Avaya WebRTC Snap-in Reference

Release 3.6
Issue 1
December 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya

including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes Avaya WebRTC Snap-in characteristics and capabilities, including overview and feature descriptions, interoperability, and performance specifications. The document also provides instructions on how to deploy, configure, and troubleshoot Avaya WebRTC Snap-in.

This document is intended for people who need to install, configure, and administer the Avaya WebRTC Snap-in. This document contains specific information about this snap-in. For an overview of Avaya Breeze® platform, see the *Avaya Breeze® platform Overview and Specification*. For information on how to install, configure, and test an Avaya Breeze® platform snap-in, see *Administering Avaya Breeze® platform*.

Chapter 2: WebRTC Snap-in overview

Avaya WebRTC Snap-in supports the establishment of secure calls from web browsers to endpoints to which Avaya Aura® can deliver calls. For example, users can directly call contact centers from web browsers. You can also use WebRTC Snap-in to enable click-to-call from internal enterprise websites, such as corporate directories and help desks.

The snap-in supports a separate web application to control the user experience, the identity presented for the caller, and authentication and authorization of calls. The web application also sends contextual data about calls, which can be leveraged by Avaya Breeze® platform snap-ins, Engagement Designer, Experience Portal, contact center applications, and contact center agents.

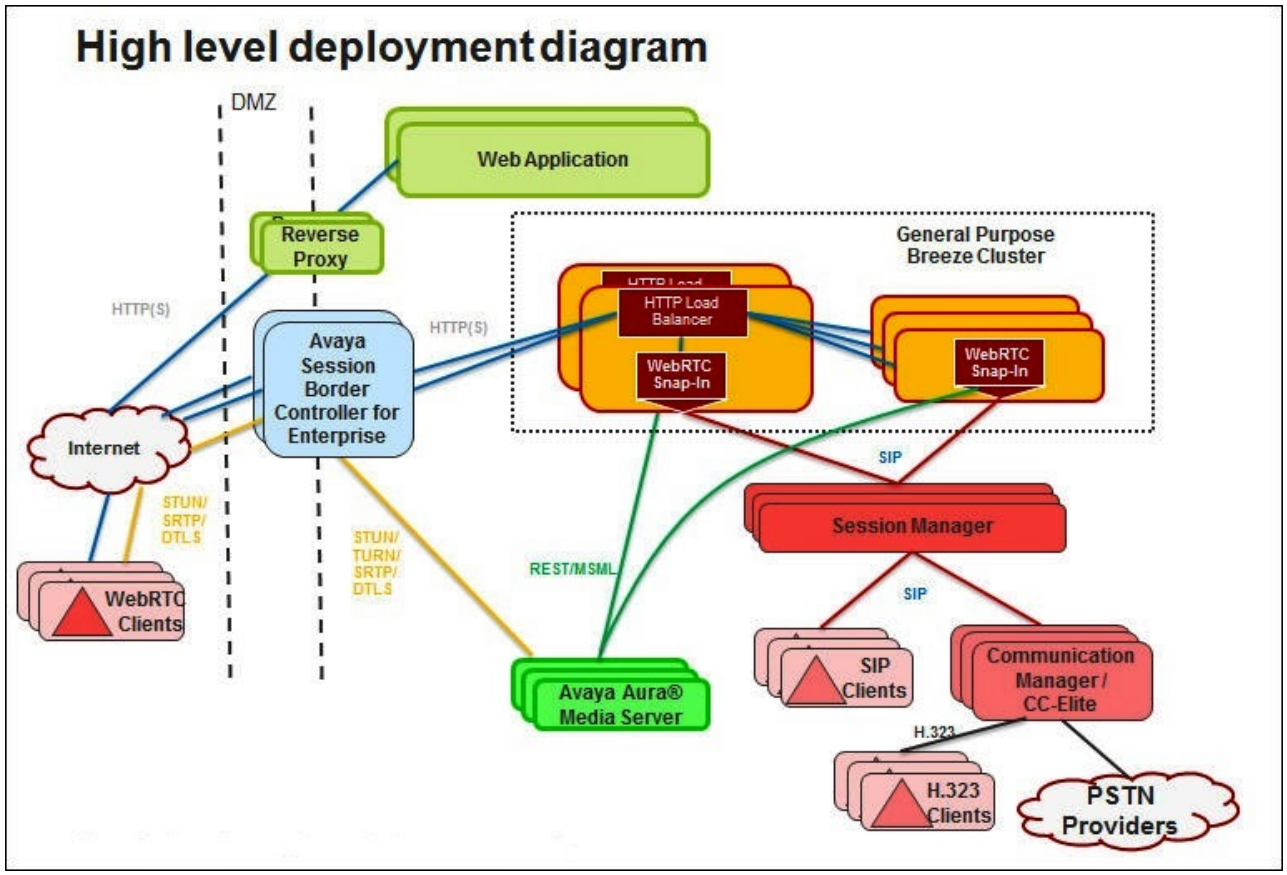
WebRTC Snap-in must be purchased separately from Avaya Breeze® platform and requires its own license.

Example

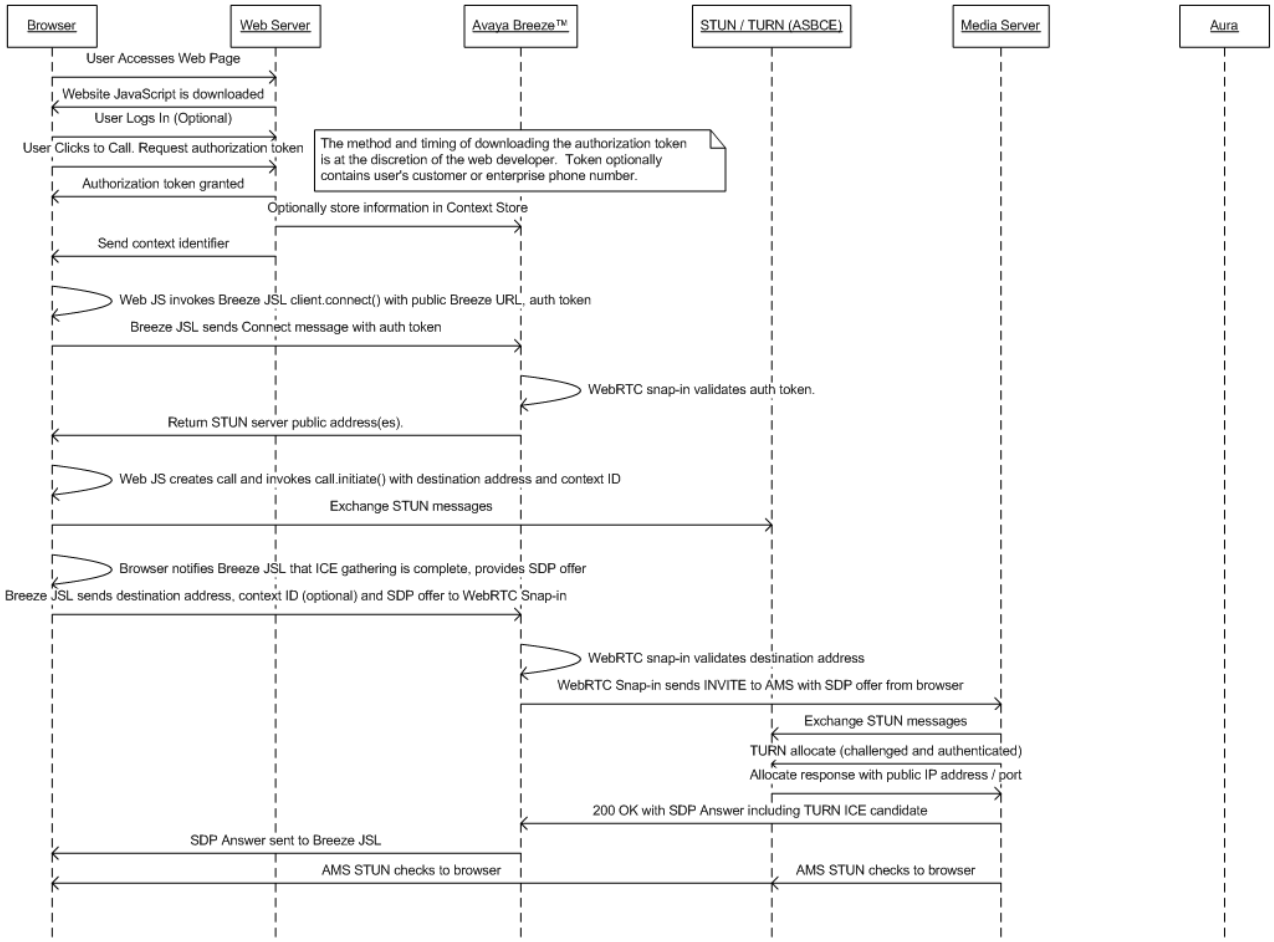
A customer is filling out a loan application on a bank website. The customer runs into a problem with which they need help, so they click the click-to-call button on the website and is connected with a bank representative through the web browser.

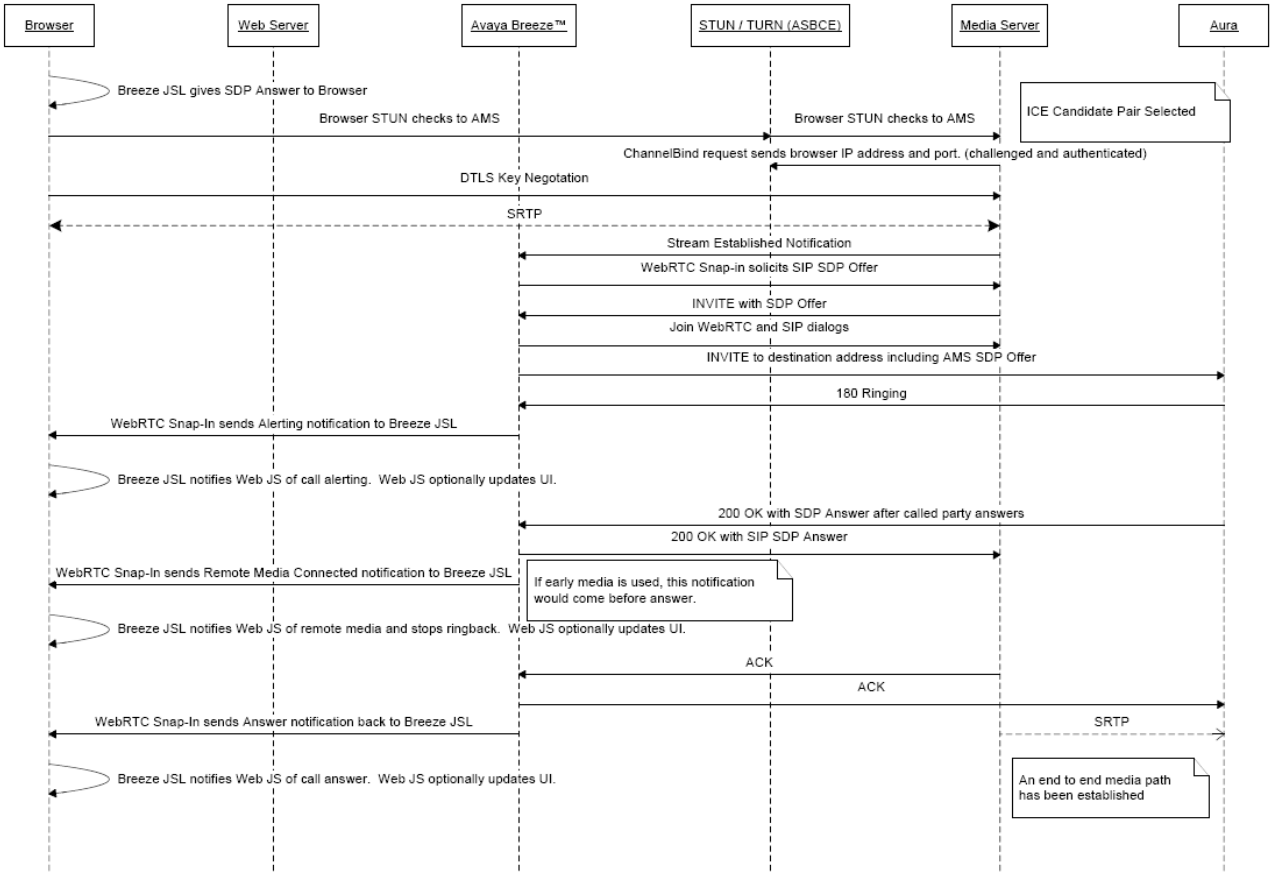
Instead of having to go through the typical IVR self-service, the call is routed to a relevant agent immediately. The data about the customer and the loan application that they filling is sent with the call, so the bank representative is familiar with the customer’s information. WebRTC Snap-in also sends the customer’s phone number with the call, so they get the same treatment as if they called from that phone.

WebRTC Snap-in topology



WebRTC call sequence





WebRTC Snap-in security

WebRTC Snap-in supports the authentication and authorization of calls, which includes the capability to assert the phone number of a calling user and restrict the numbers that can be called.

Avaya SBCE uses the industry-standard TURN protocol. Avaya SBCE supports the secure firewall traversal of HTTP and SRTP packets, facilitates sending DTLS to provide secured key exchange for SRTP flows, and processes all security requirements in the TURN protocol.

You can also use existing reverse proxies or Application Delivery Controller for HTTP signaling between web browsers and Avaya Breeze® platform.

WebRTC Snap-in API and SDK

The simple WebRTC Snap-in API does not require developers to be familiar with ICE, STUN, TURN, and SDP. The WebRTC Snap-in solution contains an SDK that provides the required resources, Javadoc on Javascript libraries, and sample applications.

The web application needs the SDK to invoke the functions provided by runtime snap-in capabilities on Avaya Breeze® platform. The SDK provides functions for WebRTC-enabled browsers to work with Avaya WebRTC Snap-in. You can download the SDK from the Avaya DevConnect website.

Related links

Downloading the WebRTC Snap-in SDK on page 12

WebRTC Snap-in high availability

Avaya Breeze® platform platform configurations with multi-node clusters support automatic establishment of new WebRTC calls when Avaya Breeze® platform instances fail. Voice calls continue during Avaya Breeze® platform failures, but messages to disconnect, hold, or unhold calls are not processed.

If Avaya Aura® Media Server instances fail, all calls processed by the server are disconnected.

Avaya Aura® Session Manager, Avaya SBCE, and Avaya Aura® Communication Manager have their own high availability strategies.

WebRTC Snap-in interface terms

The WebRTC Snap-in interface terms might be different from the terms used in other protocols, such as SIP and H.323. This table maps the WebRTC Snap-in terms with similar terms used in SIP and H.323.

WebRTC Snap-in	SIP	H.323
user	From P-Asserted-Identity	Calling
destinationaddress	To Request-URI	Called
contextid	UUI	UUI

Downloading the WebRTC Snap-in SDK

About this task

You must be a registered member of Avaya DevConnect to download the SDK. User registration on Avaya DevConnect is free.

Avaya WebRTC Snap-in supports applications built with the Release 3.2 SDK, but you must update the applications to the latest SDK release to use the latest functions that the snap-in supports.

Procedure

1. Go to www.avaya.com/devconnect.

   You can also go to www.avaya.com/BreezeDeveloper and download the WebRTC Snap-in SDK.
2. Log in to the Avaya DevConnect site.
3. Click **Downloads** > **All Downloads**.
4. In **Start**, type `WebRTC Snap-in`, and select **WebRTC Snap-in** from the drop-down list.
5. In **Filters**, select the WebRTC Snap-in release.
6. Download the relevant SDK version.

Related links

WebRTC Snap-in API and SDK on page 11

Chapter 3: Interoperability

Product requirements

Avaya WebRTC Snap-in supports applications built with earlier versions of the JavaScript libraries. The applications work without modifications, but you must update the applications to use the latest SDK version. The latest version gives you access to the latest features and functions of the snap-in.

Avaya WebRTC Snap-in needs the following products:

- Avaya Breeze® platform Release 3.5
- Avaya Aura® System Manager Release 7.1.2
- Avaya Aura® Media Server Release 7.8
- Avaya Aura® Communication Manager Release 6.3.5 or later
- Avaya Session Border Controller for Enterprise Release 6.3 or later

  Avaya SBCE requires separate Advanced and Standard licenses from the license pool for each concurrent session.

For the latest and most accurate compatibility information, go to https://support.avaya.com.

Web browsers supported

- Mozilla Firefox Release 59 and later
- Google Chrome Release 62 and later

Note:

WebRTC Snap-in does not support mobile devices.

Chapter 4: Snap-in licensing

Avaya Breeze® platform snap-ins must be purchased separately from Avaya. The snap-ins are not included with Avaya Breeze® platform. Each licensed snap-in requires its own license. You must activate and download the license from Avaya PLDS and install the license on WebLM servers, such as System Manager WebLM.

A license supports the current release and all previous releases of snap-ins. For every major release of a snap-in, the snap-in requires a new license. Different releases of the snap-in might be in different license modes.

Avaya provides a 30–day grace period from the time a license error is first detected. When the error is detected, the snap-in enters license error mode and a major alarm is raised but the snap-in remains fully functional. The grace period provides enough time to fix the error before the snap-in stops working. You can view the license mode of the snap-in on the Avaya Breeze® platform Service Management page in System Manager. The license modes are:

- Normal: No license error is detected. Indicated by a green check mark on the Service Management page.
- Error: There is a license error, but the snap-in continues to operate normally. Indicated by a yellow caution icon on the Service Management page. The Service Management page also shows the date when the 30-day grace period expires. Avaya Breeze® platform raises a major alarm when the snap-in enters license error mode.
- Restricted: There is a license error, and the 30–day grace period has expired. Indicated by a red cross mark on the Service Management page. The snap-in is automatically removed. Avaya Breeze® platform raises a critical alarm when the snap-in enters license restricted mode. To correct this problem, you might need to get a license file or update the license to the new major release.

WebRTC Snap-in licensing

WebRTC Snap-in is licensed as a small, medium or large gateway and is a Designated System (DS) license type.

Material code	Description	Notes
308442	WEBRTC R3 VOICE GATEWAY SMALL PACKAGE LIC S	<2000 BHCC per Avaya Breeze® platform cluster.
308443	WEBRTC R3 VOICE GATEWAY MEDIUM PACKAGE LIC S	2000-5000 BHCC per Avaya Breeze® platform cluster
308444	WEBRTC R3 VOICE GATEWAY LARGE PACKAGE LIC S	>5000 BHCC per Avaya Breeze® platform cluster

Chapter 5: WebRTC Snap-in deployment

Configuration information worksheet

Information	Details	Data for reference during configuration
Provisioned URL to WebRTC Snap-in	The URL for the WebRTC Snap-in web application. • If only web browsers located within the enterprise network firewall can gain access to the web application, the URL must be the Avaya Breeze® platform cluster address for WebRTC Snap-in. • If web browsers are located outside the enterprise network, the URL must be the address of the reverse proxy or Avaya SBCE. The following is a sample URL: https://myAvayaBreezeCluster.example.com/services/WebRTC/WebRtcServlet	
Encryption key used to encrypt the authorization token	The key used to encrypt the authorization token when a web application is being developed. This field is part of the WebRTC Snap-in attribute configuration.	
Anonymous URI	The phone number or URI that is used when there are no assertions from web applications. The Anonymous URI domain must match the far-end domain in the Communication Managersignaling group that has a SIP trunk between Communication Manager and Session Manager. The default value is Anonymous@anonymous.invalid.	
STUN server address	The following IP address and port based on the enterprise network: • If you use Avaya SBCE, the Avaya SBCE IP addresses and port. • If web browsers are located outside the enterprise network, the external IP address. • If web browsers are located within the enterprise network, the private IP address.	

Table continues…

Information	Details	Data for reference during configuration
	• If there are web browsers that are located outside and within the enterprise network, the external IP address. The enterprise network must be connected to the external IP address of Avaya SBCE. The format of the IP addresses and ports that you enter must be address:port. Use comma (,) as a delimiter. The default STUN port is 3478. The default port must be accessible in the firewall. **Note:** Avaya SBCE configured as a TURN/STUN server does not support NAT servers for WebRTC. To mitigate this lack of support for NAT servers, the external interface of Avaya SBCE must be configured with a public IP address. The TURN server relay address must be configured on the external interface of Avaya SBCE, which is connected to the external firewall of the enterprise DMZ. The external firewall provides Layer 3 security to the TURN relay address. The enterprise gateway must be configured to send all data packets through the external firewall of DMZ. These data packets reach the Avaya SBCE external interface which is visible to public networks. WebRTC Snap-in does not support hiding the external interface IP address of Avaya SBCE from public networks.	

SIP-based components must use the same transport protocol throughout enterprise networks. SIP entity links that are involved in WebRTC Snap-in call flows cannot use both TCP and TLS.

For example, if the SIP entity link between Session Manager and Communication Manager uses TLS, the SIP entity links between the following components must also use TLS:

- Session Manager and Avaya Breeze® platform
- Session Manager and Avaya SBCE
- Session Manager and Avaya Aura® Media Server

Installing the license file in WebLM of System Manager

Before you begin

Download the snap-in license file from PLDS.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install License**.
3. On the Install License page, do the following:
   a. Browse to the location of the snap-in license file.
   b. Select the license file and click **Open**.
   c. Click **Accept the License Terms & Conditions**.
   d. Click **Install**.

      System Manager installs the license file.
4. In the navigation pane, click **Licensed Products** to view the installed license.

Loading the snap-in

About this task

This task describes how to load a snap-in to System Manager from your development environment or alternate location. You can skip this step when installing a pre-loaded snap-in. Pre-loaded snap-ins are provided with the Avaya Breeze® platform Element Manager in System Manager. However, you can skip this step only if the pre-loaded snap-ins are not removed from System Manager by the administrator. If the pre-loaded snap-ins are removed, the administrator needs to reload the snap-in.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Click **LOAD**.

   You can load multiple snap-ins at a time.
3. On the Load Service page, depending on the browser used, click **Browse** or **Choose File**, and browse to your snap-in file location.

   Note:

   You can select up to 50 files or a maximum of 3 GB files whichever limit is reached first.
4. Browse and select the snap-in (`.svar`) file required, and then click **Open**.

A snap-in file ends with `.svar`. For a snap-in that Avaya provides, the `.svar` file must be downloaded from PLDS.

5. On the Load Service page, click **LOAD**.
6. On the Accept End User License Agreement page, click **Accept** to accept the agreement.

   When the snap-in is loaded, the **Service Management** > **Services** page displays the **State** of the snap-in as **Loaded**.

   The system displays all the `.svar` files that you loaded in the All Services table on the **Service Management** > **Services** page.

Installing the snap-in

About this task

Use this task to install the snap-in to specific clusters.

Note:

For `.svar` files larger than 50 MB, schedule the snap-in installation during a maintenance window.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the snap-in that you want to install.
3. Click **Install**.
4. Select the clusters on which you want to install the snap-in, and click **Commit**.
5. To see the status of the snap-in installation, click **Refresh**.

   ***Installed** with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform servers in the cluster. * **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

6. To track the progress of a snap-in installation, on the Server Administration page, click **Service Install Status** for an Avaya Breeze® platform server.

   The Service Status page displays the installation status of all the snap-ins installed on that server.

7. **(Optional)** To designate a snap-in as the preferred version, do the following:

   a. Verify that the snap-in is in the installed state for the targeted clusters by opening the System Manager web console, and clicking **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

b. From the **All Services** list, select the version of the snap-in you want to mark as Preferred.

c. Click **Set Preferred Version**.

d. Select the clusters for which you want this to be the preferred version, and click **Commit**.

WebRTC Snap-in configuration

Checklist for configuring WebRTC Snap-in

No.	Task	Link	✔
1	Configure the WebRTC Snap-in attributes.	Configuring the WebRTC Snap-in attributes on page 20	
2	If there are multiple Avaya Breeze® platform servers, configure load balancing.	Configuring load balancing for WebRTC Snap-in on page 21	
3	Configure the WebRTC Snap-in HTTP security.	Configuring the HTTP security for WebRTC Snap-in on page 21	

Configuring the WebRTC Snap-in attributes

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. Click one of the following tabs:
   - Service Clusters
   - Service Globals
3. Do one of the following:
   - If you selected the Service Clusters tab, from the **Cluster** drop-down list, select the cluster.
   - If you selected the Service Globals tab, from the **Service** drop-down list, select **WebRTC**.
4. Do the following to configure the attributes:
   a. Select the **Override Default** check box of the attribute.
   b. Configure the attribute with a new value.

5. Click **Commit**.

Configuring load balancing for WebRTC Snap-in

About this task

Configure load balancing if there are multiple Avaya Breeze® platform servers.

Before you begin

- Configure the WebRTC Snap-in attributes.
- Change the state of the cluster for load balancing to Deny New Service.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the cluster, and click **Edit**.
3. Select the following check boxes:
   - **Is load balancer enabled**
   - **Is session affinity enabled**
4. Click **Commit**.

Configuring the HTTP security for WebRTC Snap-in

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **HTTP Security**.
2. Click the HTTP CORS tab.
3. **(Optional)** Select **Allow Cross-origin Resource Sharing for all** only to enable HTTP CORS in test environments.
4. Add the host address of web applications that use WebRTC Snap-in.
5. Click **Commit**.

WebRTC Snap-in field descriptions

DEFAULT_GROUP field descriptions

Name	Description
Anonymous URI	The phone number or URI that is used when there are no assertions from web applications.

Table continues…

Name	Description
	The Anonymous URI domain must match the far-end domain in the Communication Managersignaling group that has a SIP trunk between Communication Manager and Session Manager. The default value is Anonymous@anonymous.invalid.
Authorization	The option to enable or disable the authorization and authentication of calls. The default value is **true**. When **Authorization** is set to **true**, the client must create the authorization token.
Avaya Signed	The trust status indicates and whether WebRTC Snap-in is Avaya-signed. The WebRTC Snap-in is always Avaya-signed and you cannot change the value from **Yes**.
Maximum number of calls per session	The maximum calls that WebRTC Snap-in supports for client sessions between customer applications and WebRTC Snap-in. The default value is 10.
Maximum number of stored tokens	The maximum number of stored GUIDs of calls for security tokens. The number indicates maximum supported simultaneous security tokens or authorized calls. The default value is 1000.
Shared Secret	The string used to set the shared secret used for authentication. The shared secret attribute encrypts the authorization token.
STUN Servers	The following IP address and port based on the enterprise network: • If you use Avaya SBCE, the Avaya SBCE IP addresses and port. • If web browsers are located outside the enterprise network, the external IP address. • If web browsers are located within the enterprise network, the private IP address. • If there are web browsers that are located outside and within the enterprise network, the external IP address. The enterprise network must be connected to the external IP address of Avaya SBCE.

Table continues…

Name	Description
	The format of the IP addresses and ports that you enter must be address:port. Use comma (,) as a delimiter. The default STUN port is 3478. The default port must be accessible in the firewall. **Note:** Avaya SBCE configured as a TURN/STUN server does not support NAT servers for WebRTC. To mitigate this lack of support for NAT servers, the external interface of Avaya SBCE must be configured with a public IP address. The TURN server relay address must be configured on the external interface of Avaya SBCE, which is connected to the external firewall of the enterprise DMZ. The external firewall provides Layer 3 security to the TURN relay address. The enterprise gateway must be configured to send all data packets through the external firewall of DMZ. These data packets reach the Avaya SBCE external interface which is visible to public networks. WebRTC Snap-in does not support hiding the external interface IP address of Avaya SBCE from public networks.
Supplier Id	The unique identity of the supplier of snap-ins. All the snap-ins from a supplier have identical supplier IDs. The default supplier ID of WebRTC Snap-in is 10000000. WebRTC Snap-in is an Avaya snap-in, and you cannot change the supplier ID of the snap-in.
TRUST_STATUS	The trust status of WebRTC Snap-in . WebRTC Snap-in is always trusted and you cannot change the value from **Trusted**.

License Features field descriptions

Name	Description
FEAT_WRTC_EXPIRATION	The option to enable or disable the WebRTC Snap-in license grace period expiration feature. The license file populates the value in **FEAT_WRTC_EXPIRATION**. The status of the

Table continues…

Name	Description
	expiration feature is always active, and you cannot change the value.
FEAT_WRTC_VOICE_GATEWAY	The option to enable or disable the WebRTC Snap-in gateway activation feature. The license file populates the value in **FEAT_WRTC_VOICE_GATEWAY**. The status of the expiration feature is always active, and you cannot change the value.
VALUE_WRTC_MODE	The WebRTC Snap-in mode. The options are: • **Production**: Allows simultaneous calls using the WebRTC Snap-in. This is the default value. • **Trial**: Allows only one call at a time using WebRTC Snap-in without purchasing the snap-in.

Related links

Configuration information worksheet on page 16
Configuring the Avaya SBCE TURN/STUN service for WebRTC Snap-in on page 25

Avaya SBCE configuration

Checklist for configuring Avaya SBCE for WebRTC Snap-in

No.	Task	Link	✔
1	Configure the Avaya SBCE TURN/STUN service.	Configuring the Avaya SBCE TURN/STUN service for WebRTC Snap-in on page 25	
2	Configure the Avaya SBCE reverse proxy service.	Configuring the Avaya SBCE reverse proxy service for WebRTC Snap-in on page 27	
3	Configure the Avaya SBCE HTTP port range.	Configuring the Avaya SBCE HTTP port range for WebRTC Snap-in on page 29	
4	Restart all Avaya SBCE instances.	Restarting an Avaya SBCE application on page 30	

Configuring the Avaya SBCE TURN/STUN service for WebRTC Snap-in

About this task

Avaya SBCE configured as a TURN/STUN server does not support NAT servers for WebRTC. To mitigate this lack of support for NAT servers, the external interface of Avaya SBCE must be configured with a public IP address.

The TURN server relay address must be configured on the external interface of Avaya SBCE, which is connected to the external firewall of the enterprise DMZ. The external firewall provides Layer 3 security to the TURN relay address.

The enterprise gateway must be configured to send all data packets through the external firewall of DMZ. These data packets reach the Avaya SBCE external interface, which is visible to public networks.

WebRTC Snap-in does not support hiding the external interface IP address of Avaya SBCE from public networks.

Before you begin

Install and configure WebRTC Snap-in.

Procedure

1. Log in to Avaya SBCE.
2. In left navigation pane, click **Device Specific Settings** > **TURN/STUN Service**

   Avaya SBCE displays the TURN STUN Configuration tab.
3. Click **Edit Configuration Parameters**, and configure the following fields:
   - **Listen Port**: Configure port 3478.
   - **Media Relay Port Range**
   - **Authentication**: Select the check box.
   - **UserName**
   - **Realm**
   - **FingerPrint**: Select the check box.
   - **UDP**: Select the check box.
   - **UDP Relay**: Select the check box.
   - **TCP**: Do not select the check box.
   - **TCP Relay**: Do not select the check box.
   - **TLS**: Do not select the check box.
   - **DTLS**: Do not select the check box.
4. Click **Finish**.

5. Click **Add Listen/Relay IP Pair**, and configure the listen and media relay IP addresses for the public and private interfaces.

   Configure a:

   - Public IP address for the B1 interface as the media relay IP address.
   - Private IP address on the A1 interface for the listen IP address.

   Avaya SBCE supports multiple public and private interface pairs, so the interfaces could also be B2 and A2.

6. Click **Finish**.

TURN STUN Configuration field descriptions

Name	Description
Listen Port	The default listen port is 3478.
Media Relay Port Range	The port range used for SRTP and STUN packets exchanged between the web browser and Avaya Aura® Media Server. The default port range is 50000 – 55000. The port range must not overlap port ranges that Avaya SBCE uses for other protocols, such as SIP.
Authentication	The user name and password of the must match the TURN STUN server credentials configured on Avaya Aura® Media Server.
UserName	The TURN STUN server user name and password configured on Avaya Aura® Media Server.
Realm	The realm used in the TURN authentication. Usually, the realm is the same as the SIP domain of Avaya Aura®.
FingerPrint	The option to enable FingerPrint.
UDP	The option to enable UDP. If you change the transport protocol from UDP to TCP, the WebRTC service is affected. For any change in the transport protocol, you must restart the application.
UDP Relay	The option to enable the UDP relay.
TCP	The option to enable TCP. If you change the transport protocol from TCP to UDP, the WebRTC service is affected. For any change in the transport protocol, you must restart the application.

Table continues…

Name	Description
TCPRelay	The option to enable TCP relay.
TLS	The option to enable TLS.
DTLS	The option to enable DTLS.

Configuring the Avaya SBCE reverse proxy service for WebRTC Snap-in

Procedure

1. Log in to Avaya SBCE.
2. In left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**

   Avaya SBCE displays the Relay Services page.
3. In the Reverse Proxy tab, click **Add**.

   Avaya SBCE displays the Add Reverse Proxy Profile page.
4. Configure the following fields:
   - **Service Name**
   - **Enabled**: Select the check box to enable the profile.
   - **Listen IP**
   - **Listen Port**
   - **Listen Protocol**
   - **Listen TLS Profile**
   - **Server Protocol**
   - **Server TLS Profile**
   - **Connect IP**
   - **Load Balancing Algorithm**: Select **None**.
   - **PPM Mapping Profile**: Select **None**.
   - **Allow Web Sockets**: Clear the check box.
   - **Whitelisted IPs**: Do not configure this field.
   - **Server Addresses & Ports**
5. Click **Next**.
6. Click **Finish**.

Next steps

Configure the Avaya SBCE HTTP port range.

Add Reverse Proxy Profile field descriptions

Name	Description
Service Name	The reverse proxy profile name.
Enabled	The check box to enable the reverse proxy service.
Listen IP	The external IP address and network name. The listen IP address is the URL that the web browser uses to connect to Avaya Breeze® platform. The listen IP address is usually configured for the B1 interface.
Listen Port	The listen port for HTTP or HTTPS is a unique port relative to the other reverse proxy configuration for the port. It is better if the listen port is the same as the server port, but this is not required. If you use: • HTTP, the listen port and the server port must be 80. • HTTPS, the listen port and the server port must be 443. These specific ports based on the protocol used are used to gain access to the customer-developed Avaya Breeze® platform service, WebRTCSampleApplication, and the WebRTC service. Web browsers use the listen port to connect to the services on Avaya Breeze® platform. If a non-standard port is used, the port must be specified in the WebRTC Snap-in URL that the web application uses.
Listen Protocol	The protocol that the listen port uses to gain access to the customer-developed Avaya Breeze® platform service, WebRTCSampleApplication, and the WebRTC service. The options are: • HTTP • HTTPS
Listen TLS Profile	The option to select the TLS profile based on the protocol used: • For HTTP, the TLS profile must be *None*. This is the default option.

Table continues…

Name	Description
	• For HTTPS, the TLS profile must be *AvayaSBCServer*.
Server Protocol	The protocol that Avaya SBCE uses: The options are: • HTTP • HTTPS
Server TLS Profile	The option to select the TLS profile based on the protocol used: • For HTTP, the TLS profile must be *None*. This is the default option. • For HTTPS, the TLS profile must be *AvayaSBCClient*.
Connect IP	The network name and IP address that Avaya SBCE uses to communicate with WebRTC Snap-in. The connect IP address is usually configured for the A1 interface.
Load Balancing Algorithm	The algorithm used for load balancing. The options are: • Round-Robin • IP Hashing • Least # of Connections • None
PPM Mapping Profile	The PPM Mapping profile.
Allow Web Sockets	The option to enable web sockets.
Whitelisted IPs	The list of whitelisted IP addresses. You can specify maximum five IP addreses.
Server Addresses & Ports	The Avaya Breeze® platform server IP address and port. The port must be 80 or 443.

Configuring the Avaya SBCE HTTP port range for WebRTC Snap-in

About this task

The HTTP port range must be more than four times the supported maximum number of simultaneous calls.

For example, to support 1000 simultaneous calls the port range should be minimum 5000 to 9000 ports.

Procedure

1. Log in to Avaya SBCE.
2. In left navigation pane, click **Device Specific Settings** > **Advanced Options** > **Port Ranges**

   Avaya SBCE displays the Port Ranges tab.
3. Configure **HTTP Port Range**.
4. Click **Save**.

Next steps

Restart all Avaya SBCE instances.

Restarting an Avaya SBCE application

Procedure

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

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click **Restart Application** corresponding to the Avaya SBCE security device that you want to restart.

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

Result

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

DMZ Firewall Open Port Requirements

For a complete list of ports utilized by Avaya Breeze® platform, see the Avaya Port Matrix Documents website.

Protocol	Port / Port Range	Description	Communicating Devices

Table continues…

UDP	3478	Listen Port setting on the SBC for TURN/STUN service	PC (external) <=> SBC (external-B1)
	50000 — 55000	Media Relay Port Range setting on the SBC	PC (external) <=> SBC (external-B1)
TCP	80	Required if HTTP is used for service access	PC (external) <=> SBC (external-B1)
			SBC (internal-A1) <=> Avaya Breeze® platform
TLS	443	Required if HTTPS is used for service access	PC (external) <=> SBC (external-B1)
			SBC (internal-A1) <=>Avaya Breeze® platform

Note:

The SBC Listen ports on B1 of the example can have any TCP port assigned for http or https. The open port firewall settings for external PCs reaching the SBC should match the SBC Reverse Proxy administration.

Configuring Avaya Aura® Media Server for WebRTC Snap-in

About this task

Configure multiple Avaya Aura® Media Server instances in the Avaya Breeze® platform cluster. The high availability configuration of Avaya Aura® Media Server is not available for WebRTC Snap-in.

When an Avaya Aura® Media Server instance fails, all WebRTC calls on the particular instance are disconnected, but the additional Avaya Aura® Media Server instances process new calls.

Before you begin

Configure:

- Avaya Aura® Media Server, including the nodes and routes, for Avaya Breeze® platform. For more information, see *Deploying Avaya Breeze® platform*.
- Avaya Session Border Controller for Enterprise for WebRTC Snap-in.

Procedure

1. Log in to the Avaya Aura® Media Server Element Manager.
2. Click **System Configuration** > **Server Profile** > **General Settings**.
3. Enable **Firewall NAT Tunneling Media Processor**, and click **Save**.
4. Click **System Configuration** > **Media Processing** > **ICE** > **TURN/STUN Servers** > **Accounts**.

5. Create a TURN/STUN account.

   The TURN/STUN account ID and password must match the account created on Avaya SBCE.

6. Click **System Configuration** > **Media Processing** > **ICE** > **TURN/STUN Servers** > **Servers**.
7. Add the TURN/STUN connection to the Avaya SBCE server.
8. **(Optional)** Click **System Configuration** > **Media Processing** > **ICE** > **General Settings**
9. **(Optional)** Verify that the correct codecs are enabled in Avaya Aura® Media Server.

   WebRTC Snap-in supports OPUS and G.711–ULAW.

10. **(Optional)** Click **System Configuration** > **Media Processing** > **ICE** > **General Settings**.
11. **(Optional)** Select the **Force Media Through a Configured TURN Server** checkbox, and click **Save**.

    Select the **Force Media Through a Configured TURN Server** option if most web browsers are located outside the corporate firewall. WebRTC Snap-in sends all UDP traffic through a trusted TURN server instead of sending the UDP traffic directly through the firewall using ICE.

12. Restart Avaya Aura® Media Server.
    a. Go to **System Status** > **Element Status**.
    b. Click **Restart** and then **Confirm**.

Related links

Avaya Aura Media Server TURN/STUN configuration on page 32

Avaya Aura® Media Server TURN/STUN configuration

Use the information in the following table to configure the TURN/STUN for Avaya Aura® Media Server **System Configuration** > **Media Processing** > **ICE** > **TURN/STUN Servers**

Field	Configuration information
Accounts	
Account Alias	Name that defines the TURN/STUN client configuration
User ID	The same TURN User ID that was configured for Avaya SBCE
Password	This is the TURN User password (the same as the one administered on Avaya SBCE)
Servers	

Table continues…

Field	Configuration information
Name	Enter a name for the Avaya SBCE TURN/STUN server
Description	Enter a description
Type	Choose **STUN and TURN**
Server Address	Internal address of the Avaya SBCE
Port	This is the same port as Avaya SBCE (The default value is 3478)
Protocol	Select UDP
Account Alias	This needs to match the Account Alias from the Accounts section above

Verifying the WebRTC Snap-in deployment

Procedure

1. Confirm that all of the corresponding fields have green check-marks on the Avaya Breeze® platform Service Management page.
2. Deploy, configure, and run the sample application that is included in the SDK. See: `Avaya-WebRTC-SDK > WebAppSample > documents > WebRTC Sample Application.pdf` for instructions.

Upgrading WebRTC Snap-in

About this task

Use this procedure to upgrade WebRTC Snap-in Release 3.0 or later. You can remove the older version of the snap-in after you upgrade to the latest version. Avaya Breeze® platform supports the installation of only one version of the snap-in in a server cluster.

You need to remove WebRTC Snap-in from all the server clusters during the upgrade, so upgrade the snap-in during a scheduled maintenance.

Before you begin

- Upgrade Avaya Breeze® platform. For more information, see *Upgrading Avaya Breeze® platform* at the Avaya Support website: https://support.avaya.com
- If you use HTTPS, do the following:
  - If the snap-in uses the WebRTC function, you must change the global-level or cluster-level attributes for the connection to the WebRTC server. Change the port number for the connection to the WebRTC server to 443.
  - If the connection to the WebRTC server establishes through SBC, configure SBC to use port 443.

Procedure

1. Verify that the older version of the WebRTC Snap-in is set as the preferred version on the Services page of the Avaya Breeze® platform element on the System Manager web console.
2. Install the new WebRTC Snap-in license file.
3. Load WebRTC Snap-in.
4. Install WebRTC Snap-in, and verify the installation.
5. Change the preferred version of WebRTC Snap-in to the upgraded version.
6. Verify that the activity counter of the older version of WebRTC Snap-in on the server cluster is 0.

   The activity counter might take a few minutes to reset to 0.
7. Remove the older version of WebRTC Snap-in from all server clusters.

Next steps

Delete the older version of WebRTC Snap-in.

Related links

Installing the license file in WebLM of System Manager on page 18
Loading the snap-in on page 18
Installing the snap-in on page 19

Chapter 6: Performance

Performance

The WebRTC Snap-in supports 1800 simultaneous calls at a rate of 28,000 BHCC in the following deployment model:

- 1 Avaya Breeze® platform server
- 1 Avaya Session Border Controller for Enterprise (Avaya SBCE) server
- 8 Avaya Aura® Media Servers

Chapter 7: Security

WebRTC Snap-in security summary

HTTP ingress into the enterprise network

HTTP messages either go through a third-party reverse proxy or through the Avaya SBCE reverse proxy function. This traffic might be challenged and authenticated by the third-party reverse proxy, but usually it is not. HTTP authentication at the enterprise edge would only be applicable for situations where enterprise users were accessing a website that they were using to initiate calls.

While the messages will not be authenticated, other standard reverse proxy policies will be applied.

Validation of the authorization token

The WebRTC Snap-in will validate the authorization token created and encrypted by the web server. If the snap-in can decrypt the token and ensure that the time stamp is valid, it determines that the incoming HTTP request is valid. The time stamp will usually be short lived; on the order of 5-10 seconds to protect against reply attacks. For more information, see the following document in the SDK: `Avaya-WebRTC-SDK > How to Create an Authorization Token.pdf`.

Avaya Aura® Media Server authentication with TURN server

The only authentication mechanism specified by the TURN specification is digest authentication. In the Avaya Breeze® platform WebRTC solution architecture, the client of the TURN server is not a browser, but the Avaya Aura® Media Server. A single user name and password will be provisioned in both the Avaya Aura® Media Server and Avaya SBCE TURN function for authentication. Use a suitably strong password.

RTP ingress to the enterprise network

With traditional SIP Border Controllers, the SBC was able to determine which UDP packets to allow into the enterprise because all SIP signaling also passed through the SBC. Any packets coming from an unknown source are discarded.

With WebRTC, on the other hand, there is no standard signaling protocol. Even if the signaling protocol was known, the HTTP-based signaling might not pass through the Avaya SBCE reverse proxy. Therefore, the TURN relay will have to have some other means of knowing which packets to accept. The ChannelBind TURN request is the key to this. After ICE candidate selection has completed and the Avaya Aura® Media Server is aware of the far end IP address / port, Avaya Aura® Media Server will issue a ChannelBind request to the TURN server including this information. The TURN server will only accept incoming UDP packets from:

1. An authenticated endpoint or
2. An address specified in a ChannelBind request from an authenticated endpoint.

There is a configuration option on Avaya Aura® Media Server that instructs it to only generate TURN candidates. This forces all UDP packets through the TURN server even if they could perhaps have traversed the firewall using hole-punching.

SRTP policy

The media stream between the browser and Avaya Aura® Media Server will always be encrypted using SRTP. If Avaya Breeze® platform and Avaya Aura® Media Server are properly configured, then the media stream between Avaya Aura® Media Server and Avaya Aura will be encrypted as well. Information about configuring Avaya Breeze® platform and Avaya Aura® Media Server can be found in *Deploying Avaya Breeze® platform*.

Chapter 8: Maintenance and Troubleshooting

Maintenance and troubleshooting

If WebRTC Snap-in calls do not work:

1. Check the HTTP/ HTTPS settings — HTTP OR HTTPS should be used throughout the WebRTC Snap-in configurations.
2. Check that the Avaya Aura® Media Server username and password setup is consistent with the Avaya SBCE settings for STUN/TURN access.
3. Check Avaya Aura® Media Server node, routes, and outbound proxy configuration. For details see *Deploying Avaya Breeze® platform*.
4. Check that the links between Avaya Breeze® platform and System Manager, and System Manager and Avaya Aura® Media Server are all either TLS or TCP.
5. Check the Avaya SBCE configuration again, using the steps in this document.
6. Check the HTTP Security settings in the *Configuring the WebRTC Snap-in* topic.
7. Check the cluster attribute setting for HTTP/HTTPS.
8. Check that the load balancing and session affinity options are selected on the cluster if there are multiple Avaya Breeze® platform nodes and you want to distribute the load.

If the WebRTC Snap-in application was written using the WebRTC Javascript API and still cannot make calls, check that the URL used to connect to WebRTC Snap-in is in the following format: `http://<ip address>/services/WebRTC/WebRtcServlet` or `https://<ipaddress>/services/WebRTC/WebRtcServlet` to access the snap-in. The `<ip address>` can be an Avaya Breeze® platform asset IP, or Avaya SBCE IP if there is an Avaya SBCE in the network. If there are issues getting calls to work through Avaya SBCE, use the Avaya Breeze® platform asset IP address to confirm that the configuration outside of the Avaya SBCE is correct.

See the sample application in the WebRTC SDK for details about using the Javascript library and how to connect to the WebRTC Snap-in.

Log files

The WebRTC Snap-in log files are stored here: `/var/log/Avaya/services/WebRTC`

Check the Avaya Aura® Media Server and Avaya SBCE documentation for details on log files pertaining to those products.

WebRTC calls with Avaya SBCE configured as a STUN server do not work

Cause

WebRTC calls might be configured to traverse through a NAT server.

Solution

1. Configure the TURN relay address on the external interface of Avaya SBCE.

   The external interface of Avaya SBCE must be configured to interact with the external firewall of the enterprise DMZ.

2. Configure the enterprise gateway router to send all data packets through the external firewall.

   The data packets reach Avaya SBCE through the external interface that is visible to public networks, which ensures successful establishment of WebRTC calls.

Chapter 9: Resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Description	Audience
Understanding		
Avaya Breeze® platform Overview and Specification	Describes tested Avaya Breeze® platform characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements.	• Customers • Sales engineers • Services and support personnel • System administrators
Implementing		
Deploying Avaya Breeze® platform	Describes the procedures to deploy and administer Avaya Breeze® platform.	• Services and support personnel • System administrators
Using		
Administering Avaya Breeze® platform	Provides the procedures to administer and configure Avaya Breeze® platform and snap-ins.	• Services and support personnel • System administrators
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Provides snap-in troubleshooting procedures. Answers questions such as “Why did my SDK installation fail?”	• Developers • System administrators • Services and Support personnel
Avaya Breeze® platform Snap-in Development Guide	Describes the key concepts needed to develop the different types Avaya Breeze® platform snap-ins.	• Developers • System administrators
Administering Avaya Session Border Controller for Enterprise	Provides procedures to administer and configure Avaya SBCE.	• System administrators • Services and Support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/.

Important:

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

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.

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

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

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Avaya DevConnect

Avaya DevConnect provides additional resources for Avaya Breeze® platform and Avaya WebRTC Snap-in developers. You must register to gain access to DevConnect.

The basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos
- Webinar recordings
- Forums

The upgraded membership options offer developer-oriented technical support and other program services.

The DevConnect website at www.avaya.com/devconnect contains developer support for use of SDK, including documentation, videos, webinar recordings, tier 1 to 4 Enhanced Developer Support, as well as a developer forum.

Training

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

Course code	Course title
4128W	Avaya Breeze® platform Fundamentals
4310W	Real-time Communications Applications: Avaya Breeze® platform and Snap-ins (Part 1)

Avaya Breeze® platform videos

Avaya Breeze® platform provides the following videos to help in the development and deployment of snap-ins. Access these videos at http://www.avaya.com/breezedeveloper.

Title	Audience
Getting Started with the Avaya Breeze® platform SDK: Windows	Programmers
Getting Started with the Avaya Breeze® platform SDK: Linux	Programmers
Creating Your First Service — Part 1	Programmers
Creating Your First Service — Part 2	Programmers
Server Installation and Configuration with vCenter	System Administrators, Services and Support personnel
Server Installation and Configuration without vCenter	System Administrators, Services and Support personnel
Service Installation, Configuration, and Test	Programmers
Understanding the Hello Sample Service	Programmers
Understanding the Multi-Channel Broadcast Sample Service	Programmers
Understanding the Whitelist Sample Service	Programmers

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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

M

O

P

R

S

T

U

W