Avaya WebRTC Snap-in Reference

Release 3.2
Issue 1
October 2016

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see

the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

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™, see the *Avaya Breeze™ Overview and Specification*. For information on how to install, configure, and test an Avaya Breeze™ snap-in, see *Administering Avaya Breeze™*.

Change history

Issue	Date	Summary of changes
1	August 2015	Initial issue
2	December 2015	• Document supports Avaya WebRTC Snap-in release 3.1.1. • Revised for Avaya WebRTC Snap-in release 3.1.1 interoperability, particularly changes from release 3.1 for Avaya Breeze™ and System Manager product requirements.
3	May 2016	Rebrand for name change to Avaya Breeze™.
4	October 2016	• Document supports Avaya WebRTC Snap-in release 3.2. • Revised for Avaya WebRTC Snap-in release 3.2 interoperability and upgrading the WebRTC Snap-in 3.0 or 3.1 or 3.1.1 to WebRTC Snap-in 3.2. • Added “WebRTC Snap-in licensing” and “Avaya DevConnect” topics. • Updated the “Required configuration information worksheet” and “WebRTC Snap-in field descriptions” topics.

Chapter 2: WebRTC description

Avaya WebRTC Snap-in overview

Description

The Avaya WebRTC Snap-in enables users inside or outside the Enterprise to make a secure call from their web browser to any endpoint to which Avaya Aura® can deliver calls. For example, customers can call from a web browser directly into a Contact Center. The snap-in enables the separate web application to control: the user experience; identity presented for the caller; and authorized destination for the call. The web application can additionally convey context about the call that can be leveraged by Avaya Breeze™ snap-ins, Contact Center applications, and Contact Center Agents. The Avaya WebRTC Snap-in can also be used to simplify Enterprise operations by enabling click to call from an internal Enterprise website like a corporate directory or helpdesk. The Avaya WebRTC Snap-in is purchased separately from Avaya Breeze™ and requires its own license file. The Chrome and Firefox web browsers support WebRTC.

The web application must use the SDK that is available for download on the DevConnect website to invoke the functionality provided by the runtime snap-in capabilities that run on Avaya Breeze™. You require the functionality provided by the SDK for a WebRTC-enabled browser to work with the Avaya WebRTC Snap-in.

Architecture

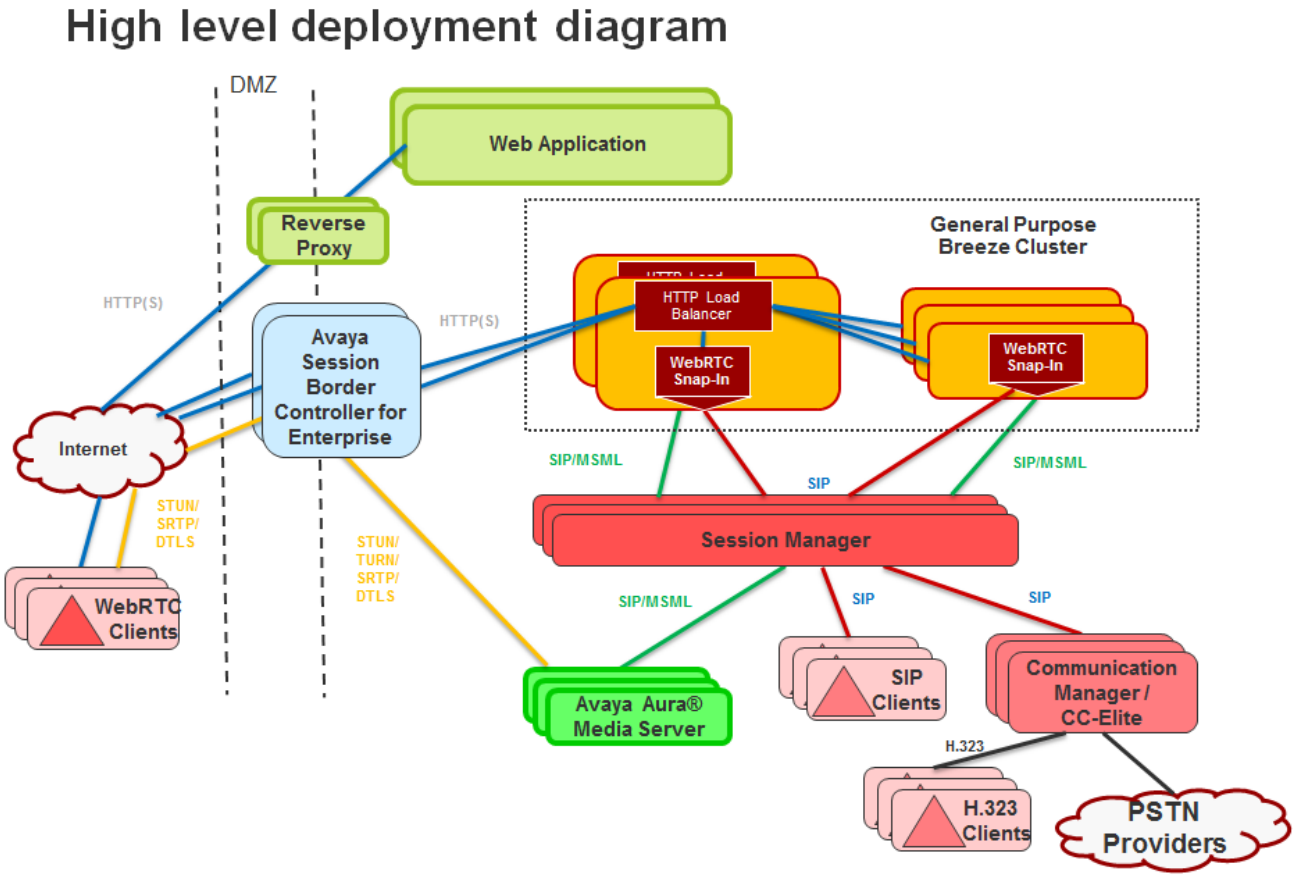
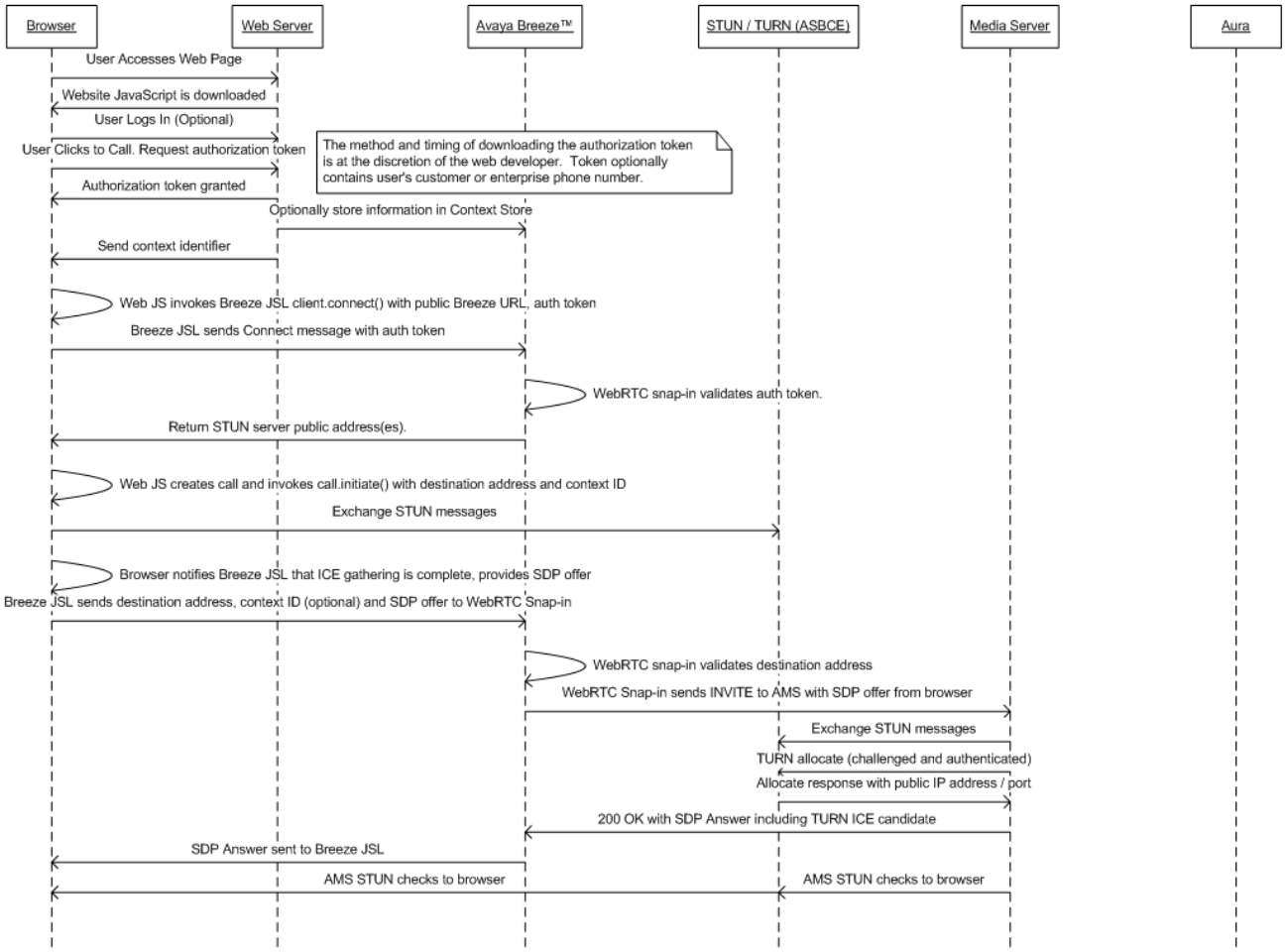
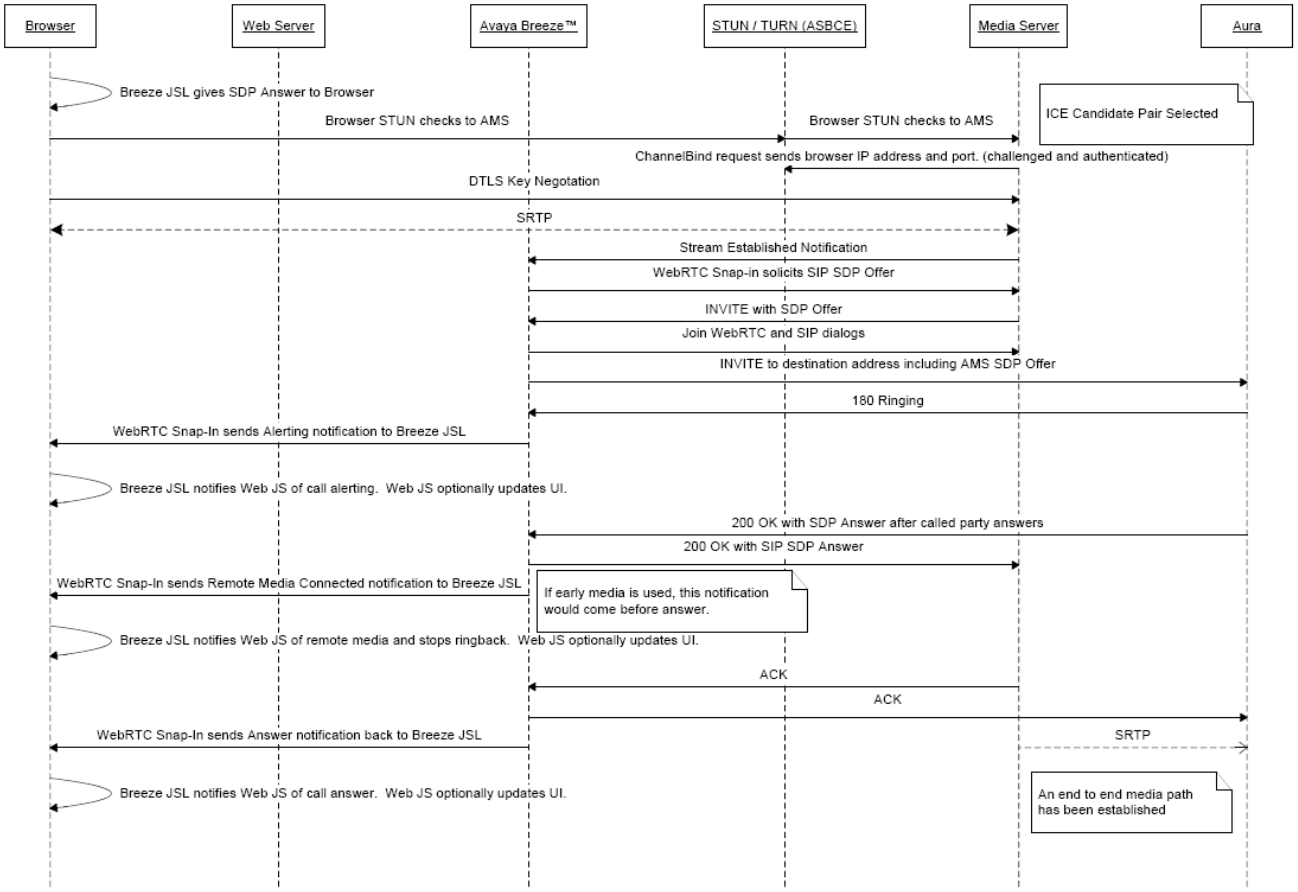


Figure 1: WebRTC architecture diagram

Sequence diagram for a WebRTC call





Features

Security

One of the primary differentiating features for the WebRTC Snap-in is that the web application handles authentication and authorization of calls. This includes the capability to assert a calling user's phone number and restrict the numbers that can be called. The Avaya SBCE enables secure firewall traversal for HTTP and SRTP packets, facilitates sending DTLS to provide secured key exchange for the SRTP flow, and takes care of all security requirements mentioned in the TURN protocol for the solution. Avaya SBCE uses the industry standard TURN protocol. In addition to Avaya SBCE, customers have the option to use an existing reverse proxy / Application Delivery Controller for HTTP signaling between the browser and Avaya Breeze™.

API/SDK

One of the benefits of the WebRTC Snap-in API is that it is simple and spares the web developer from needing to know the details of ICE, STUN, TURN, and SDP. As part of the WebRTC solution, there is an SDK available for download from the DevConnect website. The SDK provides all of the required resources and javadoc on Javascript library, as well as sample applications.

High Availability

In platform configurations with multinode clusters, new WebRTC calls are automatically established when an Avaya Breeze™ instance is lost. Voice calls will continue on a failure, however, a disconnect or hold/unhold message will not go through. Only the voice path will be preserved. If an Avaya Aura® Media Server is lost then all calls going through that server will be lost. Avaya Aura® Session Manager, Avaya SBCE, and Avaya Aura® Communication Manager have their own HA strategies.

Other Features

The WebRTC Solution makes it possible to store contextual data about calls and pass a reference to that data so it is available to Engagement Designer, Experience Portal, and Application Enablement Services applications.

WebRTC Snap-in example

The WebRTC Snap-in makes the following example interaction possible.

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 a button on the website and are connected with a bank representative through the browser. Instead of having to go through the typical IVR self-service, the call is routed to a relevant agent immediately. Data about the customer and the loan that they had been working on was sent with the call, so the bank representative is up to speed with the customer's information. The WebRTC Snap-in also sent the customer's phone number with the call, so they get the same treatment as if they called from that phone.

Downloading the WebRTC Snap-in SDK

Before you begin

You must register or be a member of Avaya DevConnect to download the SDK.

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. Click **Downloads**.
3. Search for the latest version of the Avaya WebRTC Snap-in SDK.

   For example, search for Avaya WebRTC Snap-in SDK, Release 3.2.

4. Download the applicable version.

Note:

You require a valid DevConnect ID and you must be logged on to the DevConnect site to download to WebRTC Snap-in SDK.

Chapter 3: Interoperability

Interoperability

Avaya product requirements

The Avaya WebRTC Snap-in release 3.2 requires the following:

- Avaya Breeze™ 3.2
- System Manager release 7.0 with the Service Pack integrated patch installed to update the Avaya Breeze™ Element Manager to release 3.2
- Avaya Aura® Media Server 7.7
- Avaya Aura® Communication Manager 6.3.5 or later
- Avaya Session Border Controller for Enterprise 6.3 or later

  Advanced and Standard Avaya SBCE licenses are required for each concurrent session.

Note:

For the latest and most accurate compatibility information, go to www.avaya.com/Support.

Supported Browsers

The Avaya WebRTC Snap-in supports the following browsers:

- Chrome 52 and above
- Firefox 47 and above

Chapter 4: Snap-in licensing

Some Avaya Breeze™ snap-ins are separately purchasable from Avaya. They are not included with Avaya Breeze™ . Each licensed snap-in, including this one, requires its own license file. Activate and download the file from PLDS and install it on System Manager WebLM.

A single license file supports the current version of the snap-in and all previous versions. For every major release of the snap-in, the snap-in requires a new license file. For this reason, different versions 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. This provides enough time to fix the error before the snap-in stops working. You can view the **license mode** for the snap-in on the Avaya Breeze™ **Service Management** page. 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™ 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 automatically uninstalls. Avaya Breeze™ raises a critical alarm when the snap-in enters license restricted mode. To correct this problem, you might need to get a license file if you don't have one, or update to a license file for 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.

Code	Description	Notes
308442	WEBRTC R3 VOICE GATEWAY SMALL PACKAGE LIC S	<2000 BHCC per Collaboration Environment Cluster.

Table continues…

Code	Description	Notes
308443	WEBRTC R3 VOICE GATEWAY MEDIUM PACKAGE LIC S	2000-5000 BHCC per Collaboration Environment Cluster
308444	WEBRTC R3 VOICE GATEWAY LARGE PACKAGE LIC S	>5000 BHCC per Collaboration Environment Cluster

Chapter 5: Deployment

Required configuration information worksheet

Information	Details	Your data (for reference during configuration)
Provisioned URL to WebRTC Snap-in	If the web application is only accessed by browsers inside the firewall, then provision the Avaya Breeze™ cluster address for WebRTC. If any of the browsers are external, then it is the address of the reverse proxy or the Avaya SBCE. Sample URL: https://myAvayaBreezeCluster.example.com/services/WebRTC/WebRtcServlet	
Encryption key used to encrypt the authorization token	Configure this attribute as part of the WebRTC snap-in attribute configuration. The value entered should be used to encrypt the authorization token when a web application is being developed.	
Anonymous URI	This is the phone number or URI used when none is asserted by the web application. The default value is "Anonymous@anonymous.invalid". The Anonymous URI domain needs to match the Far-end domain in the signaling group on Avaya Aura® Communication Manager. The signaling group should correspond to the SIP trunk administered on Avaya Aura® System Manager between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.	

Table continues…

Information	Details	Your data (for reference during configuration)
STUN server address	If the Avaya SBCE is in use, then populate one of the SBC IP addresses and port (3478) here. If all browsers are external, this is the public side, or external, IP address. If all browsers are internal, this is the private IP address. If there are both external and internal browsers, use the public side, or external, IP address. Make sure that the enterprise data network is configured to reach the public side, or external, IP address of the SBC. The STUN port 3478 should be reachable and opened in the firewall as well.	

Note:

SIP administration needs to use the same transport end to end. TCP and TLS on SIP entity links involved with the WebRTC Snap-in call flow cannot be combined when using this feature. For example, if the Session Manager to Communication Manager entity link is SIP/TLS, then the Session Manager to Avaya Breeze™ entity link, the Session Manager to Avaya SBCE entity link, and the Session Manager to Avaya Aura® Media Server entity link also need to be SIP/TLS.

Installing the license file

Before you begin

Download the snap-in license file from PLDS. For additional information about downloading a license file from PLDS, see *Deploying Avaya Breeze™*.

Procedure

1. On System Manager navigate to **Home** > **Services** > **Licenses**.
2. Select **Install License**.
3. Browse to the location of the snap-in license.
4. Select the license file and click **Open**.
5. Click **Accept the License Terms & Conditions** and click **Install**.

   The system installs the license file.

   In the left navigation pane, the system displays the snap-in under **Licensed Products**.

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™ 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 will need to reload the snap-ins.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the navigation pane, click **Service Management**.
3. Click **LOAD**.

   You can load multiple snap-ins at a time.
4. 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.
5. Browse and select the snap-in (`.svar`) file required, 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.

   The system displays all `.svar` files that you have selected in the service table on the Service Management page.
6. On the Load Service page, click **LOAD**.

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

Installing the snap-in

About this task

Use this task to install the snap-in to a specific cluster(s).

Note:

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

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze**.

2. In the left navigation pane, click **Service Management**.
3. Select the snap-in that you want to install.
4. Click **Install**.
5. Select the cluster(s) where you want the snap-in to reside, and click **Commit**.
6. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze™ 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.
7. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze™ server.

   The Service Status page displays the installation status of all the snap-ins installed on that server.
8. **(Optional)** Designate the Preferred Version.

   To designate a snap-in as the preferred version, you must administer the user profile.

   If you want to designate the snap-in as the preferred version, do the following:

   a. Verify that the snap-in is in the installed state for the targeted cluster(s) by opening the System Manager web console, and clicking **Elements** > **Avaya Breeze** > **Service Management**.
   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 cluster(s) for which you want this to be the preferred version, and click **Commit**.
   e. Modify the existing service profile or create a new service profile using the **Advanced** option next to the targeted snap-in.

Configuring the WebRTC Snap-in

Procedure

1. Configure the WebRTC Snap-in attributes.

   a. On System Manager, in **Elements** click **Avaya Breeze™** > **Configuration** > **Attributes**, and then click the Service Clusters or Service Globals tab.
   b. Select `WebRTC` from the **Service** drop-down menu. If attributes are being configured at the cluster level, select the cluster from the **Cluster** drop-down menu.
   c. Click the **override default** box for any attributes that need to be configured differently.

The Anonymous URI is one attribute that generally needs to be configured. The Anonymous URI domain should usually match the Far-end domain in the signaling group on Avaya Aura® Communication Manager.

Use the Shared Secret attribute to encrypt the authorization token.

d. Click **Commit** to save changes after all attributes have been configured.

2. Check the load balancer and session affinity boxes if you have multiple Avaya Breeze™ nodes and want the load to be distributed.
   a. On System Manager, in **Elements** click **Avaya Breeze™** > **Cluster Administration** and select the cluster.

      The cluster must be in the deny new service state before attempting to edit it.

   b. Click **Edit**.
   c. Check the boxes by **Is load balancer enabled** and **Is session affinity enabled**.
   d. Click **Commit**.
3. Configure the HTTP Security.
   a. On System Manager, in **Elements** click **Avaya Breeze™** > **Configuration** > **HTTP Security**.
   b. On the HTTP CORS tab, add the host address of each web application using the WebRTC Snap-in, and save the change by clicking **Commit**.

      Warning:

      Only select "Allow Cross-origin Resource Sharing for all” to enable HTTP CORS in test environments.

WebRTC Snap-in field descriptions

See “Required configuration information worksheet” for information that you require to reference while configuring the WebRTC Snap-in.

DEFAULT_GROUP field descriptions

Name	Description
Anonymous URI	This is the phone number or URI used when the web application does not assert any calling party identity. The Anonymous URI domain must match the Far-end domain in the signaling group on Avaya Aura® Communication Manager. The signaling group must correspond to the SIP trunk administered on Avaya Aura® System Manager between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Table continues…

Name	Description
	The default value is `Anonymous@anonymous.invalid`.
Authorization	This enables or disables 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	This specifies the trust status of the WebRTC Snap-in and whether the WebRTC Snap-in is Avaya signed. The WebRTC Snap-in is always Avaya signed and you cannot change the value of Yes.
Maximum number of calls per session	This specifies the maximum calls that the WebRTC Snap-in supports for a client session. The default value is 10.
Maximum number of stored tokens	This specifies the maximum number of stored GUIDs calls for security tokens The default value is 1000.
Shared Secret	This specifies the string used to set the shared secret used for authentication. The shared secret attribute encrypts the authorization token.
STUN Servers	If you are using Avaya SBCE, then specify the SBCE IP addresses and port in the **STUN Servers** field. If all browsers are external, this is the public side, or external, IP address. If all browsers are internal, this is the private IP address. If there are both external and internal browsers, use the public side, or external, IP address. Make sure that the enterprise data network is configured to reach the public side, or external, IP address of the SBCE. You must specify the IP address and port in the `address:port` format and use comma as the delimiter. The default STUN port is 3478 and this port must be reachable and opened in the firewall. For details about configuring Avaya SBCE, see “Configuring Avaya SBCE for the WebRTC Snap-in”.
Supplier Id	The Supplier id uniquely identifies the supplier of a particular snap-in offered through the Avaya Snapp-store. All the snap-ins from a given supplier have the same Supplier Id. The Supplier id is mandatory for

Table continues…

Name	Description
	the snap-ins offered through the Avaya Snapp-store and is optional for other snap-ins. **Note:** The WebRTC Snap-in is a Avaya provided snap-in and always has the Supplied Id value of 10000000. You cannot change this value.
TRUST_STATUS	This specifies the trust status of the WebRTC Snap-in . The WebRTC Snap-in is always Trusted and you cannot change this value.

License Features field descriptions

Name	Description
FEAT_WRTC_EXPIRATION	This enables or disables the WebRTC Snap-in license grace period expiration feature. **Note:** The value for the **FEAT_WRTC_EXPIRATION** field comes from the license file and is always on. You cannot change this value.
FEAT_WRTC_VOICE_GATEWAY	This enables or disables the WebRTC Snap-in gateway activation feature. **Note:** The value for the **FEAT_WRTC_VOICE_GATEWAY** field comes from the license file and is always on. You cannot change this value.
VALUE_WRTC_MODE	This specifies the WebRTC mode. You can choose one of the following values: • **Production**: Allows simultaneous calls using the WebRTC Snap-in. Production is the default value. • **Trail**: Allows only one call at a time using the WebRTC Snap-in.

Related links

Required configuration information worksheet on page 16
Configuring Avaya SBCE for the WebRTC Snap-in on page 23

Configuring Avaya SBCE for the WebRTC Snap-in

Before you begin

The Avaya Session Border Controller for Enterprise needs to be installed and working before making the following configuration changes specifically for the WebRTC Snap-in.

About this task

Perform the following administration tasks in Avaya SBCE for the WebRTC Snap-in. The TURN/STUN Service is configured first, followed by configuring the reverse proxy.

Procedure

1. Log in to Avaya SBCE and go to **Device Specific Settings** on the left menu.
2. Click **TURN/STUN Service**, and then click **Edit Configuration Parameters** to fill out the fields on the TURN STUN Configuration tab according to the following table:

Table 1: TURN/STUN configuration table

Parameter	Details
Listen Port	3478
Media Relay Port Range	This is the port range used for SRTP and STUN packets exchanged between the browser and Avaya Aura® Media Server. This range must not overlap port ranges used by the Avaya SBCE for other protocols such as SIP. The default range is 50000 – 55000.
Authentication	The User name and Password must match the credentials set up on the Avaya Aura® Media Server.
Realm	This is the realm used in TURN authentication. In most cases this matches the SIP domain that is in use in the Avaya Aura® system.
FingerPrint	Check the box.
UDP	Check the box.
UDP Relay	Check the box.
TCP	Box should remain unchecked.
TCP Relay	Box should remain unchecked.
TLS	Box should remain unchecked.
DTLS	Box should remain unchecked.

Note:

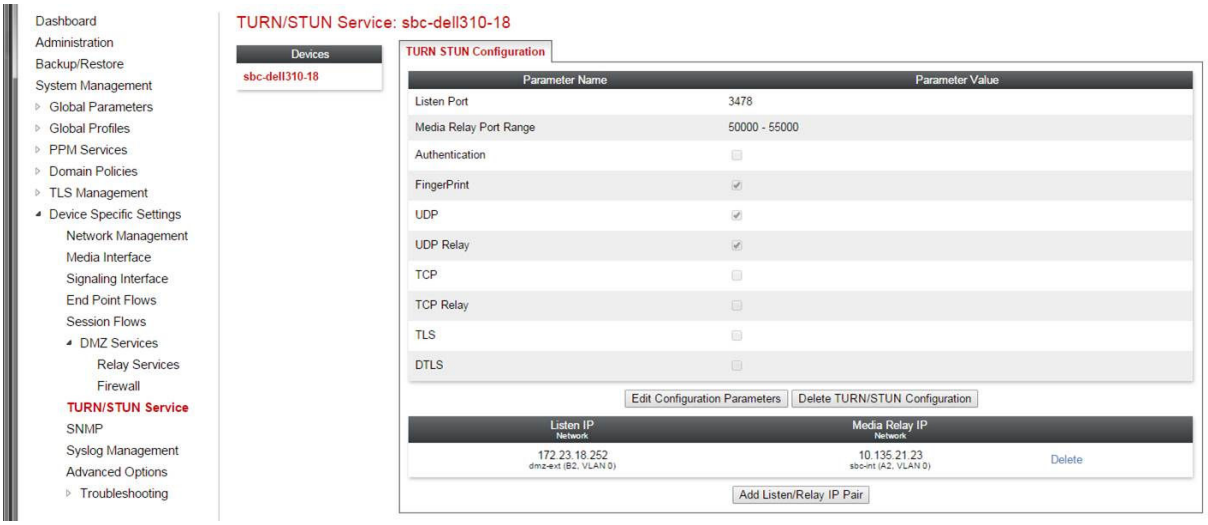
Avaya SBCE does not support NATting of WebRTC calls. The Turn relay address must be configured on the external interface of the Avaya SBCE. This address must be exposed on the external firewall of the DMZ. However, the external firewall must still provide layer 3 protection for the TURN relay address. The enterprise gateway router

must be configured to route any packet through the external firewall. The packets can be destined for the external address of Avaya SBCE that is visible to public network. The WebRTC Snap-in does not have a mechanism to hide the external interface address of the Avaya SBCE in the DMZ from the public network.

3. Click **Finish**.
4. Click **Add Listen/Relay IP Pair**.
5. Add the Listen/Relay IP Pair for the public and private interfaces and then click **Finish**.

   The recommended configuration is to have the Relay address as the Public side, or external, address on the B1 interface and the Listen address as the Private address on the A1 interface. However, Avaya SBCE supports additional interface pairs so it could be B2 and A2.

   The following example shows the Listen IP set to External SBC IP (B2) — 172.23.18.252. The Media Relay is set to Internal SBC IP (A2) — 10.135.21.23.



6. Go to **Device Specific Settings** > **DMZ Services** > **Relay Services** > **Reverse Proxy** and click **Add** to add the HTTP and HTTPS instances for the reverse proxy.

   The reverse proxy table should be filled out according to the desired target protocol (HTTP or HTTPS).

   - If HTTP is to be used, the Listen Port and the Server Port should be set to 80.
   - If HTTPS is to be used, the Listen Port and the Server Port should be set to 443.

   The Listen Port for HTTP or HTTPS can be any unique port relative to the other reverse proxy table entries for this same field. It is recommended that the Listen Port be the same as the Server Port, but it is not required.

   Note:

   HTTP configuration: Port 80 is used to access both the customer developed Avaya Breeze™ service / WebRTCSampleApplication and the WebRTC service.

HTTPS configuration: Port 443 is used to access the customer developed Avaya Breeze™ service / WebRTCSampleApplication and the WebRTC service.

Table 2: Add reverse proxy profile field descriptions

Field	Details
Service Name	Enter a meaningful name for the profile.
Enabled	Check the box to enable to profile.
Listen IP	This is the URL used by the external browser to connect to Avaya Breeze™, and is usually the B1 interface.
Listen Port	The port number can be any number. This is the port that will be used on the Outside PC browser to connect to the services on Avaya Breeze™. The port can be any unique listen port relative to the other reverse proxy table entries for this same field. If a non-standard port is used, this port must be specified in the Avaya Breeze™WebRTC Snap-in URL used by the Web Application.
Listen Protocol	Select HTTP or HTTPS.
Listen TLS Profile	For HTTP, default is None and the default should be kept. For HTTPS select `AvayaSBCServer`.
Server Protocol	Select HTTP or HTTPS.
Server TLS Profile	For HTTP, default is None and the default should be kept. For HTTPS select `AvayaSBCClient`.
Connect IP	This is the URL used to reach the WebRTC services on the inside, and is usually the A1 interface.
Load Balancing Algorithm	None is the default. Keep the default.
PPM Mapping Profile	None is the default. Keep the default.
Allow Web Sockets	Leave unchecked.
Whitelisted IPs	Leave blank.
Server Addresses & Ports	This is the Avaya Breeze™ Server IP and port. The port can be either 80, or 443.

7. Click **Next**. then click **Finish**.
8. Go to **Device Specific Settings** > **Advanced Options** > **Port Ranges** and configure the **HTTP Port Range**.

   The range should be more than four times the maximum number of simultaneous calls. For example, to support 1000 simultaneous calls the port range should be at least 5000–6000 ports.
9. Click **Save**.

10. Go to **System Management** > **Devices** and click **Restart Application** on each Avaya SBCE device to activate the changes.

Example

For this section the following IP examples are used:

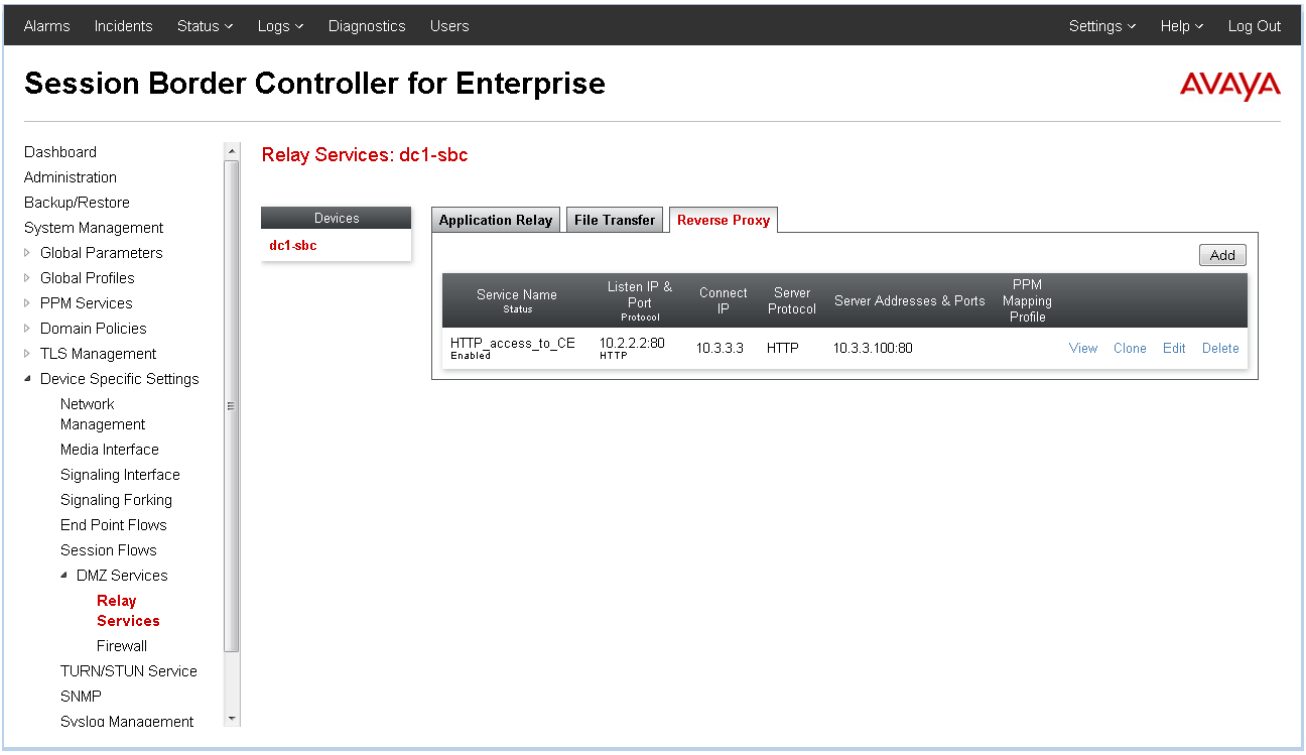
External Subnet = 10.2.2.0/24

- SBC External IP = 10.2.2.2

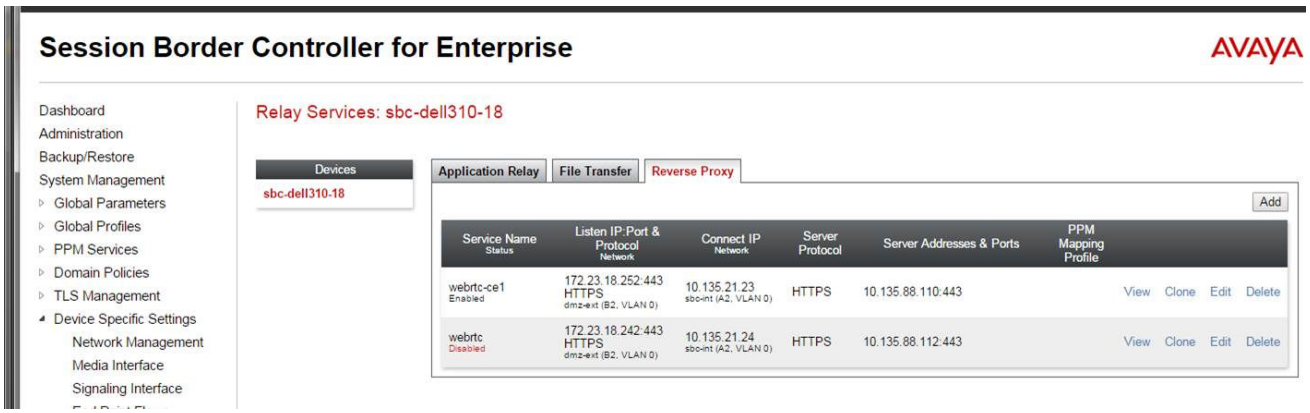
Internal Subnet = 10.3.3.0/24

- SBC Internal IP = 10.3.3.3
- Avaya Breeze™ Internal IP (Avaya Breeze™ security module IP) = 10.3.3.100

HTTP configuration



HTTPS configuration



DMZ Firewall Open Port Requirements

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

Protocol	Port / Port Range	Description	Communicating Devices
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™
TLS	443	Required if HTTPS is used for service access	PC (external) <=> SBC (external-B1)
			SBC (internal-A1) <=>Avaya Breeze™

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.

Provisioning Avaya Aura® Media Server for the WebRTC Snap-in

Before you begin

The Avaya Aura® Media Server needs to be set up to work with Avaya Breeze™ as described in *Deploying Avaya Breeze™* before making the following WebRTC Snap-in changes.

Also, the Avaya Session Border Controller for Enterprise needs to be set up and configured for use with the WebRTC Snap-in before doing these Avaya Aura® Media Server configuration steps.

About this task

Perform the following administration tasks in Avaya Aura® Media Server for the WebRTC Snap-in.

Procedure

1. Log in to the Avaya Aura® Media Server Element Manager.
2. Check that Avaya Aura® Media Server nodes and routes are set up correctly.

   See *Deploying Avaya Breeze™* for details on configuring Avaya Aura® Media Server for Avaya Breeze™.
3. Go to **System Configuration** > **Server Profile** > **General Settings**, enable **Firewall NAT Tunneling Media Processor** and then click **Save**.
4. Go to **System Configuration** > **Signaling Protocols** > **SIP** > **General Settings**, enable **Always use SIP default outbound proxy**, and then click **Save**.

   Note:

   SIP administration needs to use the same transport end to end. TCP and TLS on SIP entity links involved with the WebRTC call flow cannot be combined when using this feature. For example, if the Session Manager to Communication Manager entity link is SIP/TLS, then the Session Manager to Avaya Breeze™ entity link, the Session Manager to Avaya SBCE entity link, and the Session Manager to Avaya Aura® Media Server entity link also need to be SIP/TLS.
5. Go to **System Configuration** > **Media Processing** > **ICE** > **TURN/STUN Servers** > **Accounts** and create a TURN/STUN account. This account ID and password must match the account created on the Avaya SBCE.
6. Go to **System Configuration** > **Media Processing** > **ICE** > **TURN/STUN Servers** > **Servers** to add the TURN/STUN connection to the Avaya SBCE server.

   See “Avaya Aura® Media Server TURN/STUN configuration” for additional details.
7. (Optional) Go to **System Configuration** > **Media Processing** > **ICE** > **General Settings** and verify that the correct codecs are enabled in Avaya Aura® Media Server. The WebRTC Snap-in supports OPUS and G.711–ULAW.
8. (Optional) Go to **System Configuration** > **Media Processing** > **ICE** > **General Settings**, click the **Force Media Through a Configured TURN Server** checkbox and then click **Save**.

Select this option if most browsers are outside of the corporate firewall, and it is desirable to send all UDP traffic through a trusted TURN server rather than using ICE to cross the firewall directly.

9. 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 29

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	
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

Testing the WebRTC Snap-in deployment

Procedure

1. Confirm that all of the corresponding fields have green check-marks on the Avaya Breeze™ 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 the Avaya WebRTC Snap-in

About this task

Use this procedure to upgrade from WebRTC Snap-in 3.0 or 3.1 or 3.1.1 to WebRTC Snap-in 3.2.

Note:

Plan to do this upgrade during a maintenance window so the cluster or clusters can be off-loaded.

The upgrade procedure is different based on usage of HTTP/HTTPS.

Before you begin

You must upgrade Avaya Breeze™ to release 3.2 before upgrading to WebRTC Snap-in 3.2.

Procedure

1. If you are using HTTP, then follow these steps:
   a. Verify that the WebRTC Snap-in release 3.0 or 3.1 or 3.1.1 is set as the preferred version at **System Manager** > **Avaya Breeze™** > **Service Management**.
   b. Install the WebRTC Snap-in license file.
   c. Load the WebRTC Snap-in 3.2 snap-in.
   d. Install the WebRTC Snap-in 3.2 snap-in.
   e. Verify installation and then change the preferred version to WebRTC release 3.2.
   f. Verify that the activity counter for WebRTC 3.0 or 3.1 or 3.1.1 is 0 on this cluster.
   g. Uninstall the WebRTC Snap-in 3.0 or 3.1 or 3.1.1 snap-in from all clusters.
   h. Delete the WebRTC Snap-in 3.0 or 3.1 or 3.1.1 snap-in from System Manager.
2. If you are using HTTPS, perform the following additional steps while upgrading from WebRTC Snap-in 3.0 or 3.1 to WebRTC Snap-in 3.2.
   a. Depending on the snap-in using the WebRTC functionality, the global attribute or cluster attribute setting for connection back to the WebRTC Server URL needs to be modified for which you must change port 9443 to port 443. Also, if the connection is established using an SBC, you must provision SBC to use port 443 instead of port 9443.
   b. Install the WebRTC Snap-in license file.
   c. Load the WebRTC Snap-in 3.2 snap-in.
   d. Install the WebRTC Snap-in 3.2 snap-in.
   e. Verify installation and then change the preferred version to WebRTC release 3.2.

f. Verify that the activity counter for WebRTC 3.0 or 3.1 or 3.1.1 is 0 on this cluster.
g. Uninstall the WebRTC Snap-in 3.0 or 3.1 or 3.1.1 snap-in from all clusters.
h. Delete the WebRTC Snap-in 3.0 or 3.1 or 3.1.1 snap-in from System Manager.

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

Chapter 7: Security

WebRTC Snap-in security summary

Introduction

The following sections outline several key points about security policy use in the WebRTC Snap-in.

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 knows 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™ 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 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™ 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™ and Avaya Aura® Media Server can be found in *Deploying Avaya Breeze™*.

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™*.
4. Check that the links between Avaya Breeze™ 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™ 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™ 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™ 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.

Chapter 9: Resources

Documentation

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

Title	Description	Audience
Understanding		
Avaya Breeze™ Overview and Specification	Describes tested Avaya Breeze™ 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™	Describes the procedures to deploy and administer Avaya Breeze™.	• Services and support personnel • System administrators
Using		
Administering Avaya Breeze™	Provides the procedures to administer and configure Avaya Breeze™ and snap-ins.	• Services and support personnel • System administrators
Avaya Breeze™ 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™ Snap-in Development Guide	Describes the key concepts needed to develop the different types Avaya Breeze™ 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

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Avaya DevConnect

Avaya DevConnect provides additional resources for Avaya Breeze™ and Avaya WebRTC Snap-in developers.

You must register to access the DevConnect.

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

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

Use a browser to navigate to the www.avaya.com/devconnect contains developer support for use of the 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™ Fundamentals
4310W	Real-time Communications Applications: Avaya Breeze™ and Snap-ins (Part 1)

Support

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

Index

T

U

W