Avaya Co-Browsing Snap-in Reference

Release 3.8.1
Issue 3
November 2021

© 2015-2021, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License 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

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

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).

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction ... 8
Purpose ... 8
Change history ... 8
Chapter 2: Avaya Co-Browsing Overview ... 9
Avaya Co-Browsing Snap-in overview ... 9
Prerequisites for integration with customer website ... 9
Features ... 10
Customer-initiated co-browsing ... 10
Agent-initiated co-browsing ... 11
Data masking ... 11
Highlight text ... 11
IFrame support ... 12
Multiple end points / Context name ... 12
CSS3 support ... 12
Annotation ... 13
Data Marker ... 13
Agent Browser Refresh ... 14
Pseudo class element ... 14
AngularJS and ReactJS support ... 15
Multiple jQuery support ... 16
Serviceability feature for Oceana monitoring ... 16
RTL support ... 16
Chapter 3: Avaya Co-Browsing requirements and compatibility ... 17
Avaya product requirements ... 17
Accessing the Compatibility Matrix ... 17
Supported browsers and devices ... 18
Database requirements ... 18
Hardware requirements ... 18
Chapter 4: Licensing overview ... 20
License requirements ... 20
Configuring Avaya Co-Browsing Snap-in licenses ... 21
Chapter 5: Deployment overview ... 22
Avaya Co-Browsing Snap-in deployment process flow ... 22
Avaya Co-Browsing Snap-in deployment checklist ... 24
High availability ... 25
Avaya Co-Browsing Snap-in on a multi-node Avaya Breeze® platform cluster ... 25
Avaya Co-Browsing Snap-in on a single node Avaya Breeze® platform cluster ... 26
Creating an Avaya Co-Browsing Snap-in cluster ... 26
Installing Avaya Co-Browsing Snap-in ... 27

Loading Avaya Co-Browsing Snap-in.... 27
Creating JDBC providers and datasources.... 28
Configuring Intersystem Cache database.... 30
Configuring an Avaya Co-Browsing Snap-in user.... 30
Setting the Intersystem Cache password in System Manager.... 31
Configuring global attributes.... 32
Runtime service configuration attributes.... 32
Avaya Co-Browsing Snap-in database attributes.... 34
Omnichannel database configuration.... 36
Avaya Co-Browse feature attributes.... 37
Installing Avaya Co-Browsing Snap-in.... 37
Starting a service.... 38
Stopping a service.... 38
Verifying a Avaya Co-Browsing Snap-in deployment.... 39
Editing attributes for Avaya Co-Browsing Snap-in.... 39
Upgrading Avaya Co-Browsing Snap-in.... 40
Upgrade overview.... 40
Upgrading Avaya Co-Browsing Snap-in services.... 40
Setting the preferred version for upgrades.... 42
Uninstalling and deleting Avaya Co-Browsing Snap-in.... 42
Avaya Co-Browsing Snap-in uninstallation overview.... 42
Uninstalling Avaya Co-Browsing Snap-in.... 42
Deleting Avaya Co-Browsing Snap-in.... 43
Avaya Co-Browsing Snap-in server API endpoints.... 44
Chapter 6: Security overview.... 46
Selecting the Transport Layer Security version for a snap-in service.... 46
Certificate-based authentication overview.... 47
Data security.... 48
Port utilization.... 48
Data protection and data privacy support.... 48
Data Subject Rights management.... 49
Personal data retention.... 49
Data encryption.... 51
Consent Management for Processing and Storage of Personal Data.... 52
Chapter 7: Performance.... 54
Capacities and scalability.... 54
Chapter 8: Reports.... 55
Reports.... 55
Generating reports.... 55
Session Summary report.... 56
Agent Summary report.... 58
Customer Summary report.... 59
Viewing reports results.... 60

Chapter 9: Troubleshooting ... 62
Failed installation ... 62
Fails to run after database reboot ... 62
Alarms ... 63
Overview ... 63
Attribute value failed to initialize ... 63
Invalid value reported for attribute ... 64
Avaya Breeze® platform license service failed to initialize ... 64
Server unable to reach Cobrowse database ... 65
Unable to load localization property ... 65
Oceana Monitor service and CoBrowse service messages ... 66
Logging ... 67
Chapter 10: Resources ... 69
Localization ... 69
Documentation ... 69
Training ... 70
Viewing Avaya Mentor videos ... 74
Support ... 75
Appendix A: About sample reference client ... 76
Configuring files for agent JavaScript on Tomcat server ... 76
Configuring files for customer JavaScript on Tomcat server ... 77
Configuring files for reports on Tomcat server ... 78

Chapter 1: Introduction

Purpose

This document describes the characteristics, features, capabilities, and performance specifications of Avaya Co-Browsing Snap-in. If you have knowledge of JavaScript, jQuery, HTML, and Cascading Style Sheets (CSS), you can use this document to install, configure, administer, and integrate Avaya Co-Browsing Snap-in with the website for which you want to enable co-browsing.

Change history

Issue	Date	Summary of changes
3	November 2021	Minor updates throughout the document.
2	April 2021	Updated the “Supported browsers and devices” section.
1	April 2021	Initial release.

Chapter 2: Avaya Co-Browsing Overview

Avaya Co-Browsing Snap-in overview

Avaya Co-Browsing Snap-in provides a set of consolidated services for sharing a webpage content. Using Avaya Co-Browsing Snap-in, a customer and an agent can browse the same webpages to collaborate on certain tasks. The agent can assist the customer to perform various actions on the Avaya Co-Browsing Snap-in enabled webpages. For example, an agent can help a customer in navigating through the webpages and filling out forms. Using the snap-in, you can also generate summary reports about agents, sessions, and customers.

Avaya Co-Browsing Snap-in leverages the Document Object Model (DOM), which is an application programming interface (API) for valid HTML documents.

Avaya Co-Browsing Snap-in consists of the following components:

- Server: CoBrowse snap-in svar, which is installed on Avaya Breeze® platform. It provides REST Web Service API that is used by the co-browsing client SDK called Sharing Services.

  For more information about APIs, see the Programming guide for Sharing Services under Avaya Breeze® Client SDK at DevConnect.

- Client SDK or Sharing Services: CoBrowse JavaScript SDK to integrate with the website for which you want to enable co-browsing.

Note:

Only one concurrent co-browse session can take place between an agent and a customer.

Prerequisites for integration with customer website

Avaya Co-Browsing Snap-in integrates closely with a customer website by using the JavaScript Sharing Services component. To extend the co-browse functionality, you must:

1. Ensure that the customer website is functional.
2. Analyze the extent of customizations and technologies needed on the customer website to integrate with Co-Browsing Snap-in. Co-Browsing Snap-in is most suitable for integration with customer websites that are developed using JavaScripts, Angular, jQuery, and HTML 5.
3. Analyze the different elements from the customer website.

4. Interact with the customer web development and user experience team to understand how the customer website is developed and how it can be integrated with Co-Browsing Snap-in.
5. Analyze the webpages that support co-browsing and identify the navigation strategy between the co-browse-enabled pages and normal pages of the customer website.
6. Identify the secure fields or elements on the customer website that can be enabled for co-browsing.
7. Compare the namespace of the customer website or webpages with the co-browse namespace for any potential conflict.
8. Analyze the customer website JavaScript libraries for site-specific JavaScripts. In a co-browse session, some JavaScripts can cause unexpected functionality. Analyze the JavaScripts and take action accordingly to ensure that the co-browse session does not display unwarranted issues.

Important:

Co-Browsing Snap-in supports only HTTPs traffic.

Note:

- For more information on integrating with customer websites, see the Programming guide for Sharing Services under Avaya Breeze® client SDK at DevConnect.
- For more information on installing and configuring sample reference client, see the “Appendix A: About sample reference client” section of this document.

Features

Customer-initiated co-browsing

A customer can start a co-browsing session to request assistance from an agent. For the agent to join the session, the customer must share the system-generated session key, which is an 8-digit number with a space after four digits. For example, 1234 5678.

A customer initiated co-browsing session is a one step process. After the session key is generated, the customer automatically becomes a part of the session. Moreover, the session remains active even if the customer does not share the session key with the agent.

To get assistance during a session, the customer can give control of the co-browse enabled webpage to the agent. By default, the agent has view-only permissions for the webpage. However, the agent can request control of active co-browse session from the customer. The agent gets restricted access to the webpage despite getting the control. The customer can revoke the control from the agent, or the agent can voluntarily release the control at any time.

A session initiator can change the language setting of the session only at the beginning of the session from a list with the available values. The webpage does not display all the values in the list to the joining party. Also, the joining party cannot override this setting during an ongoing

session. If the initiator does not change the setting, the default setting from System Manager automatically gets selected.

- The user name of the customer cannot have more than 99 characters.
- The user name supports apostrophe (‘) as a charater in a customer username.

Agent-initiated co-browsing

An agent can start a co-browsing session to assist a customer. For the customer to join, the agent must share the system-generated session key, which is an 8-digit number with a space after four digits. For example, 1234 5678.

An agent-initiated co-browse session is a two step process. After a session key is generated, the agent does not automatically become a part of the session. An agent must use the key to join. The agent can also cancel a session even after generating a session key

Depending on the requirements of a session, an agent can request for control of the customer page to enter or change any field details. An agent can also cancel the control request sent to a customer anytime during a session.

The agent who is the session initiator can change the language setting of the session only at the beginning of the session from a list with the available values. If the initiator does not change the language setting, the default setting from System Manager gets selected by default.

The user name of an agent cannot have more than 99 characters.

Data masking

You can ensure data privacy and secure co-browsing by using security measures such as hiding sensitive information, preventing certain actions, and hiding certain elements. Depending on the legal and location-specific requirements, you can apply data masking to fields such as social security number or credit card number. You can also block certain actions so that agents do not submit any information on behalf of customers.

Note:

Ensure that the field that is masked for security cannot be edited by any other JavaScript events.

Highlight text

In a co-browsing session, a customer or an agent can highlight static text. You can enable and disable the highlight functionality and can also configure the highlight color. The highlighted text is visible to the both the initiator of the session and the co-browser when they are in control of the session. When the customer pauses the session, the highlight gets removed for the previous selected text and the customer cannot use the highlight feature during the pause state.

The highlighted effect disappears automatically when:

- The session control is passed on from the agent to the customer and vice versa.
- The agent or the customer clicks or double-clicks the mouse button.

Note:

Highlight text does not apply to elements such as text box, text area, or select box. The customer or the agent can highlight the text only through mouse selection or using double-click.

IFrame support

An agent can see IFrames on a customer's webpages. Using IFrame support, an agent can add or modify the content of the different HTML elements present inside an IFrame in an active co-browsing session.

Important:

Co-Browsing Snap-in supports only two levels of nested IFrames in a webpage.

Note:

An IFrame having contents from a different domain can not be co-browsed due to security restrictions imposed by the browsers for cross domain contents.

Multiple end points / Context name

CoBrowse service end points can be accessed with the context name as services or avservice.

For example, to know the end point service status you can use the following links:

https://CoBrowse-Snapin/services/CoBrowse/v1/server/status/

https://CoBrowse-Snapin/avservice/CoBrowse/v1/server/status/

CSS3 support

Co-Browsing Snap-in supports the following features as a part of the CSS3 support:

- Selectors: Patterns used to select the element you want to style.
- Box model: A box that wraps around every html element. It consists of margins, borders, padding, and the actual content.
- Background and borders: Properties used to define the background effects for elements.
- Image value and replaced content: A generic sizing algorithm for images and other replaced content.

- Text effects: An option to provide different effects to text on a page. For example, you can allow long words to be broken and wrapped onto the next line.
- Multiple column layout: Layout options to specify the number of columns that you can divide an element into.

For more information about CSS3 styles, see the *Client SDK* guide in DevConnect.

Annotation

During an active co-browsing session, a customer or an agent, whoever is in control of the session, can draw geometric figures on the selected data on a webpage by using a mouse pointer. The geometric figures that a customer or an agent can draw in Co-Browsing Snap-in are:

- Rectangle
- Square
- Circle
- Freehand

A customer or an agent can choose the color and thickness of the annotation while using this feature. When the user does not specify any shape, color, or thickness of the annotation, the default values specified for shape, color, or thickness take precedence.

During an active session, the customer or the agent can do the following while using this feature:

- Remove selected or all annotations created by self during an active session.
- Hide or unhide all annotations that are created by the other party to differentiate self-created annotations from those annotations.
- Hide or unhide all annotations created by self while having the control of the page.

Note:

A customer or an agent cannot change the values of any field in the webpage during the annotation process.

Important:

A customer or an agent can enable or disable the annotation functionality during an active co-browsing session.

Data Marker

During an active co-browsing session, a customer or an agent can mark data on a static webpage. An agent or a customer can do the following using this feature:

- Mark static text with any color or style.

- Remove self-created markers by clicking the marked text.
- Hide or unhide markers created by the other party.
- Hide or unhide markers created by self while having the page control

Important:

Ensure that you disable the highlight text feature to enable data marker. You cannot use the highlight text feature and the data marker features at the same time.

Agent Browser Refresh

Avaya Co-Browsing Snap-in provides the option to reconnect to an ongoing session after doing a browser refresh. For an agent browser refresh, the customer data gets synced with agent after reconnecting, while for a customer browser refresh, the customer can reconnect to the current session.

Using the Agent Browser Refresh feature, Avaya Co-Browsing Snap-in stores acstoken in browser cookies for both the customer and the agent during every co-browse session. This token gets stored in the respective browser cookies of the agent and the customer as a part of initialization. After the termination of the session, this cookie gets removed.

Impact on customer website after agent browser refresh:

- Any data that the customer enters during a session gets lost.
- Any annotation and markers that the customer uses during the session gets lost

Impact on agent co-browsing website after agent browser refresh:

- The expanded menu option does not get displayed in expanded mode because co-browse does not store previous activities, actions, or events.
- The mouse-over, the links, and tooltips that got displayed earlier does not get displayed because co-browse does not store the earlier state of selected items.

Note:

After certain time,when there is a disconnect between the client (customer or Agent) and the CoBrowse retry client is not able to reconnect. The end user can reconnect the session by doing page refresh if the session has not been terminated.

Pseudo class element

A pseudo class is used to define a special state of an element. Avaya Co-Browsing Snap-in supports state synchronization of the following pseudo class elements on webpages:

- Selection: To make the selected text red with a yellow background.
- Active: To select and style an active link.

- Target: To match an element that is the target of the referring Uniform Resource Identifier (URI).
- Valid: To select and style an element only if the value of the input element is valid.
- Hover: To select a particular element with a pointing device when the user hovers with a cursor, or a mouse pointer.

For more information about pseudo class elements, see the *Client SDK* guide in DevConnect.

AngularJS and ReactJS support

To enhance user experience and save time, Co-Browsing Snap-in supports the following versions of AngularJS and ReactJS web based applications.

- AngularJS versions: 6, 7, 8, and 9
- ReactJS version: 16.7.0

The supported components for AngularJS and ReactJS are:

AppBar	Chip	Icon	Select/Combo Box	Tabs
Badge	Dialog	Input	Slide	TextField
Button	Divider	List	Snackbar	Toolbar
Card	ExpansionPanel	Menu	Switch	Tooltip
CheckBox	GridList	Radio	Table	Header
SvgIcon	FormControl	Virtual Scrolling	Numeric input increment decrement arrows	cdkDrag
Slider	Google Map			

Limitations

- Angular 7:
  - cdkDragList is not supported.
  - contraints applied on cdkDrag are not supported.
- Angular 9: Google Map is supported only when customer is in control. The change of map location is not supported when the agent is in control.
- Slider component:
  - Does not support inputs through keyboard in Microsoft Edge and Internet Explorer.
  - Live updates of the slider movements are not reflected at the other end when the user in control moves the mouse to change the slider. The final position of the slider is updated only after the mouse is released.

Multiple jQuery support

Co-Browsing Snap-in supports Multiple jQuery used in a web portal. The supported releases are 1.x, 2.x, and 3.x. The major versions for these releases are:

- For 1.x- JQuery Core 1.11 and 1.12
- For 2.x- JQuery Core 2.1 and 2.2
- For 3.x- JQuery Core 3.1, 3.2, 3.3, and 3.4

Serviceability feature for Oceana monitoring

Co-Browsing Snap-in can send heartbeat messages to the Oceana Monitoring service, and you can track the messages and heartbeat information through System Manager. Heartbeat messages are visible on the Monitor Service page. You can view heartbeat messages through System Manager only if you set the value of the Oceana serviceability feature enable attribute to `true`.

RTL support

Avaya Co-Browsing Snap-in supports webpages that are designed for compatibility with RTL scripts. In RTL (right-to-left, top-to-bottom) scripts, writing of any content starts from the right of the page and continues to the left or from top of the page to the bottom.

Chapter 3: Avaya Co-Browsing requirements and compatibility

Avaya product requirements

Install the following Avaya products before installing Avaya Co-Browsing Snap-in:

Avaya products	Version
Avaya Breeze® platform	The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana® and Avaya Co-Browsing Snap-in. Check the Compatibility Matrix page at https://support.avaya.com/CompatibilityMatrix/Index.aspx on the Avaya Support site.
Avaya Aura® System Manager	

Accessing the Compatibility Matrix

About this task

The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya Oceana®.

Procedure

1. Access the Compatibility Matrix page at https://support.avaya.com/CompatibilityMatrix/Index.aspx.
2. From the list of products, select **Oceana® Solution**.
3. Select the release number applicable to your solution.
4. When the page refreshes, scroll to the bottom of the page and select the appropriate release from the **Release** drop-down menu.

   The Compatibility Matrix lists the compatible Avaya products and their versions.

Supported browsers and devices

Device	Operating System version	Default Browser Version
Nexus 5 Phone	Android 6.0.1	Chrome 81
Nexus 7 TAB	Android 6.0.1	Chrome 81
iPhone 6	iOS 9.3.3	Safari 9.3.3
iPad Air	iOS 9.3.3	Safari 9.3.3
MacBook OS	macOS Catalina version- 10.15.7	Safari Version 13.1.3
Laptop	Windows 10	Chrome - 89
Laptop	Windows 10	Firefox STD - 86
Laptop	Windows 10	Firefox ESR - 78.8.0
Laptop	Windows 10	Internet Explorer - 11
Laptop	Windows 10	MS edge Chromium - 89.
Laptop	Windows 10	Microsoft Edge - 44

Important:

- Enable the JavaScript support in your browser for the Avaya Co-Browsing Snap-in. For more information, see http://www.enable-javascript.com/.
- Enable cookies support in your browser for Avaya Co-Browsing Snap-in to work properly. For more information, see http://www.whatarecookies.com/enable.asp.

Database requirements

Avaya Co-Browsing Snap-in supports the following external databases:

- Oracle 19c
- MS SQL Server 2019
- PostgreSQL 12.2
- Intersystem Caché Database 2018

Hardware requirements

The Avaya Co-Browsing Snap-in hardware requirements are based on the Avaya Breeze® platform and System Manager requirements. For more information, see the respective product documentation. You must use Avaya Breeze® platform with 4 vCPU, 8 GB RAM, and 100 GB HDD.

Note:

- For more information on hardware requirements for deploying Avaya Co-Browsing Snap-in as a standalone snap-in, see the “Performance” chapter in this document.
- For more information on hardware requirements for deploying Avaya Co-Browsing Snap-in with Avaya Oceana®, see the *Deploying Avaya Oceana®* document.

Chapter 4: Licensing overview

License requirements

To use Avaya Co-Browsing Snap-in, you must procure the valid Avaya Co-Browsing Snap-in and Avaya Breeze® platform license files.

Avaya Co-Browsing Snap-in uses the snap-in service licensing feature provided by Avaya Breeze® platform. The platform and snap-in licenses are available through PLDS. You must install these licenses on the WebLM server of Avaya Aura® System Manager, which manages the platform and snap-in licenses.

In Avaya Co-Browsing Snap-in, a digital signature that the Avaya Breeze® platform Element Manager uses confirms that the licenses are applicable to these services. If the signature is invalid, the system does not load the service.

A single license containing the information for each licensed feature applies to Avaya Co-Browsing Snap-in.

License modes

The different license modes indicate the status of the services installed on Avaya Breeze® platform.

The following license modes apply to all Avaya Breeze® platform and Avaya Co-Browsing Snap-in licenses:

- **License Normal Mode**: This mode indicates that the installed license file is valid. The complete functionality is available for the Avaya Breeze® platform instance.
- **License Error Mode**: This mode displays the license error. The Avaya Breeze® platform instance is in a 30 day grace period during this mode. In this mode, the complete functionality is available during the grace period. System Manager displays the warning icon with the date and time of the grace period expiration in the **License Mode** column. If the grace period expires and you do not correct the license error, the snap-in enters License Restricted mode and gets uninstalled from all the clusters.
- **License Restricted Mode**: The Avaya Co-Browsing Snap-in instance goes into the restricted mode after the 30 day grace period expires. As a result of this unresolved license error, the snap-in is in the License Restricted mode and gets uninstalled from all clusters.

  If you install a license file, the Avaya Co-Browsing Snap-in server goes into the normal mode and automatically returns to service.

For more information about licensing modes and licensing for Avaya Breeze® platform, see *Administering Avaya Breeze® platform*.

The Avaya Breeze® platform licensing audit runs every 9 minutes. Any license changes, including install or uninstall actions on the WebLM server, take time to reflect on the user interface. The

latest license information therefore, takes maximum 9 minutes to reflect in Avaya Breeze® platform Element Manager.

Configuring Avaya Co-Browsing Snap-in licenses

About this task

Configure Avaya Co-Browsing Snap-in licenses in System Manager.

- Get the Avaya Co-Browsing Snap-in license from Avaya PLDS.
- Get the primary Host ID from System Manager to generate the Avaya Co-Browsing Snap-in license. To get the ID, navigate to Server properties in the Licenses section on the Avaya Breeze® Services tab.
- Ensure that the Avaya Co-Browsing Snap-in license is installed on the WebLM server that is integrated with System Manager.
- Ensure that the Avaya Breeze® platform license is installed on System Manager. To see the current status of each Avaya Breeze® platform server license, navigate to Server Administration in the Avaya Breeze® Elements tab.

Procedure

1. On the System Manager home page, click **Services** > **Licenses**.
2. On the left navigation pane, click **Install license**.
3. Browse to the location of the Avaya Co-Browsing Snap-in license, select the license file, and click **Install**.

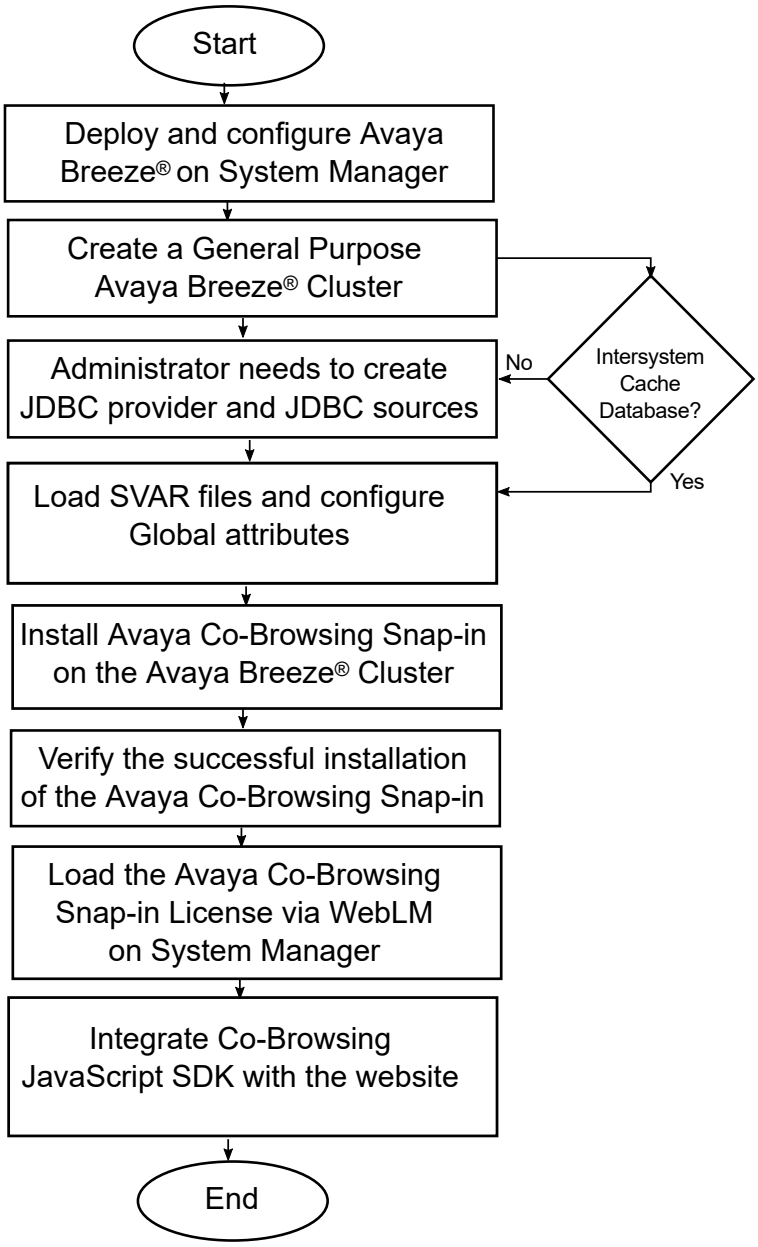
   System Manager installs the license file and displays `COLLABORATIVE_BROWSING_SNAP_IN` under the Licensed Products section located on the left navigation pane.
4. To verify if the license file is installed successfully, do the following:
   a. Click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

      System Manager displays the Services page.
   b. In the All Services table, scroll down to the CoBrowse row, and verify that the License Mode column displays a tick mark. If you hover your mouse on the tick mark, the screen displays the following message:`License Normal Mode — This snap-in has no license errors.`

Chapter 5: Deployment overview

Avaya Co-Browsing Snap-in deployment process flow

The following diagram depicts the process flow for installing the Co-Browsing Snap-in for the first time:


Start
Deploy and configure Avaya Breeze® on System Manager
Create a General Purpose Avaya Breeze® Cluster
Intersystem Cache Database?
No
Yes
Administrator needs to create JDBC provider and JDBC sources
Load SVAR files and configure Global attributes
Install Avaya Co-Browsing Snap-in on the Avaya Breeze® Cluster
Verify the successful installation of the Avaya Co-Browsing Snap-in
Load the Avaya Co-Browsing Snap-in License via WebLM on System Manager
Integrate Co-Browsing JavaScript SDK with the website
End

Avaya Co-Browsing Snap-in deployment checklist

No.	Task	Notes
1	Ensure that Avaya Aura® System Manager is running.	Access the Avaya Aura® System Manager web console and check if you can login as an administrator.
2	Install and configure the Avaya Breeze® platform server.	Before turning on the Avaya Breeze® platform server, ensure that you set the memory to 8 GB of RAM.
3	Create an Avaya Co-Browsing Snap-in cluster.	Assign a Avaya Breeze® platform server to the Avaya Co-Browsing Snap-in cluster. **Note:** When you administer a new Avaya Breeze® platform server, you must add the server to a cluster. If not, the Avaya Breeze® platform asset is not usable. Ensure that you have enabled **Only allow secure web communication** check box. If you are using a multi-instance clustered environment, then enable **Is load balancer enabled** and **Is session affinity enabled** check box.
4	Download the Avaya Co-Browsing Snap-in services from PLDS.	The Avaya Co-Browsing Snap-in services are available as Service Archive (SVAR) files, and the client CoBrowse JavaScript SDK is available as zip files. **Note:** Do not add any space between the file name and the service name while saving the SVAR file.
5	Load the Avaya Co-Browsing Snap-in SVAR file in System Manager.	None.
6	Configure JDBC provider and JDBC sources for Oracle, PostgreSQL, and MS SQL Server databases.	For more information about this, see Creating JDBC Providers DataSources on page 28. If you are using Intersystem Cache database, you do not need to configure JDBC providers.
7	Configure global attributes.	For more information about this, see Configuring Global Attributes on page 32.
8	Load the Avaya Co-Browsing Snap-in license via WebLM.	For more information on licensing, see License requirements on page 20.
9	Install Avaya Co-Browsing Snap-in.	None.

Table continues…

No.	Task	Notes
10	Verify the installation.	None.
11	Configure alarms on System Manager.	None.
12	Install and configure sample reference client.	For more information on this, see the “Appendix A: About sample reference client” section in this document.

High availability

The customers can deploy the co-browse application on multiple nodes of an Avaya Breeze® platform cluster. The actual Avaya Breeze® platform node handling the request is transparent to the API client. You can deploy Avaya Co-Browsing Snap-in either on an independent Avaya Breeze® platform cluster with session affinity enabled. If you disable the session affinity on the Avaya Breeze® platform cluster, then you must use an external load balancer to achieve high availability.

Avaya Co-Browsing Snap-in on a multi-node Avaya Breeze® platform cluster

You can install Avaya Co-Browsing Snap-in on a multi-node Avaya Breeze® platform cluster. If the session affinity is disabled , you will need an external load balancer to achieve high availability. The external load balancer IP address or FQDN is used as the CoBrowse service address. The external loadAvaya Breeze® platform balancer must be able to support:

- Session affinity: To ensure that subsequent requests coming from the same client are routed to the same node. You can achieve session affinity using features like ip_hash, hash, or cookie-based session affinity.
- Routing based on URL parameters: To route the join request and subsequent request after join from the client to land on the respective node where CoBrowse session is created.
- Load balancing requests: To ensure that each node has well distributed amount of CoBrowse session creation requests.

Note:

To ensure that the breeze node IP is not visible in any REST calls set the attribute **Use Security IP for Multi-Node** value is set to `False`. You need an external load balancer with the defined routing rules to map the breeze nodes against the token provided in the URL parameter "affinity". The default value for the attribute Use Security IP for Multi-Node is set to `True`.

.

Avaya Co-Browsing Snap-in on a single node Avaya Breeze® platform cluster

If at least one node in the Avaya Breeze® platform cluster is active and accepting new requests, the cluster IP will service incoming requests. The scope of the cluster support does not imply support for the following:

1. Load balancing: An even distribution of incoming requests to various nodes within the Avaya Breeze® platform cluster is not provided. The mechanism for even load distribution is Avaya Breeze® platform dependent.
2. High availability: A backup Avaya Breeze® platform node takes 5 to 7 minutes to start serving requests after the primary Avaya Breeze® platform node is unable to serve requests. During this period, the cluster IP might be unable to service new requests.
3. Session preservation: Ongoing sessions being serviced by a particular node will not be preserved when that Avaya Breeze® platform node is no longer available to serve requests.

Note:

Ensure that the **Use Security IP for Multi-Node** attribute value is set to `True`.If the administrator does not want to display the node IP in any REST calls, then you need to set the node IP to `False`.

Creating an Avaya Co-Browsing Snap-in cluster

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®**.
2. In the left pane, click **Cluster Administration**.
3. On the Cluster Administration page, click **New**.

   The system displays the Cluster Editor page.
4. In the **Cluster Profile** drop-down list, select the **General Purpose** profile.

   The system refreshes the Cluster Editor page and populates the profile attributes.
5. In the **General** tab, type the details in the following fields:
   a. **Cluster Name**: The unique name of the cluster.
   b. **Cluster IP**: The cluster IP address. The cluster IP address is mandatory if you enable the load balancer. If you enable the load balancer, ensure you select session affinity.

      For information on setting up the load balancer, see *Administering Avaya Breeze® platform*.
   c. **Description**: The description of the cluster.

   d. Ensure that you have selected **Only allow secure web communication** check box.
   e. If you want to deploy Avaya Co-Browsing Snap-in on multiple nodes, ensure you select the **Is load balancing enabled** check boxes.

6. In the **Servers** tab, in the **Unassigned Servers** table, click the plus sign (**+**) next to the **Name** column to add the Avaya Breeze® platform server to the cluster.

   If the server is assigned to another cluster, remove the server from the existing cluster before you add to the Avaya Co-Browsing Snap-in cluster.

7. Click **Commit** to create the cluster.

   On the Cluster Administration page, the **Service Install Status** field displays a green check mark after the cluster is successfully created.

8. **(Optional)** To view the Avaya Breeze® platform instances in the cluster, click **Show** in the **Details** column of the cluster.

   The system displays the members of the cluster and the status of each instance in the cluster.

9. **(Optional)** To view the details of the Snap-ins installed on that instance, click a specific Avaya Breeze® platform instance in the cluster.

Installing Avaya Co-Browsing Snap-in

Loading Avaya Co-Browsing Snap-in

Before you begin

- Install a WebLM license of Co-Browsing Snap-in on System Manager.
- Download the Avaya Co-Browsing Snap-in services from PLDS.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Click **Load**.
3. On the Load Service window, click **Choose File**.
4. In the Load Service dialog box, click **Browse** to select the `CoBrowse-<3.8.1.0.xxxx>.svar` file from your local machine, where x, y, and z denotes the Co-Browsing Snap-in version.
5. Click **Load**.

   System Manager checks the licensing of Co-Browsing Snap-in. On successful validation, System Manager displays the Accept End User License Agreement dialog box.

6. Click **Accept**.

   System Manager adds Avaya Co-Browsing Snap-in to the list of services.

7. To ensure that Co-Browsing Snap-in is in loaded state, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services** page.

   The row for the Co-Browsing Snap-in services displays the status as loaded.

Creating JDBC providers and datasources

About this task

Use this procedure to create JDBC providers and datasources.

Important:

Skip this procedure if you use the Intersystem Cache database.

Before you begin

Ensure you download the JDBC driver `.jar` file compatible with the database version you want to use from the database vendor website. Ensure you are using the correct `.jar` file and the implementation class for that `.jar` file.

Refer to the *System Manager* guide for additional information about configuring JDBC providers and datasources.

The following table lists the database and the corresponding `.jar` files:

Database	.jar file
Oracle	ojdbc7.jar
PostgreSQL	postgresql-42.2.10 jar
MS SQL Server	mssql-jdbc-8.2.2.jar

Procedure

1. Log in to **System Manager**.
2. Navigate to **Home** > **Avaya Breeze®** > **Configuration** > **JDBC Providers**.
3. Click **New**.
4. In the Jar field, create a JDBC provider using the JDBC driver `.jar` file.

   In the **JDBC Provider Editor**, specify the class name as mentioned in the JDBC Provider Class Name on page 30.

   In the **Jar File**, select the `.jar` file. For example, if you are creating JDBC provider MS SQL server TestProvider, then use the MS SQL server JDBC driver `mssql-jdbc-8.2.2.jar` file.

5. Navigate to **Home** > **Avaya Breeze®** > **Service Management** > **Services**.
6. Search for the JDBC provider you created in step 3.

7. Select the provider and click **Install**.

   The system displays a popup list of clusters.
8. Select the cluster on which you want to install the provider and click **Commit**.
9. After you successfully install the JDBC provider, reboot all **Avaya Breeze®** instances for the cluster.
10. Navigate to **Home** > **Avaya Breeze®** > **Configuration** > **JDBC Sources**.
11. Add a new datasource from the JDBC datasource page.
12. On the JDBC Data Source editor page, under **Basic** section, select the cluster on which you installed the provider.

    The system populates the installed provider name in the **JDBC Provider** drop-down.
13. Specify a JNDI name. you can specify the JNDI name as `jdbc/<anyname>`. For example, if you creating JDBC source for SQL, then mention the JNDI name as `jdbc/sql`.
14. Specify the database URL, username, and password to connect to the database. For example, `jdbc:oracle:thin:<DB server IP address>:<port number>:oracledb`.
15. Under **Custom Properties** section, in the **Name** tab, specify the database name as `databaseName` and under the **Value** tab, specify the value as configured on the MS SQL server and PostgreSQL.
16. Under the **Name** tab, specify the port number as `portNumber` and under the **Value** tab, specify the value as configured on the MS SQL server and PostgreSQL.
17. Under the **Name** tab, specify the server name as `serverName` and under the **Value** tab, specify the value as configured on the MS SQL server and PostgreSQL.
18. Under the **Name** tab, specify the user name as `user` and under the **Value** tab, specify the value as configured on the PostgreSQL.
19. Under the **Name** tab, specify the password name as `password` and under the **Value** tab, specify the value as configured on the PostgreSQL.
20. Click **Commit**.
21. On the JDBC Data Sources page, click **Test Connection**.

    This page displays the status of the connection to the database.
22. Reboot Avaya Breeze® platform server after test connection is successful.

JDBC Provider Class Name

Database	JDBC Provider Class Name	JDBC Sources sample DB URL
Oracle	oracle.jdbc.pool.OracleConnectionPoolDataSource	`jdbc:oracle:thin:@<Databaseserver IP or FQDN>:port number:<database name>` • serverName • databaseName • portNumber: default is 1521
PostgreSQL	org.postgresql.jdbc2.optional.ConnectionPool	`jdbc:postgresql:// <Database server IP` Ensure you configure the following custom properties: • serverName • databaseName • portNumber: default is 5432
MS SQL Server	com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource	`jdbc:sqlserver://<Database server IP or FQDN>` Ensure you configure the following custom properties: • serverName • databaseName • portNumber: default is 1433

Configuring Intersystem Cache database

Use the following procedures sequentially to configure the Intersystem Cache database while deploying Avaya Co-Browsing Snap-in with Avaya Oceana®:

Configuring an Avaya Co-Browsing Snap-in user

About this task

Use the following steps to modify the Avaya Co-Browsing Snap-in user password in the InterSystems Cache database.

Procedure

1. Log in to the system where you installed the InterSystems Cache instance.
2. To open the InterSystems Cache Management portal, enter the following url on your web browser:

`https://<INTERSYSTEM_CACHÉ_DATABASE_IP>:57772/csp/sys/UtilHome.csp`, where `<ServerIP>` is the IP address of the server where you installed the Omnichannel database.

3. On the InterSystems Cache Management Portal login page, do the following:
   a. In the **User Name** field, type `_admin`.
   b. In the **Password** field, type `Oceana16`.
   c. Click `LOGIN`.
4. To switch to the COBROWSE namespace, in the **Namespace** field, click **Switch**.

   The InterSystems Cache Management portal displays the Namespace Chooser page.
5. In the Available Namesapces section, click **COBROWSE**.
6. Click **OK**.
7. On the left navigation pane, click **System Administration** > **Security** > **Users**.

   The InterSystems Cache Management portal displays the User page with a list of user definitions.
8. Scroll down to the Cobrowse row, and click **Profile**.

   The InterSystems Cache Management portal displays the summary of the privilege for the Cobrowse user.
9. Click **Edit User**.
10. In the **Password** field, click **Enter New Password**.

    The Edit User page displays the password field.
11. Enter the password and confirm your password.
12. Click **Save**.

    The **Save** option is located on the top of the page.

    The Edit User page displays the message: `User saved`.

Setting the Intersystem Cache password in System Manager

About this task

Use this procedure to set the Intersystem Cache password in System Manager.

Before you begin

Configure a Co-Browsing Snap-in user.

Procedure

1. Log in to System Manager.

2. Go to **Access ElementsAvaya Breeze Configuration** > **Attributes**.
3. Click **Service Clusters**.
4. In the **Cluster** field, select the CoBrowse cluster.
5. In the **Service** field, select the CoBrowse service.
6. Scroll down to the Omnichannel Database Configuration section.
7. In the **Database Password** field, enter a valid password.
8. Click **Commit** and restart the CoBrowse service.

Configuring global attributes

About this task

Configuring values for the Avaya Co-Browsing Snap-in is a one-time activity that you must perform before installing Avaya Co-Browsing snap-in.

Procedure

1. On the System Manager Home page, in **Elements**, select **Avaya Breeze®** > **Configuration** > **Attributes**.
2. Click the **Service Globals** tab.
3. In **Service**, click the service that contains the attributes you want to configure.

   The table displays all attributes that you can configure for a CoBrowse service with the description of each attribute.
4. For the attribute you want to change:
   a. Click **Override Default**.
   b. In the **Effective Value** field, enter the new value or string.
5. Click **Commit** to save your changes.

   The cluster level service attributes persist after an uninstall from the cluster. The values are retained for a subsequent installation, so that you do not have to re-configure all attributes when changing service versions.

Runtime service configuration attributes

In Avaya Co-Browsing Snap-in, you can set the default group attributes as follows:

Name	Description
Enable Centralized Logging	Indicates that centralized logging is required for the snap-in after the snap-in is installed. This attribute is not editable. **Note:** This feature is available only when Avaya Co-Browsing Snap-in is used with Avaya Oceana®.
Inactive Timeout (Minutes)	Displays the value in minutes. The system ends a session if the owner of the co-browse session is idle for the time, which is configured in Inactive time out (minutes). The minimum value is 2 minutes and maximum value is 29 minutes. The default value is 2 minutes.
Inactive Timeout (Message)	Displays the message after the system ends the session. You can add your custom message.
Session Timeout (Minutes)	Displays the value in minutes. The system ends a session during a regular clean up activity which runs at the interval of every 30 minutes, if the session does not end properly. The minimum value is 30 minutes and maximum value is 1440 minutes. The default value is 60 minutes.
Supported Locale	Displays the supported locales by Collaborative Browsing Server. The default values are en_US, de, es, fr, it, ja, ko, ru, zh_CN, pt_BR, zh_TW, ar_SA co-browse session server can support the following locales: • en_US: English • de: German • es: Spanish • fr: French • it: Italian • ja: Japanese • ko: Korean • ru: Russian • zh_CN: Chinese • pt_BR: Portuguese (Brazilian) • zh_TW: Traditional Chinese • ar_SA: Arabic
Server Default Locale	Displays the default locale. You can configure the locale as per requirements. For example, if you want the co-browse session to support English only, you can set the default locale as en_US or you can change the preference of the language.

Table continues…

Name	Description
Enable Tokenless Access	Setting the value to true allows the client to request access to the resource end-points without any authorization token. The options are: • true: This is the default value • false: Need Authorization token to access resource end-points.
Oceana Serviceability Feature Enable	Displays the snap-in heartbeat and life cycle messages on Avaya Aura® System Manager by enabling the monitor service when you set this value to true. The options are: • true: Select this value while deploying Avaya Co-Browsing Snap-in with Avaya Oceana®. • false: This is the default value.
Use Security IP for Multi-node	If you do not want the security IP to be used as the value of parameter "Affinity", then set this parameter value to "False". The default token name "Route" is used instead of the IP. You can change the token name by changing the attribute "Collaborative Browsing Breeze Node Token name". The options are: • true: This is the default value. It indicates that the security IP address is used for the request redirection as URL parameter **Affinity**. • false: When you set the value to false, then the **Breeze Node token name** value is used in the request redirection REST calls instead of Breeze node IP, then enter a unique collaborative browsing breeze node token name in the **Collaborative Browsing Breeze Node Token name** attribute. The default token name used is **Route**.
Collaborative Browsing Breeze Node Token name	If the customer and the agent are created on different nodes, you can use a unique collaborative browsing breeze node token name to redirect requests while joining agent and customer for a co-browsing session. **Important:** You must use this option only when you are not using the security IP address. The default value is Route. However, you can create a unique name as an unique identifier.

Avaya Co-Browsing Snap-in database attributes

You must set the database attributes before you install the Avaya Co-Browsing Snap-in.

Note:

The default values for the database attributes are for reference. You must create a database before you install the Avaya Co-Browsing Snap-in.

Name	Description	Default value
Enable JNDI	This value must be true if you use an external database. This value must be false if you use the Intersystem cache database configuration.	The default value is false.
Database JNDI Name	The name of the external database. You must use the JNDI name created in Creating JDBC Providers DataSources on page 28. If you change the value, you must stop and start the co-browse service.	This is a mandatory attribute if you are not using the Intersystem Cache Database.
Database Type	This is a mandatory attribute used to specify the external database type used for Co-Browsing. You can enter one of the following values depending on the database you want to use: • oracle • sqlserver • postgres • intersystemcache If you change the value, you must stop and start the co-browse service.	NA
Database Dialect	The external database dialect. If you change the value, you must stop and start the co-browse service.	This is a mandatory attribute. You can enter one of the following values depending on the database you use: • Oracle:*org.hibernate.dialect.Oracle10gDialect* • SQL:*org.hibernate.dialect.SQLServerDialect* • Postgres: *org.hibernate.dialect.PostgreSQLDialect* • Intersystem Cache: *org.hibernate.dialect.Cache71Dialect*

Important:

If you change any of the database attributes after installing Avaya Co-Browsing Snap-in, you must stop and start the co-browse service for the changes to take effect.

Omnichannel database configuration

Use this configuration when:

- You set the JNDI attribute to False
- You use Intersystem Cache Database

Note:

Use only while deploying Avaya Co-Browsing Snap-in with Avaya Oceana®.

Name	Description	Default value
Database User Name	The username for external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	NA
Database Password	The password for external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	NA
Database Driver Class	The driver class name for external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	`com.intersys.jdbc.CacheDriver`
Database IP/FQDN	The IP address or FQDN for accessing external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	NA

Table continues…

Name	Description	Default value
Database Port	The port used for accessing external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	The default port number is 1972.
Database Name	The name of the external database. This is a mandatory attribute if you are using the Intersystem Cache Database. If you change the value, you must reboot the cluster.	The default name is COBROWSE.
Secure InterSystem Cache	Setting this to true enables a secure connection to the Omnichannel database. If you set this to true, ensure you create the relevant certificates in System Manager and Omnichannel database.	The default value is false.

Avaya Co-Browse feature attributes

In Avaya Co-Browsing Snap-in, you can set the feature attribute as follows:

Name	Description	Default value
Enable Request Control Feature	Administrator can allow or restrict the Agent to take control of the Co-Browse webpage. **Note:** This feature is available only when Avaya Co-Browsing Snap-in is not deployed with Avaya Oceana®	The default value is True.

Installing Avaya Co-Browsing Snap-in

Before you begin

- Load Co-Browsing Snap-in.
- Ensure that you know the cluster name to install the Co-Browsing Snap-in.
- Configure all database attributes in the service global tab using System Manager.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. In the services name list, select the Avaya Co-Browsing Snap-in and then click **Install**.

   The system displays a list of cluster names in the Confirm Install services dialog box.
3. Select the cluster name to install the Avaya Co-Browsing Snap-in, and then click **Commit**.

   The system starts installing the service and changes the state of the service to `Installing`. After installation, the system changes the state to `Installed`, which indicates that the service has started.

Starting a service

About this task

You can now start a service without rebooting the cluster.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the service that you want to start.
3. Click **Start**.

   The system starts the selected service.

Stopping a service

About this task

You can now stop a service without rebooting the cluster.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the service that you want to stop.
3. Click **Stop**.

   The system stops the selected service.

Verifying a Avaya Co-Browsing Snap-in deployment

Procedure

1. Open a web browser.
2. To check the query management REST API, type the following URL:

   `https://<Cluster_IP>/services/CoBrowse/v1/server/status`

   where <*Cluster_IP*> is the IP address of the Avaya Co-Browsing Snap-in cluster where the service that you want to verify is running.

   Note:

   For a single Avaya Breeze® platform instance, provide the security IP address instead of cluster IP.

   The system displays the following message: `{"statusCode":"200", "acsResult":"success", "acsResponse":"Successfull", "errorCode":"", "errorMessage":"", "options":null}`

Editing attributes for Avaya Co-Browsing Snap-in

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®**.
2. On the Server Administration page, click **Configuration** > **Attributes**.

   The system displays the Attributes Configuration page.
3. Configure attributes on the following tabs:
   - **Service Clusters:** The attributes are used by all Avaya Co-Browsing Snap-ins that are part of the cluster that you select.
   - **Service Globals:** The attributes are used by all occurrences of the Avaya Co-Browsing Snap-ins except when overridden by attributes administered for a specific cluster.

   Note:

   After installing snap-in, the **Effective value** for all attributes in **Service Clusters** are same as **Service Globals**. If you change the attribute value in **Service Globals**, then the value in **Service Clusters** changes automatically. To customize a specific attribute for a specific cluster, select the cluster from the drop-down, select the service as CoBrowse, and then select the **Override default** check box in **Service Clusters** for the specific attribute.
4. To configure attributes for **Service Clusters**, click the **Service Clusters** tab.
   a. In the **Cluster** field, select the cluster where the Snap-in is installed.

b. In the **Service** field, select the service name as **CoBrowse**.

   The system displays a list of attributes that you can configure.

c. In the **Override Default** column, specify the attributes by selecting the corresponding check box.

d. **(Optional)** In the **Effective Value** column, change the value of the attributes.

   To restore the default options, clear the **Override Default** check box.

5. Click **Commit** to save the configuration.

Upgrading Avaya Co-Browsing Snap-in

Upgrade overview

To upgrade Avaya Co-Browsing Snap-in service in Avaya Breeze® platform, you must install a new version of the Snap-in service.

When you upgrade the Avaya Co-Browsing Snap-in SVAR, the system does not remove the Avaya Co-Browsing Snap-in that is already deployed.

You can upgrade by using the preferred version or the latest version.

Preferred version

When you deploy a new version of the Avaya Co-Browsing Snap-in service, the previous version of the service continues servicing the REST requests. To bring the newly deployed SVAR into service, you must set the newer version as the preferred version on the **Avaya Breeze®** > **Service Management** > **Services** page. For more information, see Setting Preferred Version on page 42.

Latest version

When you deploy a new version of the Avaya Co-Browsing Snap-in service, the new version of the Snap-in service starts servicing the REST requests automatically.

When you deploy a Avaya Co-Browsing Snap-in service in a new Avaya Breeze® platform instance, the service is set to **latest** by default.

If you do not set any version as the preferred version, the system uses the latest version value.

When a version is set as the preferred version, the system does not give the option to set the latest version in the **Services** page.

Upgrading Avaya Co-Browsing Snap-in services

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

2. Make a note of the existing attribute values of the old Co-Browse service before you upgrade.
3. Uninstall and delete the old Co-Browse service.
4. Ensure that the service name is “CoBrowse” by navigating to **Attributes** > **Service Global**.
5. On the **Services** page, click **Load**.
6. Click **Browse** next to **Local PC** to locate the latest `Avaya Co-Browsing Snap-in<CoBrowse-x.y.0.0.zzzzzz>.svar`, where x, y, and z denotes the Co-Browsing Snap-in version..
7. Click **Open**.
8. In the Load Service window, click **Load** to load the Avaya Co-Browsing Snap-in service.
9. On the End User License Agreement (EULA) page, click **Accept**.

   The Service Management page displays the service with the `LOADED` state.
10. In the left navigation pane, click **Attributes** > **Service Global** and select “CoBrowse” service.
11. In the left navigation pane, click **Cluster Administration**.
12. For the cluster that you want to upgrade, select **Deny New Service** from the **Cluster State** drop-down.
13. To upgrade to the latest version of the Avaya Co-Browsing Snap-in service, perform one of the following steps:
    - On the **Services** page, select and install the latest version of the CoBrowse service.
    - On the **Cluster Administration** page, edit the cluster to select and commit the latest version of the Avaya Co-Browsing Snap-in service.

    The Services page displays the service with the `INSTALLED` state.

    - If you set the preferred version option for a service, the service continues to service the requests. The new service version comes in to service only after you set the new version as the preferred version option in the **Services** page.
    - If you do not set the preferred version option for the service in the cluster, the newly deployed version comes in to service after successful deployment. However, it is advisable to set the preferred version for the newly installed service to avail the features of that release.
14. Verify if the services are installed successfully. For more information, see *Verifying a Avaya Co-Browsing Snap-in deployment*.
15. For the upgraded cluster, select **Accept New Service** state from the **Cluster State** drop-down.
16. Verify the co-browsing deployment functionality after the upgrade.

Related links

Setting the preferred version for upgrades on page 42

Setting the preferred version for upgrades

Before you begin

Install the Snap-in service on Avaya Breeze® platform.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the service that you want to set as the default version.
3. Select **Set Preferred Version**.

   The system displays the list of clusters.
4. Select the clusters for which you want to set the preferred version.
5. Click **Commit**.

   The **Preferred Version** column displays the clusters for which you have set the preferred version.
6. Verify whether the updated service can service requests successfully. For more information, see *Verifying Avaya Co-Browsing Snap-in deployment*.

Uninstalling and deleting Avaya Co-Browsing Snap-in

Avaya Co-Browsing Snap-in uninstallation overview

The options are:

- Uninstall a service Snap-in: When you uninstall a service, the system does not remove the attributes from the Avaya Breeze® platform Postgres database. For more information, see Uninstalling Avaya Co-Browsing Snap-in on page 42.
- Delete a service Snap-in: When you delete a service, the system removes the attributes from the Avaya Breeze® platform Postgres database. For more information, see Deleting Avaya Co-Browsing Snap-in on page 43.

Uninstalling Avaya Co-Browsing Snap-in

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.

2. On the Services page, select the check box for **CoBrowse** . Ensure that you select the correct version.
3. Click **Uninstall**.
4. Select the **Cluster Name** from which you want to uninstall the **CoBrowse** service.
5. Click **Commit**.

Next steps

To verify that the service is uninstalled, click **Elements** > **Avaya Breeze®** and perform the following steps:

1. On the Services page, verify that the **State** of the service is **Loaded**.
2. On the Cluster Administration page, perform the following steps:
   a. Identify the co-browse cluster.
   b. Click **Show**.
   c. Click the **Avaya Breeze®** server, and verify that the Service Status page does not display the uninstalled service.

Deleting Avaya Co-Browsing Snap-in

Before you begin

Ensure that the Avaya Co-Browsing Snap-in is in Loaded state.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, perform the following steps:
   a. Verify that the **State** of the service is **Loaded**.
   b. Select the service that you want to delete, and then click **Delete**.
   c. In the dialog box, select the **Please Confirm** check box.
   d. Click **Delete**.

Next steps

To verify that the service is deleted, click **Elements** > **Avaya Breeze®**, and perform the following steps:

1. Click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Verify that the Services page does not display the deleted service.

Avaya Co-Browsing Snap-in server API endpoints

Avaya Co-Browsing Snap-in provides the following Customer and Agent REST API endpoints. . If you need to configure firewall, proxy, or any other filters, you must allow the following endpoints for Avaya Co-Browsing Snap-in.

Note:

The Customer and Agent REST APIs are used by the co-browsing client SDK. Hence, the request and response parameters are not mentioned here.

Endpoint Interface	REST API version	REST API	Description
Customer	V1	/services/CoBrowse/v1/customer/session/request	Allows customer to generate passphrase and join the co-browse session. This is customer-initiated session.
		/services/CoBrowse/v1/customer/session/join	Allows customer to join the co-browse session initiated by an agent.
		/services/CoBrowse/v1/customer/session/logout	Allows customer to logout from the co-browse session.
		/services/CoBrowse/v1/customer/status	Customer status.
Agent	V1	/services/CoBrowse/v1/agent/session/request	If autojoin is true, allows agent to generate passphrase and join the co-browse session. (one step process) If autojoin is false, only passphrase is generated. (two-step process)
		/services/CoBrowse/v1/agent/session/join	In the above request, when autojoin is passed as false, this request is required to join the co-browse session in the two-step process. Agent first generates the passphrase in the first step and joins in the second step.

Table continues…

Endpoint Interface	REST API version	REST API	Description
		/services/CoBrowse/v1/agent/session/live/join	Allows agent to join co-browse session when customer has already joined and is waiting for the agent.
		/services/CoBrowse/v1/agent/session/logout	Allows agent to logout from the session.
		/services/CoBrowse/v1/agent/status	Agent status.
Server Status	V1	/services/CoBrowse/v1/server/status	Returns co-browse server status as successful or not.

sockjs endpoint	REST API version	REST API	Description
Customer		/services/CoBrowse/sockjs/cobrowse/customer/	Handles the co-browse traffic over the websocket from customer.
Agent		/services/CoBrowse/sockjs/cobrowse/agent/	Handles the co-browse traffic over the websocket from agent.

To check the co-browse server status, type the following URL:

```
https://<Cluster_IP>/services/CoBrowse/v1/server/status
```

where <Cluster_IP> is the IP address of the Avaya Co-Browsing Snap-in cluster where the service that you want to verify is running.

Chapter 6: Security overview

Avaya Co-Browsing Snap-in utilizes Avaya Breeze® platform to provide all security configurations to access all Avaya Breeze® platform services. Avaya Breeze® platform provides configuration for HTTPS, Mutual TLS (Client Certificate Challenge), Cross Origin Resource Sharing (CORS), Whitelists, Trust Certificates, and Data Encryption. In addition, System Manager provides a flexible platform for administering certificates and authorities.

For more information about the security configuration, see the *Avaya Breeze® platform* and *System Manager* product documentation.

Selecting the Transport Layer Security version for a snap-in service

About this task

Avaya Breeze® platform supports the selection of the minimum Transport Layer Security (TLS) version for the SIP and HTTPS services in each cluster.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®**.
2. In the left navigation pane, click **Cluster Administration**.
3. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
4. On the Cluster Editor page, perform the following steps:
   a. Click the **Services** tab.

      System Manager displays the list of services installed in the cluster.

   b. Select the check box next to the snap-in service for which you want to select the TLS version.

   c. From the **Select TLS Version for the Selected Snap-in(s)**, select the relevant TLS version.

   The TLS version column corresponding to the service snap-in displays the selected TLS version.

Note:

You must configure the relevant TLS version for the selected Snap-in(s).

5. Click **Commit**.
6. Restart the cluster for the changes to take effect.

Certificate-based authentication overview

For Avaya Co-Browsing Snap-in certificate-based authentication, perform the following procedures on the System Manager web interface:

- Configure client certificate challenge through the **Avaya Breeze®** > **Configuration** > **HTTP Security** page.
- Create a client keystore.
- Download the Avaya Breeze® platform trusted certificate from System Manager.
- Authenticate browsers.

Ensure that the client applications that access Avaya Co-Browsing Snap-in operations provide the location and credentials of their client certificate and trusted certificate to establish a secure session with the Avaya Co-Browsing Snap-in cluster.

For more information, see the *Avaya Breeze® platform* and *System Manager* product documentation.

Cross Origin Resource Sharing

Cross Origin Resource Sharing (CORS) enables access to Avaya Co-Browsing Snap-in requests that originate from specific domains. Cross-origin resource sharing allows JavaScripts from an application server that can send HTTPS requests to an Avaya Breeze® platform instance. The configuration is available on the **Avaya Breeze®** > **Configuration** > **HTTP Security** > **HTTP CORS** page.

If the originator is `xyz.com`, then add `xyz.com` as an origin in the CORS list. If the origin is `<IP address:port>`, then add `<IP Address:port>` as an origin in the CORS list.

If the originator is `IP Address`, then add `IP Address` as an origin in the CORS list.

For more information, see the *Avaya Breeze® platform* product documentation.

Note:

If you use a custom web client application, and enable the client certificate challenge, the web clients cannot authenticate the client certificate through JavaScript, that is, Ajax calls. The browser and JavaScript layers are not connected. Therefore, the system does not send the required client certificate.

Whitelist

Avaya Breeze® platform accepts HTTPS requests only from the IP Addresses listed in the table. If you do not select this (whitelist enable check box), Avaya Breeze® platform accepts any HTTPS request that passes the optional client certificate challenge.

Data security

The customer can ensure data privacy and secure co-browsing by using security measures such as hiding sensitive information, preventing certain actions, and hiding certain elements. Depending on the legal and location-specific requirements, the customer can apply data masking to certain fields such as Social Security Number or credit card number. The customer can also block certain actions so that the agent does not submit any information on behalf of the customer. For more information on data masking, see *Avaya Co-Browsing Snap-in Developer and API Reference*.

Port utilization

For Avaya Co-Browsing Snap-in port information, see the *Port Matrix for Avaya Breeze® platform* doc at http://support.avaya.com.

Data protection and data privacy support

Co-Browsing Snap-in supports data protection and data privacy to comply with data privacy laws.

In Co-Browsing Snap-in, data administrators can access, modify, delete, export, or restrict access to personal data and audit information to comply with privacy laws such as:

- Fulfillment of Data Subject Rights
- Personal Data Minimization – Retention

Co-Browsing Snap-in also supports data encryption.

Co-Browsing Snap-in provides a mechanism for consent management from customers to save personal data and audit information, which complies with the following data privacy law:

- Consent Management for Processing and Storage of Personal Data

Data Subject Rights management

Avaya Co-Browsing Snap-in provides security of your personal data by enabling the database administrator to modify, delete, export, or restrict access to customer's personal data. The administrator can either do these tasks using UI controls if any, or by using database queries.

A customer's personal information is stored in the table cb_customersession. To perform update, delete, or read operations, the database administrator can use the following fields as a unique constraint:

- cb_customeremail
- cb_customername
- cb_customersessionid
- cb_customersysteminfo

When an agent updates any information on a webpage on behalf of a customer, the information gets stored in the cb_auditlog for future audits. To perform read, update, and delete operations for this table, the database administrator can use the following field: cb_customersessionid.

Note:

You can also use other table fields to perform database query operations. To know more about customer personal information table fields, see the "Consent Management for Processing and Storage of Personal Data" table in this document.

Personal data retention

In Avaya Co-Browsing Snap-in, the database administrator has the rights to define the storage duration of personal data for each data subject. A data subject is any person whose personal data is collected, held, or processed, while personal data refers to anything from your name, home address, or your posts on social media. The personal data is stored only as long as is necessary to complete a particular task, or for the duration that the database administrator defines.

The database administrator can use the following ways to delete personal data and audit information:

- Delete data manually.
- Set job scheduler to delete data periodically.

Deleting customer data from an InterSystems Cache database

If you are deploying Avaya Co-Browsing Snap-in with Avaya Oceana®, then use the following queries to purge the customer's personal information manually in a InterSystems Cache database from cb_auditlog and cb_customersession.

Database	Audit Information	Customer Information
CacheDB	DELETE FROM (cb_auditlog JOIN cb_customersession ON cb_auditlog.cb_cobrowsesessionid= cb_customersession.cb_cobrowsesessionid), where cb_customersession.cb_customeremail=*'<customeremail>'* For example, DELETE FROM (cb_auditlog JOIN cb_customersession ON cb_auditlog.cb_cobrowsesessionid= cb_customersession.cb_cobrowsesessionid), where cb_customersession.cb_customeremail=*'customer@test.com'* **Note:** You can use cb_customeremail to get the unique constrain. However, you can use any column name.	DELETE cb_customersession FROM cb_customersession, where cb_customersession.cb_customeremail=*'<customeremail>'* For example, DELETE cb_customersession FROM cb_customersession, where cb_customersession.cb_customeremail=*'customer@test.com'* **Note:** You can use cb_customeremail to get the unique constraint. However, you can use any column name.

Setting job scheduler to delete InterSystem Cache customer data

About this task

If you are deploying Avaya Co-Browsing Snap-in with Avaya Oceana®, then use the following steps to set the job scheduler for purging the customer's personal information in a InterSystems Cache database from cb_auditlog, and cb_customersession.

Procedure

1. Launch Management portal of running cache instance.
2. Click **System Operation** > **Task Manager** > **New Task**.
3. On the **Task Scheduler Wizard** , do the following:
   a. Enter the task name and description.
   b. In the **Namespace to run task in** field, select **COBROWSE**.
   c. In the **Task type** field, select **RunLegacyTask**.
   d. In the **ExecuteCode** field, type the required code:

      ```
      (eq: do ##class(%SQL.Statement).%ExecDirect(,"DELETE cb_customersession from cb_customersession)
      ```

      , where cb_customersession.cb_cobrowsesessionid=9
   e. In the **Task Priority** field, select **Priority Normal**.
   f. In the **Run task as this user** field, select the user for whom you want to run the task.
4. Click **Next** and set the recurrence duration of the task.

5. To save the task, click **Finish**.
6. On the Task Schedule page, verify that the task is visible in the list.

Data encryption

Avaya Co-Browsing Snap-in provides secure processing of personal data by encrypting this data in end-to-end transit and at rest.

Avaya Co-Browsing Snap-in uses an in-built database encryption mechanism where the encrypted data remains separate from the device security on which the data is stored. The encryption is on the data and therefore, the data is secure regardless of how it is transmitted. This security on the data permits administrators to store and transmit data by using even unsecured means.

This data encryption method prevents data visibility in case of unauthorized data access or data theft and is commonly used to protect data in motion and also for protecting data at rest.

You must do the following for secure data encryption:

- Use encryption methods such as Advanced Encryption Standard (AES) or Rivest–Shamir–Adleman (RSA) for encryption of data at rest.
- Ensure that encrypted data remains encrypted when access controls such as usernames and passwords fail.
- Increase encryption at multiple levels.
- Implement cryptography on the database that houses the data and on the physical storage where the databases are stored.
- Update data encryption keys on a regular basis.
- Store encryption keys separately from the data.
- Enable crypto-shredding at the end of the data or hardware lifecycle. Crypto-shredding is the practice of deleting data by manually deleting or overwriting the encryption keys.
- Audit sensitive data periodically.
- Store only the most important sensitive data.

Important:

- Encrypt the database without interrupting the normal state of a system. An interrupted encryption or decryption process can leave a database in an unusable state. Therefore, keep a latest backup file before encrypting a database.
- Encrypt or decrypt the databases during a maintenance upgrade window. Encrypt the databases on each node before mirroring and restoring the backup data.

Avaya Co-Browsing Snap-in supports the data encryption of the following databases:

- Intersystems Cache 2018
- PostgreSQL 12.2

- Oracle 19C
- MS SQL 2019

Consent Management for Processing and Storage of Personal Data

Avaya Co-Browsing Snap-in provides the provision of taking customer consent to allow or deny storing of personal information in the co-browse database.

If a customer permits to store the information, then:

- The customer personal information like customer name, email address, and system information gets saved in the database.
- The fields that an agent changes while the agent is in control during a co-browse session gets automatically updated in the auditlog for audit trails.

If a customer denies permission to store the information, then:

- The customer personal information does not get stored in the database.
- The database skips the audit update for each field that an agent changes while the agent is in control during a co-browse session.

Note:

By default, Co-Browsing Snap-in stores the customer name, customer email address, and customer system information when a customer joins or initiates a co-browse session.

The customer information that Co-Browsing Snap-in stores in the database, after a co-browse session are:

Table	Database fields or identifiers	Comments
For customer personal information cb_customersession	• cb_customeremail • cb_customername • cb_customerRegistered • cb_customersysteminfo	-

Table continues…

Table	Database fields or identifiers	Comments
For auditing information cb_auditlogs	• cb_auditcssselector • cb_auditelementdisplayname • cb_auditelementvalue	The fields in this table maintains the information of a webpage element and its value, which an agent changes while the agent is in control during a co-browse session. You can use this information later to audit the data that the agent enters or updates on behalf of the customer. The fields or identifiers are: • cb_auditcssselector: The value to find the co-browse webpage element. • cb_auditelementdisplayname: The display name of the selected element. • cb_auditelementvalue: The co-browse webpage value that the agent enters on behalf of the customer.

Chapter 7: Performance

Capacities and scalability

Avaya Co-Browsing Snap-in supports 400 concurrent sessions on a two-node Avaya Breeze® platform, and supports 1200 sessions per hour.

One co-browse node supports 200 sessions.

Deployment	Maximum number of nodes	System Configuration Per Node	Average Concurrent Sessions	Average Sessions Per Hour
Avaya Breeze® platform nodes	2	4vCPUs, 8 GB RAM, and 100 GB HDD	400	1200

Note:

If your database size goes beyond 12 GB, you must purge the database. You can use the relevant purging procedures for the respective database. Ensure that you delete or purge the data from the cb_cobrowsesessiontable after you finish deleting or purging data from all other tables.

Chapter 8: Reports

Reports

A user with administrator rights can generate reports in Avaya Co-Browsing Snap-in. The supported browsers for generating these reports are Internet Explorer 11, Google Chrome, and Mozilla Firefox.

The reports are for reference only and you can generate and view three types of reports:

- Session Summary: Provides information about the sessions initiated by customers and agents.
- Agent Summary: Provides information about the sessions initiated by agents.
- Customer Summary: Provides information about the sessions initiated by customers.

Generating reports

About this task

Use this procedure to generate the following types of reports:

- Session Summary
- Agent Summary
- Customer Summary

Before you begin

You must have administrator rights to generate or view a report.

Procedure

1. On the Avaya Co-Browsing Snap-in admin url, click the report type that you want to generate.

   The Home page displays the search data fields required to generate the report.

2. To begin the search, use the following search criteria:

   a. To search records based on the status, click one of the option in the **State** field.

The options are:

- **All**: Displays open sessions with the start date and closed sessions with the start date and end date.
- **Open**: Displays open sessions with the start date only and the active sessions.
- **Close**: Displays all closed sessions.

b. To search records based on the start date and time of the session, click the calender in the **Start Date** field and select the time using the up and down arrows.

c. To search the records based on the end date and time of the session, click the calender in the **End Date** field and select the time using the up and down arrows.

d. To search records based on a specific agent, type the name of the agent in the **Agent Name** field.

   If you filter records for an agent named `ABC`, the respective report page displays all the reports where the name is equal to `ABC` or contains `ABC`.

e. To search records based on a specific customer, type the name of the agent in the **Customer Name** field.

   If you filter records for a customer named `XYZ`, the respective report page displays all reports where the name is equal to `XYZ` or contains `XYZ`.

f. To generate the report based on the selected filters you select, click **Submit**.

Next steps

If the report fetches more than 2000 records at a time and displays an error message, you must refine the search criteria.

Session Summary report

Field	Description
Session Key	A unique system-generated key to identify a session. You can click the session key to view information related to a specific session as follows: • Action By: Displays whether the action was performed by the agent or the customer. • Action: Displays all actions that the agent or the customer performs. • Timestamp: Displays the timestamp when the agent or the customer performed an action.
Customer Name	The name of the customer who initiated or joined the session.
Agent Name	The name of the agent who initiated a session or joined a session.

Table continues…

Field	Description
Session Status	The status of the session that indicates whether the session is closed, idle, waiting for customer, waiting for agent, or in progress.
Duration	The duration between the start and end of the session, in seconds.
Start	The timestamp for the start of the session.
Stop	The timestamp for the end of the session.
Initiated By	The information whether the agent or the customer initiated the session.
Ended By	The information whether the agent or the customer ended the session.
Events	The events for the session. You can view all events performed by the agent for the duration of the session. The events details are: • Event type: The type of activity performed. For example, if you enter a value in a field, the event type is text. • Event name: The actual activity performed. For example, if you enter a value in a field, the event name is keyup. • Element ID: The field that was changed. For example if you enter a value in the first name field, the element ID is first_name. • Element value: The actual value entered in the field. For example if you enter a value in the first name field as Joe, the element value is Joe. • CSS Selector: The CSS selector specified or the element ancestors. • Event By: Displays whether the activity was performed by an agent or a customer. For example, if the agent entered a value in a field, the event by is `agent`. • Timestamp: Displays the time when the activity is performed in hh:mm:ss. For example, 15:00:30.

Icon	Description
≡	To button to hide columns in the report. The columns with a check mark are displayed in the report. You can also export the report columns using the following options: • **Export all data as csv**: The system exports all the columns in a `csv` file. • **Export visible fields as csv**: The system exports only the visible columns in a `csv` file. If you hide certain columns, the file does not export the hidden columns. • **Export visible data as pdf**: The system exports only the visible columns in a `pdf` file. If you hide certain columns, the system does not export the hidden columns. **Note:** You can export only selected rows from the report in a csv. If you select specific rows, the report displays one additional options for export: • **Export selected data as csv**: The report exports only the selected rows in a `csv` file. If you hide certain columns, the report does not export the hidden columns.

Agent Summary report

Field	Description
Agent Name	The name of the agent who initiated a session.
Session Key	The unique system-generated key used to identify a session.
Customer Name	The name of the customer who initiated a session or joined a session.
Session Status	The status of the session whether it is closed, idle, waiting for customer, or in progress.
Agent Device	The device that the agent used to initiate the session. **Note:** If the agent device is running Internet Explorer 10 in compatibility view, then the report page displays the agent device as Internet Explorer 7.0.
Duration	The duration of the session from the start to the end of the session in seconds.
Start	The timestamp when the session started.
Stop	The timestamp when the session ended.
Agent Last Activity Time	The timestamp when the agent performed the last activity.
Initiated By	The information whether the customer or the agent initiated the session.
Ended By	The information whether the customer or the agent ended the session.

Icon	Description
≡	To hide columns in the report. The columns with a check mark are displayed in the report. You can also export the report columns. You can export the columns by using the following options: • **Export all data as csv**: The report exports all the columns in a `csv` file. • **Export current data as csv**: The report exports only the visible columns in a `csv` file. If you hide certain columns, the report does not display the hidden columns in the file. • **Export current data as pdf**: The system exports only the visible columns in a `pdf` file. If you hide certain columns, the report does not display the hidden columns in the file. **Note:** You can export only selected rows from the report in a csv. If you select specific rows, the report displays one additional options for export: • **Export selected data as csv**: The report exports only the selected rows in a `csv` file. If you hide certain columns, the report does not export the hidden columns.

Customer Summary report

Field	Description
Customer Name	The name of the customer who initiated a session.
Session Key	The unique system-generated key used to identify a session.
Agent Name	The name of the agent who initiated a session or joined a session.
Session Status	The status of the session whether it is closed, idle, waiting for customer, or in progress.
Customer Device	The device which the customer used to initiate the session. **Note:** If the customer device is running Internet Explorer 10 in compatibility view, then the report displays the customer device as Internet Explorer 7.0.
Duration	The duration of the session from the start to the end in seconds.
Start	The timestamp when the session started.
Stop	The timestamp when the session ended.
Customer Last Activity Time	The timestamp when the customer performed the last activity.
Initiated By	The information whether an agent or a customer initiated the session.
Ended By	The information whether an agent or a customer ended the session.

Icon	Description
≡	The button to hide columns in the report. The columns with a check mark are displayed in the report. You can also export the report columns. You can export the columns as: • **Export all data as csv**: The report exports all the columns in a `csv` file. • **Export current data as csv**: The report exports only the visible columns in a `csv` file. If you hide certain columns, the report does not export the hidden columns to the file. • **Export current data as pdf**: The report exports only the visible columns in a `pdf` file. If you hide certain columns, the report does not export the hidden columns to the file. **Note:** You can export only selected rows from the report in a `csv`. If you select specific rows, the report displays one additional option for export: • **Export selected data as csv**: The report exports only the selected rows in a `csv` file. If you hide certain columns, the report does not export the hidden columns.

Viewing reports results

About this task

Use this procedure to modify the way you view report results.

Note:

You cannot make any changes to the data in the reports. The reports are available in the view-only mode.

Procedure

1. To filter the records within the reports, ensure that the **Filter** option is set to `Enable`.
   - If you select more than one fields to filter the records, then use the AND condition AND. For example, if you filter records based on the agent name and session status, the reports page displays only those records that match both the filter criteria.
   - To filter records using fuzz match, use asterisk (*) . For example, if you type `*us*` in the **Initiated By** field, the report displays all records that contain `us`.
2. To sort a column, click the ⌄ icon in the column and then do the following:
   - To sort in the ascending order, click **Sort Ascending**.
   - To sort in the descending order, click **Sort Descending**

If you sort the report for more than one columns, then use the AND condition. For example, if you sort the first name as ascending and the last name as descending, then the record displays the first name as ascending and the last name as descending.

3. To hide a column, click the icon in the column, and click **Hide Column**.
4. To unhide a column, click the icon, and click the desired column.
5. To view the changes done during the session, click **Refresh**.

Chapter 9: Troubleshooting

Failed installation

If the installation of Avaya Co-Browsing Snap-in fails:

- Ensure you have configured all database related attributes.
- Check any existing alarms for service level alarms.

You must make the necessary changes to the attributes from System Manager or handle the alarms and then restart the **Avaya Breeze®** server, or the WebSphere node for the changes to take effect.

Fails to run after database reboot

Avaya Co-Browsing Snap-in is in failed state after Oracle database reboot

Service install status in Avaya Breeze®	`Avaya Co-Browsing snap-in is in "failed to run" state after Oracle database reboot.`
Log file message text	`ORA-01017: invalid username/password; logon denied`
Log file	`CoBrowse.log`

Problem description

Avaya Co-Browsing Snap-in changes over to "failed to run" state if you reboot the Oracle database.

Solution

1. Unlock the Oracle user using *oracle client* or any other utility. For example, **`ALTER USER username ACCOUNT UNLOCK;`**
2. In System Manager, retype the Oracle password under the **Home** > **Elements** > **Avaya Breeze®** > **Configuration** > **JDBC Sources**.
3. Click **Commit**.
4. Reboot the Avaya Breeze® platform server instances via System Manager.

Alarms

Overview

Avaya Co-Browsing Snap-in generates alarms when any error occurs. The system sends a self-service email to the configured email address.

You can view, search, filter, export, and configure alarms from the System Manager web interface. Alarm information is available on the **Services** > **Events** > **Alarms** page in System Manager. For more information, see *Maintaining and Troubleshooting Avaya Aura® Avaya Breeze® platform* at https://support.avaya.com/.

Alarm severities

Severity	Description
Critical	Critical alarms identify failures that are causing the service to stop. These alarms require immediate action.
Major	Major alarms identify failures that are causing a critical degradation of service. These alarms require immediate attention.
Minor	Minor alarms identify failures that are causing service degradation. These failures do not cause the system to be inoperable.

Alarm status

Status	Description
Raised	An alarm has been generated. Software recovery actions have failed to correct the problem.
Cleared	The problem has been fixed and the alarm has been cleared. The alarm can be auto clear or you might have to clear the alarm manually.

Attribute value failed to initialize

Alarm text	`Attribute Service initializing is failed`
Alarm ID	`CoBrowse_ATTR_ERR_001`
Alarm level	Minor
Trigger component	While installing the cobrowse service, if attribute service is unable to get the data or registration fails with Avaya Breeze® platform

Problem description

The attribute service fails to initialize as the attribute service is unable to get the data or registration fails with Avaya Breeze® platform.

Solution

1. Check the process status of Avaya Breeze® platform.
2. Start the particular process if the process is in failed state.

Invalid value reported for attribute

Alarm text	`Invalid value reported of attribute: {1}. Set default value as {2}`
Alarm ID	`CoBrowse_ATTR_ERR_002`
Alarm level	Minor
Trigger component	The administrator sets an invalid attribute value in System Manager.

Problem description

The system reports an invalid attribute value from System Manager. For example string value for Inactivity timeout.

Solution

Ensure that the attribute has a valid and correct value in System Manager.

Avaya Breeze® platform license service failed to initialize

Alarm text	`License Service initializing is failed`
Alarm ID	`CoBrowse_LIC_ERR_003`
Alarm level	Minor
Trigger component	Licenser service from Avaya Breeze® platform

Problem description

The system logs the license service in error mode, if the licenser service is unable to get the service license data from Avaya Breeze® platform while installing Avaya Co-Browsing Snap-in.

Solution

Check Avaya Breeze® platform licenser service.

Server unable to reach Cobrowse database

Alarm text	`Cobrowse database may be down or database related attributed might be configured incorrectly`
Alarm ID	`CoBrowse_DB_ERR_001`
Alarm level	Critical
Trigger component	• Case1: The cobrowse service unable to connect the cobrowse database. • Case2: The cobrowse service is running but the cobrowse database in unavailable.

Problem description

The system can raise this alarm in two cases:

- Case1: The cobrowse service unable to connect the cobrowse database during the installation of the cobrowse service.
- Case2: The cobrowse service is running but the cobrowse database in unavailable.

Solution

1. Ensure you have configured a correct value for the database attribute on System Manager.
2. Ensure that the cobrowse database is available and can communicate with the cobrowse server.

Unable to load localization property

Problem description

Alarm text	`Unable to load localization property`
Alarm ID	`PROP_ERR_001`
Alarm level	Critical
Trigger component	

Cause

The system logs the error when the properties file is not defined correctly.

Solution

1. On the System Manager Home page, in **Elements**, select **Avaya Breeze®** > **Configuration** > **Attributes**.

2. Click the **Service Globals** tab.
3. In **Service** , click the service that contains the attributes that you want to configure.

   The table displays all attributes that you can configure for a CoBrowse service with the description of each attribute.
4. Click **Server Default Locale** and do the following:
   a. Click **Override Default**.
   b. In the **Effective Value** field, enter the new value or string.
5. Click **Commit** to save your changes.

   The cluster level service attributes persist after an uninstall from the cluster. The values are retained for a subsequent installation, so that you do not have to re-configure all attributes when changing service versions.

Related links

Runtime service configuration attributes on page 32

Oceana Monitor service and CoBrowse service messages

Oceana Monitor service messages

Message	Level	Description
OceanaMonitorService heartbeat started	INFO	Indicates that the heartbeat task has started
Platform details for node successfully written	INFO	Indicates that the platform details
Attribute Update: Authorization Required to view Monitor output set to '<VALUE>'	INFO	Displays if the 'Oceana token Serviceability Security' has been updated in System Manager.
OceanaMonitorService listening for attribute changes	INFO	Indicates that the internal attribute listener is working.
OceanaMonitorService service started	OK	Indicates the the OceanaMonitorService has started successfully.
OceanaMonitorService attribute listener stopped	INFO	Indicates that the internal attribute listener is working.
OceanaMonitorService service destroyed	INFO	Indicates the OceanaMonitorService is either successfully uninstalled or is shutdown.

CoBrowse service messages

Message	Level	Description
CoBrowse Service Starting	INFO	CoBrowse service installation is in progress.

Table continues…

Message	Level	Description
CoBrowse DB initialization successfully	INFO	CoBrowse service successfully connected with the database during start up.
CoBrowse license service initialization successfully	INFO	Verified that valid CoBrowse svar installed.
CoBrowse Service Started	OK	CoBrowse Service ready to accept the request.
CoBrowse Service Stopped	INFO	CoBrowse service undeployed successfully.
CoBrowse license service initialization failed	WARN	Some issue with CoBrowse loaded svar. Avaya Breeze® platform API failed to verify the service attributes.
Co_Browse attribute " %attributeName% new value changed as %attributeValue%	OK	Notification received when the below mentioned attributes will change with valid value. • CB.INACTIVE_TIMEOUT • CB.INACTIVE_TIMEOUT_MESSAGE • CB.SESSION_TIMEOUT
Co_Browse attribute %attributename% reverted with default value	WARN	Below attributes are configured with wrong value from System Manager. • CB.INACTIVE_TIMEOUT • CB.INACTIVE_TIMEOUT_MESSAGE • CB.SESSION_TIMEOUT
CoBrowse DB initialization failed	FATAL	CoBrowse service unable to connect to the database during start up. You need to verify the database server status and verify the database attributes of CoBrowse service. CoBrowse service status displays `Installing` for couple of minutes and finally goes to in failed state in System Manager.

Logging

Avaya Co-Browsing Snap-in log files

Avaya Breeze® platform provides a separate log file for Avaya Co-Browsing Snap-in. If more than one version of Avaya Co-Browsing Snap-in is installed, all logs gets stored in the same file.

Note:

If you set the logging on the Avaya Breeze® platform to OFF, the log level for Avaya Co-Browsing Snap-in is reset to INFO level. If you want to investigate the logs, select the logging level to Finer or Finest.

The following table describes the log name and location of the logs related to Avaya Co-Browsing Snap-in:

Log Name	Location	Description
Service installation or deployment logs	`/var/log/Avaya/sm/asm.log` `/var/log/Avaya/sm/deploy.log`	Validates the snap-in service installation or deployment logs.
Service logs	`/var/log/Avaya/services/CoBrowse/CoBrowse.log`	Validates the snap-in service logs.
Alarm logs	`/var/log/Avaya/services/event.log` `/var/log/Avaya/breeze/alarms.logs`	Validates the snap-in alarm logs.

You can modify the logging level for Collaboration Designer snap-ins on the System Manager Avaya Breeze® platform login page. You can view the details of each log, perform a search for logs, and filter specific logs. Use the `/opt/avaya/contrib/bin/ce` tool to enter commands for viewing logs, changing logs configuration.

For more information, see Maintaining and Troubleshooting Avaya Breeze® platform.

Chapter 10: Resources

Localization

Avaya Co-Browsing Snap-in supports localization for G14 languages. The agent or customer can select the preferred languages during session initiation and view the online help in each language.

Note:

Sample client and reporting are not localized and are available only in English. Avaya Co-Browsing Snap-in supports localization of server-side error messages only.

Online Help on sample client application is deployed in English. For deploying localization in other languages, you must configure the global attributes in the Runtime service configuration attributes table.

For more information on configuring localization attributes, see the Support Locale and the Server Default Locale rows in the “Runtime service configuration attributes” topic.

Related links

Configuring global attributes on page 32

Documentation

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

Title	Description	Audience
Avaya Co-Browsing Snap-in Release Notes	This document contains Avaya Co-Browsing Snap-in information that is not included in the Snap-in documentation. This document highlights known issues about Avaya Co-Browsing Snap-in with workarounds that are available.	Avaya Professional Services Implementation engineers
Avaya Co-Browsing Snap-in Database dictionary	This document provides the information about database schema.	Avaya professional services

Table continues…

Title	Description	Audience
Maintaining and Troubleshooting Avaya Breeze® platform	This document contains procedures to identify and troubleshoot problems for Avaya Breeze® platform.	Avaya Professional Services Implementation engineers
Avaya Breeze® platform Overview and Specification	This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Avaya Professional Services Implementation engineers Services and Support personnel System administrators
Administering Avaya Breeze® platform	This document provides the procedures to administer and configure Avaya Breeze® platform services.	Services and Support personnel System administrators
Administering Avaya Aura® System Manager	This document provides the procedures to administer and configure System Manager.	Services and Support personnel System administrators

See the following related documentation at the DevConnect site.

Title	Description	Audience
Avaya Co-Browsing Snap-in Developer and API Reference	This document provides a client library for users to write software that interacts with a deployed Avaya Co-Browsing Snap-in system.	Avaya Professional Services Implementation engineers Software developers

Training

The following courses are available for the Avaya Oceana® program.

Table 1: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya IX™ Contact Center Solutions for Sales			
41510W	Avaya IX™ Contact Center Portfolio Overview (for Sales)	0.75	Web-based Training
41550T	APSS Avaya IX™ Contact Center Solutions	1.0	Web-based Training
ALCC –2005 Avaya IX™ Voice and Digital Solutions for Sales			

Table continues…

Course code	Course title	Course duration in hours	Delivery type
41710W	The Avaya IX™ Contact Center Automated Story	0.50	Web-based Training
41410W	Selling Avaya Oceana®	0.75	Web-based Training
41400W	Selling Avaya Avalytics™	0.50	Web-based Training
41480W	The Basics of Cost Justification and Selling Avaya Oceana® Using the ROI Tool	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 2: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Design			
34210W	Avaya Oceana® Overview for Design	1.0	Web-based Training
34810W	Designing the Avaya Oceana® Part 1 of 3	1.0	Web-based Training
34820W	Designing the Avaya Oceana® Part 2 of 3	1.50	Web-based Training
34830W	Designing the Avaya Oceana® Part 3 of 3	1.50	Web-based Training
34800X	Avaya Oceana® Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39000W	Avaya Oceana® Release 3.8 Details for Pre-Sales	1.0	Portable Document Format (PDF)
39010W	Avaya Avalytics™ Release 3.8 and 4.1 Details for Pre-Sales	1.0	PDF
39020W	Avaya Breeze® Snap-Ins for Avaya Oceana® R3.8 Details for Pre-Sales	1.0	PDF

Table 3: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana®			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
7495X	Avaya Oceana® Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			

Table continues…

Course code	Course title	Course duration in hours	Delivery type
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
ACSS-7498 Avaya Analytics ™ Insights			
74360V	Integrating and Supporting Avaya Analytics™ R4	40.0	Virtual Instructor-Led Training
74980X	Avaya Analytics™ Insights Integration and Support Exam	1.75	Exam

Table 4: Pre-requisite Courseware

Course code	Course title	Course duration in hours	Delivery type
77900W	Avaya Control Manager Training Bundle (5 courses 21900W, 77910W, 77920W, 77930W, 77940W)	5.50	Web-based Training
70160W	Avaya Breeze® Implementation and Support	30.0	Web-based Training

Table 5: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Creating Avaya Oceana® Workspaces Framework for Developers	2.0	Web-based Training	

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
24150W	Avaya Workspaces Framework R3 Test	1.0	Online Test	
ASAC-0010 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Avaya Oceana® Administration Training	40.0	Virtual Instructor-Led Training	Attached with the sale
24300T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin
ASAC-0022 Administering Avaya Analytic™ for Avaya Oceana®				
24380W	Administering Avaya Analytics™ for Oceana®	1.5	Web-based Training	https://www.avaya.com/Oceana-analyticsadmin
24310T	Administering Avaya Analytics™ R3 for Oceana® Basic Online Teat	1.0	Web-based Training	

Table 6: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
70170W	Integrating Avaya Workspaces with Avaya Aura Call Center Elite	1.0	Web-based Training	
70170T	Avaya Workspaces for Elite Integration Online Test	1.0	Online Test	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

Table continues…

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
71610T	Proactive Outreach Manager with Avaya Oceana® Integration Online Test	1.0	Online Test	
ALEU-5005 Avaya Workspaces for Elite End User				
24120W	Using Avaya Workspaces for Elite – Agents	0.75	Web-based Training	https://www.avaya.com/elite-workspaces-agent
24140W	Using Avaya Workspaces for Elite – Supervisor	0.50	Web-based Training	https://www.avaya.com/elite-workspaces-supervisor

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Appendix A: About sample reference client

You can use the sample reference client to initiate co-browse sessions. The sample client does not support control keys and hot keys for navigation.

Note:

The context-sensitive menu of the sample client is browser-dependent. If the agent and customer are not using the same browser, they might not always see the same context-sensitive menu.

Agent initiated session

An agent can initiate a session or join a live session. For an agent initiated session, the system generates a session key and displays the session key on screen. The customer must use the key to join the session. An agent can initiate a session and cancel the session even after the session key is generated. The system cancels the session key and the agent can start a new session. An agent can request control from the customer. When an agent requests control, the customer can allow or deny sharing the control. The agent can logout from the session. If the agent, that is, the session owner is idle for some time, then the system automatically closes the session. You can configure the inactivity time out. The default value is 2 minutes.

Customer initiated session

A customer can initiate a session or join a live session. For customer initiated session, the system generates a session key and displays the session key on screen. The agent must use the key to join the session. The customer can pause and resume the current session. If the customer is in control of the session, the customer can pause a session. Only when the customer resumes the session, the changes made are synchronized and visible to the agent. The customer can stop the session. If the customer, that is, the session owner is idle for some time, then the system automatically closes the session. You can configure the inactivity time out. The default value is 10 minutes. While the agent is controlling the session, the customer can revoke the access at any point of time.

Configuring files for agent JavaScript on Tomcat server

Before you begin

Get the following information from your administrator:

- Network Parameters: Avaya Breeze® platform IP or FQDN, port, and TLS on or off
- Certificate for TLS connections to Avaya Breeze® platform

Procedure

1. Download the `SharingPackage_Javascript-3.x.0.0.xxxxxx.zip` file, where x is the release number for example 7 for release 3.7.
2. Unzip the file and copy the `sample/cobrowse_test_app` directory to `webapps/cobrowse_test_app`.
3. Configure the properties in the agent file `cobrowse_test_app/cobrowse/agent/js/app.js` as follows:

```
_cbconfig.serverInfo.hostName=<IP/hostname of cobrowse snap-in server>
_cbconfig.serverInfo.port=<port to access>
_cbconfig.serverInfo.isSecure=<true/false>
```

4. Restart the Tomcat server.
5. To access the sample agent URL, go to `http://<hostname:port>/cobrowse_test_app/cobrowse/agent`.

Configuring files for customer JavaScript on Tomcat server

Before you begin

Get the following information from your administrator:

- Network Parameters: Avaya Breeze® platform IP or FQDN, port, and TLS on or off
- Certificate for TLS connections to Avaya Breeze® platform

Procedure

1. Download the `SharingPackage_Javascript-3.x.0.0.0600032.zip` file., where x is the release number for example, 7 for release 3.7.
2. Unzip the file and copy the `sample/cobrowse_test_app` directory to `webapps/cobrowse_test_app`.
3. Configure the properties in the customer file `cobrowse_test_app/cobrowse/customer/js/app.js` as follows:

```
_cbconfig.serverInfo.hostName=<IP/hostname of cobrowse snap-in server>
_cbconfig.serverInfo.port=<port to access>
_cbconfig.serverInfo.isSecure=<true/false>
```

4. Restart the Tomcat server.
5. To access the sample agent URL, go to `http://<hostname:port>/cobrowse_test_app/cobrowse/customer`.

Configuring files for reports on Tomcat server

Before you begin

Get the following information from your administrator:

- Network Parameters: Avaya Breeze® platform IP or FQDN, port, and TLS on or off
- Certificate for TLS connections to Avaya Breeze® platform

Procedure

1. Download the `SharingPackage_Javascript-3.x.0.0.0600032.zip` file, where x is the release number for example, 7 for release 3.7.
2. Unzip the file and copy the `sample/cobrowse_test_app` directory to the `webapps/cobrowse_test_app`.
3. Configure the properties in the admin file `cobrowse_test_app/cobrowse/admin/js/app.js` as follows:

   ```
   var serverURL = 'https://<Avaya Breeze_cluster>/services/CoBrowse'
   ```

   , where

   `<Avaya Breeze_cluster>` is the URL of Avaya Breeze® platform on which the co-browse service is installed.
4. Restart the Tomcat server.
5. To access the sample reports website, go to `http://<hostname:port>/cobrowse_test_app/cobrowse/admin`.

   Note:

   Avaya Co-Browsing Snap-in provides ReST APIs to audit cobrowsing session information. The sample reports website is created using audit Rest APIs and does not use cobrowsing JavaScript SDK.

Index

Special Characters

_multiple end points / context name 12

A

Agent Summary report 55
alarm overview 63
alarm severities 63
assign the servers 26
attributes 32
AttributeValueFailedToInitialize 63
Avaya Co-Browsing Snap-in checklist
    checklist for Avaya Co-Browsing Snap-in 24
Avaya Co-Browsing Snap-in process flow 22
avaya cobrowse feature attributes 37
Avaya support website 75

B

browsers and devices supported 18

C

capacity
    scalability 54
    sessions 54
certificate based authentication overview 47
classname 30
Co-Browsing Snap-in
    Fulfillment of Data Subject Rights 48
    Privacy by Default 48
    Security of Processing 48
    Storage of Personal Data 48
configure attributes 39
configure attributes for Service Clusters 39
configure attributes for Service Globals 39
configure attributes for Service Profiles 39
configure certificate based authentication 47
configure global attributes 32
configuring
    agent JavaScript SDK 76
    co-browse user 30
    customer JavaScript SDK 77
    reports 78
configuring alarms 63
configuring licenses 21
Consent Management 52
cookie management 14
create
    Avaya Co-Browsing Snap-in cluster 26
creating JDBC provider and datasources 28
Customer Summary report 55

D

data encryption 51
data security 48
data subject rights fulfillment 49
database attributes 34
database error 65
database requirements 18
delete 43
delete a service Snap-in 42
delete personal data 49
deleting
    InterSystem Cache 50
deleting Avaya Co-Browsing Snap-in 43
document changes
    Issue 2 8
    Release 3.7 8

E

encrypt personal data 51
encypting
    Intersystems Cache database 49
export personal data 49

F

failed installation 62
feature
    Agent Browser Refresh 14
    Agent-initiated co-browsing 11
    AngularJS support 15
    annotation 13
    CSS3 support 12
    data marker 13
    data masking 11
    highlight text 11
    IFrame support 12
    multiple jQuery support 16
    Pseudo class elemen 14
    ReactJS support 15
    RTL support 16
    serviceability feature for Oceana monitoring 16
features
    customer-initiated co-browsing 10
filtering
    reports 60

G

generating
Agent Summary 55
Agent Summary report 55
Customer Summary 55
Customer Summary report 55
Session Summary 55
Session Summary report 55
global attributes 32

H

hiding
report columns 60

I

install a WebLM license on System Manager 27
install Avaya Co-Browsing Snap-in 37
install the services 26
installation failed 62
intended audience 8
Intersystem Cache database 30
Intersystem Cache database for Oceana 30
InvalidAttributeValue 64

J

jdbc provider 30
JDBC provider and datasources 28

L

license configuration 21
license requirements 20
license service 64
load Avaya Co-Browsing Snap-in 27
localization 69
logs
realtimespeech 67

M

Marker tool 13
modify personal data 49

O

omnichannel attributes 36
overview 9

P

personal data access 49
personal data minimization 49
personal data retention 49
port matrix 48
port utilization 48
preferred version
preferred upgrade option 42
prerequisites 9
process flow for Avaya Co-Browsing Snap-in 22

R

report
Agent Summary 58
Customer Summary 59
Session Summary 56
reports 55
generating 55
requirements 18
restrict personal data 49
right to left script 16
Rights of the data subject 49

S

sample client 76
secure data 48
security overview 46
server API endpoints 44
Service Clusters tab 39
Service Globals tab 39
service profile 42
Service Profiles tab 39
service start 38
service stop 38
Session Summary report 55
setting
Intersystem cache 31
Setting job scheduler
delete InterSystem Cache 50
sorting
report columns 60
Storage of Personal Data 52
support 75
supported browsers and devices 18
supported databases 18
system requirements 18

T

training 70

U

unable to load localization 65
uninstall a service Snap-in 42
uninstallation 42, 46

uninstalling Avaya Co-Browsing Snap-in 42
uninstalling service snap-ins 46
upgrade 40, 42
upgrading Avaya Co-Browsing 40

V

verify
    deployment 39
videos 74