

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

LYM; Reviewed:	Solution & Interoperability Test Lab Application Notes
SPOC 8/25/2016	©2016 Avaya Inc. All Rights Reserved.

- 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: <u>info@ilinknet.com.sg</u>
- Web: <u>http://www.ilinknet.com.sg</u>

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	7.0.0.2.13
96x1 Series (H.323) IP Telephones	6.6029
WebRTC Media Gateway	2.0.0
Tetherfi Omni Channel Management running on	1.4.4.4
Microsoft Windows 2012 R2 with Microsoft SQL	
2012 application	
Tetherfi Multimedia Agent Client accessed	1.4.4.4
through browser on PC running on Microsoft	
Windows 7 SP1	

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:				
	are turned on as below.				
	Maximum Administered SIP	Frunks : 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-o OPT	options Page 2 of 12 CONAL FEATURES			
	IP PORT CAPACITIES	USED			
	Maximum Adminis	stered H.323 Trunks: 12000 80			
	Maximum Concurrenciy Reg. Maximum Administered Re	emote Office Trunks: 12000 0			
	Maximum Concurrently Registered Remo	ote Office Stations: 18000 0			
	Maximum Concurrently H	Registered IP eCons: 414 0			
	Max concur Registered Unauthentica Maximum Vide	eo Capable Stations: 41000 0			
	Maximum Video Capable Stations: 41000 6 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 & log	in to effect the permission changes.)			
	display system-parameters customer-o	options Page 5 of 12			
	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 Extended Cvg/Fwd Admin? v	Malicious Call Trace? v			
	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? v			
	Global Call Classification? y	Multimedia Call Handling (Basic)? y			
	Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y			
	Hospitality (G3V3 Enhancements)? y IP Trunks? y	Multimedia IP SIP Trunking? y			
	II IIunks: y				
	IP Attendant Consoles? y (NOTE: You must logoff & log	in to effect the permission changes.)			

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved.

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)				
	conceptionante in Address (in this example, 10.1.10.00)				
	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				
	sm2 10.1.10.60				
	5				
	(10 of 33 administered node-names were displayed)				
	Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name				
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				
	tact				
	change 1p-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:				
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				
	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				
	UDP Port Min. 2048				
	UDP Port Max: 3329				
	DIFFSERV/TOS PARAMETERS				
	Call Control PHB Value: 46				
	Audio PHB Value: 46 Video PHP Value: 26				
	802.1P/O PARAMETERS				
	Call Control 802.1p Priority: 6				
	Audio 802.1p Priority: 6				
	Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS				
	H 323 Link Bounce Recovery? v				
	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 subm	ission 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 GROU	JE			
	Group Number: 7 Group Type: sip				
	Q-SIP? n				
	IP Video? y Priority Video? y Enforce SIPS URI for SRTP? y				
	Prepend '+' to Outgoing Calling/Alerting/Dive	erting/Connected Public Numbers? y			
	Remove '+' from Incoming Called/Calling/Alert:	'+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
	Near-end Node Name: procr	ear-end Node Name: procr Far-end Node Name: sml			
	ear-end Listen Port: 5061 Far-end Network Region: 6				
	raf-end Network Region: 6				
	Far-end Domain: sglab.com	Supass If IP Threshold Exceeded? n			
	Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n			
	DTMF over IP: rtp-payload Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y			
	Enable Layer 3 Test? y	Initial IP-IP Direct Media? y			
5	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.				
	Crown Name	Enter enpropriate name			
	• Group Ivanie .	Enter appropriate name			
	• Group Type .	Enter tio			
	• Service Type : Enter ue				
	• Signaling Group: Enter /				
	 Number of Memory Numbering Formet: 	Enter privot o			
	 Numbering Format: Support Doquest Ustore 	Enter v			
	 Support Request filstory Tolonhone Event Devices 	. Linci y Type: Enter 101			
	• relephone Event rayload	Type. Line IVI			

Step	Description
	add trunk-group 7 Page 1 of 21
	TRUNK GROUP
	Group Number: 7 Group Type: sin CDP Reports: V
	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
	Number of Members: 14
	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
	Penlace Pestricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
	Show ANSWERED BY on Display? Y
	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
	Cond Diversion Header() n
	Support Request History? v
	Telephone Event Payload Type: 101
	Convert 180 to 183 for Early Media? n
	Always Ose fe-invite for Display Opdales; n Identity for Calling Darty Display: P-leserted-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
~	Enter the game translation common dite contents: may-nave-extra-aights
5.	Enter the save translation command to save the changes to the system. This
	completes the configuration of Communication Manager.

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** \rightarrow **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.

			Last topped on at work in your photons.
Tantas T			
+ Hann / Domante / feedbay / Damains			0
1.201012312313143111111	Concerning and Concerning		Help 7
Domain Management	Consul Carlos		
			2000/00/00/00/00
1 10.0	T-20071	11577-5	
Rate	Talan	Bullet	
* Judek.com	10		
	Canent Cancel		
	Inem / Demant / Realing / Inemane Domain Management I Tase I Tase Tase Tase Tase Tase Tase Tase Taget cm		

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** \rightarrow **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.

AVANA Arts System Hamper 70			and instant of the second s
Hore: Session Hanag	er * Huders *		
* Basting	 Huma / Desents / Reality / Locations 		0
Demates	1010-0220-0220-0210	12 + FORMULA (12 - 12 - 12 - 12 - 12 - 12 - 12 - 12	Halp 7
-Locations	Location Details	Circuit Carol	
Adaptations	General		
Silf Latitud	- Andrews and	· Minney Location	
CONVISION		And a second second	
- then Hampen		DOCKING.	

Note: screen has been abbreviated for clarity.

Location Pattern			
Add Remove			
1 Item 😂			Filter: Enable
IP Address Pattern	<u></u>	Notes	
* 10.1.*			
Select : All, None			
			Commit Cancel

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** \rightarrow **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.

AVANA Ann Sylan Henge 7.0			Lond Longert an at fact 11, 2014 10-17 fm Class
feren feature *			
T Barting	- mane / Elements / Rooming / SIP Easter	,	0
Transiers.	*		Help 7
Louisee	SIP Entity Details	Correct. Carnet	
Adaptetions	General		
SIF Extition		* Reme: aml	
Letity Lists		* FQDN or TP Address: 10.1.10.60	
These Mangers		Type: Sumon Haraper	
Routing Publices		Notes: 305 vare 30.5.10.137	
third stationers			
Regelier Copressions		Location: Location:	
Determ		Outboard Prony: a	
		Time Zwas: Assa/Singapore	
		Credestial susse:	
	53P Link Horitoring	SDP Liek Modifiering: User Senson Manager Configuration	

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
•	Туре:	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.

Aug Talan Manager 10				Constant and a part of a provide a part of the second seco
Name Asstag *				
T finding	• Honn / Khonnis / Bodieg / MP Esti	pès.		0
Constituee	SIP Entity Details		Canon	Traduct P
Adoptations nor Labitas	General	* frame: 104-	digler }	
Faithe Links Time Rangers		* POINt or 1P Address: 10.1 Type: Chi	.18.234	
Clief Palterns		Adaptetion:		
Definition	1	Tocation: Loss	stant •	
		* SIP Timer B/F (in seconds): A Credential name:	1	
		Securable: 🗐 Call Debail Recording: Toti		
	Enop Detection	the second second second second	121	
	SUP Link Monitoring	SIP Link Monifording: Unit	Section Manager Cireliguration	

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
•	Туре:	Select "SIP Trunk"
•	Notes:	Enter a brief description. [Optional].
٠	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.

				and special and the second s
Here Session Parage	a Anatas .			
- Breting	. Hone / Threets / Sources / All* in	tities .		•
Demailue Locatione	SIP Entity Details		(Connet) (Connet)	Helde 3
Adapteters	General	* Name:	webRTC Media Estevas	
Foldity Links		* FQDS or IP Address:	10.3.10.123	
Tion Ranges		Type:	HIP Truck +	
Utal Patterne		inter.		
Repúblic Laprendian Defaallis		Adoptation Location	al Lecation (a)	
		SIP Thear 8/F (in seconds):	Altersingation	
		Credential name: Securable:		
		Cell Outal Recording:	agrana (m)	
	Loop Detection	And the second second second		
	SIP Link Manitoring	Long Delectore Hode: -	vr 187	
		50 ^r Link Hosituring:	Link Hendoring Disabled	

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** \rightarrow **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.

and Printers * in	antes Recepter . *									
Reading .	. Hone / Threads / Rea	they / thethy Ladia								
freedos transfere	Entity Links			3	Canoni Cancel					Testp
- Résplations										
And in Lines.	Liten C									Pitter: Drates
Teel Bargers	C] Marra	ALC CASES 1	Promoted	Print	807 Ewildy 2	DAS. Habertale	Pert.	Convection Pulsia	Deni New Aprox	Biller.
Routing Publics	E Fand to contra	Ala - Kawat	1 149 181	* 3081	· Qonages		* 594	fronted ini	6	
Elsi Petimini	Select 1 40, Inexe 1								-	
Regulat Papersitent										

6.4.2. WebRTC Media Gateway

To add an Entity Link, expand **Elements** \rightarrow **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.

AVAVA Intel Series Margar 70								The second	Fing off adam
Harm Destine Habays	Andre 1								
Routing	A Hone / Demoste / Red	ing / Websty Listen							
dessales Locathan	Entity Links			Consul (Cancel)					Halp Y
Sill Intiles									
Fording Links	Liter C.								- Piter Bruth
Han Barges	C. Norbit	add statisty 4	Protocal Past	107 3 abdy 2	Dans -	et.	Connection Addate	Service Name	Rethini
Realing Fulling	CI SADOWSKICKS	+ Quest	(102/18) · 5066	· Q WEEKTC Halls Dationale	0	586	monthed in	13	L
Utal Patteries Regular Laprovision Defaults	Select : =0, Norme								
			1	Constit Carook					

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.**

LYM; Reviewed:	Solution & Interoperability Test Lab Application Notes	15 of 27
SPOC 8/25/2016	©2016 Avaya Inc. All Rights Reserved.	TVAC_CMSM7

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.

Aure System Manager 72			an and increased in an avoid in. Another play the inter-
mane Boston *			
7 Reading	+ Horne / kineseth / Southing / Routing Palaties		0
Domatos Locations	Routing Policy Details	(doment) (cannot)	Trub P
Adaptations Soft Locks Failing Clocks Show Hampels Routing Polisies Dail Politeres	General	* Neuros: To-CM-Septer Disabledi. [] * Retrino: 0	
Regular Experiment	50P Lutity as Destination Select j Reven Chi Aphr	region se in Additions 10.1.10.209	Page Nation

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** \rightarrow **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.

AVAVA Arts' types through 12							en somt mit ber id, sins ideal in Flag off advan
ment brains *							Linker and
* Andres	Huma / Threads / Kintley / Hist Pattern						0
townin. Incolines	Dial Pattern Details		Current Cancel	1			Hulp 9
Adaptetives	General						
SIP Initian India Links		* Pattern: 1					
Tien Gargen Realing Folicies		· Mage 1					
olal Patteres		Energency Cell:					
Regular Expressions		Energency Priority:					
Oxforts		Emergency Type:					
		S2P Domains	44. in 10 OH-Explore				
	Driginating Locations and Ronting P	talicies					
	add Agenove						
	LDan े						The costs
	E Drephiling London Rame -	Degewing Location Roles	Redley Falley Roser	5++b	Bouting Fallers Disabilitied	Bauweg Public Destanding	Reading Pality Mades
	10 Mar		Te-DNR-shades		- 11	Che diales	
	Senit / AL Nove						

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.

and find the se	CONTRACTOR OF A						
Services (Local)	Services (Local)						
	Tetherfi, WebRTCGateway	Nama	Description •	thetas	Stertup Type	Log On Ae	10
	The state of the second second	S Back Inflaming English	The Base Fillering Engelse (Shawad	Automatic	Cocal Service	
	Tarter the service	CNG Key Isslation	The CNS sey lightion sent-		Manual (Trig	Local Syde	
	Delter of the second	BCOM Server Process Launcher	The DCOMLAUNCH servic	Busning	Autometic	Local Synte	
	1 Stanford and	Diagnorthic Policy Service	The Diagnostic Policy Servi-	Building	Automatic (D_	Local Service	
	Description	Ca Diagnostic Service Host	The Diagnostic Service Hos		Metual	Local Service	
	Fine WebKits, Gateway Server of End SP United Communications	Chogeostic, System Hest	The Diagnostic System Hos-		Mansat	Local Syste	
	System	Childrent Client	The DNS Client service (dn	Ratterig	Automatic (T_	Network 5	
		Extensible Authentication Protocol	The Estemplate Authenticati		Manual	Local Systel.	
		Function Discovery Provider Host	The FDPHOST service host		Manual	Local Service	
		18E and AuthilP IPsec Keying Modules	The IKEEXT service boots thus	Running	Automatic (T_	Local System	
		Intel(R) PROSet Monitoring Service	The lotel(R) PROSet Monit	Bussing	Automatic .	Local Syste-	
		S Network Access Protection Agent	The Network Access Protect		Metual	Network 5	
		Remote Procedure Call (RPC)	The RPCSS service is the Sec.	Bunning	Automatic	Network S.,	
		Cross Folicy Client	The service is responsible f	Butning	Automatic (T_	Local Syde	
		Security Accounts Manager	The startup of this service i	Running	Automatic	Local Syste	
		C Wardows Color System	The WosPhightService servi-		Manual	Local Service	
		Q Patriert, Web/172Canoner	The WebSTC Gateway Serve-	Ratting	Administra	Lincat Spring 2	
		Windows Process Activation Service	The Windows Process Acts	Burning	Manual	Local Syste-	
		Wired AutoConfig	The Wired AutoConfig (DO		Manual	Local System	
		Aktivork Store Interface Service	This service delivers networ-	Butning	Automatic	Local Service	
		Q User Profile Service	This service is responsible f	Russing	Intomatic .	Local Syste	
		Q User Access Logging Service	This service logs unique ch	Ruteing	Automatic (D	Local System	
		C Windows Event Log	This service manages event	Rateing	Automatic	Local Service	
		Windows Event Collector	This service manages pand	1010316	Marrial	Retwork S	
		Printer Externiovo and Notifications	This service opens custors		Marriell	Local System	
		Possiblers Reports and Solutions Control Panel	This pervice provider papp-		Matuat	Local Byth	
		Print Spooler	This service speeds print jo	Running	Adomatic	Local System	
		C Background Wellagert Transfer Service	Transfers files in the lanckur	Summing	Automatic (I)	Local Syste	

ep	Description		
1.	Launch a web browser	and enter https:// <ip address="" of="" th="" webrt<=""><th>C Media</th></ip>	C Media
	Gateway:9287/WebR7	[C/index.html> to access the console web	based interface.
	Log in to console using	an administrative login and password (not	shown).
	Total Web0: Galaxy ★ ←		
		Tetherfi WebRTC Gateway	
		(increase)	
		Hammeth	
		Automatine the	
		Bigs Hill	
		Address and the	
2	The administrative hom	e screen is shown below. Check that the li	cense is sufficien
2.	The administrative nom	e sereen is shown below. Check that the h	
	Tetter Becci Gateway *		8 ·
	 C (2 https://10.1.10.123.9387/webstc/#/ bitther/fi 	Jacobin	
	Summary	Version I.O.D	
	Burrrary Witten	Version: 2.0.0 Luxense: 10.52 Edition	
	Burnnary Wittant Domm	Version: E.O.D Laamse: 10-50, Elitton	
	Burmany Witzant Decram Research	Version 200 Loame 10.50 fattori	
	Burnnary Witzent Domain Reserve mittings	Version: 2.0.0 Ladmae 10.90 fillitor	
	Burnnary Witcom Domain Research Bertings	Version: E0.0 Lizame: 10.50 Elitton	

_	Description				
3.	Add the Session M	anager IP address in th	e Domain field.	Below shows the r	esult of
	addition.	-			
	Tenert WestTL Gaterias X	stants) Stratul Institution			
	e - C	And and a constant of a constant		110	-
				and the second se	
	_				
	dammary .	Domains			
	Work				
	thinset.	Outain		Aat	
	Bane				
	Settings	Domain	Action		
		14.1 10.65			
1	Create a route to th	Section Manager for	the following:		
	tesherfi				
					Sgi Oil
	Summary	EDIT ROUTE			agri Oir
	Summary Wazard	EDIT ROUTE			-Sigs Ox
	Summary Wittend Domain				-Sgi Or
	Summary Wittand Domain Rustes				-Sigi Ost
	Summary Wittand Domain Restings	EDIT ROUTE	efhod		-Sign Ost
	Summary Wittant Domain Rustes Settings	EDIT ROUTE	ethod		-Sgi Ox
	Summary Wittand Domain Ruttles Settings	EDIT ROUTE	ethod enti: p:10.1.10.60:5500;x.t/denge		-Sigi Ost
	Summury Wittand Domain Rissens Settings	EDIT ROUTE	effrod ent. 0.10.1.10.60:5060;#Jtionege		-Sigi Ost
	Summary Wittant Domain Rustes Settings	EDIT ROUTE	ethod: estil: 0:10.1.10.60:5060.#.tränege det		-Sgi Oir
	Summary Wittaint Domain Risates Settings	EDIT ROUTE	ethod ethod or 10, 1, 10, 60: 5000; it thérago det an éxpressiant to match and resorte Self aseeds that consist at any digits in the le provergen, com Centination	JHD, The arguing if Pile	Sign Ox
	Summary Wittant Domain Ristles Settings	EDIT ROUTE	ethod ethod ethod p:10.1.10.60:5000.w.trianse det assedy that consol a traffy dapts in the la periority dapts in the la periority of consol a traffy dapts in the la	UIIIn The angular IP Fee	Sign Ox
	Summary Wittand Domain Russives Settings	EDIT ROUTE	ethod: estri 0.10.1.10.00:5060.#.tridenop det ar depression to marce and rewrite Sar- guedy fuel constant a min digits in the la periority digits in the la	HID: The sequence of the seque	Sign Ost

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**.

stat	us aesvcs	cti-li	.nk				
			AE SERVICES	CTI LINK STAT	TUS		
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd	
1 2		no no		down 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**.

Αναγα	ŝ	Application Enables Management C	ment Services Desole	Between the Representation of the Second Sec
Hoden 2 Al Services Communit ation Messager Mink AuditmWy	Services Services Server Lythic Eduction, Sciences, 20 or	- Marci		mane indu Log
A Linesson	Service	State	Incl	Cana
T PRINTERSON	CHIAN Dervice	(Owned)	2004-04-12 10:22:09	DODMA.
a Belestking	DLC Service	OPPUME *	2010-04-12 18-28-89	Dio_UCRASE_ACOUNED
- Service	DRCC Bevie	(34,34)	305e-64-12 18:03:18	DEPHA
Contraction of the local data and the local data an	TEPI Service	124.818	3050-04-12 18:33.38	30MA
Alare Vewer Los Mayape - Urap - Battal and Cartrol	P The states of the Dibble and East	entries and within the Johnson of Phil	NG. Step. Pro 12 ¹⁹ -1318 status would appear wither unit a lim	n is administered of a solid lawran is provided.

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).

₩eb Chat		
	#Login	
	Name	Natrie
	NRIC	12345678
		-Start Reset

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**.

Chat Box		
igent lease wait while we connect you with our representative	01mi + 5 1118	

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 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.

Chat Box		
bios-+d iii++	User .	
Ngent 40w zan i Ivelp you	0010+111+1	
Agent do you want video.?	Q1110-4-7 11-47	
German + 3 12 45 985	User	
Type your mession freez-		

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

1 11802/12802 - Year Ven - Section Libration		
18 10 17 10 1.19 123 mod Addition reed bro	n*	
	PAR	
wallsord	O The Vend	
185 * Shaffed And City	Product and a second design of the second design of	Gataner
Select 1 0 0	Sam 22342678 PHAN 90077342	Here
Para di Santa di Sant	Agent Read was allely on content you with an integrationalise Text	a
	Hidany Internation Data 0. 86/04/2016.04/22:19 - Churl - 322455/29 (202481204-6281-6531-6876-5467206652) 0. 88/04/2016.04:19/22 - Churl - 322455/29 (20248822-0636-4766-6855-426008.042) 0. 89/04/2016.11:10:05 - Churl - 3234554/29 (20048881-8606-6356-6356-6355-426008.042) 0. 00000000000000000000000000000000000	
A	Relative to March Mallow THAC	@ 10100440, 11 (17 44

Solution & Interoperability Test Lab Application Notes ©2016 Avaya Inc. All Rights Reserved. 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.

1 100171000 (from pard - though Channes	the second se	HERE AND
Bleff/10110126/machimerscoreshitm#		A1014
and the second se		Avaya Charles and Charles Contraction
Wollboard	• ***	
same ingto Avail 100	Har WE Part	Contrare .
tain 1 8 1	Sen ILLIGUZE BUITLAD	Totana
From 1 of 1 = - (3) * Service generation + Economic	Agent Person and while we convert pro official representation	
	Makey	
	n 0//0//2015 01/01/5 1/. 0//0//2015 01/01/5 (0///13) 0//0//2016 01/01/5 (0///13) 0//0//2016 01/5/11/2 (f/// 12) 0//0//2016 01/2016 01/2016 (f/// 12) 0//0//2016 01/2016 01/2016 (f/// 12) 0//0//2016 (f/// 12) 0//0//2016 (
S a to Teller & Multimedia Agent (Tent.		THLAC @ 20180412,1818:19

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.

S Chill Box		
Spent Hease wait while we connect you with our representative	Come+3 36.00 +	
The second second second		

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

12. Conclusion

These Application Notes describe the configuration steps required for TetherfiTM 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 <u>http://support.avaya.com</u>.

[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.

©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 <u>devconnect@avaya.com</u>.