. |
| **From URI** | Specifies the source of the heartbeat signal. |
| **To URI** | Specifies the destination of the heartbeat signal. |

### Registration options

| Name | Description |
|---|---|
| **Register with All Servers** | To send a REGISTER message to all servers.<br>• For the **DNS Query Type** as None/A, Avaya SBC sends the REGISTER message to the server configured in the DNS server or the resolved IP address by the DNS server.<br>• For **DNS Query Type** as SRV or NAPTR, Avaya SBC sends the REGISTER message to all servers resolved in the DNS response. |
| **Register with Priority Server** | To send a REGISTER message to the highest priority server as received in the DNS query response. Enable this option when using the DNS SRV for trunk registration feature.<br>If the highest priority server is non-functional on DNS TTL expiry, Avaya SBC sends the REGISTER message to the second highest priority server.<br>**Register with Priority Server** field is disabled if **DNS query type** is **NONE/A**. |
| **Refresh Interval** | Specifies the time, in seconds, after which Avaya SBC sends a REGISTER message to servers. |
| **From URI** | Specifies the source of the REGISTER message. |
| **To URI** | Specifies the destination of the REGISTER message. |

### Ping options

| Name | Description |
|---|---|
| **Enable Ping** | Select this option to enable ping on the server connections. |
| **Ping Interval** | Specifies the amount of time, in seconds, between ping messages sent to the server. |
| **Response Timeout** | Specifies the time, in seconds, after which a ping message times out. |

### Advanced options

| Name | Description |
|---|---|
| **Enable DoS Protection** | Indicates whether DoS protection is enabled for the SIP server.<br>• When you select the **Enable DoS Protection** check box, the EMS server displays **Next** at the bottom of the page. When you click **Next**, the EMS server displays a second Edit Server Configuration Profile – Advanced page, prompting for the number of users on the Call Server.<br>• When you configure the DoS protection for the SIP server, the EMS server displays two new tabs: **DoS Whitelist** and **DoS Protection** on the Server Configuration page.<br>The EMS server does not display this option for a Recording Server. |

*Table continues…*

| Name | Description |
|---|---|
| **Enable Grooming** | Indicates whether the same connection is used for the same subscriber or port. You must enable this field while using TCP or TLS. The **Enable Grooming** field is enabled by default.<br>If grooming changes are done on a production system, you must restart the application to clean up the old connections.<br>The **Enable Grooming** field is unavailable when the **Server Type** is Remote Branch Office. |
| **Interworking Profile** | Specifies the Interworking profile to be used for the SIP server. |
| **Signaling Manipulation Script** | Specifies the signaling manipulation script for the SIP server.<br>Specify a signaling manipulation script in this field in one of the following conditions:<br>• One server flow is associated with the server.<br>• All server flows associated with the server use the same signaling manipulation script.<br>**Note:**<br>If you select different scripts in the server configuration and the server flow, the EMS server uses the signaling manipulation script selected in the server flow. However, if you apply the manipulation as INBOUND and AFTER_NETWORK, the EMS server uses the script selected in the server configuration. |
| **Securable** | Specifies whether the server can be secured.<br>Avaya endpoints can display an end-to-end secure indicator for calls that use secure protocols for both halves of the call. Avaya SBC provides a **Securable** field on the Server Configuration page to indicate whether the server is securable. Avaya SBC uses the **Securable** field to determine whether the trunk and call server can use secure protocols, and sets appropriate values for the Av-Secure-Indication header. |
| **Enable FGDN** | Enables a Failover Group Domain Name (FGDN) that Avaya SBC uses to route SIP traffic through an alternate Session Manager when a Session Manager is unreachable. |
| **TCP Failover Port** | Specifies the TCP port used during failover to the FGDN.<br>This field is available only when you select the **Enable FGDN** check box. |
| **TLS Failover Port** | Specifies the TLS port used during failover to the FGDN.<br>This field is available only when you select the **Enable FGDN** check box. |
| **Tolerant** | Specifies whether the server processes both IPv4 and IPv6 addresses. |

*Table continues…*

| Name | Description |
|---|---|
| **Traffic Type** | Specifies the traffic type. The options are:<br>• **Trunk Traffic**<br>• **Remote Users**<br>• **Trunk Traffic and Remote Users**<br>The EMS server displays this field only when you select the **Enable DoS Protection** field. |
| **Max Concurrent Sessions** | Specifies the maximum number of concurrent sessions. The default value is 1000.<br>The EMS server displays this field only when you select the **Enable DoS Protection** field. |
| **Number of Remote Users** | Specifies the number of remote users.<br>The EMS server displays this field only when you select the **Enable DoS Protection** field.<br>When you select the **Remote Users** or **Trunk Traffic and Remote Users** option, the EMS server enables the **Number of Remote Users** field. |
| **URI Group** | Select the URI group you want to use with this profile, if any. |
| **NG911 Support** | Select this option to enable NG911 support for NG911 CS trunks. This option is required for adhoc conference support. |

## DoS Whitelist window

| Name | Description |
|---|---|
| **URI/Domain** | Specifies the URI or domain that is allowed from an external source.<br>The EMS server displays this tab only when you select the **Enable DoS Protection** check box on the **Advanced** tab. |

## DoS Protection

| Name | Description |
|---|---|
| **Traffic Type** | The type of traffic. |
| **Max Concurrent Sessions** | The maximum number of concurrent sessions. |
| **SIP Service** | The SIP service affected by the DoS attack. The options are:<br>• **TOTAL**<br>• **Registrations**<br>• **Calls**<br>• **Presence Updates**<br>• **Subscriptions**<br>• **Misc** |

*Table continues…*

| Name | Description |
|---|---|
| **SIP Method** | The SIP Method of the SIP service. The options are:<br>• **All**<br>• **REGISTER**<br>• **INVITE**<br>• **SUBSCRIBE**<br>• **PUBLISH**<br>• **OPTIONS** |
| **Initiated Threshold (per 10 seconds)** | The maximum number of sessions that you can start within 10 seconds . |
| **Pending Threshold** | The maximum number of pending session initiations. |
| **Failed Threshold (per 10 seconds**) | The maximum number of failed session initiations. |
| **Action** | The action to be performed after any of the above thresholds are exceeded.<br>The options are :<br>• **Alert Only**: An alert displays the DoS incident, but the call is not blocked.<br>• **Enforce Limit**: The call is not blocked until the specified limit is reached.<br>• **Enforce Limit Response**: The call is blocked, and the EMS server sends the specified response when the specified limit is reached.<br>• **SIP Challenge**: To initiate authentication.<br>**Note:**<br>Do not select the SIP Challenge action for a DoS profile configuration because Avaya phones do not respond the second time when they are again authenticated by Avaya after being challenged by Avaya SBC.<br>• **Whitelist**: The call is not blocked if the call originator exists in the **Whitelist**. |

# Configuring certificates

## Procedure

1. Get a root certificate and an intermediate CA chain certificate from a standard CA.
2. Install the certificates on the Avaya SBC server profile. Set peer verification to none.
3. Install the certificates on the Avaya SBC client profile. Enable peer certificate verification and import any Microsoft Teams CA certificates. You can get the certificates from Teams or run `openssl` on the sip.pstnhub.microsoft.com connection point.

# Chapter 5: Configuration of Microsoft Teams

## Configuring Microsoft® Teams options required for integration with Avaya SBC

This section contains the high-level configuration requirements you must administer when setting up Microsoft® Teams (Teams) in an Avaya SBC deployment. For detailed information about configuring Teams when using the Direct Routing features of Avaya SBC, see the following Teams website:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page

### Avaya SBC-related options

You must configure the following Avaya SBC information on the Teams system:

- Public IP address – A public IP address that can be used to connect to the Avaya SBC system. Avaya SBC supports NAT.
- Fully Qualified Domain Name (FQDN) – An FQDN for the Public IP address towards the Microsoft Teams side of the Avaya SBC system. The domain portion of the FQDN is one of the registered domains in your Microsoft 365 or Office 365 organization. For more information, see the following website:

  https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sbc-domain-names
- Public DNS entry – A public DNS entry mapping the Avaya SBC FQDN to the public IP address.
- Public trusted certificate – A certificate for the Avaya SBC to be used for all communication with Direct Routing. For more information, see the following website:

  https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

### Connection points for Direct Routing

The connection points for Direct Routing are the following three FQDNs:

- sip.pstnhub.microsoft.com – The global FQDN, it must be tried first.
- sip2.pstnhub.microsoft.com – The secondary FQDN, it geographically maps to the second priority region.
- sip3.pstnhub.microsoft.com – The tertiary FQDN, it geographically maps to the third priority region.

For more information, see the following website:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns

### Media servers

The Teams media servers use the IP addresses of the Teams connection points sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com. This resolves in the following IP address:

- 52.114.148.0
- 52.114.132.46
- 52.114.75.24
- 52.114.76.76
- 52.114.7.24
- 52.114.14.70
- 52.114.16.74
- 52.114.20.29

### Firewall settings

The following items must be opened in the Teams firewall settings:

- The signaling address should be open for the connection point FQDNs sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com.
- The media port of the range that is configured on the Avaya SBC media interface that points to the Teams SIP server or media server.
- The PSTN side signaling IP address and port.
- The media IP address and media port range on the Avaya SBC media interface pointing to the PSTN SIP server or media server.

For more information, see the following website:

https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

### OPTIONS format

Microsoft Teams must use the standard format of OPTIONS. Avaya SBC sends OPTIONS with the FQDN of the Avaya SBC system. Teams adds the FQDN of the Avaya SBC system in its ACL list. Teams sends OPTIONS for which the Avaya SBC system answers back with a 200OK message.

### SIP signaling using TLS

The Teams SIP signaling is set up to use TLS port 5061. For security reasons, the TLS version must be TLS 1.2.

For media server use the following range of IP addresses:

- 52.112.0.0/14 (IP addresses from 52.112.0.1 to 52.115.255.254)
- 52.120.0.0/14 (IP addresses from 52.120.0.1 to 52.123.255.254)

Use the port range: Port range from 49152 to 53247.

### SIP Response Codes

When configured correctly, you should expect 18x and 200OK messages from the Avaya SBC system. The standard error codes would be 408 (Request Timeout), 480 (Temporarily Unavailable, Teams client reachability problem), 488 (Not Acceptable Here, media interworking problems), 500 (Internal Server Error), and 503 (Service Unavailable).

### Elliptical Curve Cryptography (ECC) ciphers

Teams requires the use of the following ECC ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

### Secure Real-Time Transport Protocol (SRTP) calls

For SRTP calls, Teams must have SRTCP enabled, no Master Key Identifiers (MKI), and a default value of $2^{31}$ for its lifetime.

# Chapter 6: Configuration of Avaya SBC

## Configuration checklist

Use this checklist to identify the tasks required to configure Avaya SBC when used with Microsoft Teams. When you have finished the task, mark the task as completed.

| Task | Reference | ✔ |
|---|---|---|
| Configure server interworking. | Add server interworking profiles as described in About configuring server interworking for Microsoft Teams on page 56 and Adding a server interworking profile on page 57. | |
| Configure Session Manager adaptations for number manipulation. | Creating a new signaling rule on page 67<br>Adding a URI Manipulation rule on page 75<br>For more information about configuring these rules, see *Administering Avaya Session Border Controller*. | |
| Configure topology hiding. | About configuring topology hiding for Microsoft Teams on page 75 | |
| Configure signaling manipulation (SigMa). | About configuring signaling manipulation for Microsoft Teams on page 77 | |
| Configure transcoding. | About configuring Avaya SBC for transcoding and transrating on page 79 | |
| Configure RTCP generation. | RTCP monitoring generation support on page 83 | |

## Server interworking

### About configuring server interworking for Microsoft Teams

You must configure the following server types on Avaya SBC to make connections with Microsoft Teams:

- A trunk server for the PSTN.
- A call server for each of the Microsoft Teams SIP proxy servers.

Each of the Microsoft Teams SIP proxy servers act as a call server, so it must be configured with an Avaya SBC interworking profile to provide interworking functionality.

When configuring the interworking profiles, you must configure the following options in addition to any normal interworking options:

- The **Hold Support** option in the **General** tab must be set to **Microsoft Teams**.
- The **183 Handling** option must be administered with **No SDP**. This is required so that ringback is heard on trunks.
- The **Refer Handling** option in the **General** tab must be enabled. Usually for Teams, all sub-options of **Refer Handling** must be disabled or set to **None**. If required by the PSTN side and the topology, the sub-options can be enabled.
- The **Record Routes** option in the **Advanced** tab must be set to **Both Sides**.
- The **Extensions** option in the **Advanced** tab must be set to **Lync** (prior name for Microsoft Teams software).

# Adding a server interworking profile

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. On the Interworking Profiles screen, click **Add**.

   The EMS server displays the Interworking Profile window.
5. In the **Profile Name** field, type a name for the new interworking profile, and click **Next**.

   The system displays a series of configuration windows. Administer the profile options as required based on the options described in Interworking profile field descriptions on page 58.

   **Note:**

   Options for the **URI Manipulation** and **Header Manipulation** rules cannot be added until after you administer the basic interworking options. After you add a new profile, you can add these rules using the **Add** button located on the two rule tabs.
6. Click **Next** after configuring the options in each window.
7. Click **Finish** to save the settings.

# Interworking profile field descriptions

## General options

| Name | Description |
|---|---|
| **Hold Support** | Indicates the standard to be used to provide HOLD support. The options are:<br>• **None**<br>• **RFC 2543 - c=0.0.0.0**<br>• **RFC 3264 - a=send only**<br>• **Microsoft Teams**<br>The **Microsoft Teams** option is required for Microsoft Teams deployments to handle the hold/resume feature of Microsoft Teams. It enforces the Microsoft Teams side to send the “a=inactive” message. When this option is set, none of the following messages are sent towards Microsoft Teams: “a=sendonly”, “a=recvonly”, or “c=0.0.0.0”.<br>In addition, when you select the **Microsoft Teams** option, a Feature Flag is set in the Call Detail Record (CDR) by Avaya SBC. The Feature Flag is the 35th field in the CDR and is set to a value of 8. The Feature Flag identifies the call in CDR as a Microsoft Teams call. |
| **180 Handling** | Determines how 180 Ringing messages are handled. The options are:<br>• **None**<br>• **SDP**<br>• **No SDP** |
| **181 Handling** | Determines how 181 Call Forwarding messages are handled. The options are:<br>• **None**<br>• **SDP**<br>• **No SDP** |
| **182 Handling** | Determines how 182 Queued messages are handled. The options are:<br>• **None**<br>• **SDP**<br>• **No SDP** |

*Table continues…*

| Name | Description |
|---|---|
| **183 Handling** | Determines how 183 Session Progress messages are handled. The options are:<br>• **None**<br>• **SDP**<br>• **No SDP**<br>For Microsoft Teams, the **183 Handling** option must be administered with **No SDP**. This is required so that ringback is heard on trunks. |
| **Refer Handling** | Indicates whether Avaya SBC passes or consumes the REFER message. When an endpoint invokes a supplementary service, such as a call transfer, the endpoint generates and sends an in-dialog REFER request to Avaya SBC through the enterprise call server. Avaya SBC applies URI-based routing to the new **INVITE** message triggered towards the transfer target.<br>Refer Handling feature works in either of the following two modes:<br>• **Send Hold**<br>• **Delayed Offer**<br>When configuring a profile to use with Microsoft Teams, enable the **Refer Handling** option. |
| **URI Group** | Indicates the URI group that is required for REFER handing.<br>**Note:**<br>Avaya SBC enables the **URI Group** field only when you select the **Refer Handling** checkbox.<br>When configuring Microsoft Teams, it is recommended that the **URI Group** option be set to **None**. However, this option can be enabled if required by the PSTN side and topology. |
| **Send Hold** | Indicates whether Avaya SBC sends a HOLD message to a trunk when processing REFER messages for that trunk. Disable this setting for trunks that do not support SIP HOLD. By default, this setting is on.<br>**Note:**<br>Avaya SBC enables the **Send Hold** check box only when you select the **Refer Handling** check box.<br>When configuring Microsoft Teams, it is recommended that the **Send Hold** option be disabled. However, this option can be enabled if required by the PSTN side and topology. |

*Table continues…*

| Name | Description |
|---|---|
| **Delayed Offer** | Indicates whether Avaya SBC sends an INVITE message to the transferee without SDP. If you select **Delayed Offer**, Avaya SBC gets the complete capabilities of the transferee as an SDP Offer message.<br><br>Avaya SBC enables the **Delayed Offer** check box only when you select the **Refer Handling** check box.<br><br>When configuring Microsoft Teams, it is recommended that the **Delayed Offer** option be disabled. However, this option can be enabled if required by the PSTN side and topology. |
| **3xx Handling** | Indicates whether the Avaya SBC security device will handle the *3xx Redirection Response* messages. |
| **Diversion Header Support** | Indicates whether the Avaya SBC security device supports diversion headers.<br><br>**Note:**<br><br>When you select the **3xx Handling** check box, the system enables the **Diversion Header Support** check box. |
| **Delayed SDP Handling** | Indicates whether the Avaya SBC security device processes delayed SDP packets.<br><br>**Important:**<br><br>The features Media Unanchoring and Delayed SDP Handling cannot both be enabled for a call. For more information about administering those features, see *Administering Avaya Session Border Controller*. |
| **Re-Invite Handling** | Indicates whether Reinvite Handling is enabled for Avaya SBC. If a trunk or call server does not want in-dialog **RE-INVITES**, then enable Reinvite Handling.<br><br>Precondition: **RE-INVITE SDP** must be the same as the previous INVITE transaction SDP. For example, consider a trunk server that has Reinvite Handling enabled. When the first **INVITE** with SDP goes to the trunk server, Avaya SBC stores this message. When the next **INVITE** goes to the trunk server, Avaya SBC tries to match the current **INVITE SDP** with the stored SDP. If both SDPs are same, Avaya SBC stops **INVITE** and responds . However, if a second INVITE comes without any SDP change, while adding extra SDP parameters to Hold or Resume, Avaya SBC handles **RE-INVITE**.<br><br>**Important:**<br><br>When **Re-Invite Handling** is enabled, the far end should not change its CODEC, SRTP, and media parameters mid-call. If any of these parameters change, Reinvite Handling will not work |

*Table continues…*

| Name | Description |
|---|---|
| **Prack Handling** | Indicates whether Provisional Response Acknowledgement (PRACK) handling is enabled. When called party sends provisional requests with 100 rel option in the Require header, called party must receive PRACK message in the response to ensure end to end successful communication. If the trunk or call server does not send 100 rel option in the supported header for the initial INVITE request then by selecting **Prack Handling**, Avaya SBC sends the PRACK for that particular trunk or call server to the called party. |
| **Allow 18X SDP** | Indicates whether a PRACK message is permitted in an 18x record route header. |
| **T.38 Support** | Indicates whether Avaya SBC security device. supports the T.38 FAX Relay standard. |
| **URI Scheme** | Indicates the URI scheme that the Avaya SBC security device will use. The options are:<br>• **SIP**<br>• **TEL**<br>• **ANY** |
| **Via Header Format** | Indicates the header format used by the Avaya SBC security device. The options:<br>• **RFC3261**<br>• **RFC2543** |
| **SIPS Required** | Use this option to control the SIP/SIPS URI scheme handling for SRTP calls. By default, this option is enabled.<br>When doing an upgrade to Release 8.1.2 or later, this option is automatically enabled after the upgrade. For any configurations that do not use this feature, you must manually disable this option after you do the upgrade. For example, you must disable this option in Server Interworking profiles when the deployment has or uses Microsoft Teams, Skype for Business, or Lync.<br>**Note:**<br>When Assured SIP (AS-SIP) mode is enabled, the **SIPS Required** option is grayed out and is not available. |
| Mediasec Handling | Use this option to distinguish security mechanisms that apply to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label such security mechanisms. |

## SIP Timers options

| Name | Description |
|---|---|
| **Min-SE** | Specifies the minimum value for the SIP min-SE timer. The Min-SE timer is used for a SIP refresh (Re-Invite/Update) session as the minimum session expire time value.<br>The time range is 90 to 86400 seconds. |

*Table continues…*

| Name | Description |
|---|---|
| **Init Timer** | Specifies the initial request retransmission interval. This interval corresponds to Timer T1 in RFC 3261. This timer is used when sending a request over UDP.<br>The time range is 50 to 1000 milliseconds. |
| **Max Timer** | Specifies the maximum retransmission interval for non-INVITE requests. This interval is for non-INVITE requests and corresponds to Timer T2 in RFC 3261.<br>The time range is 200 to 8000 milliseconds. |
| **Trans Expire** | Specifies the Transaction Expiration timer. The default value for this field is 32 seconds.<br>Any request that the server sends times out if the server does not receive a response within the time set as the Transaction Expiration time. To use alternate routing, you must set a shorter transaction expiration value than the default value of 32 seconds.<br>The time range is 1 to 64 seconds. |
| **Invite Expire** | Specifies the transaction expiration time for an INVITE transaction after what receives a provisional response .<br>The time range is 180 to 300 seconds. |
| **Retry After** | Specifies the maximum time after which the server sends the routing request again.<br>The time range is 2 to 32 seconds. |

## Privacy options

| Name | Description |
|---|---|
| **Privacy Enabled** | Indicates whether privacy is used between the Avaya SBC security device and the SIP server.<br>**Note:**<br>When you select the **Privacy Enabled** checkbox, the system enables the following fields: **User Name**, **P-Asserted-Identity**, **P-Preferred-Identity**, and **Privacy Header** fields. |
| **User Name** | Specifies the user name to be used for privacy authentication. |
| **P-Asserted-Identity** | Indicates that Avaya SBC rewrites the FROM header in a trusted SIP message with the P-Asserted-ID.<br>This field is used for maintaining privacy for the FROM header. Trunk servers usually Accept SIP INVITE with P-asserted ID. For some Trunk servers, Avaya SBC inserts this header into the FROM header, insert the header in P-asserted ID and change From as Anonymous user, and send out the request. not clear |
| **P-Preferred-Identity** | Indicates that Avaya SBC uses the P-Preferred-ID during private sessions. |
| **Privacy Header** | Specifies the Privacy Header to be used during privacy sessions. |

### Advanced options

| Name | Description |
|---|---|
| **Record Routes** | Directs the Avaya SBC security device to record route information. The options are:<br>• **None**: Avaya SBC does not add any record route. However, to remove all record routes, enable Topology Hiding (TH) with record route auto.<br>• **Single Side**: Avaya SBC adds only one record route. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed.<br>• **Both Sides**: Avaya SBC adds two record routes. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed and only one record route is retained.<br>When configuring a profile to use with Microsoft Teams, enable the **Both Sides** option.<br>• **Dialog Initiate Only (Both Sides)**: Avaya SBC adds two record routes, but not to the in-dialog message. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed and only one record route is retained.<br>• **Dialog Initiate Only (Single Side)**: Avaya SBC adds one record route, but not to the in-dialog message. If Avaya SBC receives a 200 OK message, Avaya SBC passes the same record route outside the enterprise network. If TH is enabled, the 200 OK record routes are removed. |
| **Include Endpoint IP for Context Lookup** | Directs the Avaya SBC security device to use endpoint IP while looking for Avaya SBC internal SIP context. |
| **Extensions** | Directs the Avaya SBC security device to use functionality specific to different environments. The available options are:<br>• **Avaya**<br>**Important:**<br>You must use the **Avaya** option if you want to use the `traceSBC` command to search for Av-Global-Session-ID (GSID) headers to filter SIP call traces.<br>• **Nortel**<br>• **Lync**<br>**Note:**<br>When configuring a profile to use with Microsoft® Teams, enable the **Lync** option. “Lync” was a prior name for Microsoft® Teams.<br>• **Cisco** |

*Table continues…*

| Name | Description |
|---|---|
| | • **KDDI** |
| **Diversion Manipulation** | Directs the Avaya SBC security device to copy SIP Diversion header from 3xx messages to Sip Request messages while 3xx handling is enabled on Avaya SBC security device. |
| **Diversion Condition** | Specifies the diversion condition.<br>**Note:**<br>When you select the **Diversion Manipulation** check box, the system enables the **Diversion Condition** field. |
| **Diversion Header URI** | Specifies the Avaya SBC security device to add SIP Diversion header on the SIP Invite message.<br>**Note:**<br>When you select the **Diversion Manipulation** check box, the system enables the **Diversion Header URI** field. |
| **Has Remote SBC** | Directs the Avaya SBC security device to use far-end firewall functionality. |
| **Route Response on Via Port** | Directs the Avaya SBC security device to use SIP Via header port to route response. |
| **Relay INVITE Replace for SIPREC** | Select this option to enable **Relay INVITE Replace for SIPREC**. |
| **MOBX Re-INVITE Handling** | Select this option to enable **MOBX Re-INVITE Handling**.<br>Enable this feature for calls made by Mobile Extension (MOBX) users that are calling through a Mobile Service Provider (MSP) serviced by an Avaya SBC system. The Avaya SBC can terminate these mobile calls to a PSTN user through SIP-PRI gateways or to a user connected to an Avaya private network communication server.<br>Use this option to allow Avaya SBC to filter the reinvite messages coming from an Avaya private network communication server to the MSP. The Re-INVITE handling configuration must be enabled on the MSP trunk server interworking profiles. |
| **NATing for 301/302 Redirection** | When **NATing for 301/302 Redirection** is enabled for server interworking, Avaya SBC will NAT 301/302 contact addresses going to the server.<br>Select this option for Adhoc conferencing support with the Next Generation 911 feature. When enabled, Avaya SBC will NAT on 301/302 contact address received from the Next Generation Core Services (NGCS) conference factory.<br>This option has no affect operation of 301/302 messages on Remote Worker configurations. |
| **DTMF Support** | These options define whether and how RFC 2833 DTMF touch-tone signals are converted to SIP messages. When conversion occurs, the DTMF signals and SIP messages are sent in parallel in the call path to support signaling devices that require either DTMF signals (such as an IVR) or SIP messages (such as SIP trunks). You must have interworking profiles for both inbound |

*Table continues…*

| Name | Description |
|---|---|
| | calls (always set to **None**) and outbound calls (using one of the options defined below). You must define the profiles for the servers.<br><br>**Note:**<br><br>DTMF signal conversion to SIP messages will not happen when a registered user is involved in the call.<br><br>**Important:**<br><br>Avaya recommends that for deployments where personal data protection based on GDPR requirements are critical, you should not use DTMF interworking. For more information about Avaya SBC support for GDPR, see *Avaya Session Border Controller Overview and Specification*.<br><br>• **None** – RFC 2833 DTMF touch-tone signals are passed through and are not converted to SIP messages.<br>• **SIP Notify** – RFC 2833 DTMF touch-tone signals are converted to out-of-band SIP Notify messages. Conversely, SIP Notify messages are converted back to RFC 2833 DTMF touch-tone signals.<br>• **RFC 2833 Relay & SIP Notify** – RFC 2833 DTMF touch-tone signals passed through and are also converted to out-of-band SIP Notify messages. Conversely, SIP Notify messages are converted back to RFC 2833 DTMF touch-tone signals. See the information below about how this option is used for MOBX calls.<br>• **SIP INFO** – RFC 2833 DTMF touch-tone signals are converted to out-of-band SIP Info messages. Conversely, SIP Info messages are converted back to RFC 2833 DTMF touch-tone signals.<br>• **RFC 2833 Relay & SIP Info** – RFC 2833 DTMF touch-tone signals passed through and are also converted to out-of-band SIP Info messages. Conversely, SIP Info messages are converted back to RFC 2833 DTMF touch-tone signals. See the information below about how this option is used for MOBX calls.<br>• **Inband** – RFC 2833 DTMF touch-tone signals are converted to in-band DTMF. Conversion in the opposite direction is not supported.<br><br>Avaya SBC uses the **RFC 2833 Relay & SIP Info** or **RFC 2833 & SIP Notify** options to fork the incoming RFC 2833 DTMF touch-tone signals and SIP Info or SIP Notify messages to carry the DTMF signals in SIP signaling messages. The MOBX URI group configuration is required to configure these DTMF options.<br><br>MOBX calls use standard mobile user features that invoke RFC 2833 DTMF touch-tone signals, such as digits for an IVR. Avaya SBC must pass the original DTMF touch-tone signals to a media gateway or endpoint in parallel with sending the SIP Notify or SIP Info messages to an Avaya private network communication server.<br><br>Any server configured on Avaya SBC that supports MOBX users on a Mobile Service Provider (MSP) must also have a URI group configured that identifies the MSP users. |

### URI Manipulation options

**Note:**

Options for the **URI Manipulation** and **Header Manipulation** rules cannot be added until after you administer the basic interworking options. After you add a new profile, you can add these rules using the **Add** button located on the two rule tabs.

| Name | Description |
|---|---|
| **User Regex** | The Regex rule to be used to match the **User** field in the SIP message. |
| **Domain Regex** | The Regex rule to be used to match the **Domain** field in the SIP message. |
| **User Action** | The action that the Avaya SBC security device takes on finding a User Regex match . The options are:<br>• **None**<br>• **Add prefix [Value]**<br>• **Remove prefix [Value]**<br>• **Replace with [Value]**<br>• **Replace [Value 1] with [Value 2]** |
| **User Values** | The values to be used as specified in the **User Action** field.<br>**Note:**<br>When you select the **Replace [Value 1] with [Value 2]** option, the system enables the second text box. |
| **Domain Action** | The action that the Avaya SBC security device takes on finding a Domain Regex match . The options are:<br>• **None**<br>• **Add prefix [Value]**<br>• **Remove prefix [Value]**<br>• **Replace with [Value]**<br>• **Replace [Value 1] with [Value 2]** |
| **Domain Values** | The values to be used as specified in the **Domain Action** field.<br>**Note:**<br>When you select the **Replace [Value 1] with [Value 2]** option, the system enables the second text box. |

### Header Manipulation options

| Name | Description |
|---|---|
| **Header** | The SIP header field to be manipulated.<br>The options are:<br>• **Contact**<br>• **Diversion**<br>• **From**<br>• **P-Asserted-Identity**<br>• **RequestURI**<br>• **To** |
| **Action** | The action to be performed. The options are:<br>• **Add Parameter w/ [Value]**<br>• **Remove Parameter w/ [Value]** |
| **Parameter** | The parameter to be used in the action performed in the **Action** field. |
| **Value** | The value of the parameter defined in the **Parameter** field. |

# Session Manager adaptations

## Creating a new signaling rule

### About this task

Use the following procedure to create a new Signaling Rule.

**Caution:**

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

### Procedure

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

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

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

The EMS server displays the second signaling rule window.

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

### Result

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

**Related links**

Signaling Rules field descriptions on page 68

## Signaling Rules field descriptions

### Add Signaling Rule

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

*Table continues…*

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

*Table continues…*

| Name | Description |
|---|---|
| Enable Content-Type Checks | Option to enable checks for the content part of the SIP signaling message. |
| Action | Drop-down menu from which you choose the action to be taken by the Avaya SBC security device when considering the content portion of SIP signaling messages. The following options are available:<br>• **Allow**: Allows the content in each SIP signaling message to pass, with the exception of those items contained in the Exceptions List that are removed.<br>• **Remove**: Removes all content from each SIP signaling message, with the exception of the items contained in the Exceptions List that are allowed to pass. |
| Exception List | The specific terms to be passed or blocked, according to the action specified in the **Action** field. |
| Multipart Action | Drop-down menu from which you choose the action to be taken by the Avaya SBC security device when considering the multipart content portion of SIP signaling messages. The following options are available:<br>• **Allow**: Allows the multipart content in each SIP signaling message to pass, with the exception of those items contained in the Exception List that are removed.<br>• **Remove**: Removes all the multipart content from each SIP signaling message, with the exception of the items contained in the Exception List that are allowed to pass. |
| Exception List | The specific terms to be passed or blocked, according to the action specified in the **Multipart Action** field. |
| QoS | |
| Enabled | Indicates whether the Signaling Quality-of-Service (QoS) feature is enabled. |

*Table continues…*

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

*Table continues…*

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

## Add Request Control

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

*Table continues…*

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

## Add Response Control

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

## Add Header Control

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

*Table continues…*

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

## Add Response Header Control

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

**Related links**

Creating a new signaling rule on page 67

## Adding a URI Manipulation rule

### Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Server Interworking**.
4. Click **URI Manipulation** tab.
5. Click **Add**.
6. Administer the options as described in Interworking profile field descriptions on page 58.
7. Click **Finish**.

# Topology hiding

## About configuring topology hiding for Microsoft Teams

You must configure the Topology Hiding feature of Avaya SBC when setting up a connection to the Microsoft Teams system. Topology Hiding masks the IP address of the Avaya SBC system used with Microsoft Teams, but exposes an FQDN that the Microsoft Teams SIP proxy can use for connectivity.

For example, you might set up the options as follows:

- Header = From
- Criteria = IP/Domain
- Replace Action = Overwrite
- Overwrite Value = the FQDN of the Avaya SBC system

For more details about Topology Hiding, see *Administering Avaya Session Border Controller*.

## Creating a Topology Hiding profile

### About this task

Topology Hiding masks the FQDN or IP address portion of SIP headers. For example, SBC@avaya.com can become SBC@135.122.18.7, or just the opposite. Though changing the headers can mask the internal topology, the headers can be adapted into the format that the recipient requires. All SIP Service Providers require the domain to be expressed as an IP address, but some connections can use an FQDN.

### Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Configuration Profiles** > **Topology Hiding**.

   The EMS server displays the existing topology hiding profiles and the corresponding topology headers.
4. Click **Add**.

   The EMS server displays the Topology Hiding Profile screen.
5. Administer the options as described in Topology Hiding Profiles field descriptions on page 76.
6. Click **Finish**.

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

## Topology Hiding Profiles field descriptions

| Name | Description |
|---|---|
| **Profile Name** | A descriptive name for the new topology hiding profile. |
| **Header** | The name of the header that will be changed with topology hiding.<br>The options are:<br>• **Request—Line**<br>• **From**<br>• **To**<br>• **Record-Route**<br>• **Via**<br>• **SDP**<br>• **Refer-To**<br>• **Referred-By** |

*Table continues…*

| Name | Description |
|---|---|
| **Criteria** | The criteria that are changed with topology hiding.<br>The options are:<br>• **IP/Domain**<br>• **IP**<br>• **Domain**<br>**Note:**<br>Ensure that the values in the **Header** field and the **Criteria** field with topology hiding are same.<br>For example, if you are not sure about the value of the **Header** field, configure the **Criteria** field with topology hiding as **IP/Domain**.<br>If the **Header** is:<br>• **IP** : Configure the **Criteria** field with topology hiding as IP.<br>• **Domain** : Configure the **Criteria** field with topology hiding as Domain. |
| **Replace Action** | The data that replaces the header.<br>The options are:<br>• **Auto**<br>• **Next Hop**<br>• **Destination IP**<br>• **Overwrite** |
| **Overwrite Value** | The value that overwrites the header.<br>This field is available only when you select **Overwrite Replace Action**. |

# Signaling manipulation

## About configuring signaling manipulation for Microsoft Teams

You must configure Avaya SBC with signaling manipulation (SigMa) rules. SigMa rules are used to modify certain numbering plans and attributes specific to PSTN trunks. Microsoft Teams with Avaya SBC is certified using PSTN trunks. Different PSTN trunks will require specific SigMa rules for those trunks. The SigMa scripts must be attached to the SIP server that corresponds to the PSTN trunks.

The following modifications are controlled using SigMa scripts:

- Modify the Contact, Record-Route URI host with the Avaya SBC FQDN.

- Add a prefix if required by the PSTN trunk dialing plan by modifying the From, To, and Request lines.
- Add the X-MS-SBC header.
- (Optional) For incoming messages from Microsoft Teams, modify the Request line with the Avaya SBC IP address.
- (Optional) For incoming messages from Microsoft Teams, modify the Record-Route and Route headers with the Avaya SBC IP address if the Record-Route or Route header contains the Avaya SBC FQDN.

**Note:**

The last two scripts are marked optional, but you may need to create the scripts depending on your topology. Depending on your Service Providers, you might also need to apply other SigMa rules such as removing History Info and adding number manipulation. For more information, see *Administering Avaya Session Border Controller*.

# SigMa rule examples required for Microsoft Teams

This section shows examples of SigMa rules that must be added when using Microsoft Teams. For more information about SigMa rules, see *Administering Avaya Session Border Controller*.

## Remove History Info

Use the following script to remove History Info that Microsoft Teams does not understand, plus other Avaya Aura® specific headers not used by Microsoft Teams. The Avaya Aura® specific headers are shown in bold type. You must install this script.

```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {

       remove(%HEADERS["History-Info"][3]);
       remove(%HEADERS["History-Info"][2]);
       remove(%HEADERS["History-Info"][1]);
       remove(%HEADERS["Remote-Party-ID"][1]); //Remove the header
       remove(%HEADERS["Remote-Address"][1]); //Remove the header
       remove(%HEADERS["P-AV-Message-Id"][1]); //Remove the header
       remove(%HEADERS["x-nt-e164-clid"][1]); //Remove the header
       remove(%HEADERS["P-Charging-Vector"][1]); //Remove the header
       remove(%HEADERS["Av-Global-Session-ID"][1]); //Remove the header
       remove(%HEADERS["P-Location"][1]); //Remove the header
       remove(%HEADERS["Alert-Info"][1]); //Remove the header
       remove(%HEADERS["User-to-User"][1]); //Remove the header
       remove(%HEADERS["Max-Breadth"][1]); //Remove the header



    }

}
```

### Failover

Use the following script to insert the exact version of the Avaya SBC software release into the header. This is required for Microsoft Teams failover. When creating this script, use the actual release number; this is only an example of the release number.

```
within session "all"

{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"

  {
    %HEADERS["X-MS-SBC"][1] = "AVAYA SBCE-8.1.1.19158";
   }
}
```

### Number manipulations

This is an example of a script that you can used to manipulate any required numbering plan changes. The following is only an example. You must change the script to match your numbering plan.

For instance, this example shows how the number “719” is manipulated to add the string “+1” so that when a user simply dials the area code “719”, the actual digit dialed is “+1719”.

```
within session "all"

{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"

  {

        %HEADERS["From"][1].URI.USER.regex_replace("^214","+1214");
        %HEADERS["To"][1].URI.USER.regex_replace("^719","+1719");
        %HEADERS["Request_Line"][1].URI.USER.regex_replace("719","+1719");

    }
}
```

# Transcoding

## About configuring Avaya SBC for transcoding and transrating

Transcoding translates a media stream encoded by using one codec into a media codec encoded by using another codec. Avaya SBC performs transcoding when the inbound and outbound entities have incompatible codecs. The Session Description Protocol (SDP) offer contains information about the codecs that the device sending the message prefers. The device that receives the message responds to the SDP offer by using the set of codecs that the receiving device supports.

Transrating reduces the bit rate of the media while retaining the original media format. Transrating is required where bandwidth is a constraint, for example, on the Wide Area Network (WAN). Enabling transrating results in a lesser number of packets and packet overhead because the packetization period is increased. For example, the packetization period (ptime) is 40 ms on WAN

and 10 ms on an internal enterprise network for the same codec. For this example, transcoding is not required, but transrating is required because the packetization period for the same codec is different between inbound and outbound streams.

### Codecs supported for transcoding

The following codecs are supported for transcoding:

- G711
- G711A
- G711MU
- G711U
- G722
- G726-32
- G729
- G729AB
- H224
- H264/SVC
- OPUS Constrained Narrow Band
- OPUS Narrow Band
- OPUS Wide Band
- PCMA
- PCMU
- AMR-WB
- AMR-NB

The following codecs are supported specifically for Teams:

- G711A
- G711U
- G722
- G729
- OPUS

Any codecs not listed here that are used for calls passing through Avaya SBC do not receive any transcoding treatment from Avaya SBC and are simply relayed through the system.

**Note:**

Avaya SBC does not support the SILK codec, and it can be filtered if required.

# Checklist for configuring Avaya SBC for transcoding

| Task | Description | ✔ |
|---|---|---|
| Enable the transcoding and tranrating features. | Enabling transcoding and transrating on page 81 | |
| Administer codec prioritization. | Configuring codec prioritization on page 81 | |
| Add the media rule, which has transcoding enabled, to an endpoint policy group. | Configuring endpoint policy group on page 82 | |
| Add the endpoint policy group to a server flow. | Configuring a server flow for transcoding on page 82 | |

# Enabling transcoding and transrating

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the left navigation pane, click **Network & Flows** > **Advanced Options**.
4. Click the **Feature Control** tab.
5. Select the **Transcoding** check box.

   Active transcoding calls are lost when the transcoding feature is disabled.
6. If transrating is required, select the **Transrating** check box.
7. If Avaya Aura® Media Server offloading is required, select the **AMS_OFFLOADING** check box.
8. Click **Save**.

# Configuring codec prioritization

## Procedure

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

   The application pane displays the existing Media Rule sets, and the content pane displays the parameters of the selected Media Rule set.
4. Click **Codec Prioritization** tab and click **Edit**.
5. Select the **Codec Prioritization**, **Transcode When Needed**, and **Transrating** check boxes.

   The system displays `[Transcodable]` next to the codecs that can be transcoded.

In the Video Codecs section, the **Transcode When Needed** field is unavailable. Video codecs cannot be transcoded.

You can select **Transrating** and **Transcode When Needed** fields independently.

6. **(Optional)** To remove all codecs that are not included in the Preferred Codecs list , select the **Allow Preferred Codecs Only** check box.
7. In the **Available** column, select the transcodable codecs, and click the right arrow button (**>**) to move them to the **Selected** column in the order of preference.
8. In the **Ptime** column, select a packetization time.

   You can select a packetization time only if you have selected the **Transrating** field.
9. Click **Next**.
10. **(Optional)** If required, enable BFCP, FECC, and ANAT.
11. Click **Finish**.

# Configuring endpoint policy group

## Procedure

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

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

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

   The EMS server displays the Edit Policy Set window.
6. In the **Media Rule** field, click the transcode-enabled media rule.
7. Click **Finish**.

# Configuring a server flow for transcoding

## About this task

You must attach the endpoint policy group containing the transcode-enabled media rule to the server flow. This ensures that the codec policy is applied for network messaging coming from or going to the server.

## Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Network & Flows** > **End Point Flows**.

4. Click the device for which you want to change the trunk server flow.
5. Click the **Server Flow** tab.
6. In the row corresponding to the server flow that you want to change, click **Edit**.
7. In the **End Point Policy Group** field, click the endpoint policy group with the transcode-enabled media rule.
8. Click **Finish**.

# RTCP generation

## RTCP monitoring generation support

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

**Important:**

RTCP monitoring generation is applicable only for SIP trunks.

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

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

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

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

**Related links**

Round Trip Time on page 83
Configuring RTCP monitoring generation support on page 84

## Round Trip Time

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

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

T2–T1 is the time between two RTP packets

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

**Related links**

RTCP monitoring generation support on page 83

## Configuring RTCP monitoring generation support

### Procedure

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

**Related links**

RTCP monitoring generation support on page 83
RTCP Monitoring Report Generation field descriptions on page 84

### RTCP Monitoring Report Generation field descriptions

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

**Related links**

Configuring RTCP monitoring generation support on page 84

# Chapter 7: Licensing requirements

## About licensing requirements

Avaya SBC uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBC software. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBC:

- Standard Services delivers non-encrypted SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication, and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBC.

Avaya SBC uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBC license file on a primary Element Management System (EMS) using the Device Management page.

**Important:**

You must not enable the local WebLM option and install an Avaya SBC license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **Grace Period State**.

Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBC works normally during the grace period.

**Important:**

Licenses and a WebLM server are required for new installations or upgrades.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

The primary host ID of WebLM is used for creating the license file.

- Licensed features
- Licensed capacity

All hardware Avaya SBC devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBC on hardware, use a WebLM server installed on VMware or System Manager WebLM.

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

For integration with Microsoft® Teams, Avaya SBC requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBC requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

# Avaya SBC licensed features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

| License feature | Description |
|---|---|
| VALUE_SBCE_STD_SESSION_1 | Specifies the number of standard session licenses. |
| VALUE_SBCE_STD_HA_SESSION_1 | Specifies the number of standard service HA session licenses. |
| VALUE_SBCE_ADV_SESSION_1 | Specifies the number of session licenses for remote worker, media recording, and encryption.<br>**Note:**<br>You must buy and deploy a standard session license with every advanced license feature. |
| VALUE_SBCE_ADV_HA_SESSION_1 | Specifies the number of advanced service HA session licenses. |
| VALUE_SBCE_PREM_SESSION | Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams. |

*Table continues…*

| License feature | Description |
|---|---|
| VALUE_SBCE_PREM_HA_SESSION | Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams. |
| VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1 | Specifies the number of Avaya Meetings Server video conferencing session licenses. |
| VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1 | Specifies the number of Avaya Meetings Server video conferencing HA session licenses. |
| VALUE_SBCE_CES_SVC_SESSION_1 | Specifies the number of Client Enablement Services session licenses. |
| VALUE_SBCE_CES_HA_SVC_SESSION_1 | Specifies the number of Client Enablement Services HA session licenses. |
| VALUE_SBCE_TRANS_SESSION_1 | Specifies the number of transcoding session licenses. |
| VALUE_SBCE_TRANS_HA_SESSION_1 | Specifies the number of transcoding HA session licenses. |
| VALUE_SBCE_ELEMENTS_MANAGED_1 | Specifies the maximum number of Avaya SBC elements managed. |
| VALUE_SBCE_VIRTUALIZATION_1 | Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted. |
| VALUE_SBCE_ENCRYPTION_1 | Specifies that both media and signaling can be encrypted for Avaya SBC. This license is required when using any advanced licenses. |
| FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1 | Specifies the configuration of HA for the setup. |
| FEAT_SBCE_DYNAMIC_LICENSING_1 | Specifies that dynamic or pooled licensing is permitted for Avaya SBC. The quantity of this license must match the quantity of standard licensing in the system being managed. |
| VALUE_SBCE_RUSSIAN_ENCRYPTION_1 | Specifies Avaya SBC encryption only for signaling. |
| VALUE_SBCE_NG911 | Specifies the number of AMR-WB codec licenses. |
| VALUE_SBCE_NG911_HA | Specifies the number of AMR-WB codec HA licenses. |

# License installation

You can install Avaya SBC license on either of the following servers:

- The WebLM server on System Manager
- The local WebLM server

## Installing a license on WebLM server on System Manager

### Before you begin

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/.

### About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering standalone Avaya WebLM*.

### Procedure

1. Log in to the System Manager web interface.
2. On the home page, in the **Services** section, click **Licenses**.
3. In the left navigation pane, click **Install license**.
4. Browse to the location where you saved the license file, and select the file to upload.
5. Click **Install**.
6. Verify that the license is installed. If the installation is successful, a new menu item named ASBC appears in the left navigation pane. Click **ASBC** to view the licensed features.

## Installing a license file on the local WebLM server

### Procedure

1. Log in to the WebLM application. If you are logging in for the first time, the system prompts you to change the default password.
2. In the left navigation pane, click **Install License**.

   The system displays the Install License page.
3. In the **Enter license path** field, select the downloaded license from your computer and click **Install**.

   After the license is successfully installed, the system displays a new menu **ASBC**.
4. Click **ASBC** to view the license information.

# Configuring the WebLM server IP address using the EMS web interface

### Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

### Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Licensing**.
3. Do one of the following tasks:
   - For a WebLM server or standalone server installed on System Manager , in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

     The URL format of the WebLM server installed on System Manager is:

     `https://<SMGR_server_IP>:52233/WebLM/LicenseServer`

     The URL format of the standalone WebLM server is:

     `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.
   - For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.
4. Click **Refresh Existing License** to refresh the existing licenses.
5. Click **Verify Existing License** to verify the existing WebLM license to confirm it is trusted.

   If the WebLM license is trusted, a pop window will display the certificate details. Otherwise, you can select the option to trust the WebLM certificate manually.
6. On the Dashboard screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows `OK`.
7. Click the **Devices** tab.
8. Locate the Avaya SBC device you configured, and click **Edit**.

   The EMS server displays the Edit Device dialog box.
9. In the **Standard Sessions**, **Advanced Sessions**, **Scopia Video Sessions**, and **CES Sessions** fields, type the number of licensed sessions depending on the license you purchased.
10. Click **Finish**.

# Configuring the WebLM server IP address using CLI

### Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

### Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command to configure an external WebLM server URL:

   **`sbceconfigurator.py config-weblm-url <WebLM URL>`**

3. Reboot Avaya SBC.

# About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBC connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBC setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBC setup.
- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBC.

**Note:**

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBC setup.

# Chapter 8: Resources

## Documentation

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

| Title | Description | Audience |
|---|---|---|
| Design | | |
| *Avaya Session Border Controller Overview and Specification* | High-level functional and technical description of characteristics and capabilities of the Avaya SBC. | Sales engineers, solution architects, and implementation engineers |
| *Avaya Session Border Controller Release Notes* | Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions. | Sales and deployment engineers, solution architects, and support personnel |
| *Avaya Solutions Platform Overview and Specification* | Describes the key features of Avaya Solutions Platform servers. | IT Management, sales and deployment engineers, solution architects, and support personnel |
| Implementation | | |
| *Deploying Avaya Session Border Controller on a Hardware Platform* | Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers. | Sales and deployment engineers, solution architects, and support personnel |
| *Deploying Avaya Session Border Controller on a Virtualized Environment Platform* | Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers. | Sales and deployment engineers, solution architects, and support personnel |
| *Deploying Avaya Session Border Controller on a Google Cloud Platform* | Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform. | Sales and deployment engineers, solution architects, and support personnel |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| *Deploying Avaya Session Border Controller on an Amazon Web Services Platform* | Describes how to plan and deploy an Avaya SBC system on Amazon Web Services. | Sales and deployment engineers, solution architects, and support personnel |
| *Deploying Avaya Session Border Controller on a Microsoft® Azure Platform* | Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform. | Sales and deployment engineers, solution architects, and support personnel |
| *Avaya Session Border Controller Port Matrix* | Describes the incoming and outgoing port usage required by the product. | Sales and deployment engineers, solution architects, and support personnel |
| *Upgrading Avaya Session Border Controller* | Describes how to upgrade to the latest release of Avaya SBC. | Sales and deployment engineers, solution architects, and support personnel |
| *Installing the Avaya Solutions Platform 110 Appliance* | Describes how to install Avaya Solutions Platform 110 Appliance servers. | Sales and deployment engineers, solution architects, and support personnel |
| Administration | | |
| *Administering Avaya Session Border Controller* | Describes configuration and administration procedures. | Implementation engineers and administrators |
| Maintenance and Troubleshooting | | |
| *Maintaining and Troubleshooting Avaya Session Border Controller* | Describes troubleshooting and maintenance procedures for Avaya SBC. | Implementation engineers |
| *Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance* | Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers. | Implementation engineers |
| Using | | |
| *Working with Avaya Session Border Controller and Microsoft® Teams* | Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams. | Implementation engineers and administrators |
| *Working with Avaya Session Border Controller Multi-Tenancy* | Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature. | Implementation engineers and administrators |
| *Working with Avaya Session Border Controller Geographic-Redundant Deployments* | Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature. | Implementation engineers and administrators |

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

# Finding documents on the Avaya Support website

### Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

# Accessing the port matrix document

### Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

# Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

**Important:**

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**Note:**

Some functionality is only available when you log in to the website. The available functionality depends on your role.

# Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

**Note:**

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

| Course code | Course title |
|---|---|
| 20600W | Avaya Session Border Controller 8.1 Technical Delta |
| 21098W | Session Border Controller 8.0 Technical Delta |
| 20660W | Administering the Avaya Session Border Controller for Enterprise - SIP Trunk |
| 60660W | Administering Avaya SBC Release 8 for Remote Worker |
| 20660T | Administering Avaya SBC Release 8 Test |
| 20800C | Implementing and Supporting Avaya SBC — Platform Independent |
| 20800T | Avaya SBC Platform Independent and Support Test |
| 20800V | Implementing and Supporting Avaya SBC — Platform Independent |
| 26160W | Avaya SBC Fundamentals |
| 7008T | Avaya SBC for Midmarket Solutions Implementation and Support Test |
| 7008W | Avaya SBC for Midmarket Solutions Implementation and Support |
| 2035W | Avaya Unified Communications Roadmap for Avaya Equinox Clients |
| 43000W | Selling Avaya Unified Communications Solutions |
| 71300 | Integrating Avaya Communication Applications |
| 72300 | Supporting Avaya Communication Applications |

# Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

**Note:**

Videos are not available for all products.

# Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Glossary

| | |
|---|---|
| **AAA** | Authentication, Authorization, and Accounting |
| **ARP** | Address Resolution Protocol |
| **Authentication Tag (AT)** | The Secure Real-Time Transport Protocol (SRTP) field that carries message authentication data. |
| **CA** | Certificate Authority |
| **CDR** | Call Detail Record |
| **Certificate (Digital)** | A digital certificate is akin to an electronic "credit card" that establishes a client's credentials and authenticity when establishing a communication session and is issued by a certification authority (CA). It contains various information used for encrypting messages and digital signatures. In addition, the certificate contains the digital signature of the certificate-issuing authority so that it can be verified as being real. Some digital certificates conform to a standard, such X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. See also "Certificate Authority (CA)". |
| **Certificate Authority (CA)** | The CA is a trusted body that confirms the validity and identity of entities involved in public key exchange. As a user's digital certificate is the only means by which entities may trust each other, the CA must be a legitimate, regulated, and officially recognized entity. An example of a well known CA that is used by many commercial organizations, is Verisign. |
| **Certificate Signing Request (CSR)** | In a Public Key Infrastructure (PKI) systems, a CSR is a message sent from an applicant to a certificate authority to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information. |

| | |
|---|---|
| | If the request is successful, the certificate authority will send back an identity certificate that has been digitally signed with the private key of the certificate authority. |
| **CIDR** | Classless Inter-Domain Routing |
| **CLI** | Command Line Interface |
| **Client Authentication** | Refers to the process of authenticating a client identity by using the client certificate (in TLS). |
| **Codec** | Coder/Decoder |
| **CRL** | Certificate Revocation List |
| **CSR** | Certificate Signing Request |
| **CTI** | Computer Telephony Integration or Computer-Telephone Integration |
| **Day Zero Attack** | See Zero-Day Attack. |
| **DDoS** | Distributed Denial-of-Service |
| **Demilitarized Zone (DMZ)** | A computer network-related term that refers to the “neutral zone” between an enterprise’s private network and outside public network. Typically, a computer host or small network is inserted into this neutral zone to prevent outside users from getting direct access to the internal network. |
| **Denial-of-Service (DoS)** | The objective or end-result of certain types of malicious attacks or other activities against a network, where access to network services, resources, or endpoints is prohibited. |
| **DH** | Diffie-Hellman |
| **Diffie-Hellman (D-H) Key Exchange** | The process in which “session keys” are distributed between parties that have no prior knowledge of each other across an unsecure public network. This involves setting-up a secure tunnel using Public Key Encryption (PKE), through which session keys are passed. |
| **DiffServ** | Differentiated Services |
| **Digest Authentication (DA)** | A Hypertext Transport Protocol (HTTP) authentication scheme whereby user passwords are encrypted prior to being sent across the Internet, thus certifying the integrity of the Uniform Resource Locator (URL) data. The downside of DA is that although passwords are encrypted, the data being exchanged is not; it is sent in the clear. |
| **Directory Harvest Attack (DHA)** | DHA is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a SPAM database. |

| | |
|---|---|
| | A directory harvest attack can use either of two methods for harvesting valid e-mail addresses. The first method uses a brute force approach to send a message to all possible alphanumeric combinations that could be used for the username part of an e-mail address at the server. The second and more selective method involves sending a message to the most likely user names - for example, for all possible combinations of first initials followed by common surnames. In either case, the e-mail server generally returns a Not found reply message for all messages sent to a nonexistent address, but does not return a message for those sent to valid addresses. The DHA program creates a database of all the e-mail addresses at the server that were not returned during the attack.<br>This explains how a new e-mail address can start receiving spam within days or hours after its creation. |
| **Distributed Denial-of-Service (DDoS)** | A more sophisticated type of DoS attack where a common vulnerability is exploited to first penetrate widely dispersed systems or individual end-points, and then use those systems to launch a coordinated attack. Much more difficult to detect than simple DoS attacks. |
| **DMZ** | Demilitarized Zone |
| **DoS** | Denial-of-Service |
| **DoW** | Day-of-Week |
| **DSCP** | Differentiated Services Code Point |
| **EAP** | Extensible Authentication Protocol |
| **Eavesdropping** | The unauthorized interception and monitoring of voice packets or media streams. |
| **EMS** | Element Management System |
| **Encapsulating Security Payload (ESP)** | The ESP header normally forms part of an extension to the IP header, and is denoted in the IP type field by the value 50. The header itself is used to indicate the SPI Security Parameter Index (SPI) value that has been employed which, in turn, is associated to the key and algorithm that has been used to encrypt the IP payload. Only those entities privy to the Security Association (SA) have the mapping between the SPI and the key, consequently they are the only users who can decrypt the data. The ESP protocol is defined in RFC 2406. |
| **ENUM** | E Number Working Group or Electronic Numbering |
| **ESP** | Encrypted Security Payload |
| **False negative** | A malicious message that is erroneously treated as a legitimate message. |

| | |
|---|---|
| **False positive** | A legitimate message that is erroneously treated as a malicious message. |
| **FCAPS** | Faults, Configuration, Accounting, Performance, and Security |
| **FQDN** | Fully-Qualified Domain Name |
| **FW** | Firewall |
| **GARP** | Gratuitous Address Resolution Protocol |
| **Global Cluster** | Two or more nodes of a SBCAE functional element, such as Signaling or Intelligence. |
| **Global Node** | One logical SBCAE functional entity (Signaling or Intelligence) that is deployed in a network. |
| **GUI** | Graphical User Interface |
| **HA** | High-Availability or Harvest Attack |
| **High-Availability** | The Avaya SBC feature that allows two Avaya SBC security devices to be deployed as an integral pair, wherein one of the devices functions as the Primary and the other as an Alternate or Standby. Connected by a heartbeat signal and shared database, the two Avaya SBC security devices provide failover protection in the event one of the devices malfunctions. |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTP** | Hypertext Transfer Protocol |
| **ICMP** | Internet Control Message Protocol |
| **ICMP** | Internet Control Message Protocol |
| **IM** | Instant Messaging |
| **Internet Protocol Security (IPSec)** | IPSec is a general framework of open standards which provide for the integrity, confidentiality, and authentication of data exchanged between two peers. |
| **Intrusion** | A malicious user or process deliberately masquerading as a legitimate user or process. |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Protection System |
| **ITSP** | Internet Telephony Service Provider |

| | |
|---|---|
| **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”.<br><br>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.<br><br>See also “Diffie-Hellman (D-H) Key Exchange” and “Rivest, Shamir, & Adleman (RSA)”. |
| **LAN** | Local Area Network |
| **Latency** | The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination. |
| **LDAP** | Lightweight Directory Access Protocol |
| **MAC** | Message Authentication Code |
| **MAD** | Media Anomaly Detection |
| **Man-in-the-Middle Attack (MIM)** | A type of network security attack wherein an attacker takes control of an established communications session and masquerades as one of the participating end points. In this type of attack, the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them. (See also “public key infrastructure”). |
| **Master Key Identifier (MKI)** | That field of the Secure Real-Time Transport Protocol (SRTP) that identifies the master key from which the session keys were derived that authenticate and / or encrypt a particular packet. The MKI can also be |

| | |
|---|---|
| | used by key management to re-key and to identify a particular master key with the cryptographic text. |
| **MCD** | Machine Call Detection |
| **MD5** | Message Digest 5 |
| **Media Release** | See “Anti-tromboning”. See also “Tromboning”. |
| **Message Integrity** | The ability to ensure that the message that was received is same as the message that was sent. |
| **MIB** | Management Information Base |
| **MIME** | Multipurpose Internet Mail Extension |
| **MKI** | Master Key Identifier |
| **Mobile Extension (MOBX)** | An extension assigned to a mobile user on a Mobile Service Provider (MSP). |
| **MSA** | Message Sequence Analysis |
| **Multipurpose Internet Mail Extension (MIME)** | A technical standard that describes the transmission of non-text data (or data that cannot be represented in plain ASCII code). It is often used in email to deal with foreign language text as well as for audio and video data. MIME is defined in Request For Comments (RFC) 2045. |
| **MWI** | Message Waiting Indicator |
| **Naming Authority Pointer (NAPTR)** | A type of Domain Name Service (DNS) record that supports regular expression (regex)-based rewriting. See *Regular Expression (Regex).* |
| **NAT** | Network Address Translation |
| **Network Address Translation (NAT) Device** | A “barrier” device placed between two networks that translates an IP address used in one network to a different address known within the other network. One of these networks is designated the inside network (for example, an enterprise LAN) and the other is the outside network (for example, the Internet). Users on the inside network can “see” the outside network, but the outside can’t see the inside users, as all communication with the outside network is through the NAT device. |
| **Nonce** | A parameter that varies with time. A nonce can be a time stamp, a visit counter on a web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file.<br><br>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.<br><br>In SSL / TLS, a nonce is a 32-bit timestamp and a 28-byte random field that is used during key exchange to prevent replay attacks. |
| **NSAP** | Network Service Access Point |
| **NTP** | Network Time Protocol |
| **P-Asserted-ID** | A private extension used in the Session Initiation Protocol (SIP). The P-asserted-id is a Sip header field that contains a SIP Uniform resource Identifier (URI) and an optional display name such as:<br><br>`"Joe Brown" <sip:topengr@avaya.com>`<br><br>A SIP proxy server can insert a P-asserted-id header into a message and forward it to another trusted proxy. However, if the user requests that this information be kept private, then the SIP proxy must remove this field prior to forwarding it to an untrusted proxy. |
| **Packet Spoofing** | Impersonating a legitimate user transmitting data. |
| **PAP** | Protected Authentication Protocol |
| **Passphrase** | A sequence of words or other text used to control access to a protected network or system, program, or data. A passphrase is similar to a password, but generally longer and with more restrictions for added security. Passphrases are often used to control both access to and operation of cryptographic programs and systems. Passphrases are particularly application to systems that use the passphrase as an encryption key. |
| **PKI** | Public Key Infrastructure |
| **POP** | Point-of-Presence or Post Office Protocol |
| **Port Scanning** | A method used by individuals to break into a network to see which assets or services they can hi-jack for their own use or sabotage to limit their use by someone else.<br><br>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.<br><br>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.<br><br>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).<br><br>Root certificates are implicitly trusted. They are included with many software applications. The best known is Web browsers; they are used for SSL/TLS secure connections. However this implies that you trust your browser's publisher to include correct root certificates, and in turn the |

| | |
|---|---|
| | certificate authorities it trusts and anyone to whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates. This (transitive) trust in a root certificate is merely assumed in the usual case, there being no way in practice to better ground it, but is integral to the X.509 certificate chain model. |
| **RSA** | Rivest, Shamir & Adleman |
| **RTCP** | Real-Time Transport Control Protocol |
| **RTP** | Real-Time Transport Protocol |
| **SBC** | Session Border Controller |
| **SDP** | Session Description Protocol |
| **Secure Sockets Layer (SSL)** | SSL is a commonly-used method for managing the security of a message transmitted via the Internet and is included as part of most browsers and Web server products. Originally developed by Netscape, SSL gained the support of various influential Internet client/server developers and became the de facto standard until evolving into Transport Layer Security (TLS).<br><br>The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer (where a “socket” is an endpoint in a connection). SSL uses the Rivest, Shamir, and Adleman (RSA) public-and-private key encryption system, which also includes the use of a digital certificate. Avaya SBC supports certificates with 2048-bit or 4096-bit keys.<br><br>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.<br><br>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.<br>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).<br><br>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.<br><br>Although TLS is based on Netscape's SSL 3.0 protocol, the two are not interoperable. See “Secure Sockets Layer (SSL)”. |
| **Tunneling** | A security method used to ensure that data packets traversing an unsecure public network do so in a secure manner that prevents disruption or tampering. |
| **TURN** | Traversal Using Relay NAT |
| **UDP** | User Datagram Protocol |
| **URI** | Uniform Resource Identifier |
| **URL** | Uniform Resource Locator |
| **Virus** | A program that replicates itself by being copied or initiating its copying to another program, operating system, or document. Viruses are transmitted in many ways, such as in attachments to e-mails, as part of downloadable files, or be present on diskettes or CDs. |

| | |
|---|---|
| | Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances or events cause their code to be executed by the unsuspecting host. |
| **VLAN** | Virtual LAN |
| **VM** | Voice Mail |
| **VoIP** | Voice-over-Internet Protocol |
| **VPN** | Virtual Private Network |
| **XML** | Extensible Markup Language |
| **Zero-Day Attack** | A particular type of exploit that takes advantage of a security vulnerability in a network on the same day that the vulnerability itself becomes generally known. Ordinarily, since the vulnerability isn't known in advance, there is oftentimes no way to guard against an exploit or attack until it happens. |
| **Zombie** | An IP network element that has been surreptitiously taken over by an attacker, usually without the user's knowledge. |

# Index

## M



## O



## P



## R



## S



## T



## U



## V



## W