Avaya Co-Browsing Snap-in Reference

Release 3.0
Issue 1
September 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on 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: http://support.avaya.com 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.

Licenses

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

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

License types

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

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

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, 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: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://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: http://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: Avaya Co-Browsing overview and features

Intended audience

This document is intended for people who want to install, configure, and administer Avaya Co-Browsing Snap-in. A web component developer with knowledge of Java script, jQuery, HTML, and Cascading Style Sheets (CSS) can use this document to integrate Avaya Co-Browsing Snap-in with the web site that wants to support co-browsing functionality. This document contains specific information about this Snap-in. For an overview of the Avaya Engagement Development Platform, see the *Avaya Engagement Development Platform Overview and Specification*. For general information about Engagement Development Platform Snap-in deployment, see *Quick Start to Deploying Avaya Engagement Development Platform Snap-ins*.

Overview

Avaya Co-Browsing Snap-in provides a set of consolidated services for sharing a webpage session. Using Avaya Co-Browsing Snap-in, two users can browse the same webpages simultaneously to collaborate and accomplish certain tasks. The agent can assist the customer to navigate through the webpages and, if required, in filling out forms.

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 runs on the Engagement Development Platform 3.1 SP1 platform, and you do not need to install any additional software or plug-in to use the snap-in.

Avaya Co-Browsing Snap-in provides the following functionality:

- A standard REST Web Service API to provide access to the Avaya Co-Browsing Snap-in services. For more information about different APIs, see *Avaya Co-Browsing Snap-in Developer's Guide* on the Avaya Support site at https://support.avaya.com.
- A developer SDK, including a sample reference client, that provides co-browsing capabilities.
- Out-of-the box summary reports about agents, sessions, and customers.

Features

Customer-initiated co-browsing

A customer can start a co-browsing session to seek assistance from the agent. The customer must share the system-generated session key with the agent so that the agent can join the session. The session key is an eight-digit number and must have a space between four digits. For example, “1234 5678”.

In case of a customer-initiated session, after the session key is generated, the system displays a modal window. If the customer closes the modal window without sharing the session key with the agent, the session is still active as the customer auto-joins the session. The user name you specify cannot be more than 30 characters long and has to be separated with a space after the first 8 characters. For example, “Abcdefgh ijklmn”.

Agent-initiated co-browsing

An agent can start a co-browsing session to assist the customer. The agent must share the system-generated session key with the customer so that the customer can join the session. The session key is an eight-digit number and must have a space between four digits. For example, “1234 5678”. The user name you specify cannot be more than 30 characters long and has to be separated with a space after the first 8 characters. For example, “Abcdefgh ijklmn”.

Two-way co-browsing

The customer can give control of the co-browsed webpage to an agent for assistance. By default, an agent has view-only permission to a co-browsed webpage. The agent can request permission to control or the customer can promote the agent to control the webpage. During the period in which the agent has control, the agent gains restricted access to the webpage. The customer can revoke control from the agent at any point of time or the agent can voluntarily release control.

Note:

The locale settings of the session are set by the session initiator. The joining party cannot override the locale settings. If the session has not started, the locale settings default to the locale settings on System Manager. The local settings are configurable through System Manager.

An agent can cancel the session even after the agent generates a session key. The customer is always auto-joined in the session.

Note:

When a session starts, the session owner can select values from the drop-down list. Depending on the available values, the session controller sees the values in the drop-down list. The system does not display all values in the list to the other party. The right-click Windows context-sensitive menu is browser-dependent. Therefore the agent and customer will not see the same right-click Windows context-sensitive menu.

Data masking

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.

Note:

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

Highlight text

The customer or agent can highlight static text. The highlight functionality is configurable and can be enabled or disabled. The highlight color is configurable. If the customer is in control of the co-browse session and highlights some text, the highlighted text is visible to the agent. If the agent is in control of the co-browse session and highlights some text, the highlighted text is visible to the customer. If the customer pauses a session after highlighting text, the highlighted text remains visible to the agent. If the customer cancels the highlight after pausing the session, the change is not visible to the agent till the customer resumes the session. The highlighted text disappears automatically if the session control is passed on from the agent and the customer or vice versa. The highlighted text disappears automatically if the agent or the customer clicks or double-clicks the mouse button.

Note:

Elements such as textbox, text area, or select box do not support highlighting of text. The customer or agent can highlight only through mouse selection or a double-click.

Chapter 2: 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 Engagement Development Platform	3.1 SP1
Avaya Aura® System Manager	System_Manager_R7.0_Sprint_9_7903878

Supported browsers and devices

Supported browsers

- Microsoft Internet Explorer 10 and 11
- Mozilla Firefox 39
- Google Chrome 44
- Safari (Mac) 8.0

Important:

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

Supported devices

Devices	Operating system	Browser
Apple iPad	iOS 8.0	Safari 8.0
Android tablets with display size greater than 7 inches	Android 5.0	Chrome 44

Table continues…

Devices	Operating system	Browser
Apple iPhone with display size greater than 5 inches	iOS 8.0	Safari 5.1
Android-based mobile devices with display size greater than 5 inches	Android 5.0	Chrome 44

Database requirements

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

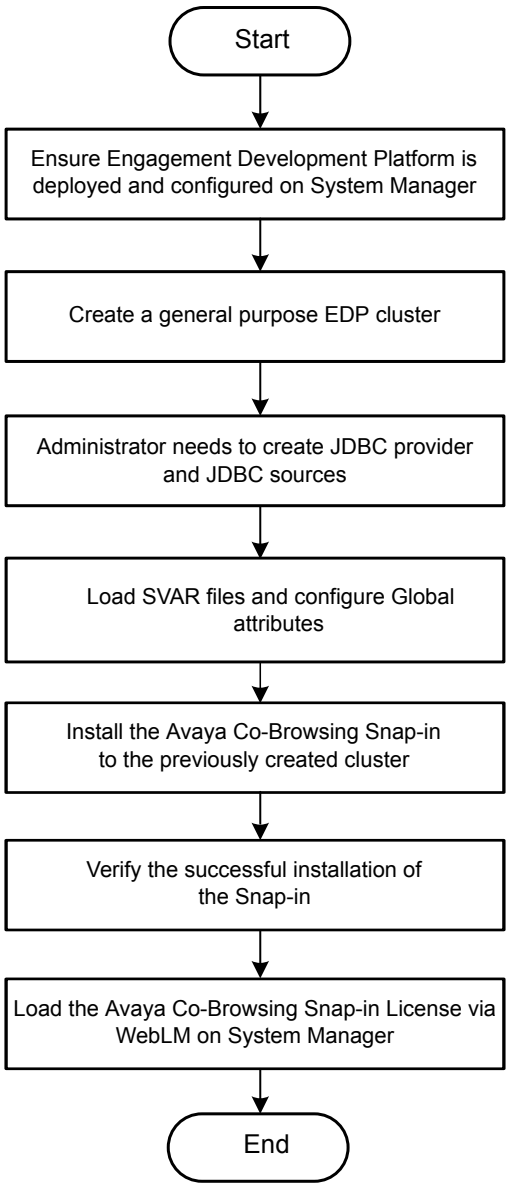
- Oracle 11g
- MS SQL Server 2014
- PostgresSQL

Hardware requirements

The Avaya Co-Browsing Snap-in hardware requirements are based on the Engagement Development Platform and System Manager requirements. For more information, see the respective product documentation. In addition, you need Avaya Engagement Development Platform with 4 vCPU and 8 GB of RAM.

Chapter 3: Avaya Co-Browsing Snap-in deployment

Avaya Co-Browsing Snap-in process flow



Avaya Co-Browsing Snap-in deployment checklist

No.	Task	Notes	✔
1	Ensure that Avaya Aura® System Manager is running.	None.	
2	Install and configure the Avaya Engagement Development Platform server.	Before turning on the Engagement Development Platform server, ensure that you set the memory to 8 GB of RAM.	
3	Create a Avaya Co-Browsing Snap-in cluster.	Assign a Engagement Development Platform server to the Avaya Co-Browsing Snap-in cluster. **Note:** When you administer a new Engagement Development Platform server, you must add the server to a cluster. If not, the Engagement Development Platform asset is not usable. Ensure that you have enabled **Only allow HTTPS traffic** checkbox.	
4	Download the Avaya Co-Browsing Snap-in services from PLDS.	The Avaya Co-Browsing Snap-in services are available as Service Archive (SVAR) 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 more information about this, see Creating JDBC Providers DataSources on page 16.	
7	Configure global attributes.	For more information about this, see Configuring Global Attributes on page 18.	
8	Load the Avaya Co-Browsing Snap-in license via WebLM.	None.	
9	Install Avaya Co-Browsing Snap-in.	None.	
10	Verify the installation.	None.	
11	Configure alarms on System Manager.	None.	

Prerequisites

Before you install Avaya Co-Browsing Snap-in, ensure you plan for the following:

- A working web-site which can use co-browsing functionality.
- Engagement Development Platform with System Manager installed and configured.
- If the deployment of your enterprise application mandates referring co-browsing application from a different domain, you must configure CORS on Engagement Development Platform. For more information, see CORS section in Certificate-based authentication overview on page 35.
- Analysis of the website for java scripts libraries. Customers might have site-specific javascripts enabled. In a co-browse session, some of these javascripts can cause unexpected behavior. The customers must closely analyze the javascripts and accordingly take action to ensure that the co-browse session does not display unwarranted behavior.
- NAMESPACE analysis of the website with the co-browse NAMESPACE for any potential conflict.
- Identify the secure fields and analyse which forms would be co-browse enabled.
- Create the JDBC provider and JDBC source. For more information, see Creating JDBC Provider and DataSource on page 16.
- Analysis of the webpages that would support co-browse and strategy for navigation between co-browse enabled pages and normal pages.
- Analysis of the events provided by the web SDK and handling of the events using APIs. For more information, see the *Avaya Co-Browsing Snap-in Developer and API Reference* guide on http://support.avaya.com.

Note:

Avaya Co-Browsing Snap-in on Engagement Development Platform supports only HTTPs traffic.

Creating an Avaya Co-Browsing Snap-in cluster

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
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.

Note:

You cannot select a new profile without canceling the page.

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 Engagement Development Platform*.
   c. **Description**: The description of the cluster.

   Ensure that you have enabled **Only allow HTTPS traffic** checkbox.
6. In the **Servers** tab, in the **Unassigned Servers** table, click the plus sign (**+**) next to the **Name** column to add the Engagement Development 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. In the **Services** tab, select the services to install on all servers in the cluster.
8. 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.
9. **(Optional)** To view the Engagement Development 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.
10. **(Optional)** To view the details of the Snap-ins installed on that instance, click a specific Engagement Development Platform instance in the cluster.

Important:

The customers can deploy the co-browse application on multiple nodes of an Engagement Development Platform cluster. If at least one node in the Engagement Development Platform cluster is active and accepting new requests, the cluster IP will service incoming requests. The actual Engagement Development Platform node handling the request is transparent to the API client.

Note:

The scope of the cluster support does not imply support for the following.

a. Load balancing: An even distribution of incoming requests to various nodes within the Engagement Development Platform cluster is not provided . The mechanism for even load distribution is Engagement Development Platform dependent.
b. High availability: A backup Engagement Development Platform node takes 5 to 7 minutes to start serving requests after the primary Engagement Development

Platform node is unable to serve requests. During this period, the cluster IP might be unable to service new requests.

c. Session preservation: Ongoing sessions being serviced by a particular node will not be preserved when that Engagement Development Platform node is no longer available to serve requests.

Installing Avaya Co-Browsing Snap-in

Loading Avaya Co-Browsing Snap-in

Before you begin

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

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.
3. On the Service Management page, click **Load**.
4. In the Load Service dialog box, click **Browse** and select the `Avaya Co-Browsing Snap-in<cecobrowsega-3.0.0.0.201>.svar` file.

   The system displays the `Avaya Co-Browsing Snap-in<version>.svar` file in the **Local PC** text field.
5. Click **Load**.

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

   System Manager adds the Avaya Co-Browsing Snap-in to the list of services.
7. On the **Engagement Development Platform** web interface, click **Service Management**, ensure the Avaya Co-Browsing Snap-in is in loaded state.

Creating JDBC providers and datasources

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.

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

Database	.jar file
Oracle	ojdbc6.jar
PostgreSQL	postgresql-9.0-801.jdbc4.jar
MS SQL Server	sqljdbc4-4.1.jar

Procedure

1. Login to **System Manager**.
2. Navigate to **Home** > **Engagement Development Platform** > **Configuration** > **JDBC Providers**.
3. 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 17.

   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 `.jar` file.
4. Navigate to **Home** > **Engagement Development Platform** > **Service Management**.
5. Search for the JDBC provider you created in step 3.
6. Select the provider and click **Install**.

   The system displays a popup list of clusters.
7. Select the cluster on which you want to install the provider and click **Commit**.
8. Navigate to **Home** > **Engagement Development Platform** > **Configuration** > **JDBC Sources**.
9. Create a datasource.
10. On the Datasource 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.
11. 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`.
12. Specify the database URL, username, and password to connect to the database.

13. 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.
14. 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.
15. 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.
16. Click **Commit**.
17. Verify that the connection to the database is working.

    You should be able to use the data source through the snap-in tool or Engagement Designer tool.
18. Reboot Avaya Engagement Development Platform server after test connection is successful.

Related links

JDBC Provider Class Name on page 17

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>:1521:<database name>` For example, `jdbc:oracle:thin:@101.133.72.26:1521:oracledb`
PostgreSQL	org.postgresql.jdbc2.optional.ConnectionPool	`jdbc:postgresql:// <Database server IP` Ensure you configure the following custom properties: • serverName • databaseName • portNumber: default is 5432 For example,`jdbc:postgresql://101.133.72.26`
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

Table continues…

Database	JDBC Provider Class Name	JDBC Sources sample DB URL
		For example, `jdbc:sqlserver://101.133.72.26`

Related links

Creating JDBC providers and datasources on page 16

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 **Engagement Development Platform** > **Configuration** > **Attributes**.
2. Click the **Service Globals** tab.
3. From the **Service** drop-down menu, select the service that contains the attributes you want to configure.

   The table displays all the attributes that you can configure for cecobrowsega. The table must include 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.

Note:

The cluster level service attributes persist after an uninstall from the cluster and the values are retained for subsequent install to ensure that you do not have to re-configure all of the attributes when changing service versions.

Avaya Co-Browsing Snap-in database attributes field descriptions

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
For MS SQL Server:		
Database Jndi Name	The name of the external database. You must use the JNDI name created in Creating JDBC Providers DataSources on page 16.	NA
Database Type	The external database type. The value is sqlserver.	NA
Database Dialect		org.hibernate.dialect.SQLServer Dialect
For Oracle:		
Database Jndi Name	The name of the external database. You must use the JNDI name created in Creating JDBC Providers DataSources on page 16.	NA
Database Type	The external database type. The value is oracle.	NA
Database Dialect		org.hibernate.dialect.Oracle10gDialect
For Postgres:		
Database Jndi Name	The name of the external database. You must use the JNDI name created in Creating JDBC Providers DataSources on page 16.	NA
Database Type	The external database type. The value is postgres.	NA
Database Dialect		org.hibernate.dialect.PostgreSQL Dialect

Important:

If you change any of the database attributes after installing Avaya Co-Browsing Snap-in, you must restart the Avaya Engagement Development Platform server, or WebSphere node for the changes to take effect. After the Avaya Engagement Development Platform server restarts, you must wait at least for 1 minute for the changes to take effect.

Timeout specific attributes

You can set the session inactivity time out values.

Name	Description
Inactive time out (minutes)	Displays the value in minutes. The system ends a session if the owner of the co-browse session is idle for the time, that is configured in Inactive time out (minutes). The default value is 2 minutes. The

Table continues…

Name	Description
	minimum value is 2 minutes and maximum value is 30 minutes.
Inactive time out (message)	The system displays the message after the system ends the session. You can add your custom message.
Session time out (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 gracefully. The default value is 60 minutes. The minimum value is 30 minutes and maximum value is 1440 minutes.

Server specific attributes

You can set server attributes.

Name	Description
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.
Supported locale	Displays the supported locales by the co-browse server. The default values are en_US, en_UK, de_DE, fr_FR. The co-browse session server can support the following locales: • en_US: English • de: German • fr: French • zh_CN: Chinese • es: Spanish • it: Italian • ja: Japanese • ko: Korean • pt_BR: Portuguese (Brazilian) • ru: Russian

Installing Avaya Co-Browsing Snap-in

Before you begin

- Load the Avaya Co-Browsing Snap-in.
- Ensure that you know the cluster name to install the Avaya 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** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.

   The system displays the Service Management page.
3. 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.
4. 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`.

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://<EDP_Security_IP>/services/cecobrowsega/v1/server/status`

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

   Note:

   Provide the Engagement Development Platform Entity IP address. Engagement Development Platform has two addresses, but the service is only available on the Entity IP address.

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

Configuring attributes for Avaya Co-Browsing Snap-in

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
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 cecobrowsega, 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 **cecobrowsega**.

      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.

      You can always restore the default by clearing the **Override Default** 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 Engagement Development 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 option.

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 **Engagement Development Platform** > **Service Management** page. For more information, see Setting Preferred Version on page 23.

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 Engagement Development 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 **Service Management** page.

Setting the preferred version for upgrades

Before you begin

Install the Snap-in service on Engagement Development Platform.

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.
3. Select the service that you want to set as the default version.
4. Select **Set Preferred Version**.

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

6. Click **Commit**.

   The **Preferred Version** column displays the clusters for which you have set the preferred version.

7. Verify whether the updated service can service requests successfully. For more information, see *Verifying Avaya Co-Browsing Snap-in deployment*.

Upgrading Avaya Co-Browsing Snap-in services

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.
3. On the **Service Management** page, click **Load**.
4. Click **Browse** next to **Local PC** to locate the latest Avaya Co-Browsing Snap-in service (.svar), and then click **Open**.

   The latest Service Archive (svar) file is provided by a service developer.

5. In the Load Service window, click **Load** to load the Avaya Co-Browsing Snap-in service.
6. On the End User License Agreement (EULA) page, click **Accept**.

   The Service Management page displays the service with the `LOADED` state.

7. To install the latest version of the Avaya Co-Browsing Snap-in service, perform one of the following steps:
   - On the **Service Management** page, select and install the latest version of the Avaya Co-Browsing Snap-in service.
   - On the **Cluster Administration** page, edit the cluster to select and commit the latest version of the Avaya Co-Browsing Snap-in service.
   - 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 **Service Management** 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.
8. Verify if the services are installed successfully. For more information, see *Verifying a Avaya Co-Browsing Snap-in deployment*.
9. **(Optional)** Uninstall the previous version of the service.
10. **(Optional)** Delete the previous version of the service.

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 Engagement Development Platform Postgres database. For more information, see Uninstalling Avaya Co-Browsing Snap-in on page 25.
- Delete a service Snap-in: When you delete a service, the system removes the attributes from the Engagement Development Platform Postgres database. For more information, see .Deleting Avaya Co-Browsing Snap-in on page 26.

Uninstalling Avaya Co-Browsing Snap-in

About this task

When you uninstall a service, the system removes the attributes from the **Engagement Development Platform** server.

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.
3. On the Service Management page, select the check box for **cecobrowsega** . Ensure that you select the correct version.
4. Click **Uninstall**.
5. Select the **Cluster Name** from which you want to install the **cecobrowsega** service.
6. Click **Commit**.

Next steps

To verify that the service is uninstalled, click **Elements** > **Engagement Development Platform** and perform the following steps:

1. On the Service Management page, verify that the **State** of the service is **Loaded**.
2. On the Cluster Administration page, perform the following steps:
   a. Click **Show**.
   b. Click the **Engagement Development Platform** 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 uninstalled. For more information, see *Uninstalling Avaya Co-Browsing Snap-in*.

About this task

When you uninstall a service, the system removes the attributes from the **Engagement Development Platform** server.

Procedure

1. On the System Manager web interface, click **Elements** > **Engagement Development Platform**.
2. In the left pane, click **Service Management**.
3. On the Service Management 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** > **Engagement Development Platform** and perform the following steps:

1. Click **Service Management**.
2. Verify that the Service Management page does not display the deleted service.

Chapter 4: Licensing

License overview

License requirements

To use Avaya Co-Browsing Snap-in, you must procure the valid Avaya Co-Browsing Snap-in and Engagement Development Platform license files.

Avaya Co-Browsing Snap-in uses the snap-in service licensing feature provided by Engagement Development 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.

Avaya Co-Browsing Snap-in contains a digital signature that the Engagement Development Platform Element Manager uses to confirm 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 the Avaya Co-Browsing Snap-in.

Configuring Avaya Co-Browsing Snap-in licenses

Before you begin

- Get the Avaya Co-Browsing Snap-in license from Avaya PLDS.
- You must get the primary HOST ID from the System Manager to generate the Avaya Co-Browsing license.

  Login to **System Manager**. Navigate to **Home** > **Services** > **Licenses** > **Server properties**.
- Ensure that the Avaya Co-Browsing Snap-in license is installed on the WebLM server that is integrated with System Manager.
- Ensure that the Engagement Development Platform platform license is installed on System Manager.

  In System Manager, click **Elements** > **Engagement Development Platform** > **Server Administration** to see the current status of each Engagement Development Platform server platform license.

About this task

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

Procedure

1. On the System Manager Home page, click **Services** > **Licenses**.
2. Select **Install License**.
3. Browse to the location of the Avaya Co-Browsing Snap-in license.
4. Select the license file and click **Install**.

   The system installs the license file.

   In the left navigation pane, the system displays Collaborative_Browsing_Snap_in in **Licensed Products**.
5. To verify if the license file is installed successfully:
   a. Click **Elements** > **Engagement Development Platform** > **Service Management**.
   b. In the **License mode** column, verify that the column displays a check mark for the Avaya Co-Browsing Snap-in mode.

      The following licensing modes apply to all Engagement Development Platform and Avaya Co-Browsing Snap-in licenses:

      - **License Normal Mode**: A valid license file is installed. The complete functionality is present for the Engagement Development Platform instance.
      - **License Error Mode**: License error is seen in this mode. The Engagement Development Platform instance is in a 30 day grace period during this mode. Complete functionality is available during the grace period. The system displays the warning icon along with the date and time of the grace period expiration in the **License Mode** column. If the grace period expires and the license error has not been corrected, the snap-in enters License Restricted mode and is uninstalled from all clusters.
      - **License Restricted Mode**: The Avaya Co-Browsing Snap-in instance goes in to the restricted mode after the 30 day grace period expires. As a result of this unresolved license error, the snap-in is in License Restricted mode and is uninstalled form 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 Engagement Development Platform, see *Administering Avaya Aura® Engagement Development Platform*.

      Engagement Development 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 thus takes maximum 9 minutes to reflect in the Engagement Development Platform Element Manager.

Chapter 5: Reports

Reports

The supported browsers for reports are Internet Explorer 11, Google chrome, and Mozilla firefox. You can generate and view three types of reports:

- Session summary report
- Agent summary report
- Customer summary report

Note:

The report fetches 2000 records at one time. If you want to refine the search, use the search criteria on Home page. If the report fetches more than 2000 records at one time, and error message is displayed, you need to further refine the search criteria. Use **Refresh** button to view the changes done during the session.

You can generate all reports based on the following search criteria on the respective home page:

Field	Description
State	Use to search the records based on the state. The states can be: • All: Displays all the open and the closed sessions. • Open: Displays all the open and active sessions. • Close: Displays all the closed sessions. For example , you can search records for all open sessions.
Start Date	Use to search the records based on the start date and time of the session. The date and time format is as per the ISO8601 format. For example, 2015-04-19T12:59:23Z
End Date	Use to search the records based on the end date and time of the session. The date and time format is as per the ISO8601 format. For example, 2015-04-19T12:59:23Z
Agent Name	Use to search the records based on a specific agent. For example, you can filter records for agent named “ABC”. The system displays all reports where the name is equal to “ABC” or contains “ABC”.

Table continues…

Field	Description
Customer Name	Use to search the records based on a specific customer. For example, you can filter records for agent named “XYZ”. The system displays all reports where the name is equal to “XYZ” or contains “XYZ”.
Submit	Use to generate the report based on the filters you select.

You can enable the filtering of the records, within the reports also. If you select more than one fields to filter the records, the condition is AND. For example, if you filter records based on agent name and session status, the system displays only those records that match both the filter criteria. You can use asterisk (“*”) to filter records using fuzz-match. For example, if you specify “*us*” in the **Intitiated By** field, then the system displays all records that contain “us”.

You can sort each column or hide a column in the report. If you sort the report on more than one columns, then the condition is AND. For example if you sort the first name as ascending and last name as descending, then the system first sorts the first name as ascending and then last name as descending.

Session Summary report

The report gives information about all sessions initiated by a customer and an agent. The following table lists all the columns:

Field	Description
Session Key	Displays the unique key used to identify a session. The session key is system generated. You can click the session key to view all information related to the specific session: • Action By: Displays whether the action was performed by the agent or the customer. • Action: Displays all actions performed by either the agent or the customer. • Timestamp: Displays the timestamp when the action was performed by the agent or the customer.
Customer Name	Displays the name of the customer who initiated a session or joined a session.
Agent Name	Displays the name of the agent who initiated a session or joined a session.
Session Status	Displays the status of the session whether it is closed, idle, waiting for customer, waiting for agent, or in progress.
Duration	Displays the duration of the session in seconds, that is, the time between the start of the session and stop of the session.
Start	Displays the timestamp when the session started.
Stop	Displays the timestamp when the session ended.
Initiated By	Displays whether the session is started by an agent or customer.
Ended By	Displays whether the session is ended by an agent or customer.

Table continues…

Field	Description
Events	Displays all the events for the session. You can view all the events performed by the agent for the duration of the session. The events details are: • Event type: Displays the type of activity performed. For example, if you enter a value in a field, the event type is text. • Event name: Displays the actual activity performed. For example, if you enter a value in a field, the event name is keyup. • Element ID: Displays the field which was changed. For example if you enter a value in the first name field, the element ID is first_name. • Element value: Displays 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: Displays either the CSS selector specified or the element ancestors. • Event By: Displays whether the activity was performed by an agent or 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. For example 15:00:30.
	Use 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 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 system 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 system displays one additional options for export: • Export visible data as pdf: The system exports only the selected rows in a .pdf file. If you hide certain columns, the system does not export the hidden columns.

Agent Summary report

The report gives information about all sessions initiated an by agent. The following table lists all the columns:

Field	Description
Agent Name	Displays the name of the agent who initiated a session.

Table continues…

Field	Description
Session Key	Displays the unique key used to identify a session. The session key is system generated.
Customer Name	Displays the name of the customer who initiated a session or joined a session.
Session Status	Displays the status of the session whether it is closed, idle, waiting for customer, or in progress.
Agent Device	Displays the device the agent used to initiate the session. **Note:** If the agent device is running Internet Explorer 10 in compatibility view, then the system displays the agent device as Internet Explorer 7.0.
Duration	Displays the duration of the session in seconds, that is, the time between the start of the session and stop of the session.
Start	Displays the timestamp when the session started.
Stop	Displays the timestamp when the session ended.
Agent Last Activity Time	Displays the timestamp when the agent performed the last activity.
Initiated By	Displays whether the session is started by an agent or customer.
Ended By	Displays whether the session is ended by an agent or customer.
	Use 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 system exports all the columns in a csv file. • Export current data as csv: The system exports only the visible columns in a .csv file. If you hide certain columns, the system does not export the hidden columns. • Export current 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 system displays one additional options for export: • Export selected data as csv: The system exports only the selected rows in a .csv file. If you hide certain columns, the system does not export the hidden columns.

Customer Summary report

The report gives information about all sessions initiated by a customer. The following table lists all the columns:

Field	Description
Customer Name	Displays the name of the customer who initiated a session.
Session Key	Displays the unique key used to identify a session. The session key is system generated.
Agent Name	Displays the name of the agent who initiated a session or joined a session.
Session Status	Displays the status of the session whether it is closed, idle, waiting for customer, or in progress.
Customer Device	Displays the device the customer used to initiate the session. **Note:** If the customer device is running Internet Explorer 10 in compatibility view, then the system displays the customer device as Internet Explorer 7.0.
Duration	Displays the duration of the session in seconds, that is, the time between the start of the session and stop of the session.
Start	Displays the timestamp when the session started.
Stop	Displays the timestamp when the session ended.
Customer Last Activity Time	Displays the timestamp when the customer performed the last activity.
Initiated By	Displays whether the session is started by an agent or customer.
Ended By	Displays whether the session is ended by an agent or customer.
	Use 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 system exports all the columns in a csv file. • Export current data as csv: The system exports only the visible columns in a .csv file. If you hide certain columns, the system does not export the hidden columns. • Export current 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 system displays one additional options for export: • Export selected data as csv: The system exports only the selected rows in a .csv file. If you hide certain columns, the system does not export the hidden columns.

Chapter 6: Performance

Capacities and scalability

Avaya Co-Browsing Snap-in supports up to 100 concurrent agent and customer sessions.

Table 1: Capacity and scalability

Specification	Capacity	Description
Maximum number of concurrent sessions	100	At any given point of time, Avaya Co-Browsing Snap-in supports 100 simultaneous sessions.
Maximum Number of request	420 Busy hour call completion (BHCC)	Avaya Co-Browsing Snap-in supports 420 sessions for busy hour call
Maximum number of session in day	10,000	Avaya Co-Browsing Snap-in supports maximum 10,000 session in day, that is, in 24 hours.

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/purge the data from the cb_cobrowsesessiontable after you finish deleting/purging data from all other tables.

Chapter 7: Security

Security overview

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

For more information about the security configuration, see the *Engagement Development Platform* and *System Manager* product documentation.

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 in Engagement Development Platform Element Manager. The configuration is available on the **Engagement Development Platform** > **Configuration** > **HTTP Security** page.
- Create a client keystore.
- Download the Engagement Development 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 *Engagement Development 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 JAVA scripts from an application server that can send HTTPS requests to an Engagement Development Platform instance.

The configuration is available on the **Engagement Development Platform** > **Configuration** > **HTTP Security** page → **HTTP CORS**.

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

For more information, see the *Engagement Development 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. Hence, the system does not send the required client certificate.

Whitelist

Engagement Development Platform accepts HTTPS requests only from the IP Addresses listed in the table. If you do not select this (whitelist enable checkbox), Engagement Development 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, see Data masking in *Avaya Co-Browsing Snap-in Developer and API Reference* guide.

Port utilization

For Avaya Co-Browsing Snap-in port information, see the *Avaya Engagement Development Platform 3.1 SP1 Port Matrix document* at https://support.avaya.com/security.

Chapter 8: 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 Engagement Development Platform 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 Engagement Development Platform	`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	`cecobrowsega.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** > **Engagement Development Platform** > **Configuration** > **JDBC Sources**.
3. Click **Commit**.
4. Reboot the Engagement Development 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® Engagement Development 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 `CECoBrowseGA_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 Engagement Development Platform

Problem description

The attribute service fails to initialize as the attribute service is unable to get the data or registration fails with Engagement Development Platform.

Solution

1. Check the process status of Engagement Development 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	`CECoBrowseGA_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.

Engagement Development Platform license service failed to initialize

Alarm text	`License Service initializing is failed`
Alarm ID	`CECoBrowseGA_LIC_ERR_003`
Alarm level	Minor
Trigger component	Licenser service from Engagement Development 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 Engagement Development Platform while installing Avaya Co-Browsing Snap-in.

Solution

Check Engagement Development 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	`CECoBrowseGA_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

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

Problem description

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

Solution

Check the configuration of the properties file.

Logging

Avaya Co-Browsing Snap-in log files

Avaya Engagement Development 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 are stored to the same file.

Note:

If you set the logging on the Avaya Engagement Development 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/deployment logs	`/var/log/Avaya/sm/asm.log`	Validates the snap-in service installation/ deployment logs.
Service logs	`/var/log/Avaya/services/cecobrowsega/cecobrowsega.log`	Validates the snap-in service logs.
Alarm logs	`/var/log/Avaya/services/event.log`	Validates the snap-in alarm logs.

You can modify the logging level for Collaboration Designer snap-ins on the System Manager Engagement Development 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 Engagement Development Platform.

Chapter 9: Additional resources

Localization

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

Note:

Sample client and reporting application 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 language. For more information about on how to deploy localization for other languages, see Avaya Co-Browsing Snap-in Reference Guide.

All the localized help files are under `client\help\`. All the agent and client zip files are under `client\help\` folder. In the default setup of Avaya Co-Browsing Snap-in, English localized files for the client are under `client\demo\CoBrowseOLHCustomer\` and for the agent are under `client\agent\CoBrowseOLHAgent\`.

If you want to test the localized help files, depending on your preferred languauge, extract the zip files from the `client\help\` to the respective client or agent folder.

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

Table continues…

Title	Description	Audience
Maintaining and Troubleshooting Avaya Engagement Development Platform	This document contains procedures to identify and troubleshoot problems for Avaya Engagement Development Platform.	Avaya Professional Services Implementation engineers
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
Avaya Engagement Development 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 Engagement Development Platform	This document provides the procedures to administer and configure Engagement Development 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
Database dictionary	This document provides the information about database schema.	Avaya professional services

Support

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

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.

Ensure you configure the HTML pages, and the `app.js` file on the agent and user end as mentioned below:

Configuration file for customer JavaScript SDK — customer/js/app.js

```
AV.COBROWSEAPI.setServerURL('https://<edp_cluster>/services/cecobrowsega')
```

where

`<edp_cluster>` is the URL of the Engagement Development Platform where co-Browse service is installed.

Configuration file for agent JavaScript SDK — agent/js/app.js

```
AV.COBROWSEAPI.setServerURL('https://<edp_cluster>/services/cecobrowsega')
```

where

`<edp_cluster>` is the URL of the Engagement Development Platform where co-Browse service is installed.

Configuration file for admin JavaScript SDK — admin/js/app.js

```
var serverURL = 'https://<edp_cluster>/services/cecobrowsega'
```

where

`<edp_cluster>` is the URL of the Engagement Development Platform where co-Browse service is installed.

Note:

Post deployment of client package, verify if the chosen deployment folder and the path given in `loader.js` files match. As best practice, do not copy multiple copies of client package in the webapp folder. This ensures there are no cross-references of client files from various folders.

Index

U

V