



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking with Avaya Aura® Communication Manager Release 5.2.1 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2.1, Avaya Session Border Controller for Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

MTS Allstream is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction	3
2.	General Test Approach and Test Results	3
2.1.	Interoperability Compliance Testing	3
2.2.	Test Results	4
2.3.	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	9
5.	Configure Communication Manager	10
5.1.	Licensing and Capacity	10
5.2.	System Features	11
5.3.	IP Node Names	12
5.4.	Codecs	12
5.5.	IP Network Region	13
5.6.	Signaling Group	16
5.7.	Trunk Group	19
5.8.	Calling Party Information	22
5.9.	Outbound Routing	23
5.10.	Incoming Call Handling	25
5.11.	Saving Communication Manager Configuration Changes	25
6.	Configure Avaya Session Border Controller for Enterprise	26
6.1.	Avaya Session Border Controller for Enterprise Login	27
6.2.	Global Profiles	29
6.2.1.	Uniform Resource Identifier (URI) Groups	29
6.2.2.	Routing Profiles	31
6.2.3.	Topology Hiding	32
6.2.4.	Server Interworking	34
6.2.5.	Signaling Manipulation	39
6.2.6.	Server Configuration	40
6.3.	Domain Policies	44
6.3.1.	Application Rules	44
6.3.2.	Media Rules	46
6.3.3.	Signaling Rules	48
6.3.4.	Endpoint Policy Groups	53
6.3.5.	Session Policy	55
6.4.	Device Specific Settings	57
6.4.1.	Network Management	57
6.4.2.	Media Interface	58
6.4.3.	Signaling Interface	59
6.4.4.	End Point Flows - Server Flow	59
6.4.5.	Session Flows	62
7.	MTS Allstream SIP Trunking Service Configuration	63
8.	Verification and Troubleshooting	64
9.	Conclusion	67
10.	References	68

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2.1, Avaya SBC for Enterprise (Avaya SBCE) and various Avaya endpoints. This documented solution does not extend to configurations without Avaya SBCE.

Customers using this Avaya SIP-enabled enterprise solution with MTS Allstream SIP Trunking Service are able to place and receive PSTN call via a broadband connection. This converged network solution is an alternative to traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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.

MTS Allstream is a member of the Avaya DevConnect Service Provider program. The general test approach is to connect a simulated enterprise to MTS Allstream SIP Trunking Service via the public Internet and exercise the features and functionality listed in Section 2.1. The simulated enterprise is comprised of Avaya Aura® Communication Manager, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

2.1. Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking Service interoperability, the following features and functionalities are covered during the interoperability compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN call to various phone types (H.323, digital and analog telephone) at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN call from various phone types (H.323, digital and analog telephone) at the enterprise. All outbound calls to PSTN are routed from the enterprise using the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) H.323 softphone. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411)... etc.
- Proper codec negotiation with G.729 and G.711MU codecs.

- DTMF tone transmissions as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- Incoming and outgoing fax over IP with G.711MU codec.
- User features such as hold and resume, transfer and conference.
- Off-net call forwarding with SIP Diversion method.
- EC500 mobility (extension to cellular).
- Routing inbound vector call to call center agent queues.
- Network Call Redirection using reINVITE for transferring of inbound call back to PSTN.
- Session Timers implementation from both ends of the enterprise and the service provider.

Items that are not supported or tested are as follows:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance test because MTS Allstream did not provide the necessary configuration.
- T.38 fax is not supported.
- Off-net call forwarding using History-Info method is not supported.
- SIP phone and 1XC SIP soft phone are not tested.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations/limitations described below.

1. **Off-net blind transfer is not successful with REFER method.** In an inbound call scenario, Communication Manager receives an initial INVITE with REFER method present in Allow header. Communication Manager transfers off-net an inbound call to PSTN with a REFER request. MTS Allstream SIP Trunking Service does not properly support REFER as it accepts the REFER with a SIP/202 message but the call transfer is not successful. Both call legs are still maintained after transfer is complete. This issue is corrected by disabling the **Network Call Redirection** flag on outgoing trunk group to make Communication Manager transfer the call with **reINVITE** request. The detail configuration is described in **Section 5.7**.
2. **Network Call Redirection is not successful with “302 Moved Temporarily”.** A vector DN is programmed to use “302 Moved Temporarily” to redirect an inbound call to PSTN before answering. MTS Allstream SIP Trunking Service does not properly support “302 Moved Temporarily” as it sends an ACK to the “302 Moved Temporarily” but does not redirect the call to PSTN party specified in the Contact header.
3. **The untrusted calling party name from Communication Manager is not examined.** In an outbound call scenario, PSTN displays the original untrusted calling party name from Communication Manager. MTS Allstream SIP Trunking Service does not examine the calling party name before sending to PSTN. This is a known issue on MTS Allstream SIP Trunking Service and there is no available resolution at this time.

4. **The calling party name for outbound call is not being displayed by PSTN.** In an outbound call scenario, Communication Manager sends both calling party name and number to PSTN. But in some cases, PSTN phone displays the Calling Party Number only and no Calling Party Name. In other cases, PSTN phone displays both Calling Party Name and Number. The Calling Party Name may be overridden by MTS Allstream SIP Trunking Service or by intermediate service providers that route the call through PSTN. This issue has low user impact, and is listed here simply as an observation.
5. **Communication Manager extension holds an inbound call but the incoming audio traffic is still being sent by MTS Allstream SIP Trunking Service.** To hold an inbound call, Communication Manager sends a reINVITE with a=sendonly in SDP. MTS Allstream SIP Trunking Service responds with 200OK and a=recvonly in SDP which means that the incoming audio traffic on Communication Manager will be deactivated. But MTS Allstream SIP Trunking Service still sends audio when the call is in “recvonly” state. This issue has low user impact, it is listed here simply as an observation.
6. **In an inbound call scenario, MTS Allstream SIP Trunking Service does not refresh the Session Timer.** MTS Allstream SIP Trunking Service sends an initial INVITE with *Session-Expires: 3600; refresher: uac Min-SE: 600*. It means, as a user agent client, MTS Allstream SIP Trunking Service should refresh the Session Timer every 300 seconds by a reINVITE or UPDATE. In the compliance test, Communication Manager does not receive any Session Timer refresh signaling. This is a known issue on MTS Allstream SIP Trunking Service and there is no resolution available at this time.
7. **Fax over IP using G.711MU codec is successful.** Communication Manager does not officially support fax call using G.711MU codec. However, in the compliance test the incoming and outgoing fax calls appear to work with G.711MU codec by setting “fax=off” in codec profile. The fax document is transmitted successfully with acceptable quality. Communication Manager handles the fax call like a regular voice call using G.711MU codec and it only supports this fax call in best effort. Notes: the codec set should have G.711MU codec as a first choice otherwise the fax call would not be successfully established. The codec set is configured in **Section 5.4** and **Section 6.3.5**.
8. **Off-net call transfer, the calling party name and number is not updated to PSTN party.** A Communication Manager extension transfers an incoming call off-net to PSTN. Communication Manager sends UPDATE with true connected Calling Party Name and Number to both PSTN parties. The calling party information is in the URI-User and URI-Host portions of Contact header. However, the Calling Party Name and Number are not updated; the calling and called PSTN parties still display Calling Party Number of Communication Manager extension. This is a known issue on MTS Allstream SIP Trunking Service. It is recommended that MTS Allstream SIP Trunking Service support the calling party information update. This feature also needs to be supported by the service provider hosting the PSTN parties. This issue has low user impact and is listed here simply as an observation.
9. **Outgoing SIP Trunk from Communication Manager is frequently out of service.** Configure an outgoing SIP trunk group on Communication Manager to send OPTIONS heartbeat to Avaya SBCE. This outgoing OPTIONS is forwarded by Avaya SBCE to MTS Allstream SIP Trunking Service. Due to WAN condition, the OPTIONS is not being responded in a timely manner causing the SIP trunk group on Communication Manager to go out of service. To resolve this issue, configure **Enable Layer 3 Test?** to n

on the trunk group configuration on Communication Manager as shown in **Section 5.6**. Also, the OPTIONS heartbeat is enabled on Avaya SBCE under Server Configuration for MTS Allstream SIP Trunking as shown in **Section 6.2.6.1**. This setting will let the Avaya SBCE keep the SIP Trunk up between the enterprise and the service provider by originating the outgoing OPTIONS heartbeat. Note: The Server Configuration for Communication Manager in **Section 6.2.6.2** has OPTIONS heartbeat disabled. This means that Avaya SBCE still forwards the incoming OPTIONS heartbeat from MTS Allstream SIP Trunking to Communication Manager but it does not originate OPTIONS heartbeat to Communication Manager.

10. **Local calls from a Communication Manager extension (Phone1) routed via MTS Allstream SIP Trunking Service to another Communication Manager extension (Phone2) results in no audio.** This problem has low user impact because all other local outgoing calls from the enterprise to PSTN (i.e. calls within the same area code) complete successfully with audio. Audio is only impacted when calling another Communication Manager via MTS Allstream SIP Trunking Service. In general, these calls would be routed within the enterprise which avoids the problem. This failure scenario is also related to shuffling because if shuffling is disabled on the service provider trunk then there is no audio issue. However, it is not recommended to disable shuffling and the failing scenario can be avoided by routing these types of calls within the enterprise.
11. **Performing an “Application Restart” or editing the SigMa script on Ayaya SBCE causes the SigMa script not working.** There is no resolution currently. If the SigMa script does not work after an “Application Restart” or editing, please contact Avaya SBCE support by telephone number 1-866-861-3113 or 1-214-269-2424.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on MTS Allstream SIP Trunking Service, please contact MTS Allstream technical support at:

- Phone: 204-941-8557 or 1-800-542-8703
- Website: <http://www.mts.ca/mts/personal/support>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunking Service (Vendor Validation circuit) through a public Internet WAN connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

The Avaya components used to create the simulated customer site included:

- Avaya S8300 Communication Manager card running on G450 Media Gateway
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® Messaging

- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (H.323)
- Avaya one-X® Communicator soft phones (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise network is Avaya SBCE. It has a public side that connects to MTS Allstream SIP Trunking Service via internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and MTS Allstream SIP Trunking Service across the public network is UDP; the transport protocol between the Avaya SBCE and Communication Manager across the enterprise network is TCP.

In the compliance testing, the Avaya CPE environment is configured with SIP domain “**avaya.com**” for the enterprise. Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to MTS Allstream SIP Trunking Service. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

Note: It is assumed the general installation and configuration of Avaya Aura® Messaging is completed and is not discussed in these Application Notes.

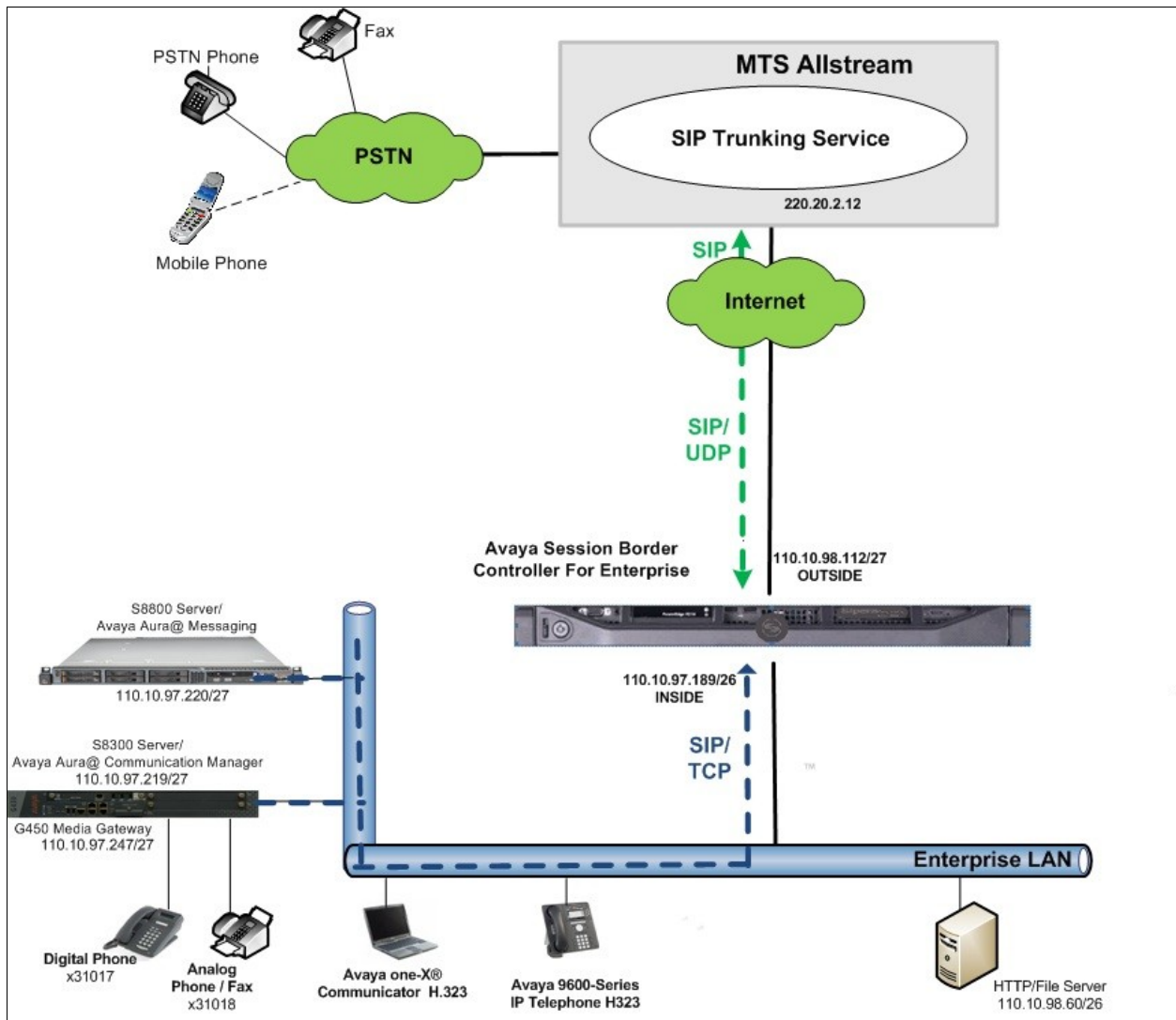


Figure 1: Avaya IP Telephony Network Connecting to MTS Allstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on Avaya S8300 Server	5.2.1 (R015x.02.1.016.4)
Avaya G450 Media Gateway	FW Version: 28.22.0 HW Vintage:1
Avaya Aura® Messaging running on Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller for Enterprise	4.0.5 Q2
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 5.2.1
Avaya one-X Communicator (H.323)	6.1.3.08-SP3-Patch2-35791
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
MTS Allstream SIP Trunking Service Components	
Component	Release
Genband S3	5.2.2.12
CS2K	CVM13

Table 1: Equipment and Software Tested

Note that this solution is compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for inter-operating with the MTS Allstream SIP Trunking Service (MTS Allstream).

Two separate SIP trunk groups are created between Communication Manager and Avaya SBCE to carry traffic to and from service provider respectively. For inbound call, the call flows from the MTS Allstream to Avaya SBCE to Communication Manager. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. Outbound call to PSTN is first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Avaya SBCE for egress to the MTS Allstream.

For the compliance test, Communication Manager sends 11 digits in the destination headers (e.g., Request-URI and To) and sends 10 digit in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). MTS Allstream sends 10 digits in destination headers and sent 11 digits in source headers.

It is assumed the general installation of the Communication Manager and the Avaya G450 Media Gateway has been previously completed and is not discussed here.

The Communication Manager configuration is performed using the System Access Terminal (SAT). Some screens in this section have been abridged for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that 450 licenses are available and 128 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sale representative to add the additional capacity or feature.

display system-parameters customer-options		Page 2 of 10
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	450	0
Maximum Concurrently Registered IP Stations:	450	0
Maximum Administered Remote Office Trunks:	0	0
Maximum Concurrently Registered Remote Office Stations:	0	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	450	0
Maximum Video Capable Stations:	450	0
Maximum Video Capable IP Softphones:	450	0
Maximum Administered SIP Trunks:	450	128
Maximum Administered Ad-hoc Video Conferencing Ports:	450	0
Maximum Number of DS1 Boards with Echo Cancellation:	0	0
Maximum TN2501 VAL Boards:	0	0
Maximum Media Gateway VAL Sources:	50	1
Maximum TN2602 Boards with 80 VoIP Channels:	0	0
Maximum TN2602 Boards with 320 VoIP Channels:	0	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming call from PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming call should not be allowed to transfer back to PSTN then leave the field set to **none**.

change system-parameters features		Page 1 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled?	n	
Trunk-to-Trunk Transfer:	all	
Automatic Callback with Called Party Queuing?	n	
Automatic Callback - No Answer Timeout Interval (rings):	3	
Call Park Timeout Interval (minutes):	10	
Off-Premises Tone Detect Timeout Interval (seconds):	20	
AAR/ARS Dial Tone Required?	y	

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of **AV-Restricted** for restricted call and **AV-Unavailable** for unavailable call.

change system-parameters features		Page 9 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
CPN/ANI/ICLID PARAMETERS		
CPN/ANI/ICLID Replacement for Restricted Calls:	AV-Restricted	
CPN/ANI/ICLID Replacement for Unavailable Calls:	AV-Unavailable	
DISPLAY TEXT		
	Identity When Bridging:	principal
	User Guidance Display?	n
	Extension only label for Team button on 96xx H.323 terminals?	n

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and Avaya SBCE. These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

```
change node-names ip
                        IP NODE NAMES
      Name             IP Address
DevASM                110.10.97.198
AvayaSBCE            110.10.97.189
default               0.0.0.0
msgserver             110.10.97.248
procr                110.10.97.219
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. MTS Allstream supports G.729 and G.711MU. To use these codecs, enter G.711MU and G.729 in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

```
change ip-codec-set 1                                     Page 1 of 2
                        IP Codec Set
Codec Set: 1
Audio      Silence   Frames   Packet
Codec      Suppression Per Pkt   Size (ms)
1: G.711MU      n         2       20
2: G.729        n         2       20
3:
```

MTS Allstream only supports fax using G.711MU codec in the compliance test. The T.38 faxing is not currently supported. Communication Manager does not officially support fax call using G.711MU codec. However, incoming and outgoing fax call using G.711MU codec appear to work during testing when configuring fax = off. Communication Manager handles the call like a regular voice call and only supports fax call using G.711MU codec in best effort. **Note:** The codec profile should have G.711MU codec as a first choice otherwise the fax call would not be successfully established.

To use G.711MU codec for fax, set the **Fax Mode** to **off** on **Page 2**.

change ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
FAX	off	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

Note: To successfully send and receive fax using G.711MU codec, the voice call has to be established with G.711MU codec. The **Session Policy** configuration on Avaya SBCE in **Section 6.3.5** makes G.711MU as the first choice in the preference codec.

5.5. IP Network Region

A separate IP network region for the service provider trunk groups is created. This allows separate codec or quality of service setting to be used (if necessary) for call between the enterprise and the service provider versus call within the enterprise or elsewhere. For the compliance test, **ip-network-region 1** is created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance test, the domain name **avaya.com** is assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP message originating from this IP region. **Note:** Topology-Hiding configuration on Avaya SBCE in **Section 6.2.3** is used to convert this private domain name to the public IP Address of the Avaya SBCE for the URI-Host portion in From and PAI headers.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level under Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```

change ip-network-region 1                                     Page 1 of 19
                                IP NETWORK REGION
  Region: 1
Location: 1              Authoritative Domain: avaya.com
    Name: MTS Allstream
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
  Codec Set: 1                      Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                                IP Audio Hairpinning? n
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                      RTCP Reporting Enabled? y
  Call Control PHB Value: 46          RTCP MONITOR SERVER PARAMETERS
    Audio PHB Value: 46              Use Default Server Parameters? y
    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

```

change ip-network-region 1										Page	3	of	19
Source Region: 1 Inter Network Region Connection Management										I		M	
										G	A	t	
dst codec direct	WAN-BW-limits		Video		Intervening		Dyn	A	G	c			
rgn set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e				
1	1								all				
2	1	y	NoLimit						n		t		
3	1	y	NoLimit						n		t		
4													

For the compliance test, devices with IP addresses in the 110.10.97.0/24 subnet are assigned to network region 1. These include Communication Manager, Avaya G450 Media Gateway and Avaya SBCE that are set up for a shared test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are assigned to network region 1 with IP address in the 110.10.98.0/26 subnet. In a production environment, different sites will typically be on different networks and ranges of IP addresses assigned by the DHCP scope serving the site. They can be entered as one entry in the network map to assign all telephones in a range to a specific network region.

The following screen illustrates a subset of the IP network map configuration used to verify in these Application Notes.

change ip-network-map				Page	1 of 63
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location Ext	
-----	-----	-----	-----	-----	
FROM: 110.10.97.0	/24	1	n		
TO: 110.10.97.255					
FROM: 110.10.98.0	/26	1	n		
TO: 110.10.98.63					
FROM:	/		n		
TO:					

Next step is to allocate the resource on Communication Manager for IP network region 1. For SIP Trunk, the IP interface **procr** is used to process SIP signaling and Avaya G450 Media Gateway is used to process media. Both IP interfaces are assigned under the same region.

To defined network region 1 for ip interface **procr**, used **change ip-interface procr** command as shown in the following screen.

change ip-interface procr		Page 1 of 1	
IP INTERFACES			
Type: procr		Target socket load: 1700	
Enable Interface? y	Allow H.323 Endpoints? y		
Network Region: 1	Allow H.248 Gateways? y		
	Gatekeeper Priority: 5		
IPV4 PARAMETERS			
Node Name: procr			
Subnet Mask: /26			

To defined network region 1 for ip interface of Avaya G450 Media Gateway, used **change media-gateway** command as shown in the following screen.

```

change media-gateway 1                                     Page 1 of 1
                                MEDIA GATEWAY
      Number: 1                      Registered? y
      Type: g450                    FW Version/HW Vintage: 28 .22 .0 /1
      Name: Media Gateway 1          MGP IP Address: 110.10 .97 .247
      Serial No: 08IS38199691        Controller IP Address: 110.10 .97 .219
      Encrypt Link? y                MAC Address: 00:1b:4f:03:51:08
Network Region: 1      Location: 1      Enable CF? n
                                      Site Data:
      Recovery Rule: none

Slot  Module Type      Name      DSP Type  FW/HW version
V1:   S8300            ICC MM      MP80      15  2
V2:
V3:   MM712            DCP MM
V4:   MM710            DS1 MM
V5:
V6:   MM711            ANA MM
V7:
V8:
V9:   gateway-announcements ANN VMM

Max Survivable IP Ext: 8

```

5.6. Signaling Group

Use the **add signaling-group** command to create two signaling groups between Communication Manager and Avaya SBCE, one for inbound calls from the service provider network and other for outgoing calls from the enterprise.

For the compliance test, signaling group 1 is created for inbound calls and is configured as follows:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test is conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between the Communication Manager and Avaya SBCE.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). The compliance test is conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5080** (the well-known port value for TCP is 5060).
- Set the **Peer Detection Enabled** field to **n**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP interface of **procr** defined in **Section 5.3**.
- Set the **Far-end Node Name** to **AvayaSBCE**. This node name maps to the IP address of Avaya SBCE as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region 1 defined for the service provider in **Section 5.5**.

- Set the **Far-end Domain** to **avaya.com**.
- Set the **DTMF over IP field** to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then Avaya Media Gateway will remain in the media path between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Direct IP-IP Early Media** is to **n**.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for inbound PSTN calls to complete through MTS Allstream.
- Default values may be used for all other fields.

Note: Once the signaling group 1 is successfully added, use command **display signaling-group 1** to verify the **Enable Layer 3 Test?** to **n**. The signaling group 1 is shown in the following screenshot. This setting disables Communication Manager to send out OPTIONS heartbeat to Avaya SBCE on the incoming trunk group. Communication Manager will use ICMP ping as an alternative to check the status of the far end system. Please refer to **Section 2.2**, observation #9 for detail information

```
display signaling-group 1
                                SIGNALING GROUP

Group Number: 1                Group Type: sip
                                Transport Method: tcp

IMS Enabled? n
    IP Video? n

Near-end Node Name: procr      Far-end Node Name: AvayaSBCE
Near-end Listen Port: 5060     Far-end Listen Port: 5060
                                Far-end Network Region: 1
Far-end Domain:avaya.com

Incoming Dialog Loopbacks: eliminate
                                Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
                                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3    IP Audio Hairpinning? n
                                Enable Layer 3 Test? n
                                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n    Alternate Route Timer(sec): 12
```

The signaling group for outbound calls from the enterprise to PSTN is similarly configured except that the Far-end Domain is set to **avaya.com**. This domain will be manipulated by Avaya SBCE to IP address in URI-Host that is known to MTS Allstream. For the compliance test, signaling group 2 is created and is shown command by **display signaling-group 2** as below.

```
display signaling-group 2                                     Page 1 of 1
SIGNALING GROUP

Group Number: 2                      Group Type: sip
Transport Method: tcp

IMS Enabled? n
IP Video? n

Near-end Node Name: procr             Far-end Node Name: AvayaSBCE
Near-end Listen Port: 5060            Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload             RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3    IP Audio Hairpinning? n
Enable Layer 3 Test? n                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? y Alternate Route Timer(sec): 12
```

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the two signaling groups created in **Section 5.6**. For the compliance test, trunk group 1 is configured for incoming calls and trunk group 2 is configured for outgoing calls as follows:

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Direction** field to **incoming** for trunk group 1 and **outgoing** for trunk group 2.
- Set the **Outgoing Display** to **y** to enable name display on the trunk.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**. The incoming trunk group 1 is set to incoming signaling group 1 and the outgoing trunk group 2 is set to use outgoing signaling group 2.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values are used for all other fields.

```
add trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 1                      Group Type: sip          CDR Reports: y
  Group Name: MTS_Inbound_Trunk      COR: 1                TN: 1          TAC: *101
  Direction: incoming                Outgoing Display? y
Dial Access? n                      Night Service:

Service Type: public-ntwrk          Auth Code? n

                                     Signaling Group: 1
                                     Number of Members: 32
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to service provider. This value defines the interval a re-INVITEs must be sent to keep an active session alive. For the compliance test, a value of **600** seconds is used.

```
add trunk-group 1                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

  SCCAN? n                            Digital Loss Group: 18
    Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y
```

On **Page 3**, set the **Numbering Format** field to **private**. Also the **Numbering Format** in the route pattern is set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoint to be replaced with the value set in **Section 5.2**, if inbound call enabled CPN block. Default values are used for all other fields.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
Show ANSWERED BY on Display? y	

On **Page 4**, the **Network Call Redirection** field is set to **y** which enables use of the SIP REFER message to transfer an incoming call back to PSTN. For more information, please refer to **Section 2.2**, observation #1.

- Set the **Send Diversion Header** field to **y**.
- Set the **Support Request History** field to **n**. This parameter determines History-Info header will be excluded in the call-redirection INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to **101**, the value is preferred by MTS Allstream.

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	

For outgoing trunk group configuration, the screen below shows **Page 1** of trunk group 2 for outgoing calls from the enterprise to MTS Allstream.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: MTS_Outbound_Trunk	COR: 1	TN: 1	TAC: *102
Direction: outgoing	Outgoing Display? y		
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk			
		Signaling Group: 2	
		Number of Members: 32	

On **Page 4** of trunk group 2, the **Network Call Redirection** is set to “n”.

Note: **Network Call Redirection** is set to “n”. This setting is used to reINVITE an off-net transfer for an incoming call back to PSTN. For more information, please refer to **Section 2.2**, observation #1.

add trunk-group 2		Page 4 of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling Number? n			
Send Transferring Party Information? n			
Network Call Redirection? n			
Send Diversion Header? y			
Support Request History? n			
Telephone Event Payload Type: 101			

The configuration on other pages of trunk group 2 is identical to trunk group 1.

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering is selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by service provider. They are used to authenticate the caller.

Normally DID number is comprised of the local extension plus a prefix. A single private numbering entry can be applied for all extensions. In the example below, all stations with a 7-digit extension beginning with **776** when receiving or calling call on trunk group 1 or 2 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
7	776	1-2	647	10	Total Administered: 4 Maximum Entries: 540

Even though private numbering is selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
7	776	1-2	647	10	Total Administered: 12 Maximum Entries: 240

5.9. Outbound Routing

Automatic Route Selection (ARS) feature is used to route outbound call via the SIP trunk to service provider. In the compliance test, a single digit 9 is used as the ARS access code. Enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown in the table below.

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 0		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
6	1	fac							
776	7	ext							
9	1	fac							
*	4	dac							
#	4	fac							

Use the **change feature-access-codes** command to define 9 as the **Auto Route Selection (ARS)** – **Access Code 1**.

change feature-access-codes		Page	1 of	8
FEATURE ACCESS CODE (FAC)				
Abbreviated Dialing List1 Access Code:				
Abbreviated Dialing List2 Access Code:				
Abbreviated Dialing List3 Access Code:				
Abbreviated Dial - Prgm Group List Access Code:				
Announcement Access Code: #007				
Answer Back Access Code:				
Attendant Access Code:				
Auto Alternate Routing (AAR) Access Code: 6				
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:		
Automatic Callback Activation:		Deactivation:		
Call Forwarding Activation Busy/DA: All:		Deactivation:		
Call Forwarding Enhanced Status: Act:		Deactivation:		
Call Park Access Code:				
Call Pickup Access Code:				
CAS Remote Hold/Answer Hold-Unhold Access Code:				
CDR Account Code Access Code:				
Change COR Access Code:				
Change Coverage Access Code:				
Conditional Call Extend Activation:		Deactivation:		
Contact Closure Open Code:		Close Code:		

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 (defined next) for outbound call which contains the SIP trunk to the service provider.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
0	1	18	2	pubu		n	
011	13	24	2	intl		n	
1	11	11	2	fnpa		n	
411	3	3	2	svcl		n	
416	10	10	2	pubu		n	
647	10	10	2	pubu		n	

As mentioned above, the route pattern defines which trunk group will be used for the outgoing calls and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern 2 as follows:

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 2 is used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** The prefix mark (**Pfx Mrk**) of 1 will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged and will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format:** **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8**.
- **LAR:** **none**.

change route-pattern 2												Page	1 of	3					
Pattern Number: 2												Pattern Name: MTS Outgoing							
SCCAN? n												Secure SIP? n							
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC						
No			Mrk	Lmt	List	Del	Digits					QSIG							
												Dgts							
													Intw						
1:	2	0			1							n	user						
2:												n	user						
3:												n	user						
4:												n	user						
5:												n	user						
6:												n	user						
BCC VALUE												TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Numbering	LAR
0 1 2 M 4 W													Request					Dgts Format	
																		Subaddress	
1:	y	y	y	y	y	n	n					rest		unk-unk	none				
2:	y	y	y	y	y	n	n					rest			none				
3:	y	y	y	y	y	n	n					rest			none				
4:	y	y	y	y	y	n	n					rest			none				
-																			

5.10. Incoming Call Handling

When an incoming call arrives, Communication Manager applies incoming handling treatment on incoming trunk group 1 (created in **Section 5.7**). MTS Allstream sends 10 digits in Request-URI and To headers identically to the assigned DID number. The incoming call handling treatment will translate this DID number to an extension. In the compliance test, the DID numbers have prefix 647, which are deleted to normalize the incoming number to match 7 digits extension on Communication Manager.

Use the **inc-call-handling-trmt trunk-group 1** command to define an incoming handling for MTS Allstream. Following table shows the configuration in detail on incoming trunk group 1.

change inc-call-handling-trmt trunk-group 1										Page 1 of 30	
INCOMING CALL HANDLING TREATMENT											
Service/	Number	Number	Del Insert								
Feature	Len	Digits									
public-ntwrk	10	647776	3								

5.11. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see Reference [7] and [8].

The compliance test comprises of configuration for two major components, trunk server for service provider and call server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is performed using the Avaya SBCE web user interface as described in the following sections.

Trunk server configuration elements for service provider MTS Allstream:

- Global Profiles
 - o URI Groups
 - o Routing
 - o Topology Hiding
 - o Server Interworking
 - o Signaling Manipulation
 - o Server Configuration
- Domain Policies:
 - o Application Rules
 - o Media Rules
 - o Signaling Rules
 - o Endpoint Policy Group
 - o Session Policy
- Device Specific Settings:
 - o Network Management
 - o Media Interface
 - o Signaling Interface
 - o End Point Flows → Server Flows
 - o Session Flows

Call server configuration elements at the enterprise for Communication Manager:


- Global Profiles:
 - o URI Groups
 - o Routing
 - o Topology Hiding
 - o Server Interworking
 - o Server Configuration
- Domain Policies:
 - o Application Rules
 - o Media Rules
 - o Signaling Rules
 - o Endpoint Policy Group

- Session Policy
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

6.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where `<ip-addr>` is the management LAN IP address of UC-Sec.

Enter appropriate credentials and click ***Sign In***.



The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the **UC-Sec Control Center** will appear as shown below.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:48:21 AM EDT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users** **Logout** **Help**

UC-Sec Control Center
Welcome

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

Alarms (Past 24 Hours)
None found.

Incidents (Past 24 Hours)

sipera: No Routing Rule matched
sipera: No Routing Rule matched
sipera: No Routing Rule matched
sipera: No Routing Rule matched

Administrator Notes [Add]
No notes posted.

Quick Links
Sipera Website
Sipera VIPER Labs
Contact Support

UC-Sec Devices	Network Type
sipera	DMZ_ONLY

To view system information that has been configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the Compliance test, a single device named **sipera** is added. To view the configuration of this device, click the **View Config** icon (the third icon from the right) as shown below.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:58:46 AM EDT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users** **Logout** **Help**

UC-Sec Control Center
System Management

Installed **Updates**

Device Name	Serial Number	Version	Status
sipera	IPCS31020134	4.0.5.Q02	Commissioned

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** is set to **SIP** and the **Deployment Mode** is set to **Proxy**. Default values are used for all other fields.

System Information: sipera

Network Configuration

General Settings		Device Settings	
Appliance Name	sipera	HA Mode	No
Box Type	SIP	Secure Channel Mode	None
Deployment Mode	Proxy	Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
110.10.97.189	110.10.97.189	255.255.255.192	110.10.97.129	A1
110.10.98.112	110.10.98.112	255.255.255.224	110.10.98.97	B1
110.10.98.108	110.10.98.108	255.255.255.224	110.10.98.97	B1
110.10.98.106	110.10.98.106	255.255.255.224	110.10.98.97	B1

DNS Configuration

Primary DNS	110.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	110.10.97.189

Management IP(s)

IP	110.10.98.85
----	--------------

6.2. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

6.2.1. Uniform Resource Identifier (URI) Groups

The **URI Group** feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

To add an **URI Group**, select **UC-Sec Control Center → Global Profiles → URI Groups**. Click on **Add Group** (not shown).

In the compliance test, a URI Group named **CM_MTSAllstream** is added with URI type **Plain** (not shown) and consists of four domain [*@anonymous.invalid](#), [*@avaya.com](#), [*@110.10.98.112](#) and [*@220.20.2.12](#). Domain “anonymous.invalid” is defined for private call

either from call server or trunk server had URI-Host masked by “anonymous.invalid”. The enterprise domain name “avaya.com” is for SIP Trunk domain defined in **Section 5.5** between Communication Manager and Avaya SBCE. For the public SIP Trunk between Avaya SBCE and MTS Allstream, the Avaya SBCE public IP address 110.10.98.112 is set as URI-Host of From, PAI and Diversion headers while the public IP address of MTS Allstream 220.20.2.12 is set as URI-Host of Request-URI and To headers.

This URI-Group is used to match the **From** and **To** headers in a SIP call dialog received from both Communication Manager and MTS Allstream. If there is a match, the Avaya SBCE will apply the appropriate **Routing Profile** and **Server Flow** to route the inbound and outbound call to the right destination. The **Routing Profile** and **Server Flow** are configured in **Section 6.2.2** and **Section 6.4.4** appropriately.

The screenshot below illustrates the URI Listing for URI group **CM521_MTSAllstream**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'URI Groups' highlighted. The main content area shows the configuration for the 'CM521_MTSAllstream' group. A table titled 'URI Listing' contains the following entries:

URI	Actions
*@110.10.98.112	[Edit] [Delete]
*@220.20.2.12	[Edit] [Delete]
*@anonymous.invalid	[Edit] [Delete]
*@avaya.com	[Edit] [Delete]

6.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by **Routing Profiles** include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a **Routing Profile**, select **UC-Sec Control Center → Global Profiles → Routing**. Click on **Add Profile** (not shown).

In the compliance test, a **Routing Profile** named **To_MTSAllstream** is created to be used in conjunction with the server flow defined for Communication Manager. This entry is to route the outgoing call from enterprise to MTS Allstream.

In the opposite direction, a **Routing Profile** named **To_CM521** is created to be used in conjunction with the server flow defined for MTS Allstream. This entry is to route the incoming call from MTS Allstream to enterprise.

6.2.2.1 Routing Profile for MTS Allstream

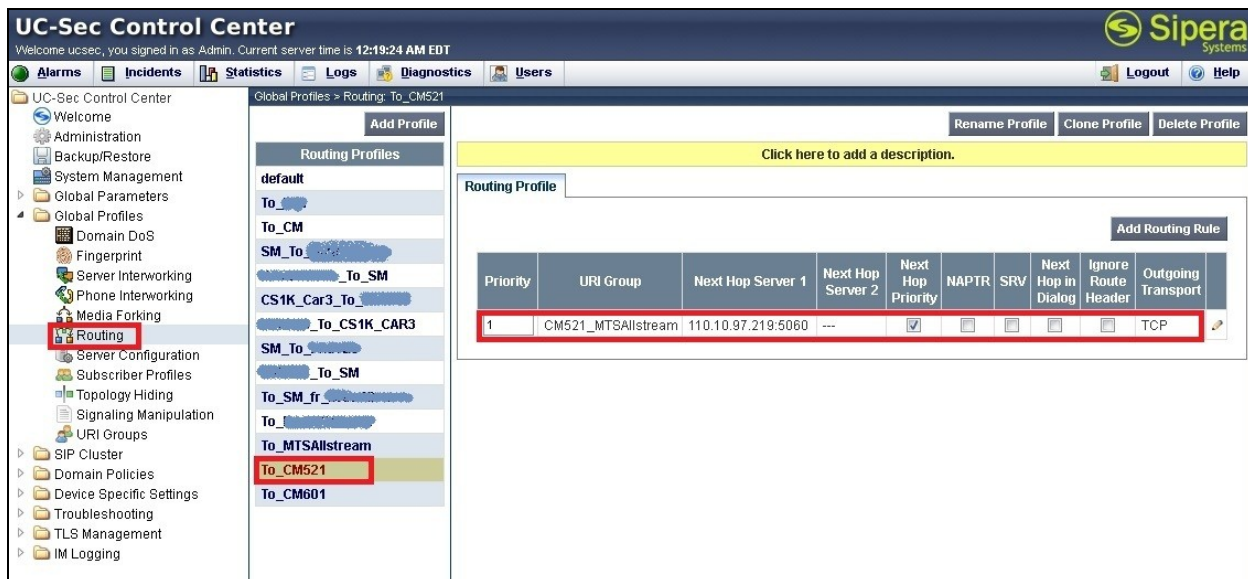
The screenshots below illustrate the **UC-Sec Control Center → Global Profiles → Routing: To_MTSAllstream**. As shown in **Figure 1**, MTS Allstream SIP Trunk is connected with transportation protocol **UDP**. If there is a match in the **To** header of the **CM_MTSAllstream** URI Group defined in **Section 6.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of MTS Allstream SIP Trunk on port **5060**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows the navigation menu with 'Routing' highlighted. The main content area is titled 'Global Profiles > Routing: To_MTSAllstream'. It features a list of Routing Profiles on the left, including 'default', 'To_CM', 'SM_To', 'To_SM', 'CS1K_Car3_To', 'To_CS1K_CAR3', 'SM_To', 'PAETEC_To_SM', 'To_SM_fr', 'To', 'To_MTSAllstream' (highlighted), 'To_CM521', and 'To_CM601'. The 'To_MTSAllstream' profile is selected, showing its configuration details. A table lists the routing rules for this profile, with the first rule highlighted in red:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_MTSAllstream	220.20.2.12:5060	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

6.2.2.2 Routing Profile for Communication Manager

The routing profile **To_CM521** is defined to route call where the **To** header matches the URI-Group **CM_MTSAllstream** defined in Section 6.2.1 to **Next Hop Server 1** which is the IP address of Communication Manager, on port **5060** as a destination. As shown in **Figure 1**, SIP Trunk between Communication Manager and Avaya SBCE is connected with transportation protocol TCP.



6.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a **Topology Hiding** profile, select **UC-Sec Control Center** → **Global Profiles** → **Topology Hiding**. Click on **Add Profile** (not shown).

In this compliance test, two Topology Hiding profiles **To_MTSAllstream** and **To_CM521** are created.

6.2.3.1 Topology Hiding Profile for MTS Allstream

Profile **To_MTSAllstream** is defined to mask the enterprise SIP domain **avaya.com** in Request-URI and To headers to IP **220.20.2.12** (the IP address MTS Allstream uses as URI-Host portion for Request-URI and To headers to meet the SIP specification requirement of MTS Allstream); mask the enterprise SIP domain **avaya.com** in From header to IP 110.10.98.112 (Avaya SBCE public IP address); and replace Record-Route, Via headers and SDP added by Communication Manager by external IP address known to MTS Allstream. It is to secure the enterprise network topology and also to meet the SIP requirement from service provider. The screenshots below illustrate the **Topology Hiding** profile **To_MTSAllstream**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Profiles, and SIP Cluster. The 'Topology Hiding' option is selected. The main panel displays the configuration for the 'To_MTSAllstream' profile. A table titled 'Topology Hiding' lists the headers, criteria, replace actions, and overwrite values.

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	220.20.2.12
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	220.20.2.12
From	IP/Domain	Overwrite	110.10.98.112

Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on **From** header also applies to **Referred-By** and **P-Asserted-Identity** headers.
- The masking applied on **To** header also applies to **Refer-To** header.

6.2.3.2 Topology Hiding Profile for Communication Manager

Profile **To_CM521** is also needed to mask MTS Allstream URI-Host in Request-URI, From, To headers to the enterprise SIP domain **avaya.com**; replace Record-Route, Via headers and SDP added by MTS Allstream by internal IP address known to Communication Manager. The screenshots below illustrate the **Topology Hiding** profile **To_CM521**.

The screenshot shows the UC-Sec Control Center interface. On the left, a tree view shows the navigation menu with 'Topology Hiding' selected. The main panel displays the configuration for the 'To_CM521' profile. A table titled 'Topology Hiding' lists the headers, criteria, replace actions, and overwrite values.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	avaya.com
To	IP/Domain	Overwrite	avaya.com
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on **From** header also applies to **Referred-By** and **P-Asserted-Identity** headers.
- The masking applied on **To** header also applies to **Refer-To** header.

6.2.4. Server Interworking

Interworking Profile features are configured differently for Call and Trunk Servers.

To create a **Server Interworking** profile, select **UC-Sec Control Center** → **Global Profiles** → **Server Interworking**. Click on **Add Profile** (not shown).

In this compliance testing, two profiles **MTSAllstream** and **CM521** are created for MTS Allstream Trunk Server and Communication Manager Call Server.

6.2.4.1 Server Interworking profile for MTS Allstream

Profile **MTS Allstream** is defined to match the specification of MTS Allstream SIP Trunking Service. The **General** settings are configured with following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **None**. Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to MTS Allstream.
- 18X Handling = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from Communication Manager unchanged to MTS Allstream.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer. It will keep the Refer message from Communication Manager unchanged to MTS Allstream.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the From header with anonymous for outbound call to MTS Allstream. It depends on the Communication Manager to enable/disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by Communication Manager to MTS Allstream.

The screenshots below illustrate the **Server Interworking** profile **MTSAllstream**.

The screenshot shows the 'Editing Profile: MTSAllstream' window with the 'General' tab selected. The window has a title bar with a close button. The 'General' tab is highlighted with a blue header. The following settings are visible:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

A red box highlights the 'None' radio button for 'Hold Support'. Another red box highlights the 'None' radio buttons for '180 Handling', '181 Handling', '182 Handling', and '183 Handling'. A third red box highlights the checked checkbox for 'Refer Handling'. A fourth red box highlights the checked checkbox for 'T.38 Support'. A red box highlights the 'Next' button at the bottom right.

The screenshot shows the 'Editing Profile: MTSAllstream' window with the 'Privacy' and 'DTMF' tabs visible. The 'Privacy' tab is active, showing the following settings:

Setting	Value
Privacy Enabled	<input checked="" type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

The 'DTMF' tab is visible below the 'Privacy' tab, showing the following settings:

Setting	Value
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

A red box highlights the checked checkbox for 'Privacy Enabled'. Another red box highlights the 'None' radio button for 'DTMF Support'. At the bottom, there are 'Back' and 'Finish' buttons, with a red box highlighting the 'Finish' button.

6.2.4.2 Server Interworking profile for Communication Manager

Profile **CM521** is defined to match the specification of Communication Manager. The **General** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **RFC3264**. Communication Manager supports hold/ resume as per RFC3264.
- 18X Handling = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from MTS Allstream to Communication Manager unchanged.
- Refer Handling = **unchecked**. Avaya SBCE will not handle **Refer**, it will keep the Refer messages from MTS Allstream to Communication unchanged.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the **From** header with anonymous for inbound call from MTS Allstream. It depends on the MTS Allstream to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by MTS Allstream to Communication Manager.

The screenshots below illustrate the **Server Interworking** profile **CM521**.

Editing Profile: CM521

General	
Hold Support	<input type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input checked="" type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

Editing Profile: CM521

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back **Finish**

6.2.5. Signaling Manipulation

The **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which is configured in the next steps through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in **Topology Hiding**.

To create a **Signaling Manipulation** script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown).

In the compliance testing, a SigMa script named **MTSAllstream** is created for Server Configuration MTS Allstream and described detail as following:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.HOST= "110.10.98.112";
  }
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].regex_replace("sip:110.10.98.112","sip:avaya.com");
    %HEADERS["To"][1].regex_replace("sip:110.10.98.112","sip:ping@110.10.98.112");
    %HEADERS["From"][1].regex_replace("sip:220.20.2.12","sip:ping@220.20.2.12");
  }
}
```

The statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** is to specify the script will take effect on all type of SIP messages for outbound calls and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement. The **Topology-Hiding** profile **MTSAllstream** could mask the P-Asserted-Identity header properly. However, as a limitation, the P-Asserted-Identity header in “response” SIP message will still have the private enterprise SIP domain. Therefore, a SigMa rule is used to correct the URI-Host of P-Asserted-Identity header.

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify the script will take effect on all types of SIP messages for inbound calls and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement. The purpose of the SigMa script **MTAllstream** is to normalize the OPTIONS received from MTS Allstream. The header **From** and **To** need to be modified to have URI-User@URI-Host format, otherwise the OPTIONS will fail to match the URI-Group defined in **Section 6.2.1**. If unmatching happens, the **Routing**

Profile and **Server Flow** (discussed in **Section 6.4.4**) will not be applied to the call and it will result dropped packets.

With the SigMa script in place, the OPTIONS heartbeat from MTS Allstream will be forwarded to Communication Manager. The 200OK response from Communication Manager will confirm the status of SIP Trunk as active. If there is no response, MTS Allstream will change the status of SIP Trunk to “out of service”.

Note: SigMa script for Communication Manager is unnecessary because in the compliance test Communication Manager is configured not to send OPTIONS heartbeat to MTS Allstream. The OPTIONS heartbeat will be implemented on Avaya SBCE under Server Configuration. Please see **Section 2.2**, observation #9 for more information.

6.2.6. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **UC-Sec Control Center → Global Profiles → Server Configuration**. Click on **Add Profile** (not shown).

In the compliance testing, two separate Server Configurations are created, server entry **MTSAllstream** for MTS Allstream, and server entry **CM521** for Communication Manager.

6.2.6.1 Server Configuration for MTS Allstream

The **Server Configuration** named **MTSAllstream** is added for MTS Allstream, it will be discussed in detail as below. **General**, **Heartbeat** and **Advanced** tabs are provisioned, but no configuration is done for **Authentication** tab as MTS Allstream did not implement Authentication on a SIP Trunk

The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. The left sidebar shows a tree view of the system configuration, with 'Server Configuration' highlighted under 'Global Profiles'. The main content area shows the 'Global Profiles > Server Configuration: MTSAllstream' page. It features a list of profiles on the left, including 'SM', 'Bell', 'Windstream', 'PAETEC', 'CS1K_Car3', 'Broadconnect', 'MTSAllstream' (highlighted), 'CM521', and 'CM601'. The 'MTSAllstream' profile is selected, and its configuration is shown in the main area. The configuration is divided into four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing the following details:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	220.20.2.12
Supported Transports	UDP
UDP Port	5060

Buttons for 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible at the top right of the configuration area.

In the **General** tab, set **Server Type** for MTS Allstream to **Trunk Server**. In the compliance testing, MTS Allstream supports UDP and listens on port 5060.

Edit Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma separated list	220.20.2.12
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
Finish	

The OPTIONS heartbeat is implemented on Avaya SBCE under Server Configuration for MTS Allstream. Please see **Section 2.2**, observation #9 for more information. The following screenshot shows the configuration in Heartbeat tab in detail.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@110.10.98.112
To URI	ping@220.20.2.12
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
Finish	

Under **Advanced** tab, for **Interworking Profile** drop down list select **MTSAllstream** as defined in **Section 6.2.4**, and for **Signaling Manipulation Script** drop down list select **MTSAllsteram** as defined in **Section 6.2.5**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from MTS Allstream. The other settings are kept as default. Click **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	MTSAllstream
Signaling Manipulation Script	MTSAllstream
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

6.2.6.2 Server Configuration for Communication Manager

The **Server Configuration** named **CM521** is added for Communication Manager is discussed in detail below. **General**, **Heartbeat** and **Advanced** tabs are provisioned, but no configuration is done for **Authentication** tab.

UC-Sec Control Center
 Welcome ucsec, you signed in as Admin. Current server time is 11:42:43 AM EDT

Global Profiles > Server Configuration: CM521

General | Authentication | Heartbeat | Advanced

General	
Server Type	Call Server
IP Addresses / FQDNs	110.10.97.219
Supported Transports	TCP
TCP Port	5060

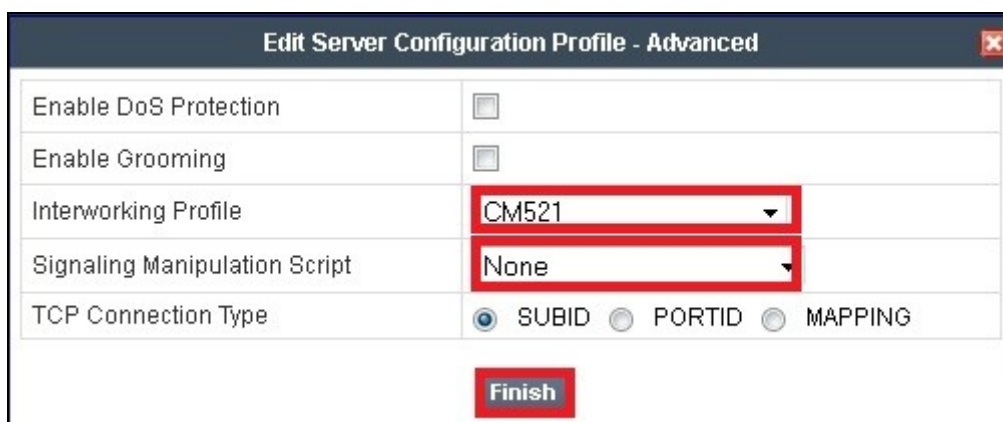
In the **General** tab, specify Server Type as **Call Server**. In the compliance testing, the link between Avaya SBCE and Communication Manager is TCP and Communication Manager listens on port 5060.

Edit Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	110.10.97.219
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
Finish	

By default the Avaya SBCE forwards the OPTIONS from MTS Allstream to Communication Manager to check for SIP Trunk status. Thus, it is unnecessary to enable heartbeat on Avaya SBCE to send OPTIONS to Call Server. In the compliance testing, the Heartbeat is kept disabled as default. The following screenshot shows the Heartbeat configuration.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input type="checkbox"/>
Method	OPTIONS
Frequency	seconds
From URI	
To URI	
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
Finish	

Under **Advanced** tab, in **Interworking Profile** drop down list select entry **CM521** as defined in **Section 6.2.4**, and for the **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default. Click **Finish**.



Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CM521
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

6.3. Domain Policies

The **Domain Policies** feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. This criterion can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created

6.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

An **Application Rule** is created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the default rule chosen, click on **Clone Rule** (not shown). Enter a rule with a descriptive name **MTSAllstream_AppR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	MTSAllstream_AppR
<input type="button" value="Finish"/>	

Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the compliance test, Communication Manager is programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section 5.7**) to the allotted number. Therefore, the values in the **Application Rule** named **CM_MTSAllstream_AR** are set high enough to be considered non-blocking. Click **Finish**.

Editing Rule: MTSAllstream_AppR ✕

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	<input checked="" type="radio"/> None <input type="radio"/> CDR w/ RTP <input type="radio"/> CDR w/o RTP
IM Logging	<input type="checkbox"/>
RTCP Keep-Alive	<input type="checkbox"/>

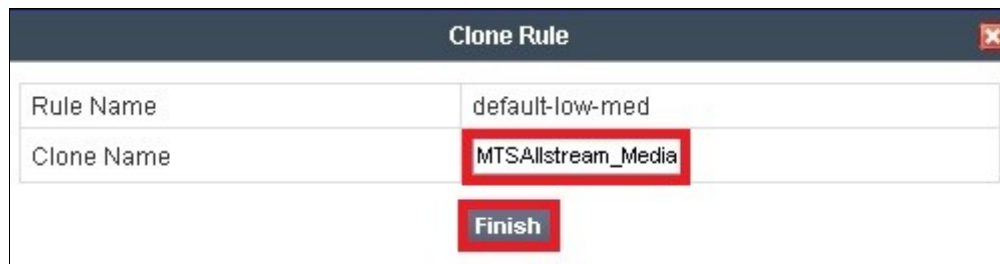
Finish

6.3.2. Media Rules

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packet matching the criteria will be handled by the UC-Sec security product.

A custom **Media Rule** is created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows **Media Rule MTSAllstream_MediaR** used for both enterprise and MTS Allstream.

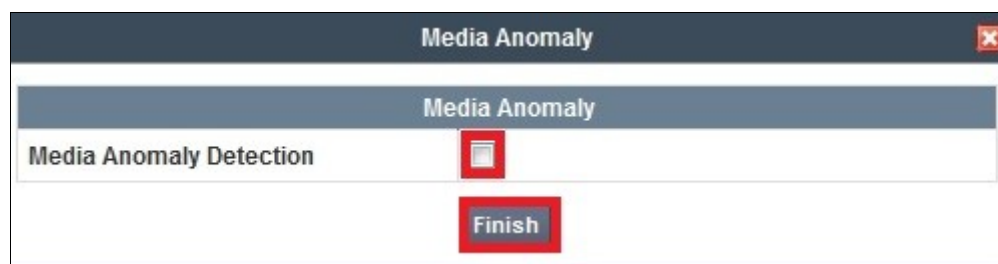
To create **Media Rule**, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** (not shown). Enter a **Media Rule** with a descriptive name **MTSAllstream_MediaR** and click **Finish**.



Clone Rule	
Rule Name	default-low-med
Clone Name	MTSAllstream_Media
Finish	

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created in the log during an audio shuffle.

To modify the rule, select the **Media Anomaly** tab (not shown) and click **Edit**, uncheck **Media Anomaly Detection** and click **Finish**.



Media Anomaly	
Media Anomaly Detection	<input type="checkbox"/>
Finish	

The **Media Silencing** feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, Avaya SBCE generates alert in the **Incidents Log**. In the compliance test, the **Media Silencing** detection is disabled to prevent the call from unexpectedly disconnected due to a RTP packet lost on public WAN. To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.

Media Silencing	
Media Silencing	<input type="checkbox"/>
Timeout (seconds)	<input type="text"/>
<input type="button" value="Finish"/>	

Select the **Media QoS** tab (not shown) and click **Edit** to configure the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for the compliance test.

Media QoS			
Media QoS Reporting			
RTCP Enabled		<input type="checkbox"/>	
Media QoS Marking			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Audio Precedence	Routine	000
	Audio ToS	Minimize Delay	1000
	Video Precedence	Routine	000
	Video ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Audio	EF	101110
	Video	EF	101110
<input type="button" value="Finish"/>			

6.3.3. Signaling Rules

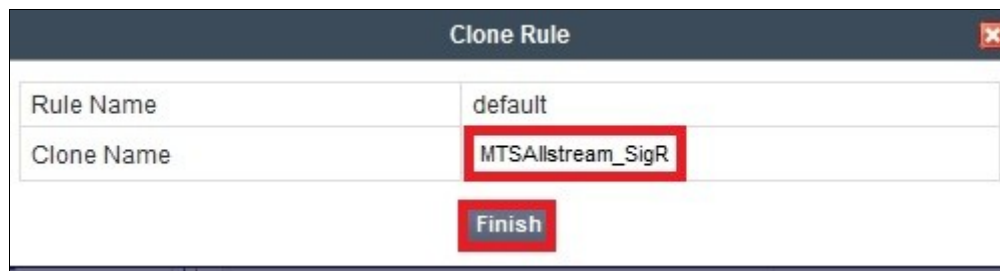
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown).

In this compliance testing, there are two **Signaling Rules** are created for MTS Allstream and Communication Manager.

6.3.3.1 Signaling Rule for MTS Allstream.

Clone a **Signaling Rule** with a descriptive name **MTSAllstream_SigR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	MTSAllstream_SigR
Finish	

The **MTSAllstream_SigR** is configured to allow MTS Allstream to accept inbound and outbound call requests. It also blocks Accept-Language, Alert-Info and P-Chanrging-Vector headers from Communication Manager because these headers are not required by MTS Allstream.

Being cloned from the **Signaling Rule default**, the **MTSAllstream_SigR** will block all requests with 403 Forbidden. To start accepting calls, go to **General** tab, click on **Edit**. Then change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.

The screenshot shows the 'General Control' configuration window. It is divided into three main sections: Inbound, Outbound, and Content-Type Policy.

Inbound Section:

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Outbound Section:

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Content-Type Policy Section:

Enable Content-Type Checks: ☒

Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	

At the bottom of the window is a 'Finish' button.

Request Headers setting is to allow or block a header in particular direction for request method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define the inbound and outbound Request header rules. The signaling rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 6.2.6.1**.

The following screenshot shows three rules added to block the **Accept-Language**, **Alert-Info** and **P-Chanrging-Vector** headers.

- **Header Name**: Select the header to be manipulated.
- **Method Name**: Select **INVITE** in an outbound call request.
- **Header Criteria**: Click on **Forbidden** to block the header.
- **Action**: Select **Remove header** to delete the header.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, and Security Rules. The 'Security Rules' category is expanded, and 'Signaling Rules' is selected. The main panel shows the configuration for the 'MTSAllstream_SigR' rule. The 'Request Headers' tab is active, displaying a table with three rules:

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Accept-Language	INVITE	Forbidden	Remove Header	No	OUT
2	Alert-Info	INVITE	Forbidden	Remove Header	No	OUT
3	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	OUT

Notes: Pre-defined list does not have P-Charging-Vector header, but the Avaya SBCE provides an option to define this proprietary header.

Response Headers setting is to allow or block a header in particular direction for response method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define inbound and outbound **Response Headers** rules. The signaling rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 6.2.6.1**.

The following screenshots show three rules added to block the **Accept-Language**, **Alert-Info** and **P-Charging-Vector** headers:

- **Header Name:** Select the header to be manipulated.
- **Method Name:** Select INVITE for an inbound call request.
- **Header Criteria:** Click on **Forbidden** to block the header.
- **Action:** Select **Remove header** to delete the header.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 6:21:47 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > Signaling Rules: MTSAllstream_SigR

Filter By Device... [v] [Rename Rule] [Clone Rule] [Delete Rule]

Click here to add a description.

General Requests Responses Request Headers **Response Headers** Signaling QoS

[Add In Header Control] [Add Out Header Control]

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction
1	Accept-Language	1XX	INVITE	Forbidden	Remove Header	No	OUT
2	Alert-Info	1XX	INVITE	Forbidden	Remove Header	No	OUT
3	P-Charging-Vector	1XX	INVITE	Forbidden	Remove Header	Yes	OUT

Notes: Pre-defined list does not have **P-Charging-Vector** header, but the Avaya SBCE provides an option to define this proprietary header.

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance test.

Signaling QoS

Enabled ☒

☐ ToS

Precedence

ToS

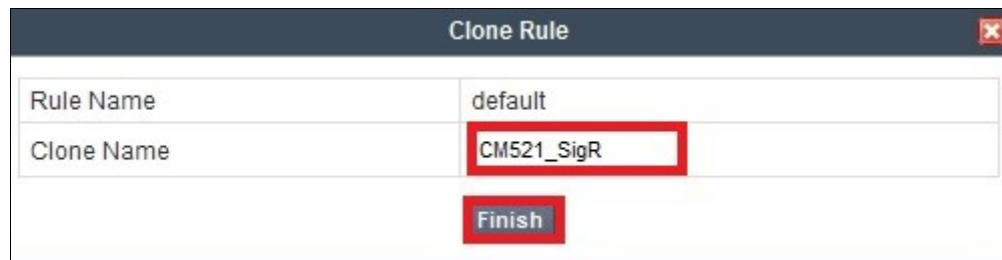
☒ **DSCP**

Value

[Finish]

6.3.3.2 Signaling Rule for Communication Manager.

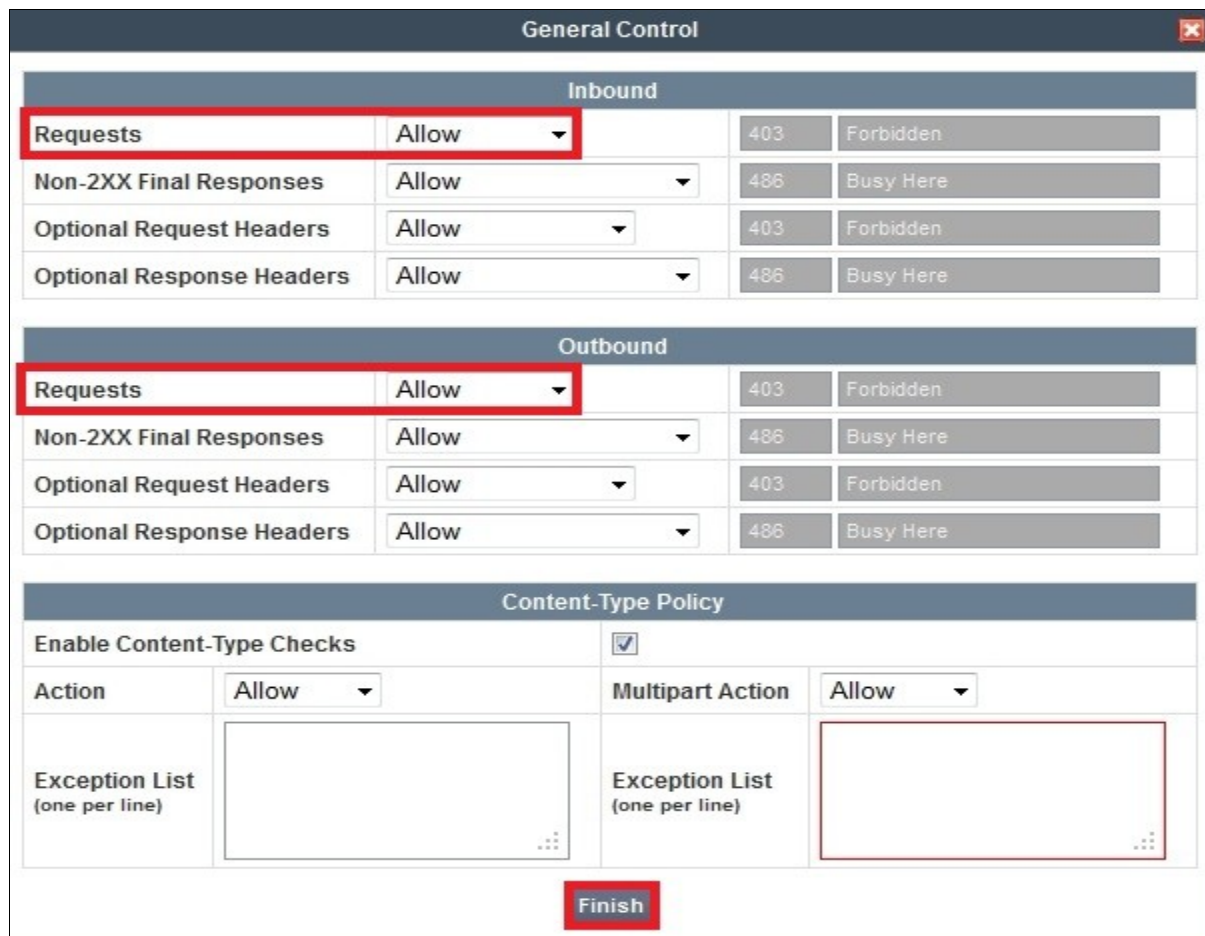
Clone a **Signaling Rule** with a descriptive name **CM521_SigR** and click **Finish**



Clone Rule	
Rule Name	default
Clone Name	CM521_SigR
Finish	

This **CM521_SigR** is configured to allow Communication Manager to accept inbound and outbound call requests.

Being cloned from the **Signaling Rule default**, the **CM_SigR** will block all requests with 403 Forbidden. To start accepting calls, select **CM_SigR** then go to **General** tab, click on **Edit** (not shown). Then change **Inbound-Requests** and **Outbound-Requests** to **Allow** as shown in following screenshot and click **Finish**.



General Control			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
Finish			

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance test.

Signaling QoS			
Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Value	EF	101110
Finish			

6.3.4. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

Endpoint Policy Groups are created for the Communication Manager and the MTS Allstream.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** (not shown).

6.3.4.1 Endpoint Policy Group for MTS Allstream

The following screen shows **MTSAllstream_PolicyG** created for MTS Allstream:

- Set **Application** and **Media** rules created in **Section 6.3.1** and **Section 6.3.2**.
- Set **Signaling** rule **CM_MTSAllstream_AR** created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various policy categories, with 'End Point Policy Groups' selected. The main area displays a list of policy groups, including 'MTSAllstream_PolicyG'. The details for this group are shown on the right, including a table of rules.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	MTSAllstream_AppR	default	MTSAllstream_MediaR	default-high	MTSAllstream_SigR	default

6.3.4.2 Endpoint Policy Group for Communication Manager

The following screen shows **CM521_PolicyG** created for **Communication Manager**:

- Set **Application** and **Media** rules created in **Section 6.3.1** and **Section 6.3.2**.
- Set **Signaling** rule **CM521_SigR** created in **Section 6.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various policy categories, with 'End Point Policy Groups' selected. The main area displays a list of policy groups, including 'CM521_PolicyG'. The details for this group are shown on the right, including a table of rules.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	MTSAllstream_AppR	default	MTSAllstream_MediaR	default-low	CM521_SigR	default

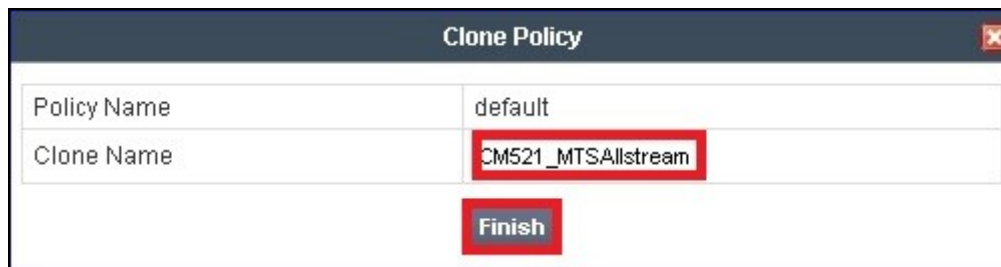
6.3.5. Session Policy

The **Session Policy** is applied based on the source and destination of a media session i.e., which codec is to be applied to the media session between its source and destination. The source and destination are defined in URI Group in **Section 6.2.1**.

In the compliance test, the **Session Policy** named **CM521_MTSAllstream** is created to match the codec configuration on MTS Allstream. The policy also allows Avaya SBCE to anchor media in off-net call transfer scenarios.

To clone a **Session Policy**, navigate to **UC-Sec Control Center → Domain Policies → Session Policies**. With the **default** rule chosen, click on **Clone Rule** (not shown).

Enter a descriptive name **CM521_MTSAllstream** for the new policy and click **Finish**.



Clone Policy	
Policy Name	default
Clone Name	CM521_MTSAllstream
Finish	

MTS Allstream supports voice codec G.729 and G.711MU in prioritized order with payload 101 for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **CM21_MTSAllstream** created above, click on **Edit** (not shown). Select **Preferred Codec #1** as G.711MU, **Preferred Codec #2** as G.729 and **Preferred Codec #3** as Dynamic (101) for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Notes:

- The T.38 fax is not yet supported by MTS Allstream SIP Trunking Service.
- This **Session Policy** prioritizes voice codec G.711MU to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both Communication Manager and MTS Allstream cannot switch the voice call using different codec to G.711MU for fax.

Codec Prioritization	
Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0) ▼
Preferred Codec #2	G729 (18) ▼
Preferred Codec #3	Dynamic (101) ▼
Preferred Codec #4	None ▼
Preferred Codec #5	None ▼
Video Codec	
Codec Prioritization	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CelB (25) ▼
Preferred Codec #2	None ▼
Preferred Codec #3	None ▼
Preferred Codec #4	None ▼
Preferred Codec #5	None ▼
Finish	

To enable **Media Anchoring** on Avaya SBCE, select Session Policy **CM_MTSAllstream** created above then select tab **Media**, click **Edit** (not shown). Check on **Media Anchoring** and click **Finish**.

Media	
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None ▼
Finish	

6.4. Device Specific Settings

The **Device Specific Settings** feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.4.1. Network Management

The **Network Management** screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address (es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and under **Network Configuration** tab verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows the navigation menu with 'Device Specific Settings' expanded and 'Network Management' selected. The main content area is titled 'Device Specific Settings > Network Management: sipera'. It features two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, showing a table of IP addresses and their associated interfaces. A warning message at the top states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for A1 Netmask (255.255.255.192), A2 Netmask, B1 Netmask (255.255.255.224), and B2 Netmask. A yellow banner indicates 'Changes will not take effect until the interface is updated.' and buttons for 'Save Changes' and 'Clear Changes' are present. The table below lists three IP addresses, each with a 'Public IP' field, a 'Gateway' field, and an 'Interface' dropdown menu.

IP Address	Public IP	Gateway	Interface	
110.10.97.189		110.10.97.129	A1	X
110.10.98.98		110.10.98.97	B1	X
110.10.98.112		110.10.98.97	B1	X

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle State** button.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 12:51:30 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Administration Backup/Restore System Management Global Parameters SIP Cluster Domain Policies Device Specific Settings

Device Specific Settings

Network Management

Media Interface Signaling Interface Signaling Forking SNMP End Point Flows Session Flows Two Factor Relay Services Troubleshooting TLS Management IM Logging

Device Specific Settings > Network Management: sipera

UC-Sec Devices

sipera

Network Configuration Interface Configuration

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

6.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. Avaya SBCE will open connection for RTP on the defined ports.

To create a new **Media Interface**, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Media Interface** and click **Add Media Interface** (not shown).

Media Interfaces are created for both the inside and outside interfaces. The following screen shows the **Media Interfaces** created in the compliance test.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 12:54:58 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Administration Backup/Restore System Management Global Parameters SIP Cluster Domain Policies Device Specific Settings

Device Specific Settings

Network Management

Media Interface Signaling Interface Signaling Forking SNMP End Point Flows Session Flows Two Factor Relay Services Troubleshooting TLS Management IM Logging

Device Specific Settings > Media Interface: sipera

UC-Sec Devices

sipera

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add Media Interface

Name	Media IP	Port Range	
InsideMedia	110.10.97.189	35000 - 40000	✎ ✕
OutsideMedia_SBCE	110.10.98.112	35000 - 40000	✎ ✕
OutsideMedia	110.10.98.98	35000 - 40000	✎ ✕

6.4.3. Signaling Interface

The **Signaling Interface** screen is where the SIP signaling port is defined. Avaya SBCE will listen for SIP requests on the defined port.

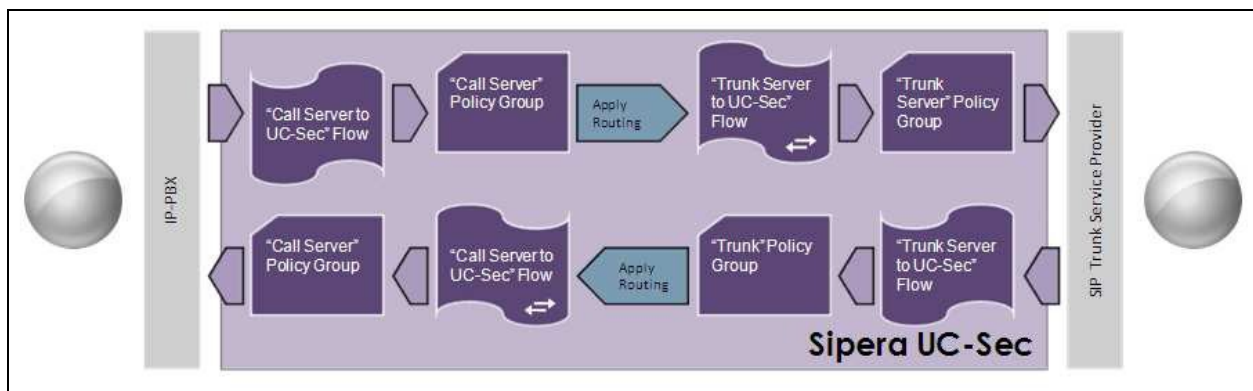
To create a new **Signaling Interface**, navigate to **UC-Sec Control Center** → **Device Specific** → **Settings** → **Signaling Interface** and click **Add Signaling Interface** (not shown).

Signaling Interfaces are created for both inside and outside interfaces. The following screen shows the signaling interfaces created in the compliance test with TCP/5060 and UDP/5060 used respectively for the inside and outside IP interface.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
InsideSIP	110.10.97.189	5060	5060	---	None
OutsideSIP_SBCE	110.10.98.112	5060	5060	---	None
OutsideSIP	110.10.98.98	5060	5060	---	None
InsideSIP_To_CM601	135.10.97.189	5080	---	---	None

6.4.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through Avaya SBCE to secure a SIP Trunk call.



In the compliance test, two separate **Server Flows** are created for MTS Allstream and Communication Manager. To create a **Server Flow**, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown). In the new window that appears (shown below), enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a **Server Configuration** created in **Section 6.2.6** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 6.2.1** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the **Signaling Interface** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 6.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 6.3.4** assigned to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 6.2.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Click **Finish**.

Criteria	
Flow Name	MTSAllstream
Server Configuration	MTSAllstream ▼
URI Group	CM521_MTSAllstream ▼
Transport	* ▼
Remote Subnet	*
Received Interface	InsideSIP ▼
Signaling Interface	OutsideSIP_SBCE ▼
Media Interface	OutsideMedia_SBCE ▼
End Point Policy Group	MTSAllstream_PolicyG ▼
Routing Profile	To_CM521 ▼
Topology Hiding Profile	To_MTSAllstream ▼
File Transfer Profile	None ▼
<input type="button" value="Finish"/>	

The following screen shows the Server **Flow Name (CM521)** configured for Communication Manager.

Edit Flow: CM521

Criteria	
Flow Name	CM521
Server Configuration	CM521
URI Group	CM521_MTSAllstream
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_SBCE
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	CM521_PolicyG
Routing Profile	To_MTSAllstream
Topology Hiding Profile	To_CM521
File Transfer Profile	None

Finish

6.4.5. Session Flows

The **Session Flows** features allows to define certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or from outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. **Session Flows** profiles SDP media parameters, to completely identify and characterize a call placed through the network.

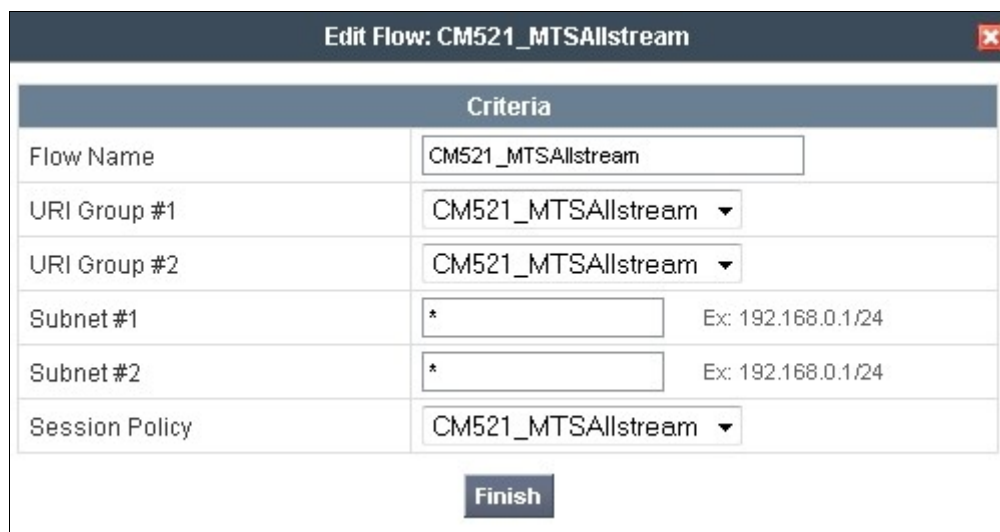
To create a session flow, navigate to **UC-Sec Control Center → Device Specific Settings → Session Flows**. Click **Add Flow** (not shown).

A common Session Flow is created for both Communication Manager and the MTS Allstream SIP Trunk. In the new window that appears, enter the following values. Use default values for the remaining fields:

- **Flow Name**: Enter a descriptive name.
- **URI Group #1**: Select the URI Group created in **Section 6.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2**: Select the URI Group to assign to the Session Flow as the destination URI Group.
- **Session Policy**: Select the session policy created in **Section 6.3.5** to assign to the Session Flow.
- Click **Finish**.

Notes: A unique **URI Group** is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the **Session Flow** named **CM521_MTSAllstream** is created



The screenshot shows a window titled "Edit Flow: CM521_MTSAllstream" with a close button in the top right corner. The window contains a table with the following fields and values:

Criteria	
Flow Name	CM521_MTSAllstream
URI Group #1	CM521_MTSAllstream ▼
URI Group #2	CM521_MTSAllstream ▼
Subnet #1	* Ex: 192.168.0.1/24
Subnet #2	* Ex: 192.168.0.1/24
Session Policy	CM521_MTSAllstream ▼

At the bottom center of the window is a button labeled "Finish".

7. MTS Allstream SIP Trunking Service Configuration

MTS Allstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at enterprise side. MTS Allstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the MTS Allstream SIP Trunking Service. The information provided by MTS Allstream includes:

- IP address of the MTS Allstream Session Border Controller.
- MTS Allstream SIP domain. In the compliance test, MTS Allstream preferred to use IP address as a URI-Host.
- CPE SIP domain. In the compliance test, MTS Allstream preferred to use IP address of Avaya SBCE as a URI-Host.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.

The sample configuration between MTS Allstream SIP Trunking Service and the Communication Manager for the compliance test is a static configuration. There is no registration on the SIP trunk implemented on either MTS Allstream or enterprise side.

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands.

Verification Steps:

1. Verify that endpoints at the enterprise site can place call to the PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive call from the PSTN and that the call can remain active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Protocol Traces:

The following SIP headers are inspected using Wireshark traces:

- Request-URI: verify the request number and SIP domain
- From: verify the display name and display number
- To: verify the display name and display number
- P-Assert-Identity: verify the display name and display number
- Privacy: verify the “user, id” masking

The following attributes in SIP message body are inspected using Wireshark traces:

- Connection Information (c line): verify IP address of near end and far end endpoints
- Time Description (t line): verify session timeout value of near end and far end endpoints
- Media Description (m line): verify audio port, codec, DTMF event description
- Media Attribute (a line): verify specific audio port, codec,ptime, send/ receive ability, DTMF event and fax attributes

Troubleshooting:

Avaya SBCE

Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between MTS Allstream and Avaya SBCE

Following is an example inbound call from MTS Allstream to Communication Manager.

- Inbound INVITE request from MTS Allstream:

```
INVITE sip:6477763571@110.10.98.112;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477763571@110.10.98.112;user=phone>
From: <sip:16139675258@220.20.2.12;user=phone>;tag=3541139386-197470
```


P-Asserted-Identity: <sip:16139675258@220.20.2.12;user=phone>
Call-ID: 20290-3541139386-197462@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bKda47b4d584d1def91ab66867fd887a59
Contact: <sip:16139675258@220.20.2.12:5060;tgrp=TOROONSBCIOT1>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 209776086 209776086 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 17658 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

- 200OK/SDP response by Communication Manager:

SIP/2.0 200 OK
From: <sip:16139675258@220.20.2.12;user=phone>;tag=3541139386-197470
To: <sip:6477763571@110.10.98.112;user=phone>;tag=0c8b6a87575e118234f6fb92c00
CSeq: 1 INVITE
Call-ID: 20290-3541139386-197462@nextone-msw-lab-3.mtsallstream.com
Contact: <sip:110.10.98.112:5060;transport=udp>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=1989;lr;transport=udp>
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO,
PUBLISH
Supported: timer, replaces, join, 100rel
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bKda47b4d584d1def91ab66867fd887a59
Require: timer
Server: Avaya CM/R015x.02.1.016.4
Session-Expires: 3600;refresher=uac
Content-Type: application/sdp
Content-Length: 166

v=0
o=- 1 2 IN IP4 110.10.98.112
s=-
c=IN IP4 110.10.98.112
b=AS:64
t=0 0
m=audio 35002 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

Following is an example outbound call from Communication Manager to MTS Allstream.

- Outbound INVITE request from Communication Manager:

INVITE sip:16139675258@220.20.2.12 SIP/2.0
From: "MTS H323 x3571"
<sip:6477763571@110.10.98.112>;tag=80b417ca7575e118834f6fb92c00
To: sip:16139675258@220.20.2.12
CSeq: 1 INVITE
Call-ID: 80b417ca7575e118934f6fb92c00
Contact: "MTS H323 x3571" <sip:6477763571@110.10.98.112:5060>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=2015;lr;transport=udp>

Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO, PUBLISH
Supported: timer, replaces, join, 100rel
User-Agent: Avaya CM/R015x.02.1.016.4
Max-Forwards: 70
Via: SIP/2.0/UDP 110.10.98.112:5060;branch=z9hG4bK-s1632-001069096723-1--s1632-
P-Asserted-Identity: "MTS H323 x3571" <sip:6477763571@110.10.98.112>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Content-Type: application/sdp
Content-Length: 237

v=0
o=- 1 1 IN IP4 110.10.98.112
s=-
c=IN IP4 110.10.98.112
b=AS:64
t=0 0
m=audio 35004 RTP/AVP 0 8 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000

- 200OK/SDP response by MTS Allstream:

SIP/2.0 200 OK
Session-Expires: 1200;refresher=uac
Require: timer
Via: SIP/2.0/UDP 110.10.98.112:5060;received=110.10.98.112;branch=z9hG4bK-s1632-001069096723-1--s1632-
Record-Route: <sip:110.10.98.112:5060;ipcs-line=2015;lr;transport=udp>
To: 101116139675258 <sip:16139675258@220.20.2.12>;tag=3541139442-614227
From: "MTS H323 x3571"
<sip:6477763571@110.10.98.112>;tag=80b417ca7575e118834f6fb92c00
Call-ID: 80b417ca7575e118934f6fb92c00
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:16139675258@220.20.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 210340399 210340399 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 17664 RTP/AVP 0 18 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

Communication Manager Verification Steps

- **list trace station** <extension number> - Traces calls to and from a specific station
- **list trace tac** <trunk access code number> - Trace calls over a specific trunk group
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station
- **status trunk** <trunk group number> - Displays trunk group information
- **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 5.2.1 and Avaya Session Border Controller for Enterprise 4.0.5 to MTS Allstream SIP Trunking Service. MTS Allstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. MTS Allstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The MTS Allstream SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 5.2.1 and Avaya Session Border Controller for Enterprise 4.0.5.

10. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager, Release 5.2, May 2009, Document Number 03-300509.*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 5.2, May 2009, Document Number 555-245-205.*
- [3] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide, Release 3.1, November 2009, Document Number 16-300698.*
- [4] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6, June 2010, Document Number 16-601944.*
- [5] *Administering Avaya one-X® Communicator, April 2011.*
- [6] *Using Avaya one-X® Communicator, April 2011.*
- [7] *UC-Sec Install Guide (102-5224-400v1.01)*
- [8] *UC-Sec Administration Guide (010-5423-400v106)*
- [9] *RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>*
- [10] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, <http://www.ietf.org/>*
- [11] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>*
- [12] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, <http://www.ietf.org/>*

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ® 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 devconnect@avaya.com.