Avaya Solution & Interoperability Test Lab

Application Notes for CBA Live Assist with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CBA Live Assist to interoperate with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1.

CBA Live Assist WebRTC embeds based High Definition (HD) voice and video calling inside mobile apps and websites. It avoids browser plugins, integrate natively with iOS and Android and support escalation to co-browsing, with integration to existing systems.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for CBA Live Assist to interoperate with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1.

CBA Live Assist WebRTC embeds various CBA Live Assist functions such as voice and video calling inside mobile apps and websites. It avoids browser plugins, integrate natively with iOS and Android and support escalation to co-browsing, with integration to existing systems. In the compliance testing, the back-end system of CBA Live Assist uses a Web Gateway with a Media Broker to integrate with Avaya Aura® Session Manager for connection to devices on Avaya telephony network with audio and/or video. The Web Gateway is part of the Fusion Client SDK (FCSDK) solution and runs on Fusion Application Server (FAS). The Media Broker runs independently of the Fusion Application Server and is responsible for the media transcoding and RTP routing between the client applications and SIP network, though it can be installed on the Fusion Application Server for small setups, as was done for compliance testing.

An FCSDK application communicates with the Web Gateway on a WebSocket, using WebRTC to send signaling and media (voice and video) traffic. The Gateway can then transform the signaling to send the same voice and video to a SIP server such as Session Manager, which sends it to Communication Manager before routing to an endpoint capable of video (such as a Vantage™ or Avaya Workplace Client). If the endpoint is not capable of video, there will only be audio.

Testing was performed using Chrome browser on PCs, mobile android FCSDK native app and iOS FCSDK native app for inbound calls.

2. General Test Approach and Test Results

The feature test cases were performed manually. Only inbound calls with CBA Live Assist were manually established with an Avaya H.323 endpoint, Avaya SIP endpoint, Avaya Vantage™ with video capability, and Avaya Workplace with video capability. Co-browsing was not in the scope of the compliance testing.

Note that CBA Live does not support transfer nor conference calls on Avaya Endpoints.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to server, server reboot and activate denial of new service on the SIP Entity.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interfaces between Session Manager and Web Gateway did not include use of any specific encryption features as requested by CBA.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included calling inbound, hang up, G.711 MuLaw/G.711 ALaw/G.729 audio codec, H.264 video codec, multiple calls, long duration, coverage, call hold/resume, audio, and/or video with mute/un-mute.

The serviceability testing focused on verifying the ability of Web Gateway to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the server, server reboot and denial of new service on the SIP Entity.

2.2. Test Results

Tests were performed to verify interoperability with CBA Live using chrome browser, android native apps and iOS device native apps. The tests were all functional in nature and performance testing or redundancy testing were not included.

All test cases were completed successfully.

2.3. Support

Support for CBA Live Assist can be obtained from CBA, Inc. below:

Web: https://cba-gbl.com

- Asia Pacific
  Email: info.apac@cba-gbl.com
  Tel: +81-046-821-3362

- Europe, Middle East and Africa
  Email: info.emea@cba-gbl.com

- Latin America and North America
  Email: info.americas@cba-gbl.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**, with **sglab.com** being the domain name.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager are not the focus of these Application Notes and will not be described.

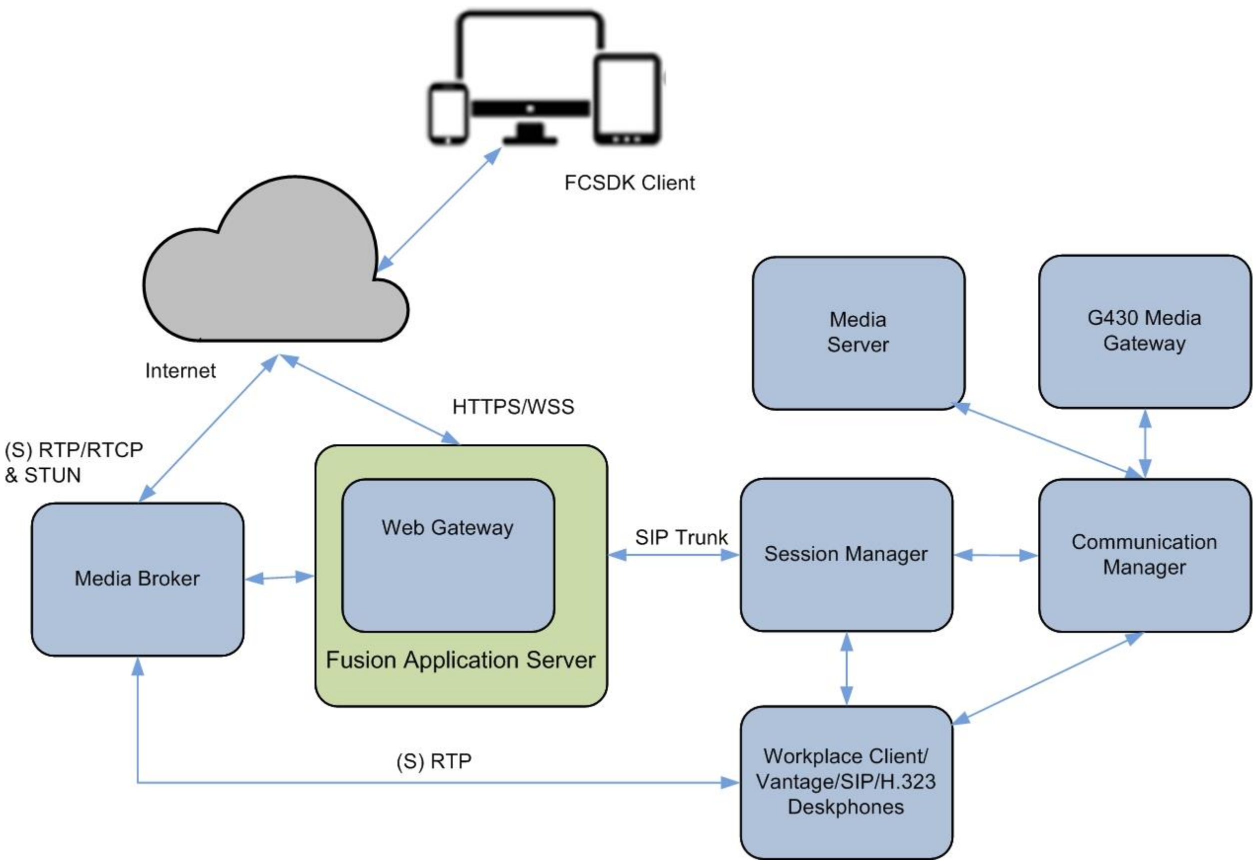


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	10.1 (10.1.0.0.0.974.27293)
Avaya G430 Media Gateway	42.4.0
Avaya Aura® Media Server in Virtual Environment	8.0.2.218
Avaya Aura® Session Manager in Virtual Environment	10.1 (10.1.0.0.1010019)
Avaya Aura® System Manager in Virtual Environment	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Workplace Client for Windows on Microsoft Windows 10	3.25 Pro
Avaya Vantage™ K155	2.2.0.5
Avaya 96x1 Deskphone (H.323)	6.8511
Avaya J100 Series Deskphone (SIP)	4.0.11
CentOS running on VMware 6.7 CBA Fusion Application Server (FAS) CBA Fusion Client SDK (FCSDK) • Web Gateway • Media Broker	7.9 2.5.23 3.4.5
Dell PCs running on Microsoft Windows 10 CBA Live native sample App	Pro Chrome
Android device CBA Live native sample App	Version 11 Native App 3.4.5.3
IOS device CBA Live native sample App	IOS 15.4.1 Native App 3.4.5.1

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer signaling group
- Administer network region
- Administer codec set

It is assumed a SIP Trunk is in placed between Session Manager and Communication Manager.

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has the appropriate permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that there is sufficient license for SIP Trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

```
display system-parameters customer-options                    Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                 Maximum Administered H.323 Trunks: 12000     90
       Maximum Concurrently Registered IP Stations: 18000     10
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations: 18000      0
          Maximum Concurrently Registered IP eCons:  414       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  41000     1
               Maximum Video Capable IP Softphones:  18000     1
                   Maximum Administered SIP Trunks: 40000     38
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999        0
```

5.2. Administer SIP Signaling Group

Use the **change signaling-group n** command, where **n** is the existing signaling group number for SIP trunk connection with Session Manager, in this case **7**. Enter the following values for the specified fields and retain the existing values for the remaining fields.

- **IP Video**: "y"
- **Initial IP-IP Direct Media**: "y"
- **Direct IP-IP Audio Connections**: "y"
- **IP Audio Hairpinning**: "n"

Leave the rest of the field as default.

Make a note of the assigned **Far-End Network Region** number, which will be used next to update the network region parameters.

```
change signaling-group 7                                            Page   1 of   2
                                SIGNALING GROUP

 Group Number: 7              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                    Far-end Node Name: sm1
 Near-end Listen Port: 5061                   Far-end Listen Port: 5061
                                           Far-end Network Region: 6

Far-end Domain: sglab.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.3. Administer Network Region

Use the **change ip-network-region n** command, where **n** is the assigned network region number from **Section 5.2**.

Enter **yes** for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** as shown below.

Make a note of the assigned **Codec Set** number, which will be used next to update the codec set parameters.

```
change ip-network-region 6                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 6       NR Group: 6
Location: 1       Authoritative Domain: sglab.com
    Name: To Session Manager 6  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 6              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. Administer Codec Set

Use the **change ip-codec-set n** command, where **n** is the assigned codec set number from **Section 5.3**.

For **Audio Codec**, G.711Mu, G.711ALaw and G.729 are supported which can be included.

```
change ip-codec-set 6                                              Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 6

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729             n         2        20
 3:
 4:
 5:
 6:
 7:
```

Navigate to **Page 2**, enable **Allow Direct-IP Multimedia** and set the two **Maximum Call Rate** parameters to the desired maximum rate for video.

In the compliance testing, Web Gateway was configured with the default video rate of 256 and the two maximum video rate parameters below were set to **4096** required for Vantage™.

```
change ip-codec-set 1                                              Page   2 of   2

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  4096:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  4096:Kbits
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer SIP users
- Administer Session Manager SIP Entity
- Add Web Gateway SIP Entity
- Add Entity Link for Web Gateway

6.1. Launch System Manager

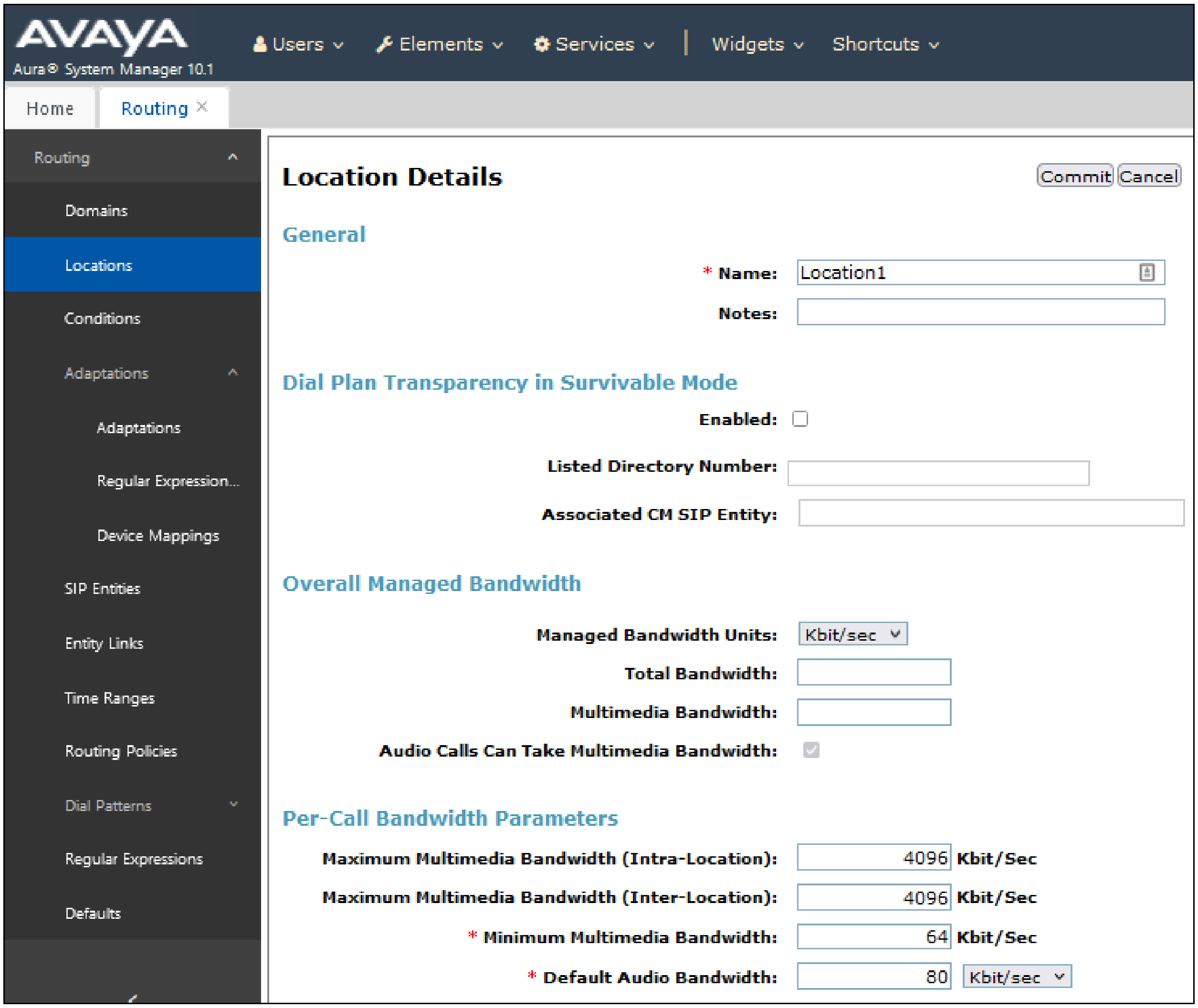
Access the System Manager web interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of System Manager. Log in using the appropriate credentials.

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements → Routing** to display the **Administration of Session Manager Routing Policies** screen below.

Select **Routing → Locations** from the left pane to display existing locations and select the pertinent location entry (not shown).

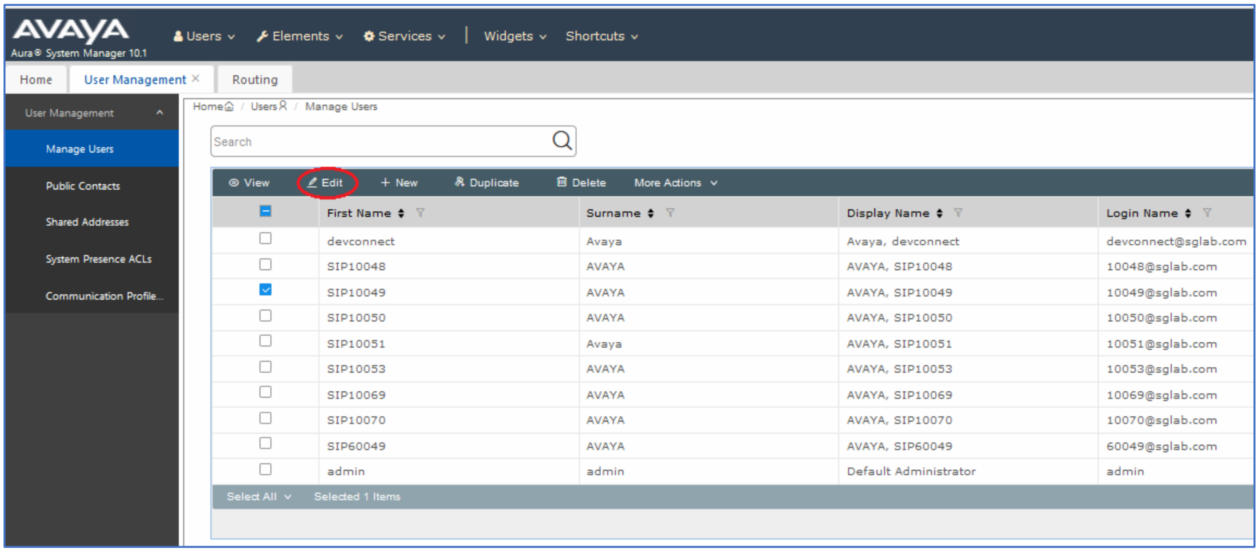
The **Location Details** screen is displayed next. In the **Per-Call Bandwidth Parameters** sub-section, set the two **Maximum Multimedia Bandwidth** parameters to the same maximum video rate value from **Section 5.4**.



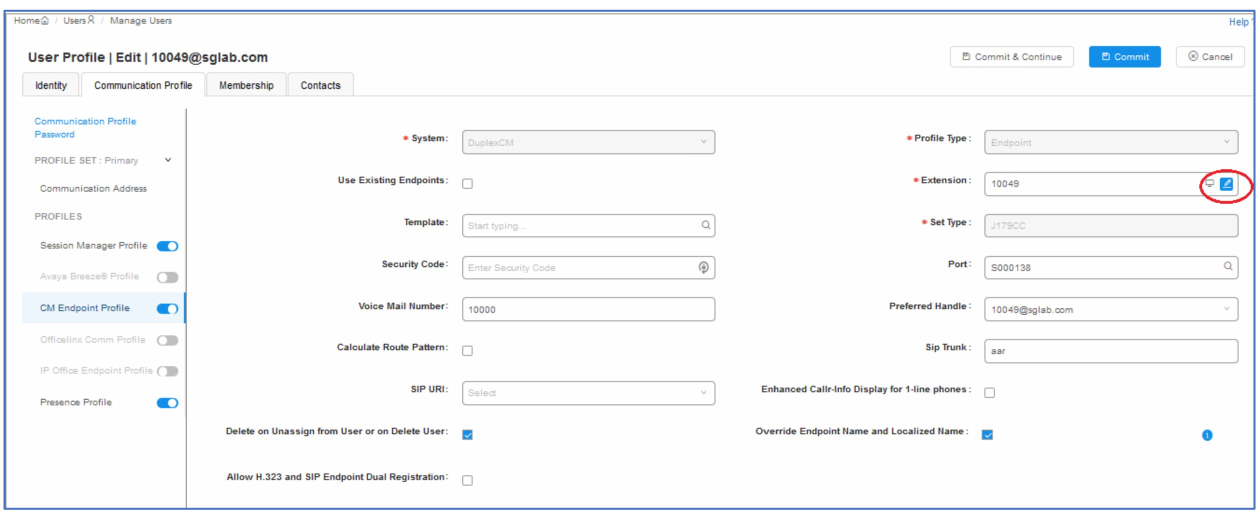
6.3. Administer SIP Users

Select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select an existing Avaya Workplace Client user, e.g., 10049 and click **Edit**.

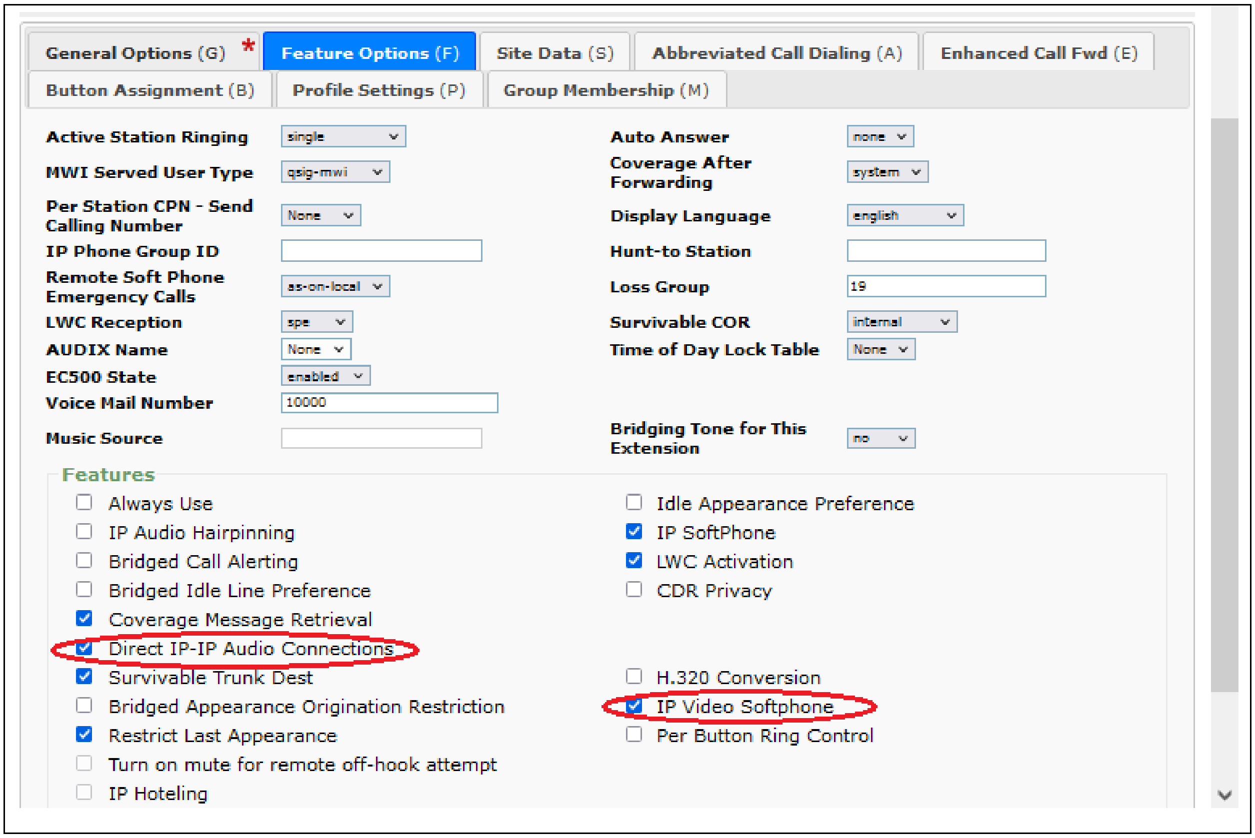


Select **CM Endpoint Profile** from the left pane. At the **Extension**, click on the **Editor** icon shown below.



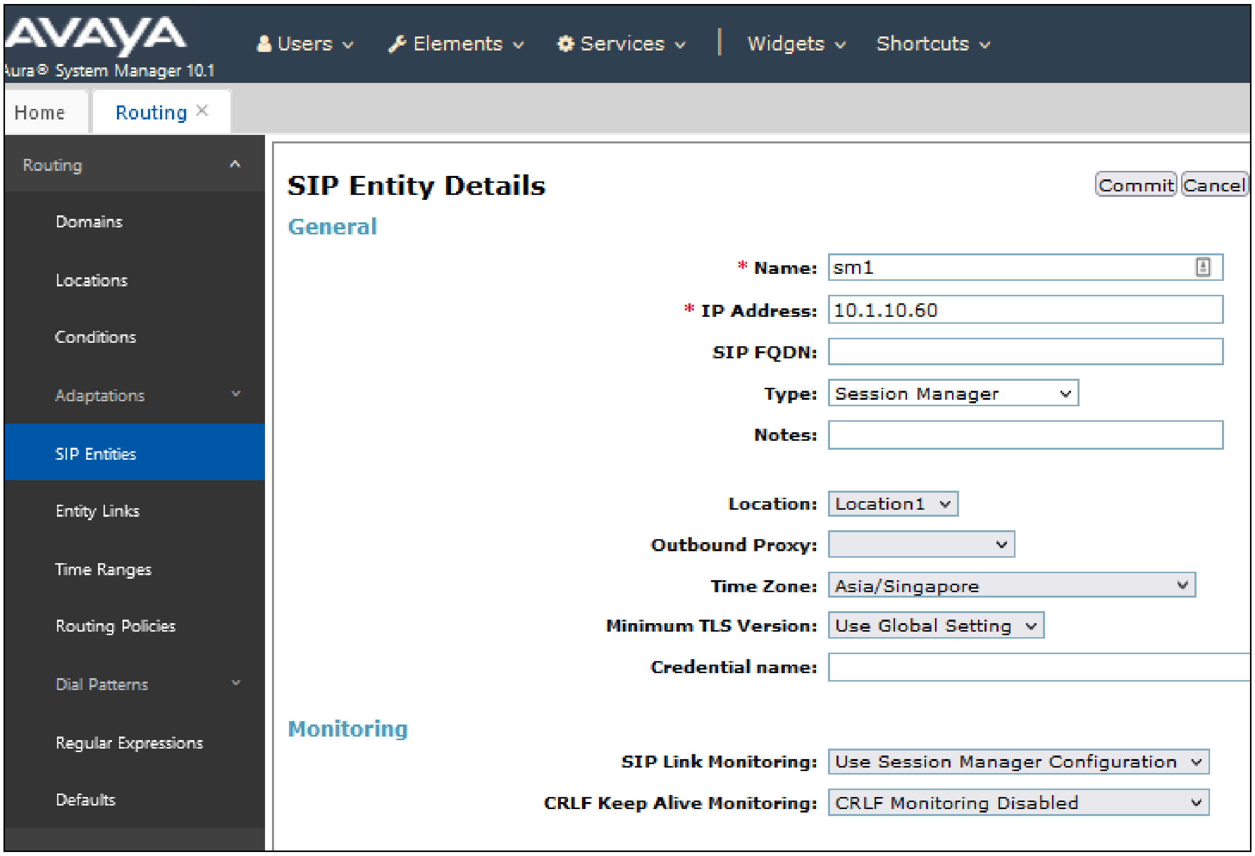
In the popped-up screen, select the **Feature Options**. Scroll the screen as necessary and check **IP Video** and **Direct IP-IP Audio Connections** as shown below.

Repeat **Section 6.3** as necessary to edit a SIP user for Video. In the compliance testing, SIP users with extension 10049 for Workplace Client and extension 10048 for Vantage™ were used as endpoints with both audio and video.

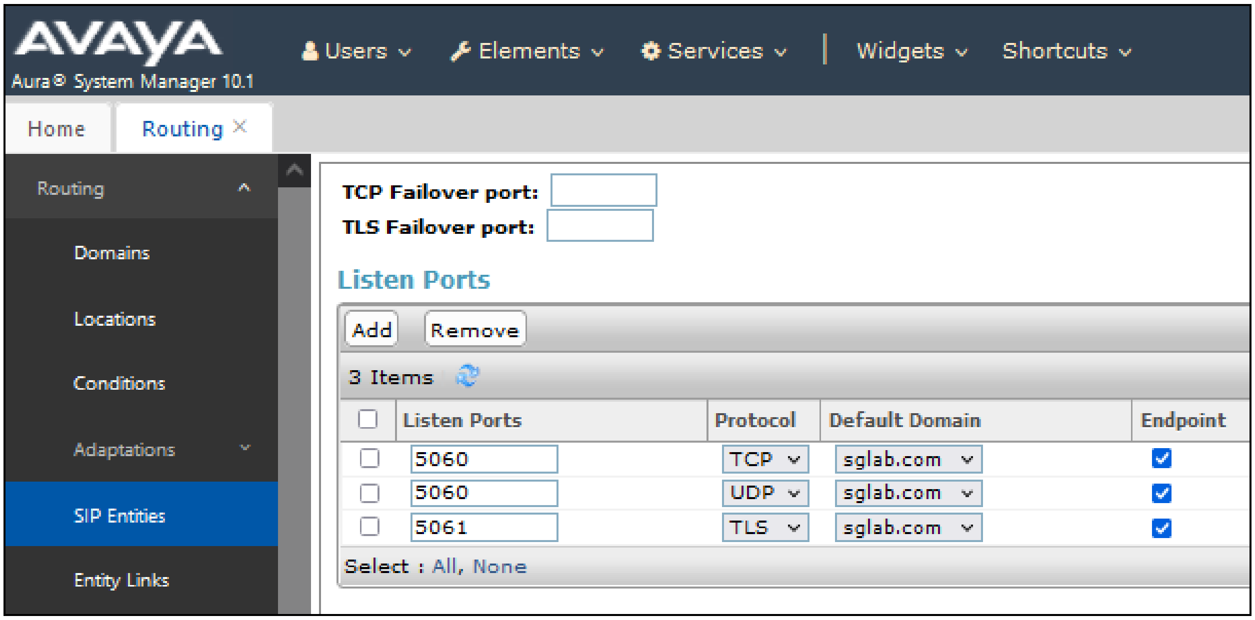


6.4. Administer Session Manager SIP Entity

Select **Elements → Routing → SIP Entities** from the top menu to display the **Routing** tab, followed by the applicable SIP entity for Session Manager from the left pane (not shown), in this case **sm1**. The **SIP Entity Details** screen is displayed.

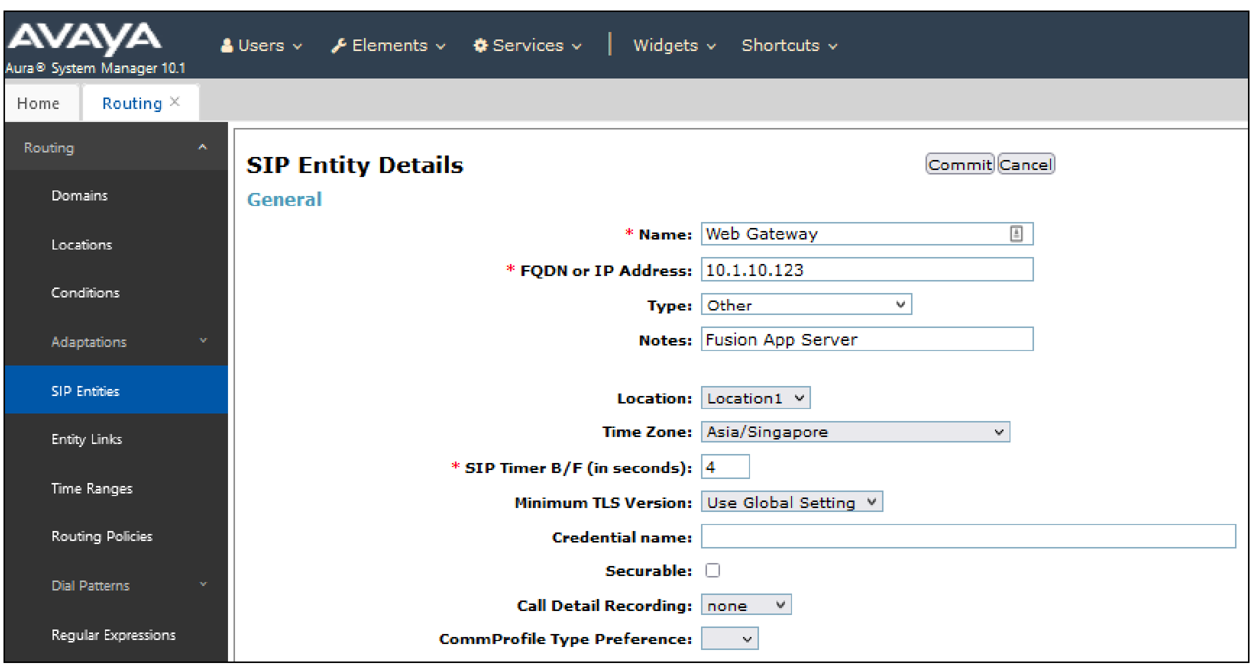


Scroll down to **Listen Ports** sub-section and verify that the transport protocol to be used by Web Gateway is specified in the list, in thise case **TCP**. Also verify that the corresponding **Endpoint** column is checked, as shown beow.



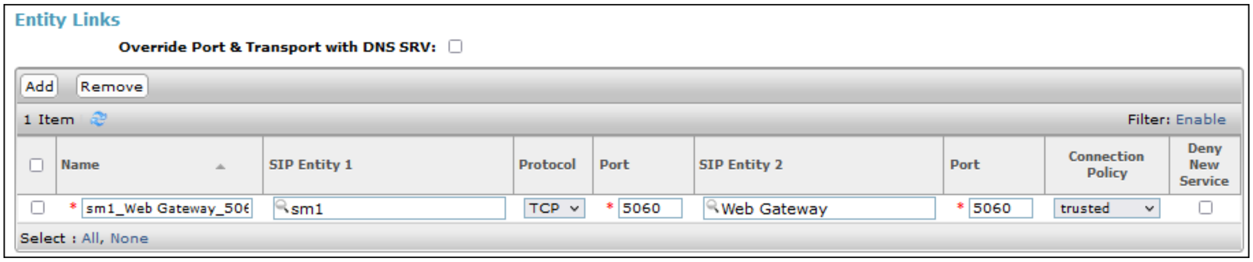
6.5. Add Web Gateway SIP Entity

From the same SIP Entities page, click on **New** (not shown) on the right pane to add the Web Gateway. **Name** the gateway as appropriate and enter the **FQDN or IP Address** with the **Type** selected as **Other**. Indicate appropriate **Notes** and select the **Location** in **Section 6.2**. Leave the rest as default. Click **Commit** to save.



6.6. Add Entity Link for Web Gateway

Select **Elements → Routing → Entity Links**. Click on **New** (not shown) on the right pane to create a new link. Enter appropriate name for the link with **SIP Entity 1** as the Session Manager **sm1** and the desired **Protocol** and **Port**. In the compliance test **TCP** was chosen with default port **5060**. For **SIP Entity 2**, enter the name **Web Gateway** created in **Section 6.5** with the default **Port 5060**. Set the **Connection Policy** as **trusted** from the drop-down menu. Click **Commit** to save.



7. Configure CBA Web Gateway

The configuration of CBA Live and its backend is performed by CBA installers and dealers. Refer to **Section 10** for more information. The procedural steps are presented in these Application Notes for **informational** purpose. This section provides the procedures for configuring the Web Gateway. Refer to the FCSDK Administration document in **Section 10** for more information. The procedures include the following areas:

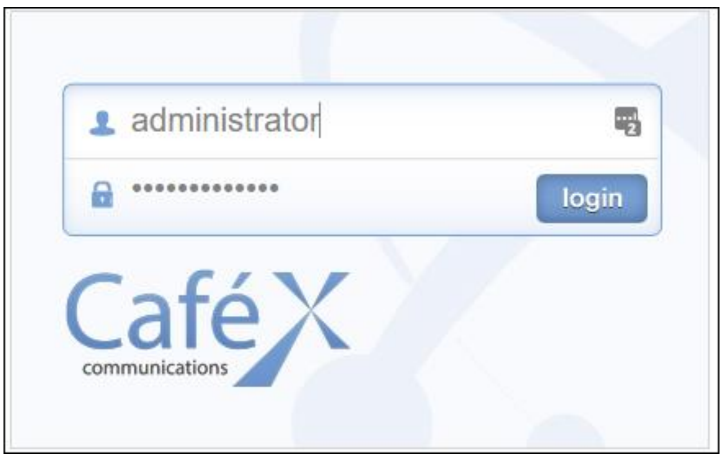
- Launch web controller
- Administer Outbound SIP Servers
- Administer Media Brokers

7.1. Launch web controller

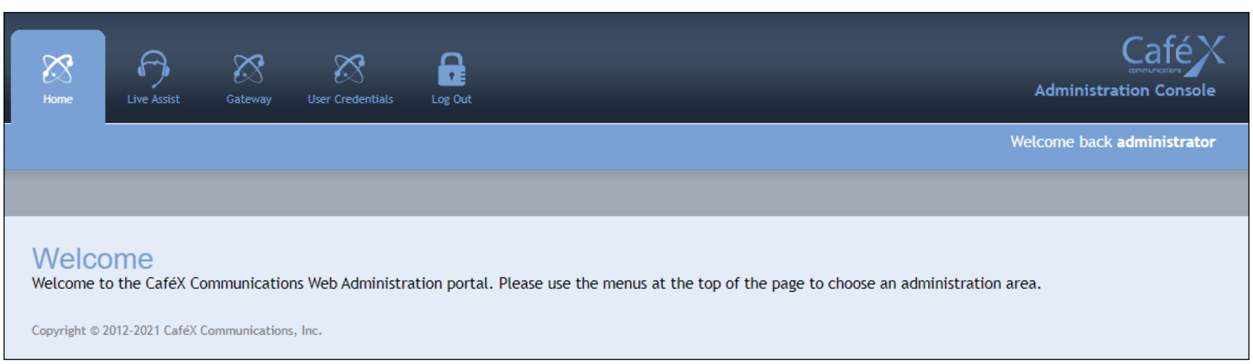
Launch the web controller at the following URL to configure the Web Gateway.

https://cbalive.sglab.com:8443/web_plugin_framework/webcontroller/gateway/

The screen below is displayed. Log in using the appropriate credentials.

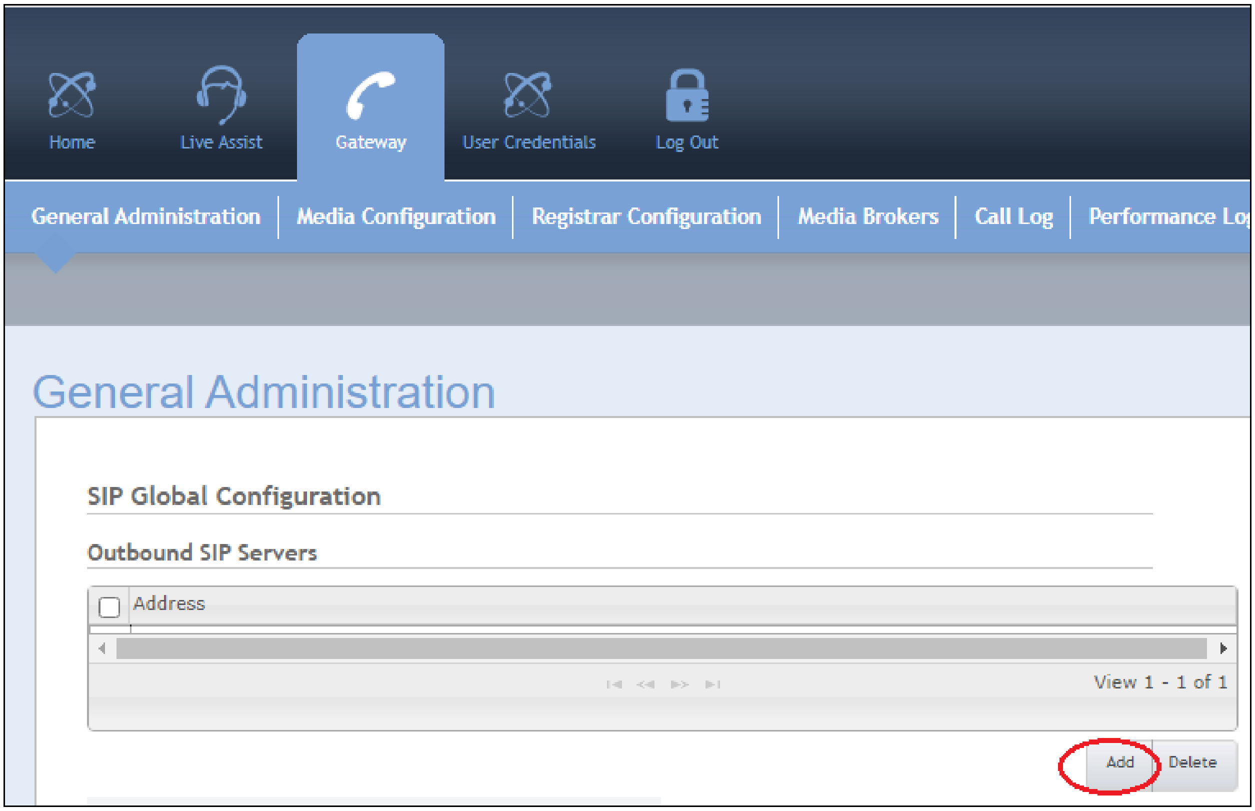


The following screen shows the initial home page.

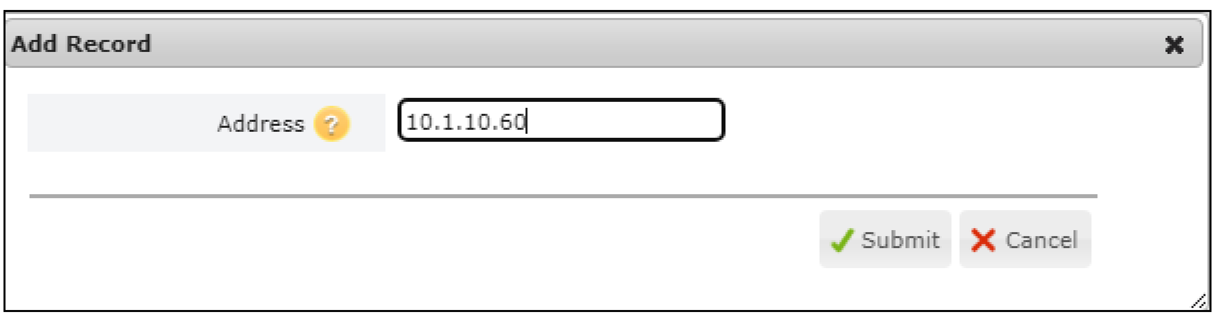


7.2. Administer Outbound SIP Servers

Navigate to **Gateway → General Administration**. Under the top section on **SIP Global Configuration → Outbound SIP Servers**, click **Add**.

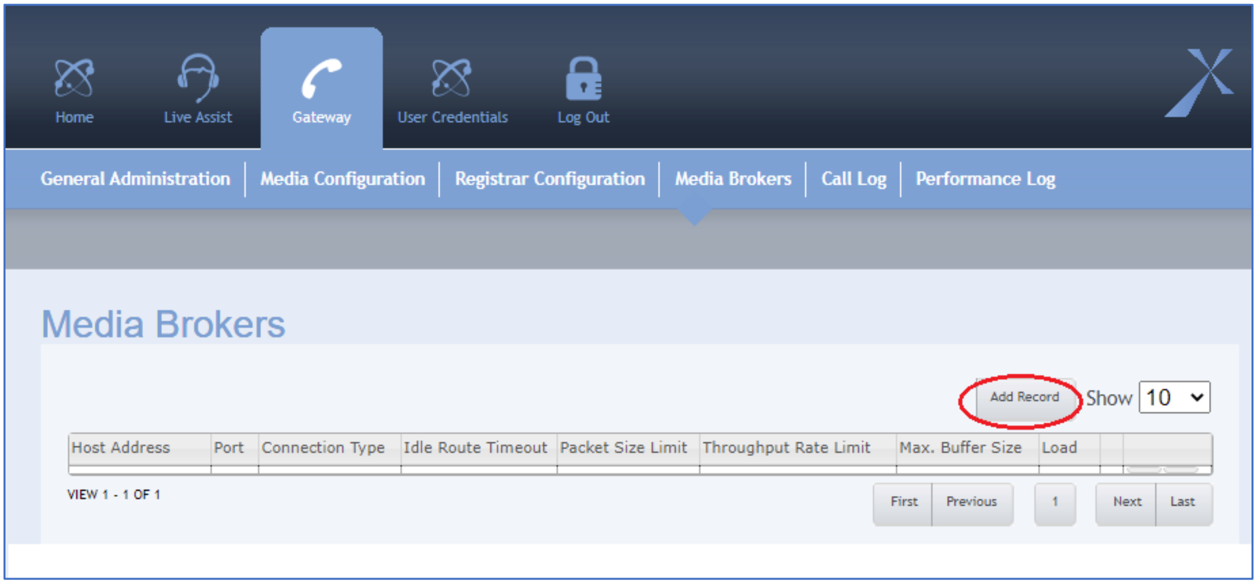


Complete the **Add Record** for the Session Manager IP address e.g., **10.1.10.60** as below and click **Submit**.

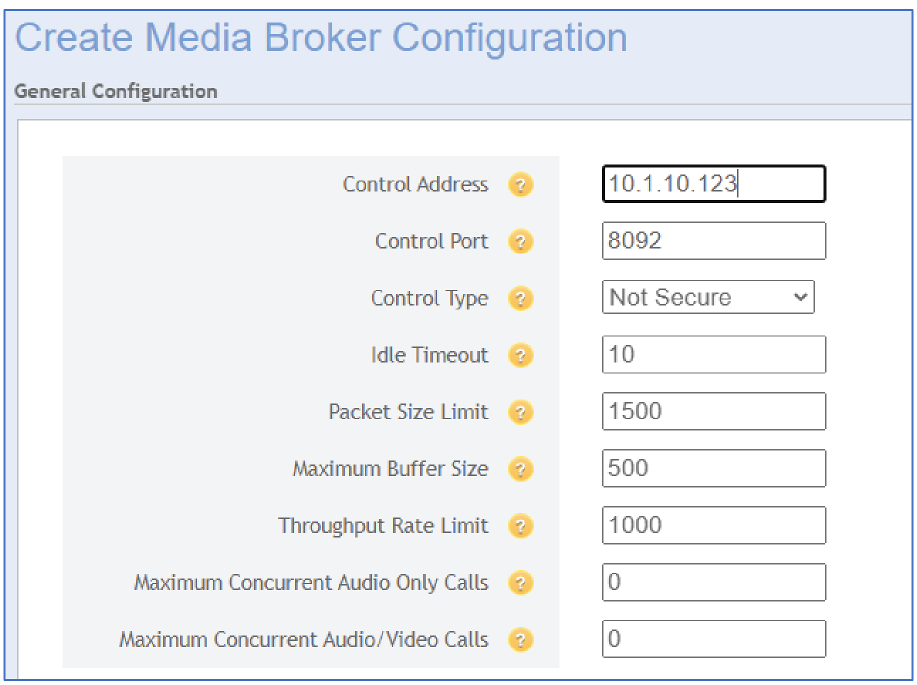


7.3. Administer Media Brokers

Navigate to **Gateway → Media Brokers**. Click on **Add Record** to configure the Media Brokers residing on the same FAS.



Enter the **Control Address** as the FAS server IP address as it resides on the same server. Leave the rest as default.



Scrolling further down, create a port range for the **SIP Network**. Below is a screen capture of the **Port Range** created. Scroll to the bottom of the screen and click **Save** (not shown).

SIP Network

	Local Address CIDR	Start Port Range	Finish Port Range
☐	all	17000	17099

Add Delete

8. Verification Steps

This section provides the test that can be performed to verify proper configuration of Communication Manager, Session Manager, and CBA Web Gateway.

8.1. Verify SIP Entity Link Status

From the System Manager web-based interface, select **Elements → System Status → SIP Entity Monitoring** from the top menu. Select the **Web Gateway** under the **SIP Entity Name** list below (not shown).

Verify that the Web Gateway Entity Link created in **Section 6.6** shows the **Link Status** and **Conn Status** as **UP**.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Web Gateway

Summary View

1 Item   Filter: Enable

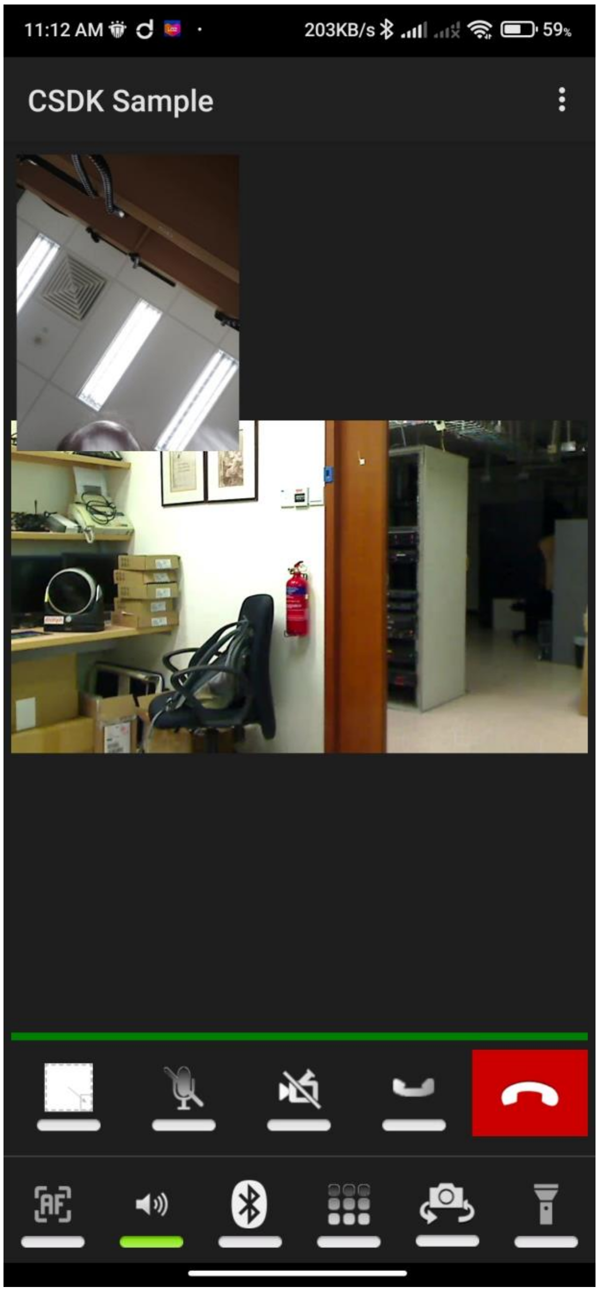
	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	sm1	IPv4	10.1.10.123	5060	TCP	FALSE	UP	404 Not found	UP

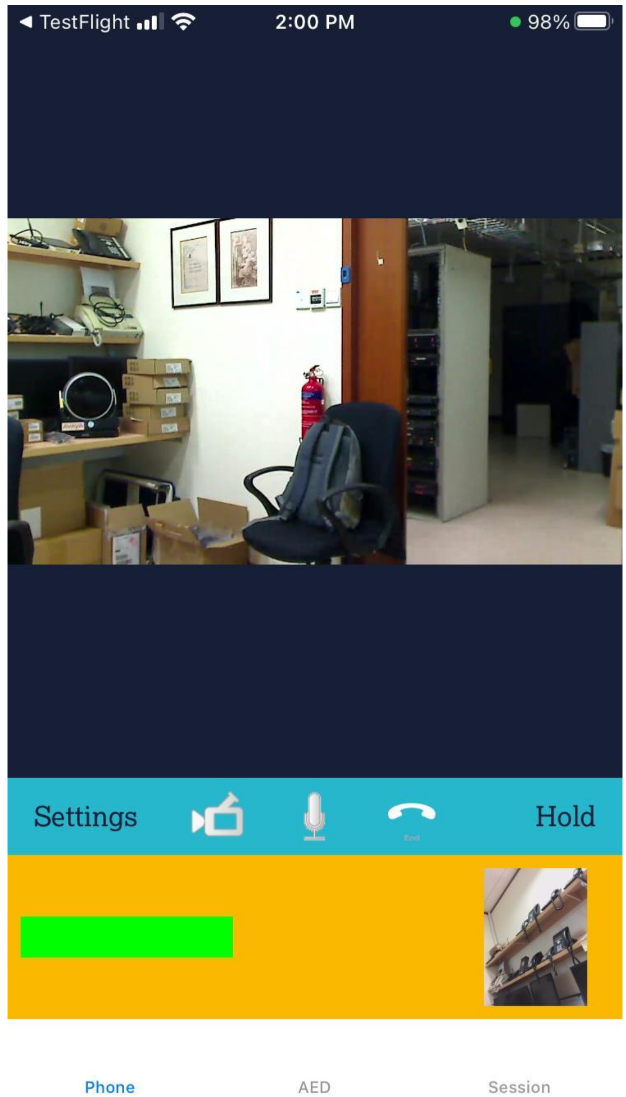
Select : None

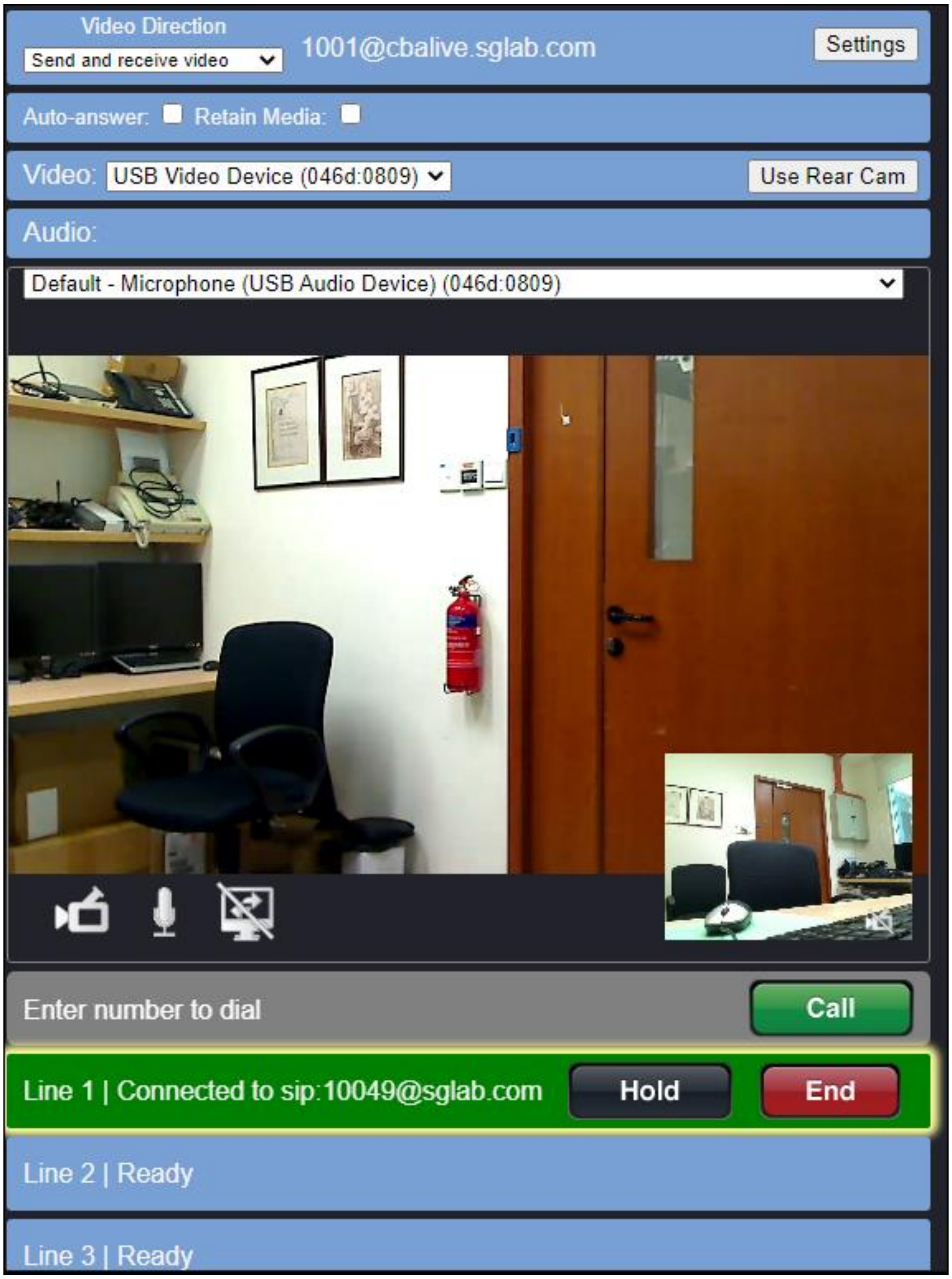
8.2. Verify with test calls from browser, Android and iOS Native app.

Make inbound test calls to the Aura® network. Calls are verified using Chrome browser, Android and iOS FCSDK Native app.

Below are screen captures of successful calls with Android (on left below), iOS (on right below) and browser (on next page).






Video Direction
Send and receive video
1001@cbalive.sglab.com
Settings
Auto-answer:
Retain Media:
Video:
USB Video Device (046d:0809)
Use Rear Cam
Audio:
Default - Microphone (USB Audio Device) (046d:0809)
Enter number to dial
Call
Line 1 | Connected to sip:10049@sglab.com
Hold
End
Line 2 | Ready
Line 3 | Ready

9. Conclusion

These Application Notes describe the configuration steps required for CBA Live Assist to successfully interoperate with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1. All feature and serviceability test cases were completed successfully.

10. Additional References

This section references the product documentation relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, Dec 2021.
[2] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 1, Dec 2021.

CBA Live product documentation can be obtained by contacting CBA Inc., (see **Section 2.3**).

[1] FCSDK Overview Guide dated Oct 2019
[2] FCSDK Architecture Guide dated Oct 2019
[3] FCSDL Administration Guide dated Oct 2019
[4] LA Solutions Guide dated Aug 2019
[5] LA Architecture Guide dated Oct 2019
[6] FAS Architecture Guide dated Oct 2019
[7] FAS Administration Guide dated Oct 2019

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.