Avaya Solution & Interoperability Test Lab

Application Notes for Tetherfi™ Omni Channel Management Video, Audio and Chat over Internet with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for Tetherfi™ Omni Channel Management (OCM) Video, Audio and Chat over Internet to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0.

Tetherfi™ OCM Video, Audio and Chat Over Internet is a web based Integrated multi-media SIP-based solution, including Video, Audio and Chat. The solution allows customers using web browsers to interact via video, audio or chat over web with Avaya Telephony platform allowing seamless transition across channels. Customers will initiate chat communication using a web browser to the WebRTC Media Gateway. The WebRTC Media Gateway in turn initiates a SIP call through a SIP Trunk via the Avaya Aura® Session Manager and Avaya Aura® Communication Manager to queue the calls to agents. Once the agent is available, customer chat is connected with an available agent and audio as well as video streaming can be started in the same session. Audio channel is established through Avaya Phone and Avaya Media Gateway, whereas video is established between Tetherfi Multimedia Agent Client (TMAC) and customer web browser.

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 Tetherfi™ Omni Channel Management (OCM) Video, Audio and Chat over internet to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0.

The solution enables web browsers to connect over the internet with the Avaya telephony platform using SIP and WebRTC capabilities. Customers will initiate chat/audio/video communication over the web browser to the WebRTC Media Gateway. The WebRTC Media Gateway will then initiate SIP trunk calls through Avaya Aura® Session Manager and Avaya Aura® Communication Manager to launch a SIP call to a pre-configured VDN (Vector Directory Number) to queue the call to an Avaya skill. Customers will be able to view "promotional videos" while waiting in queue (during call surplus scenarios and no agents are available). Once any agent becomes available, the chat/audio/video will be delivered to agents using Avaya Elite routing & handled by agents using Tetherfi Multimedia Agent Client (TMAC) on desktop PCs. Chat & Video will be delivered to TMAC screen and audio call will be on Avaya agent's phone. Once an audio path is established with an agent's phone, direct peer-to-peer video streaming starts between the customer and agent over WebRTC. Details of TMAC can be referred to the application notes in **Additional References [5]**.

2. General Test Approach and Test Results

The feature test cases were performed manually. Inbound chats were made using Chrome browser and chats were handled by agents running the TMAC. During this testing, agents were logged in from the respective phones as Avaya Elite expert agents using TMAC. Chats were handled by agents running the TMAC according to their skill levels. Once a SIP call is established with an Agent, audio and video streaming can be started manually by agents.

The serviceability test cases were also performed manually by denying and allowing new service on the Session Manager server, restarting the AES server and restarting the WebRTC Media Gateway. Arbitrary closing and re-login of customers browser was also conducted to ensure calls were tearing down properly.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following:

- Handling of incoming calls by converting text chat to audio and/or video
- Hold and Resume direct calls
- Hold and Resume transferred calls
- Consult voice transfers

- Mute and Unmute audio calls
- Stop and Resume video streaming
- Arbitrary closing of customers browser

The serviceability testing focused on verifying the ability of Tetherfi™ OCM Video, Audio and Chat to recover from adverse conditions such as denying of new service on Session Manager, restarting of Avaya AES server restarting of WebRTC Media Gateway as well as arbitrary closing of customer web browser.

2.2. Test Results

All feature test cases were successfully completed.

2.3. Support

Technical support on Interlink can be obtained through the following:

- Phone: +65-31507414
- Email: info@ilinknet.com.sg
- Web: http://www.ilinknet.com.sg

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a duplex pair of Communication Managers, Session Manager, System Manager, an Avaya G430 Media Gateway, Application Enablement Services and Avaya 96x1 H.323 IP Telephones. TMAC accessed the Tetherfi OCM through browsers installed on a Microsoft Windows 7 Professional PCs. Tetherfi OCM is installed on Microsoft Windows 2012 R2 server which communicates with the TSAPI Service on the - Application Enablement Services Server. Microsoft SQL 2012 was installed as the database on the same server. The WebRTC Media Gateway which runs on Windows is installed on the same server which connects through SIP Trunk to the - Session Manager. The Avaya 4548GT-PWR Converged Stackable Switch provides Ethernet connectivity to the servers and IP telephones.

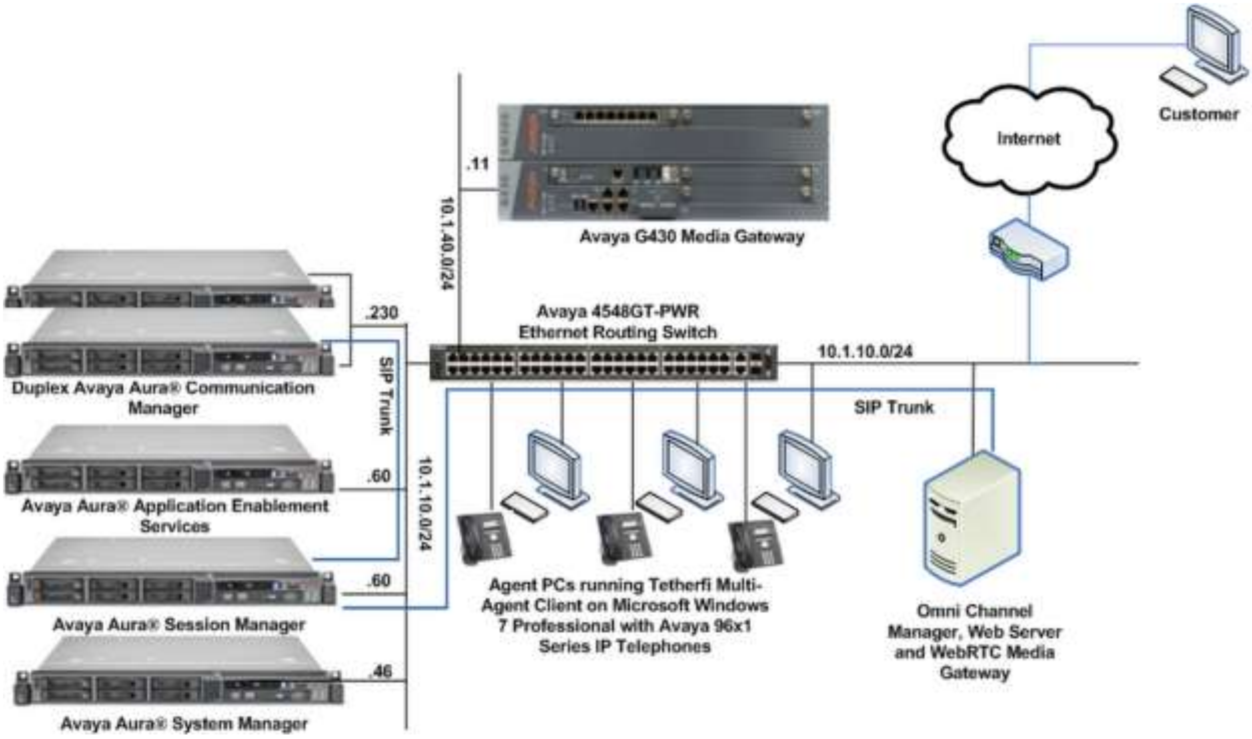


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager	R7.0-SP3 (R017x.00.0.441.0-22856)
Avaya G430 Media Gateway	37.21.0
Avaya Aura® Session Manager	7.0.0.2
Avaya Aura® System Manager	7.0.0.2
Avaya Aura® Application Enablement Services	7.0.0.0.2.13
96x1 Series (H.323) IP Telephones	6.6029
WebRTC Media Gateway	2.0.0
Tetherfi Omni Channel Management running on Microsoft Windows 2012 R2 with Microsoft SQL 2012 application	1.4.4.4
Tetherfi Multimedia Agent Client accessed through browser on PC running on Microsoft Windows 7 SP1	1.4.4.4

Note – The Avaya Aura® servers and Tetherfi application server used in the reference configuration and shown on the table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 5.X) platforms.

Table 1: Equipment/Software Validated

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring a SIP Trunk between Communication Manager and Session Manager. The setup of Agent Stations, Agent Login ID, VDNs, Hunt Groups, Trunks and Call Center features is assumed to be configured and will not be detailed here. Setup of CTI links with AES can be referred to document **[1]** in **Additional References**.

All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

Step	Description
1.	Ensure that a license is provided for the SIP Trunking to WebRTC Media Gateway are turned on as below: • **Maximum Administered SIP Trunks** : Ensure sufficient number of SIP Trunks allocated • **IP Trunks?** Must be enabled for IP Trunks • **ISDN-PRI?** Must be enabled for IP Trunks

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 80
           Maximum Concurrently Registered IP Stations: 18000 6
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 6
                       Maximum Administered SIP Trunks: 24000 28
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0


        (NOTE: You must logoff & login to effect the permission changes.)
```

```
display system-parameters customer-options                      Page   5 of  12
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                               IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                         ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                           ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                  ISDN-PRI? y
              ESS Administration? y                Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                      Malicious Call Trace? y
     External Device Alarm Admin? y                  Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                  Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step	Description
2.	Enter **change node-names ip** and add an entry for the Session Manager using an appropriately descriptive value for the **Name** (in this case, **sm1**) and the corresponding **IP Address** (in this example, **10.1.10.60**)

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
s8500-clan1         10.1.10.21
s8500-clan2         10.1.10.22
s8500-medpro1       10.1.10.31
s8500-medpro2       10.1.10.32
s8500-val1          10.1.10.36
site6               10.1.60.18
sm1                 10.1.10.60
sm2                 10.1.10.42


( 10 of 33   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Step	Description
3.	Enter **change ip-codec-set 6** and check that the supported **G711Mu (or G711Alaw)** audio codec is administered for IP Network Region 6 assigned in this compliance test.

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

                          IP CODEC SET
    Codec Set: 6

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
```

Step	Description
4.	Enter **change ip-network-region 6** to check that the **Codec Set** is set to **6** above.

```
change ip-network-region 6                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 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
```

Step	Description
4.	Enter **add sig n,** where **n** is the number of the signaling group created (in this example, signaling-group **7**). Enter the following parameters: • **Group Type :** Enter **sip** • **Transport Method :** Enter **tls** • **Peer Detection Enabled :** Enter **y** • **Peer Server :** This will be automatically detected as **SM** after submission of the form. • **Near-end Node Name:** Enter **procr** • **Near-end Listen Port:** Enter **5061** • **Far-end Node Name:** Enter **sm1** • **Far-end Listen Port:** Enter **5061** • **Far-end Network Region:** Enter **6** • **Far-end Domain:** In this case **sglab.com**

	` add 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`
	` 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.	Enter **add trunk n,** where **n** is the number of the trunk group created (in this example, trunk-group **7**). Enter the following parameter: • **Group Name :** Enter appropriate name • **Group Type :** Enter **sip** • **Service Type :** Enter **tie** • **Signaling Group:** Enter **7** • **Number of Members:** Enter appropriate value • **Numbering Format:** Enter **private** • **Support Request History:** Enter **y** • **Telephone Event Payload Type:** Enter **101**

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td><pre>
add trunk-group 7   Page   1 of 21
                                TRUNK GROUP

Group Number: 7   Group Type: sip   CDR Reports: y
  Group Name: SIP Trunk to SM1   COR: 1   TN: 1   TAC: #07
   Direction: two-way   Outgoing Display? y
 Dial Access? n   Night Service:
Queue Length: 0
Service Type: tie   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 7
                                                   Number of Members: 14
</pre></td></tr>
<tr><td></td><td><pre>
add trunk-group 7   Page   3 of 21
TRUNK FEATURES
          ACA Assignment? n   Measured: none
                                                      Maintenance Tests? y

                     Numbering Format: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

                                                Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? Y
</pre></td></tr>
<tr><td></td><td><pre>
add trunk-group 7   Page   4 of 21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
</pre></td></tr>
<tr><td>5.</td><td>Enter the save translation command to save the changes to the system. This completes the configuration of Communication Manager.</td></tr>
</table>

6. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Session Manager to support receiving of calls from WebRTC Media Gateway.

These instructions assume other administration activities have already been completed such as defining the network connection between System Manager and Session Manager, and defining Communication Manager as a Managed Element.

The following administration activities will be described:

- Define SIP Domain and Locations
- Define SIP Entity for Session Manager, Communication Manager and WebRTC Media Gateway
- Define Entity Links, which describe the SIP trunk between the Entities
- Define Routing Policies and Dial Patterns which control routing between WebRTC Media Gateway to Communication Manager via Session Manager

Configuration is accomplished by accessing the browser-based GUI of Avaya System Manager, using the URL "**http://<ip-address>/SMGR**", where "**<ip-address>**" is the IP address of Avaya System Manager. Log in with the appropriate credentials.

6.1. Define SIP Domains

Expand **Elements →Routing** and select **Domains** from the left navigation menu. Click **New** (not shown) and enter the following values and use default values for remaining fields**.**

- **Name** Enter the Authoritative Domain Name
  For the sample configuration, "**sglab.com**" was used.
- **Type** Select "**sip**" from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.

6.2. Define Locations

Locations are used to identify logical and/or physical locations where SIP Entities or SIP endpoints reside, for purposes of bandwidth management or location-based routing. Expand **Elements →Routing** and select **Locations** from the left navigation menu.

Click **New** (not shown)**.** In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

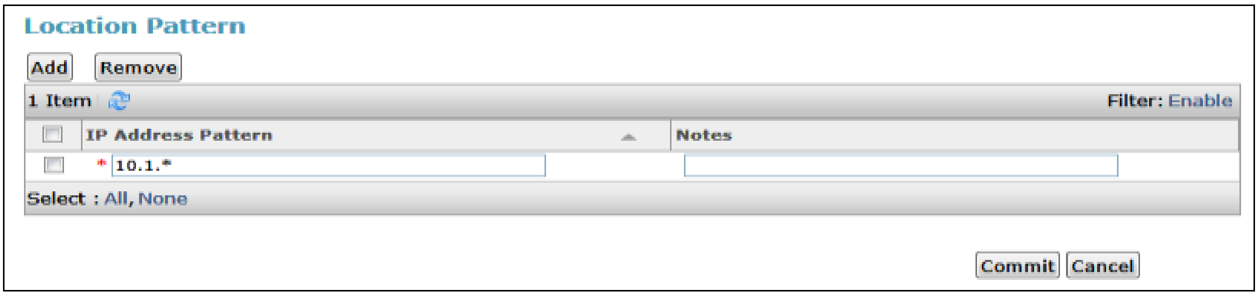
Scroll down to the **Location Pattern** section and click **Add** and enter the following values.

- **IP Address Pattern:** Enter the logical pattern used to identify the location.
- For the sample configuration, “**10.1.***” was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows a Location used for SIP entities in the sample configuration.

Note: screen has been abbreviated for clarity.



6.3. Define SIP Entities

A SIP Entity must be added for Session Manager, Communication Manager and WebRTC Media Gateway. To add a SIP Entity, expand **Elements→Routing** and select **SIP Entities** from the left navigation menu.

6.3.1. Session Manager

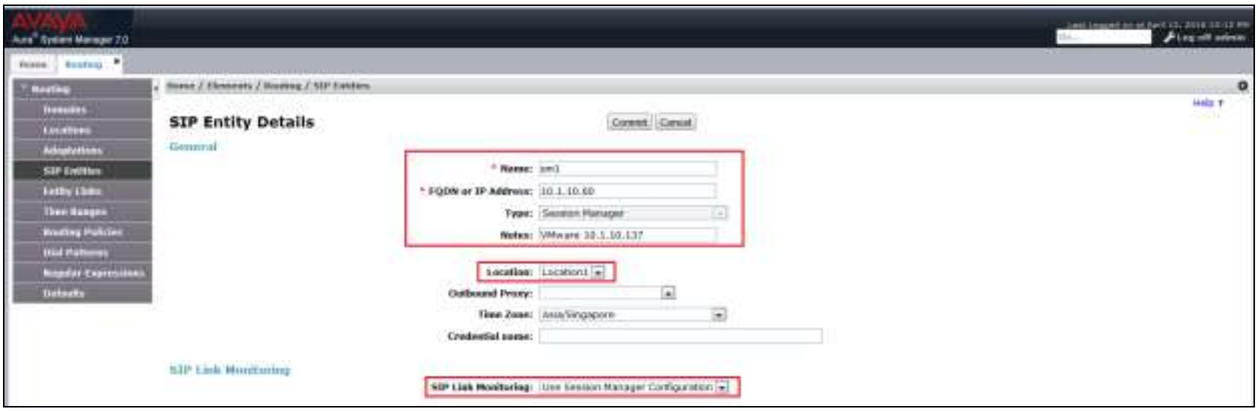
Click **New** (not shown**)** and in the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity. In the sample configuration, "**sm1**" was used.
- **FQDN or IP Address:** Enter IP address as **10.1.10.60**
- **Type:** Select "**Session Manager**"
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined in **Section 6.2**.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**".

Click **Commit** to save SIP Entity definition (not shown). The following screen shows the SIP Entity defined for Session Manager.



6.3.2. Communication Manager

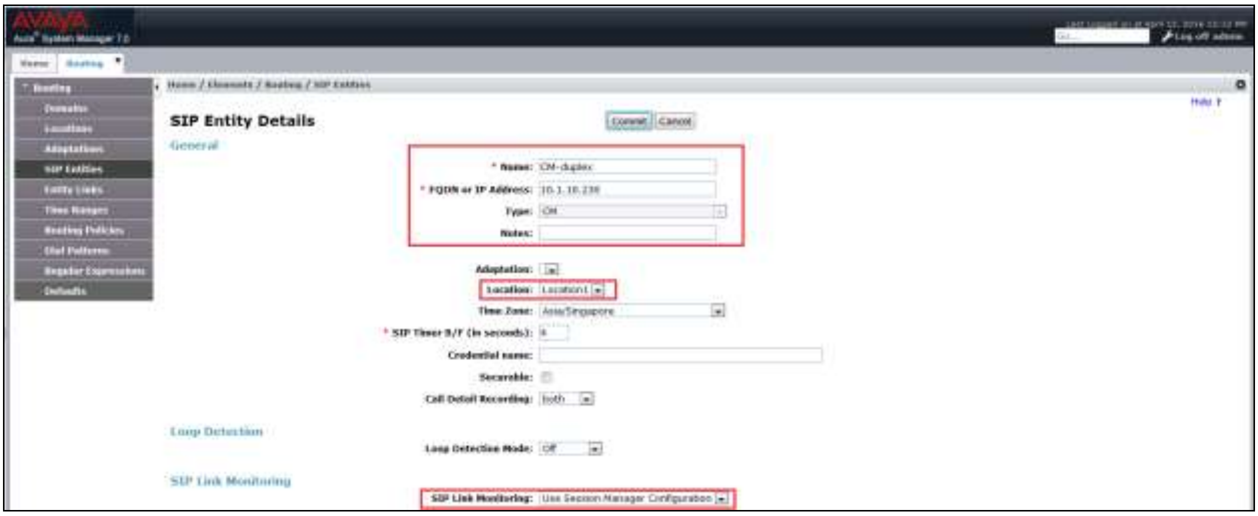
Click **New** (not shown) and in the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity.
  In the sample configuration, "**CM-duplex**" was used.
- **FQDN or IP Address:** Enter IP address as **10.1.10.230**
- **Type:** Select "**CM**"
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined in **Section 6.2**.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**".

Click **Commit** to save SIP Entity definition (not shown).
The following screen shows the SIP Entity defined for Communication Manager.



6.3.3. WebRTC Media Gateway

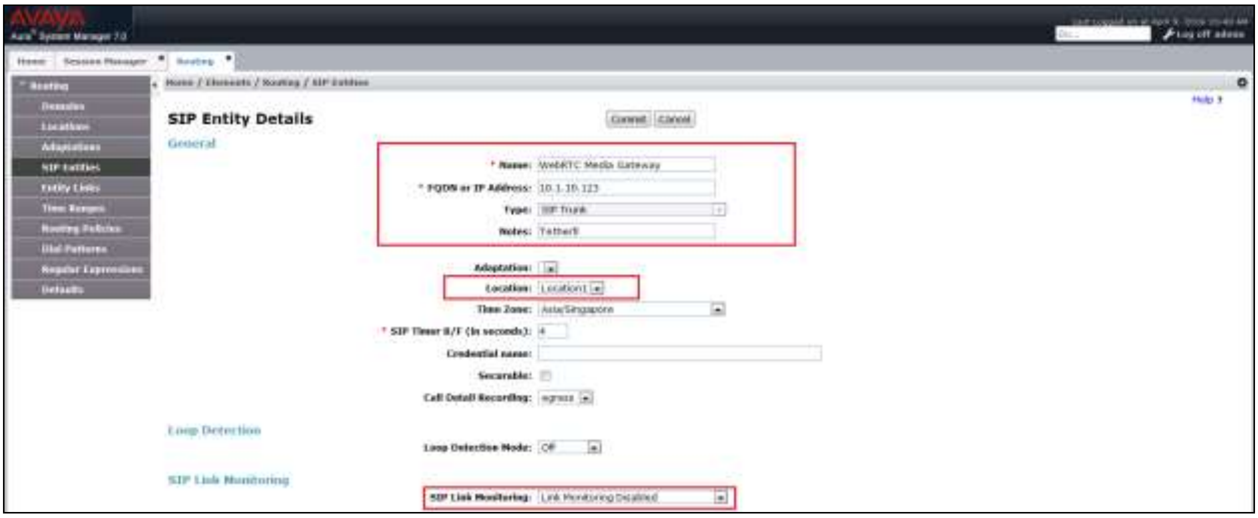
Click **New (**not shown) and in the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity.
  In the sample configuration, "**WebRTC Media Gateway**" was used.
- **FQDN or IP Address:** Enter IP address as **10.1.10.123**
- **Type:** Select "**SIP Trunk**"
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined in **Section 6.2**.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Link Monitoring Disabled**". This is because the WebRTC Media Gateway does not support OPTION requests for status.

Click **Commit** to save SIP Entity definition (not shown). The following screen shows the SIP Entity defined for WebRTC Media Gateway.



6.4. Define Entity Links

Routing entity links connect two SIP entities through the Session Manager to define the network topology for SIP routing. In the sample configuration, SIP Entity Links were added between Session Manager and Communication Manager as well as between Session Manager and WebRTC Media Gateway.

6.4.1. Communication Manager

To add an Entity Link, expand **Elements→Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to Session Manager.
- **SIP Entity 1** Select Session Manager already defined in **Section 6.3.1**.
- **SIP Entity 2** Select the SIP Entity added in **Section 6.3.2** from drop-down menu for **CM-duplex**.
- **Protocol** After selecting both SIP Entities, verify "**TLS**" is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5061**".
- **Connection Policy** Select trusted.

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Session Manager and Communication Manager.

6.4.2. WebRTC Media Gateway

To add an Entity Link, expand **Elements →Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to Session Manager.
- **SIP Entity 1** Select Session Manager already defined in **Section 6.3.1**.
- **SIP Entity 2** Select the SIP Entity added in **Section 6.3.3** from drop-down menu for **WebRTC Media Gateway**.
- **Protocol** After selecting both SIP Entities, verify "**TCP**" is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5060**".
- **Connection Policy** Select trusted.

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between WebRTC Media Gateway and Session Manager.

6.5. Define Routing Policy

Routing policies describe the conditions under which calls will be routed. This section describes the routing of calls from WebRTC Media Gateway to Communication Manager via Session Manager.

To add a routing policy, expand **Elements→Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier for routing to Communication Manager.
- **Disabled:** Leave unchecked.
- **Retries:** Retain default value of "**0**".
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the SIP Entity defined for Communication Manager and click **Select.**

The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition (not shown).

The following screen shows the Routing Policy for Session Manager.

6.6. Define Dial Pattern

This section describes the steps to define a dial pattern to route calls from WebRTC Media Gateway to Communication Manager via Session Manager.

To define a dial pattern, expand **Elements→Routing** and select **Dial Patterns.** Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

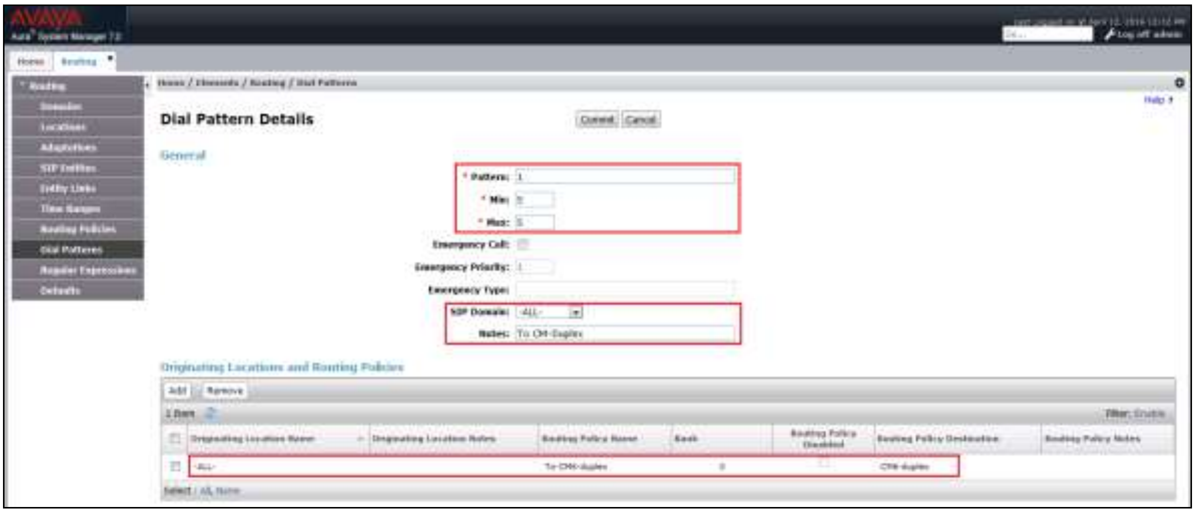
- **Pattern:** Enter dial pattern for the VDN.
- **Min:** Enter the minimum number digits that must be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select "**ALL**" if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add.**

The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select "**ALL**" .
- In **Routing Policies** table, select the appropriate Routing Policy defined for routing to Communication Manager which is defined in **Section 6.5.**
- Click **Select** to save these changes (not shown) and return to **Dial Patterns Details** page.

Click **Commit** to save the new definition. The following screen shows the Dial Pattern defined for routing calls to Communication Manager.



5-digit extensions beginning with "**1XXXX**" are assigned to pre-configured VDN which are routed to Communication Manager to queue the call and this is assumed to be defined.

7. Configure Avaya Aura® Application Enablement Services

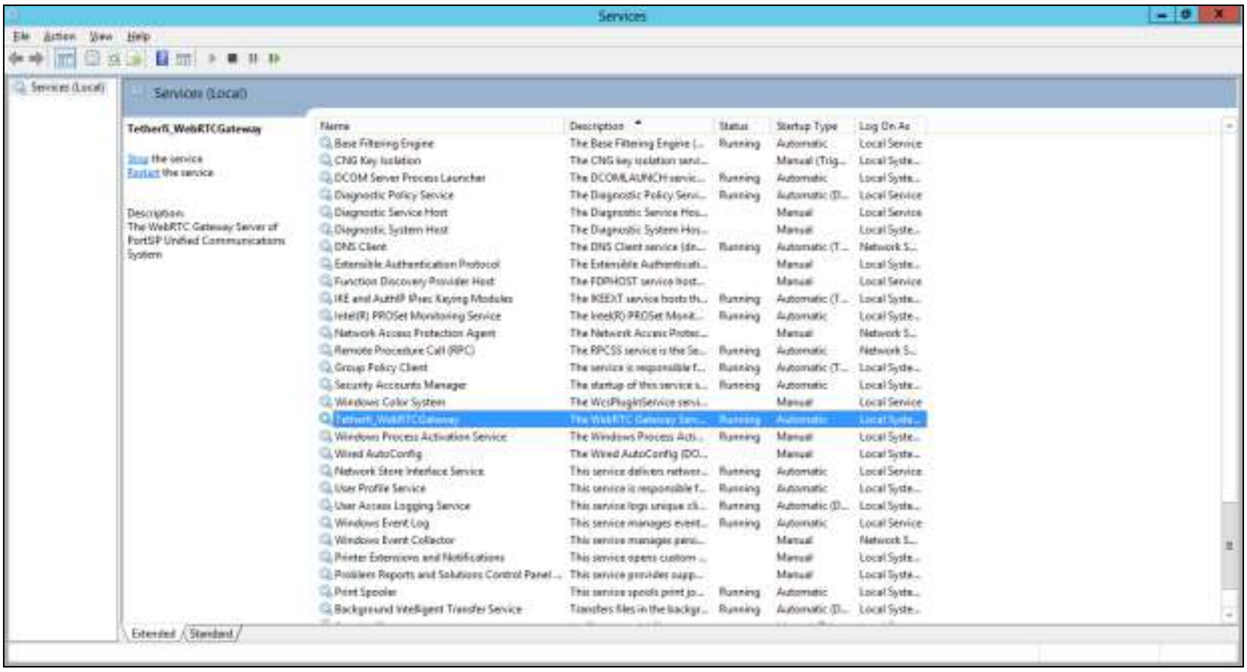
Setup of CTI links with AES can be referred to document **[1]** in **Additional References**.

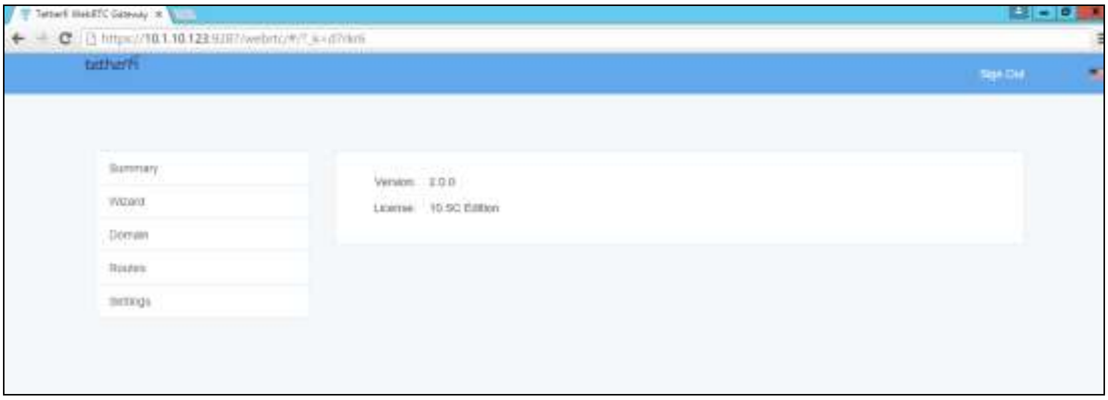
8. Tetherfi™ OCM Audio, Video and Chat over Internet

Installation and configuration of the web application for the above will be done by Interlink engineers which will not be detailed here as requirements differ depending on contact center.

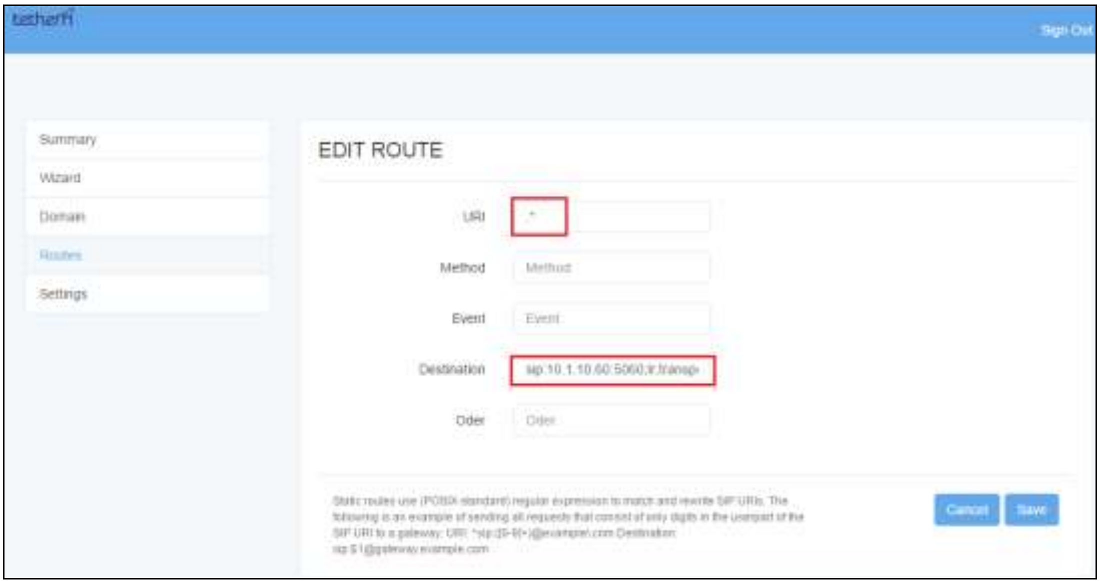
9. Configure WebRTC Media Gateway

This section highlights the configuration of the WebRTC Media Gateway. On the Windows Server, right click on the Windows Start and select **Run** (not shown). Type **services.msc** and click **OK**. Check that the **Tetherfi_WebRTCGateway** is running.



Step	Description
1.	Launch a web browser and enter **https://<IP address of WebRTC Media Gateway:9287/WebRTC/index.html>** to access the console web based interface. Log in to console using an administrative login and password (not shown). 
2.	The administrative home screen is shown below. Check that the license is sufficient. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>Add the Session Manager IP address in the Domain field. Below shows the result of addition.

</td></tr>
<tr><td>4.</td><td>Create a route to the Session Manager for the following:
URI – enter .*
Destination: sip:10.1.10.60;lr;transport=TCP
The transport corresponds to the Entity Links between Session Manager and WebRTC Media Gateway settings in Section 6.4.2.

</td></tr>
</table>

10. Configure Tetherfi Multimedia Agent Client

The configuration of TMAC will not be detailed here. Refer to document **[5]** in **Additional References** section for more information.

11. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and TMAC.

11.1. Verify Avaya Aura® Communication Manager

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

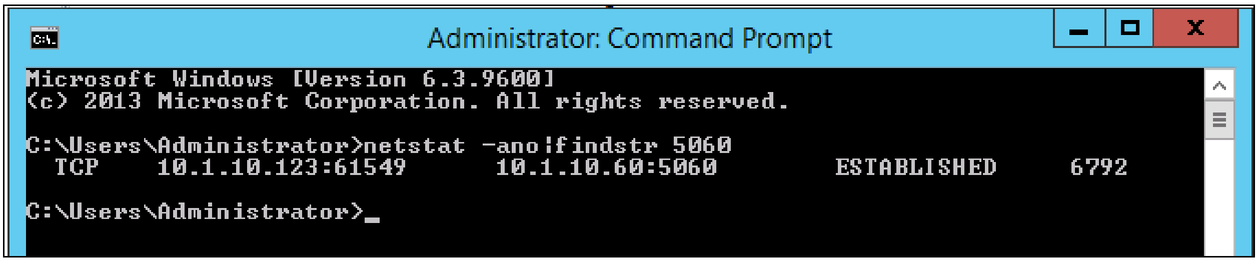
```
status aesvcs cti-link

                                AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs      Msgs
Link           Busy  Server           State         Sent      Rcvd

1              no                     down          0         0
2              no                     down          0         0
3     7        no    aes7x            established   14        14
```

11.2. Verify Avaya Application Enablement Services

From the Welcome to OAM web pages, verify the status of the TSAPI Service by selecting **Status**. The **State** field for the **TSAPI Service** should display **ONLINE** and the **Cause** is **NORMAL**.

11.3. Verify SIP Trunk with WebRTC Media Gateway

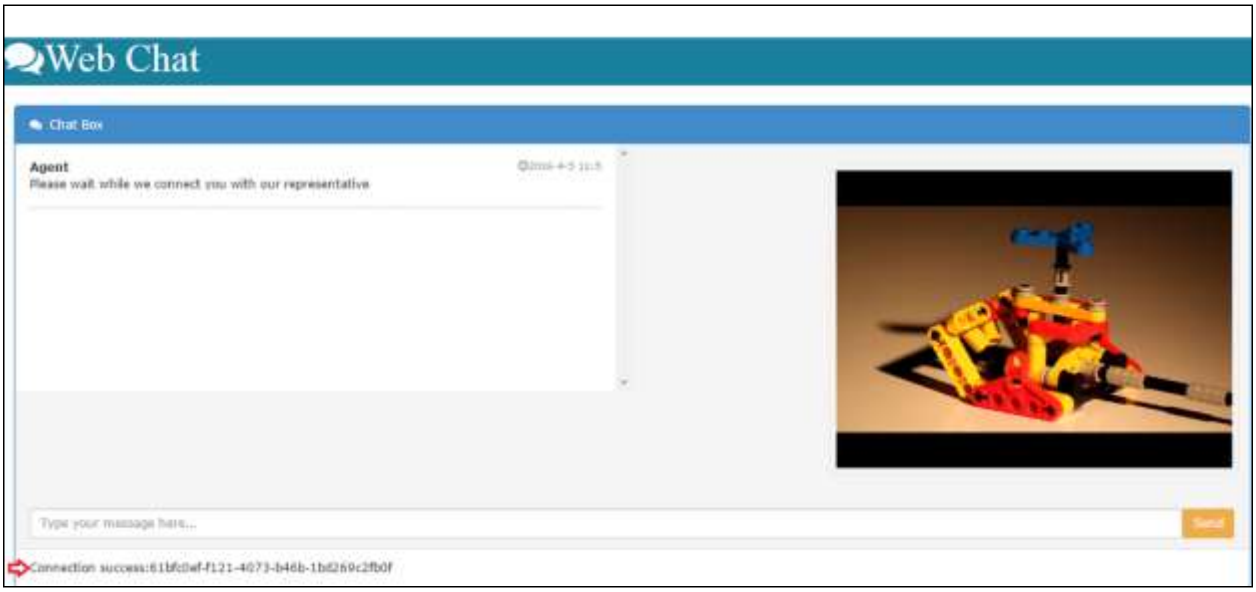
On the server, right click on the Windows Start and select **Run** (not shown). Type **cmd** and click **OK**. In the DOS command line, type "**netstat –ano|findstr 5060**". Verify that the TCP link is **ESTABLISHED** between WebRTC Media Gateway Server and Session Manager.



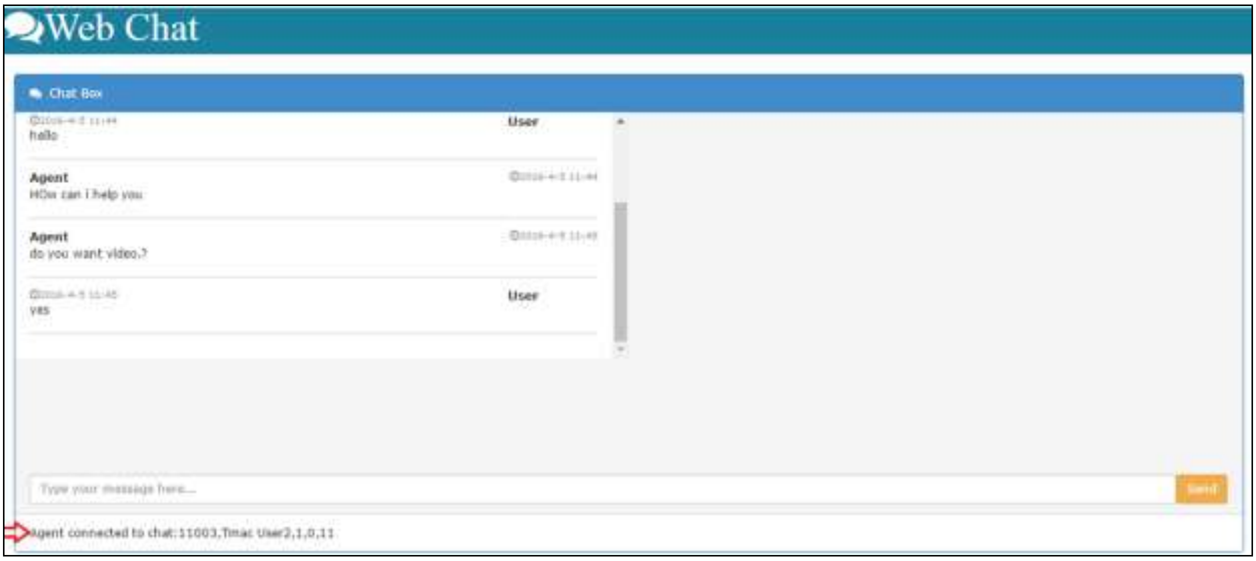
11.4. Verify Audio, Video and Chat on customer browser and Tetherfi Multimedia Agent Client (TMAC)

Launch a Chrome web browser on the customer PC and enter address **http://<FQDN or IP Address of OCM>/webchatuser/webchat.htm** to access the contact portal. Log in to a customer account with the appropriate **Name** and **NRIC** (Identification Number).

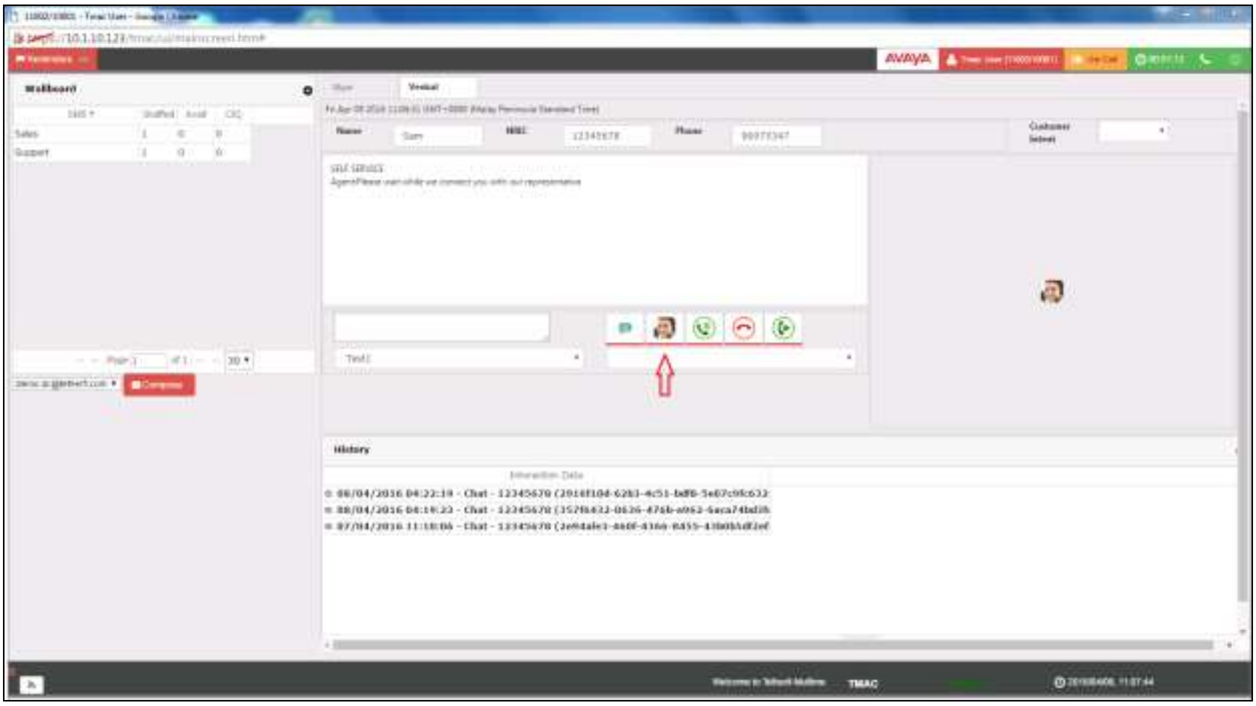
The customer will be queued to an Avaya Elite skill on Communication Manager and will see audio & video playback on the webpage. The information line on bottom left below shows **Connection success**.



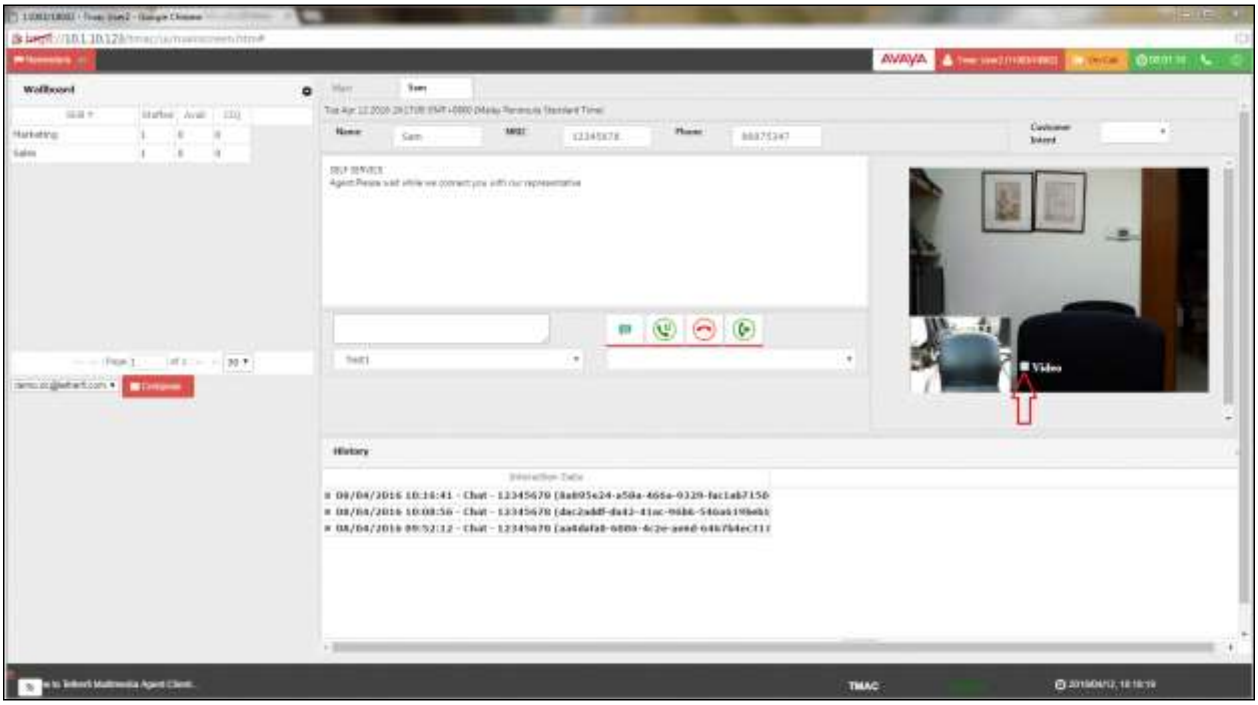
Login as an agent using TMAC on of the PCs and make the agent available. Verify the customers status line on the bottom left is showing **Agent connected** and is able to chat as shown in the sample below.



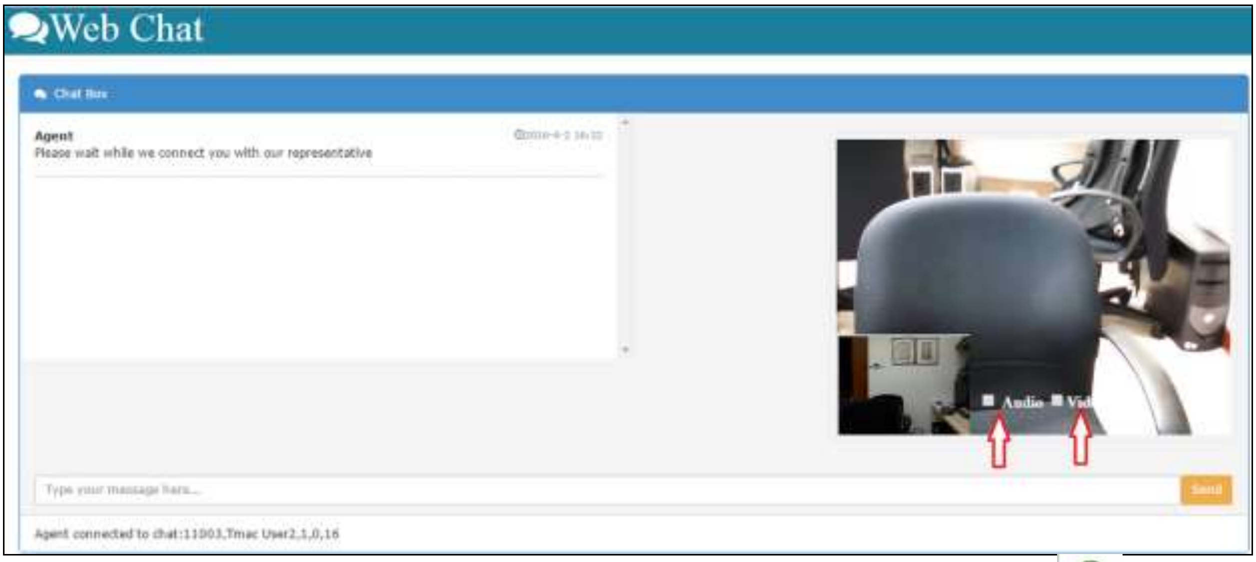
Initiate audio video chat on the TMAC by clicking the human face icon below. Only the agent can initiate the audio & video connection.



Notice only a white box is displayed for stopping the video streaming from agent to the customer. No audio white box is provided on the TMAC screen for muting/unmuting the audio as it is received and transmitted from an Avaya phone.



On the customer side, verify Audio and Video can be muted and stop respectively by unchecking the Audio and/or Video white box as below.



Verify hold and resume can be performed by toggling the hold and resume button  on the TMAC desktop.

12. Conclusion

These Application Notes describe the configuration steps required for Tetherfi™ Omni Channel Management (OCM) Video, Audio and Chat over Internet to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0. All feature test cases were completed successfully.

13. Additional References

This section references the Avaya and Tetherfi documentations that are relevant to these Application Notes.

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

[1] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.0, Aug 2015.
[2] *Avaya Aura® Avaya Communication Manager Feature Description and Implementation*, Document Number 555-245-205, Release 7.0, Issue 1, Aug 2015.
[3] *Administering Avaya Aura™ Session Manager*, Release 7.0, Issue 1, Aug 2015.
[4] *Deploying Avaya Aura® Session Manager on VMware®*, Release 7.0, Issue 1, Aug 2015.
[5] *Application Notes for Tetherfi Omni Channel Management Multimedia Agent Client with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3*, Jan 2016.

Tetherfi product documentations can be obtained from Interlink Network Systems.

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.