



Avaya Solution & Interoperability Test Lab

Application Notes for Windstream SIP Trunking Service (Metaswitch Platform) 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) trunks between Windstream 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 Aura® Session Manager and Avaya Session Border Controller for Enterprise.

Windstream 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.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support.....	7
3.	Reference Configuration	8
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity.....	12
5.2.	System Features	12
5.3.	IP Node Names	13
5.4.	Codecs.....	13
5.5.	IP Network Region	14
5.6.	Signaling Group.....	17
5.7.	Trunk Group.....	19
5.8.	Calling Party Information	21
5.9.	Outbound Routing.....	22
5.10.	Incoming Call Handling.....	23
5.11.	Saving Communication Manager Configuration Changes	23
6.	Configure Avaya Session Border Controller for Enterprise	24
6.1.	Avaya Session Border Controller for Enterprise Login.....	26
6.2.	Global Profiles	28
6.2.1.	Uniform Resource Identifier (URI) Groups.....	28
6.2.2.	Routing Profiles	29
6.2.3.	Topology Hiding.....	31
6.2.4.	Server Interworking	33
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	54
6.4.	Device Specific Settings	56
6.4.1.	Network Management.....	56
6.4.2.	Media Interface	57
6.4.3.	Signaling Interface	58
6.4.4.	End Point Flows - Server Flow	59
6.4.5.	Session Flows.....	61
7.	Windstream SIP Trunking Service Configuration.....	62
8.	Verification and Troubleshooting.....	63
8.1.	Verification Steps.....	63
8.2.	Protocol Traces	63

8.3.	Troubleshooting	64
8.3.1.	Troubleshooting Avaya SBCE.....	64
8.3.2.	Troubleshooting Communication Manager	66
9.	Conclusion	66
10.	References.....	67

1. Introduction

These Application Notes describe the steps to configure SIP trunk between Windstream SIP Trunking Service (Windstream) 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 (Avaya SBCE) 4.0.5 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Windstream are able to place and receive PSTN calls via a broadband Internet 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.

Windstream is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Windstream via the Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify Windstream SIP Trunking Service interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including 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.
- Outbound PSTN calls from various phone types including H.323, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. 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. Only H.323 protocol is tested.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted, local directory assistance (411) calls... etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper media transmissions G.711MU codecs.
- Proper Early Media transmissions G.711MU codecs.
- Inbound and outbound fax over IP with G.711MU codec.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.

- User features such as hold and resume, transfer, forward and conference.
- Off-net call transfer with REFER method.
- Inbound vector call redirection before answer with “302 Moved Temporarily” method.
- Inbound vector call redirection after answer with REFER method.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

Items that are not supported or not tested including the following:

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance testing because Windstream has not provided the necessary configuration.
- SIP phone and 1XC SIP soft phone are not supported. The SIP extension feature is comprised of Communication Manager and Session Manager functionality. The compliance testing does not cover Session Manager, therefore the SIP extension was not tested.
- T.38 fax is not supported.
- Off-net call forwarding with History-Info method is not supported.

2.2. Test Results

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

1. **The Calling Party Name is not delivered on the SIP trunk.** In an outbound call scenario, PSTN did not display the Calling Party Name from Communication Manager, it only displayed the Calling Party Number. The same observation applied to the inbound call scenario, Communication Manager extension did not display the Calling Party Name of PSTN party, it only displayed the Calling Party Number. Windstream is recommended to support name display delivery on the SIP trunk. This feature also needs to be supported by intermediate service providers involving in routing the call to/from the PSTN party. This is a known issue of Windstream SIP Trunking Service with no available resolution at this time.
2. **In off-net call transfer scenario, the Calling Party Name and Number is not updated to PSTN parties.** After transferring off-net an incoming call off-net to PSTN, Communication Manager sent UPDATE with true connected Calling Party Name and Number to both PTSN parties. The calling party information is in the “Contact” header. However, the Calling Party Name and Number have not been updated, the calling and called PTSN parties still displayed Calling Party Number of the Communication Manager extension. This is a known issue on Windstream SIP Trunking Service with no resolution

available at this time. This issue has low user impact, it is listed here simply as an observation.

3. **The off-net call transfer is successful.** When Communication Manager sent the REFER to transfer the call, Windstream responded with “403 Refer in bad call state” to reject the transfer request. Communication Manager continued the transferring with re-INVITE messages and then the call was successfully transferred to PSTN party.
4. **Fax over IP using G.711MU codec is successful.** For fax over IP, the service provider is recommended to support T.38 in order to work properly with Communication Manager. Communication Manager does not officially support fax call using G.711MU codec. When the ip-codec-set is set with “fax-off” as described in **Section 5.4**, Communication Manager supports G.711 fax call in best effort, the fax call is handled like a regular voice call using G.711 codec. However, in the compliance testing the inbound and outbound fax calls appeared to work with G.711MU codec in low traffic volume condition on the SIP trunk. The fax document was transmitted successfully with acceptable quality.
5. **In case of no matching codec on an outbound call, Windstream does not respond with appropriate signaling as expected.** Windstream should respond with a negative code .e.g. 4XX or 6XX to signal that the SDP/offer is not being accepted since there is no matching codec. However, Windstream accepted the INVITE by a 200OK with SDP/answer contains different codecs than the SDP/offer. This makes Communication Manager send CANCEL request to disconnect the call. This is a known issue on Windstream SIP Trunking Service with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
6. **The operator call fails.** An outbound call with dial digit “0” from Communication Manager to reach the operator at Windstream failed with an “Early Media” to transmit a recorded message of “The number you have dialed has not been recognized, please try again” and then followed by a regular busy tone. Then Windstream sent a “488 Address Incomplete” signaling to disconnect the call. This is a known issue on Windstream SIP Trunking Service with no resolution available at this time.
7. **The Operator Assisted Call does not terminate properly.** Windstream fails to terminate the Operator Assisted Call if PSTN phone disconnects. After being answered by Sprint’ Long Distance Operator IVR, the operator call was transferred to the attendant as per the numeric key selections. The attendant successfully transferred the call to requested destination as specified by the 10 digits in the Called Party Number. The call, however, did not successfully terminate when PSTN phone disconnected. Windstream did not send BYE to request the disconnection, this made CM continuing to keep the session active. However, CM successfully disconnected the call after the “Session Timer” expired.

8. **The Local Directory Assistance Call (411) is terminated locally on Windstream networks.** The outbound 411 call was successfully connected to an Interactive Voice Response (IVR) system located locally on Windstream networks. The IVR provided a voice prompt to indicate the 411 call has been connected to the test environment at Windstream.
9. **Windstream requires a customized outbound OPTIONS heartbeat with the presence of the subscribed DID number.** In the compliance testing, Communication Manager was configured to restrict the OPTIONS heartbeat from being sent to Windstream on the SIP trunk since the regular OPTIONS request was rejected by Windstream with a “403 From URI not recognized”. Windstream requires the presence of the subscribed DID number in the “From” header in order to accept OPTIONS with a “200 OK”. Thus, the Avaya SBCE was configured to send the customized OPTIONS heartbeat to Windstream. For detail configuration, see **Section 6.2.6.1**.
10. **The inbound call to leave a voice message for a Communication Manager extension on Avaya Aura® Messaging (AAM) is corrected.** The AAM did not respond to the INVITE request from Windstream because the INVITE contains “Allow-Events” and “Organization” headers which are not currently supported by the AAM. The workaround has been implemented to use the SigMa script on the Avaya SBCE to delete the unsupported headers then the call worked properly. The PSTN party successfully left a voice message to the mailbox of Communication Manager extension on the AAM. For detail configuration, see **Section 6.2.5**.
11. **The “coverage path” is recommended to use to forward “no-answer” an inbound to Avaya Aura® Messaging (AAM).** When the Communication Manager extension forwards “no-answer” an inbound call to leave a voice message on the AAM using the “Enhanced Call Forwarding” setting on page 3 of station form, the AAM plays a voice prompt to ask PSTN party to login instead of asking to leave messages. Thus, the usage of “Enhanced Call Forwarding” is not recommended. This issue has been fixed by using “coverage path” configuration on Communication Manager to interworking with the AAM. The call then worked properly, the PSTN party successfully left a voice message to the mailbox of Communication Manager extension on the AAM. For the detail configuration for the “coverage path”, see *Reference [2]*, Section of Call Coverage on page 437.

2.3. Support

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

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

- Phone: 1 (866) 990-3282
- Website: <http://www.windstreambusiness.com/support/customer-support>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Windstream SIP Trunking Service (Vendor Validation circuit) through a public Internet 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 Servers running Avaya Aura® Communication Manager
- 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 the Avaya SBCE. It has a public side that connects to Windstream 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. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Windstream across the public network is UDP, the transport protocol between the Avaya SBCE and Communication Manager is TCP.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “bvwnlab.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to Windstream. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

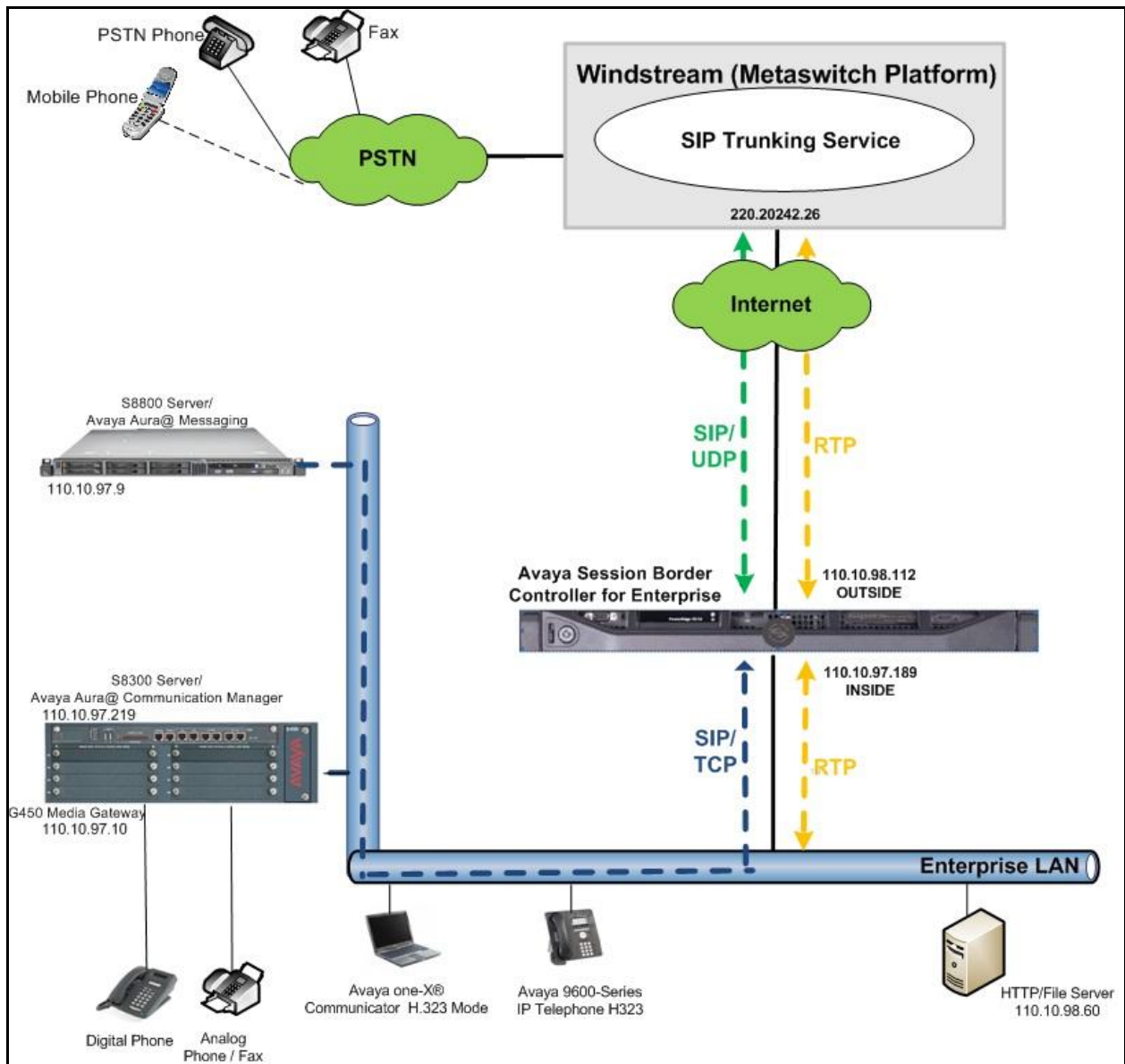


Figure 1: Avaya IP Telephony Network connecting to Windstream SIP Trunking Service

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 an Avaya S8300 Server	5.2.1 (Avaya CM/ R015x.02.1.016.4 with Service Pack 13 02.1.016.4-19880)
Avaya G450 Media Gateway	28.22.0
Avaya Aura® Messaging running on an Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller for Enterprise	4.0.5 Q09
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
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
Windstream SIP Trunking Service (Metaswitch Platform) Components	
Component	Release
Acme Packet SBC	SC6.1.0 mr7
Metaswitch CFS	V7.3.00SU30 P90.00
Metaswitch UMG	V7.3.00 SU 30 P86.00

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for inter-operating with the Windstream.

Two separate SIP trunk groups were created between Communication Manager and the Avaya SBCE to carry traffic to and from service provider respectively. For inbound call, the call flows from Windstream to the 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 outgoing 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 Session Manager toward the Avaya SBCE for egress to the Windstream network.

For the compliance testing, Communication Manager sent 11 digits in the destination headers (e.g., “Request-URI” and “To”) and 10 digit in the source headers (e.g., “From”, “Contact”, and “P-Asserted-Identity” (PAI)). Windstream sent 10 digits in destination headers and 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 212 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 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		450	0
Maximum Concurrently Registered IP Stations:		450	4
Maximum Administered Remote Office Trunks:		450	0
Maximum Concurrently Registered Remote Office Stations:		450	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	212
Maximum Administered Ad-hoc Video Conferencing Ports:		450	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	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 the Avaya SBCE. These node names will be needed for defining the service provider signaling groups in **Section 0**.

```
change node-names ip                                               Page 1 of 2
                                IP NODE NAMES

Name      IP Address
AvayaSBCE 110.10.97.189
DevAAM    110.10.97.9
default   0.0.0.0
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. Windstream supports G.711MU with ptime 20ms. To use these codecs, enter G.711MU 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 were 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:
```

To use G.711MU codec for fax, set the **Fax Mode** to **off** on **Page 2**. Windstream only supports fax using G.711 codec. The T.38 faxing is not supported. Communication Manager does not officially support fax call using G.711MU codec. However, incoming and outgoing fax call using G.711MU codec appeared 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. For more information, see **Section 2.2**, observation #4.

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	

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 testing, ip-network-region 1 was created by the **change ip-network-region** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name “bvwnlab.com” was assigned to the test environment in the Avaya test lab. This domain name appears in the “From” header of SIP message originating from this IP region. **Note:** The Topology-Hiding configuration on the Avaya SBCE in **Section 6.2.3** is used to convert this private domain name to the IP Address based URI-Host in the “From” and “PAI” headers to meet the SIP specification of Windstream.
- 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 Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to **yes**. 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: bvwlab.com
Name: SIP testing		
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		

On **Page 3**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields. The example below shows codec set 1 will be used for call between region 1 and other regions.

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

Non-IP telephones (e.g., analog, digital) derive network region from IP interface the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

For the compliance testing, devices with IP addresses in the 110.10.97.0/24 subnet were assigned to network region 1. These include Communication Manager, the Avaya G450 Media Gateway, and the Avaya SBCE. IP telephones 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.

The following screen illustrates a subset of the IP network map configuration.

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					

Under the same network region 1, the IP interface **procr** is assigned as a signaling resource which is used to process SIP signaling and the Avaya G450 Media Gateway is assigned as a media resource which is used to process media.

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

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

To define network region 1 for the Avaya G450 Media Gateway, use **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:			Max Survivable IP Ext: 8
V9:	gateway-announcements	ANN VMM	

5.6. Signaling Group

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

For the compliance testing, signaling group 1 was created for inbound calls from the service provider and is configured as follows:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to **tcp**. The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**.
- Set the **Peer Detection Enabled** field to **n**.
- Set the **Peer-Server** field to **Other**.
- 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 the 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 “bvwlabs.com”.
- Set the **DTMF over IP field** to **rtp-payload**. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to **n**. This setting restricts Communication Manager to send OPTIONS heartbeat to Windstream on the SIP trunk since the regular OPTIONS request was rejected by Windstream with a “403 From URI not recognized”. Windstream requires the presence of the subscribed DID number in the “From” header in order to accept OPTIONS with a “200 OK”. In this compliance testing, the Avaya SBCE was configured to send the customized OPTIONS heartbeat to Windstream. For detail configuration, see **Section 6.2.6.1**.
- 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 the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Direct IP-IP Early Media** is set to **n**.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **30**. This allows more time for inbound PSTN calls to complete through Windstream networks.
- Default values may be used for all other fields.

```

add signaling-group 1                                     Page 1 of 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: bvwlab.com

Incoming Dialog Loopbacks: eliminate
                                Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
                                IP Audio Hairpinning? n
                                Enable Layer 3 Test? n
                                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n
                                Alternate Route Timer(sec): 30

```

The signaling group for outbound calls from the enterprise to PSTN is similarly configured. For the compliance testing, signaling group 2 was created and is shown below.

```

add 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: bvwlab.com

Incoming Dialog Loopbacks: eliminate
                                Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
                                IP Audio Hairpinning? n
                                Enable Layer 3 Test? n
                                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n
                                Alternate Route Timer(sec): 30

```

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the two signaling groups created in **Section 0**. For the compliance testing, trunk group 1 was configured for incoming calls and trunk group 2 was 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 0**. The incoming trunk group 1 is set to signaling group 1 and the outgoing trunk group 2 is set to signaling group 2.
- Set the **Number of Members** field to 32. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- 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: WS_Inbound      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 refresh the Session Timer. For the compliance testing, a default value of **600** seconds was 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**. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers. The addition of the + sign impacted interoperability with service provider. Thus, the **Numbering Format** is set to **private** and 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 can be set to **y**. The setting of **Network Call Redirection** flag to **y** enables use of the SIP REFER message to transfer an inbound call to a back to PSTN.

- Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound call back to PSTN and Extension to Cellular (EC500) call scenarios.
- Set the **Support Request History** field to **n**. This parameter determines if 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 Windstream.

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 outbound calls from the enterprise to Windstream, the screen below shows **Page 1** of outgoing trunk group 2.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: WS_Outbound	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	

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 4-digit extension beginning with 11 when receiving or calling call on trunk group 1 or 2 will send the 10-digit calling party number as a predefined 6-digit **Private Prefix** of 501287 plus the extension number.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
4	11	1-2	501287	10	Total Administered: 2	
					Maximum Entries: 540	

Even though private numbering is selected, currently the number used in the “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	Ext	Trk	CPN	Total		
Len	Code	Grp(s)	Prefix	CPN		
				Len		
4	11	1-2	501287	10	Total Administered: 2	
					Maximum Entries: 240	

5.9. Outbound Routing

In these Application Notes, the **Automatic Route Selection (ARS)** feature is used to route outbound call via the SIP trunk to service provider. In the compliance testing, a single digit 9 was 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
11	4	ext			
6	1	fac			
9	1	fac			
*	4	dac			

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 9		
			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:		

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 testing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 for outbound call which contains the SIP trunk to the service provider (as defined next).

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 ANI
0	1	24	2	pubu	Reqd n
1	11	11	2	pubu	n
411	3	3	2	svcl	n
613	10	10	2	pubu	n

As being mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern 2 in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group 2 was 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.
- **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**.

change route-pattern 2													Page	1 of	3
Pattern Number: 2													Pattern Name: WS_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											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		

5.10. Incoming Call Handling

When an inbound call arrives, Communication Manager applies incoming handling treatment on incoming trunk group 1 (created in **Section 5.7**). Windstream sends 10 digits in “Request-URI” and “To” headers identical to the assigned DID number. The incoming call handling treatment will translate this DID number to an extension. In the compliance testing, the DID numbers had prefix 501287 which were deleted to normalize the incoming number to match 4 digits extension on Communication Manager. Use the **inc-call-handling-trmt trunk-group** command to define an incoming handling for Windstream. Following table shows the configuration in detail on incoming trunk group 1.

change inc-call-handling-trmt trunk-group 1				Page	1 of 3
Service/ Feature	Number Len	Number 501287	INCOMING CALL HANDLING TREATMENT Del Insert Digits		
public-ntwrk	10	501287	6		

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 the 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 the service provider - Windstream:

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

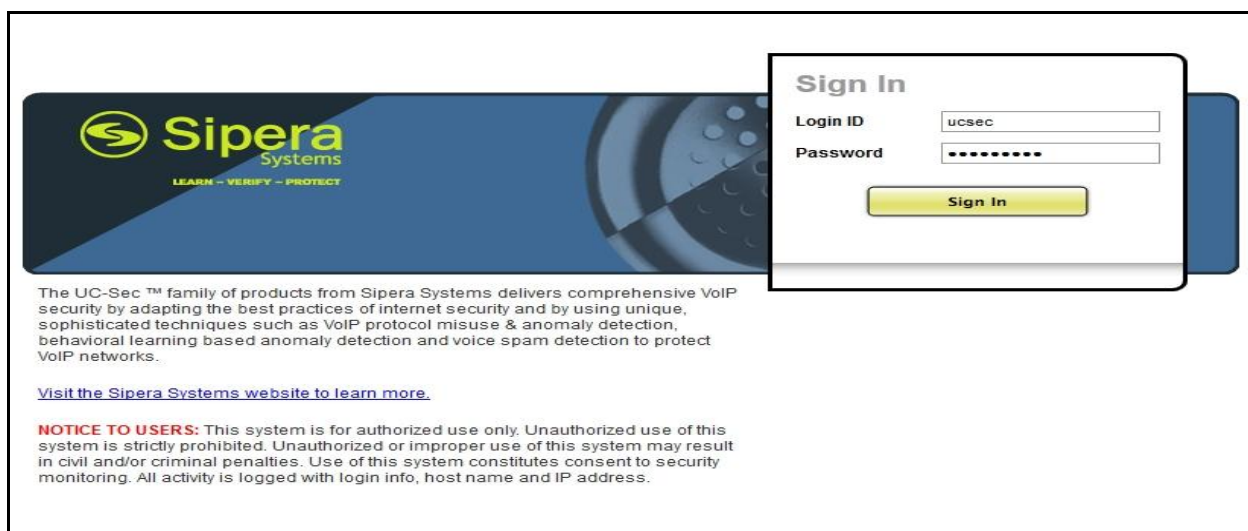
Call server configuration elements for the enterprise - Communication Manager:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - 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**.

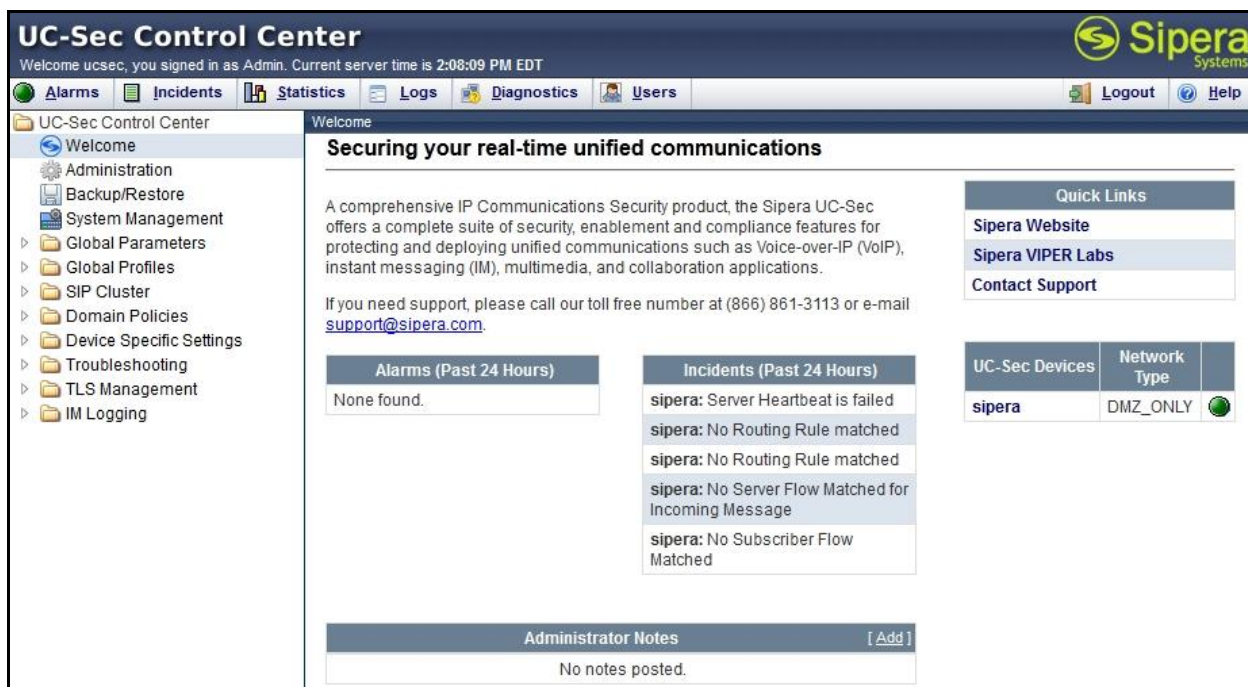


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection 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 2:08:09 PM EDT

[Alarms](#) [Incidents](#) [Statistics](#) [Logs](#) [Diagnostics](#) [Users](#) [Logout](#) [Help](#)

UC-Sec Control Center

- Welcome
- Administration
 - Backup/Restore
 - System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - Device Specific Settings
 - Troubleshooting
 - TLS Management
 - IM Logging

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: Server Heartbeat is failed
- sipera: No Routing Rule matched
- sipera: No Routing Rule matched
- sipera: No Server Flow Matched for Incoming Message
- sipera: No Subscriber Flow Matched

Quick Links

- [Sipera Website](#)
- [Sipera VIPER Labs](#)
- [Contact Support](#)

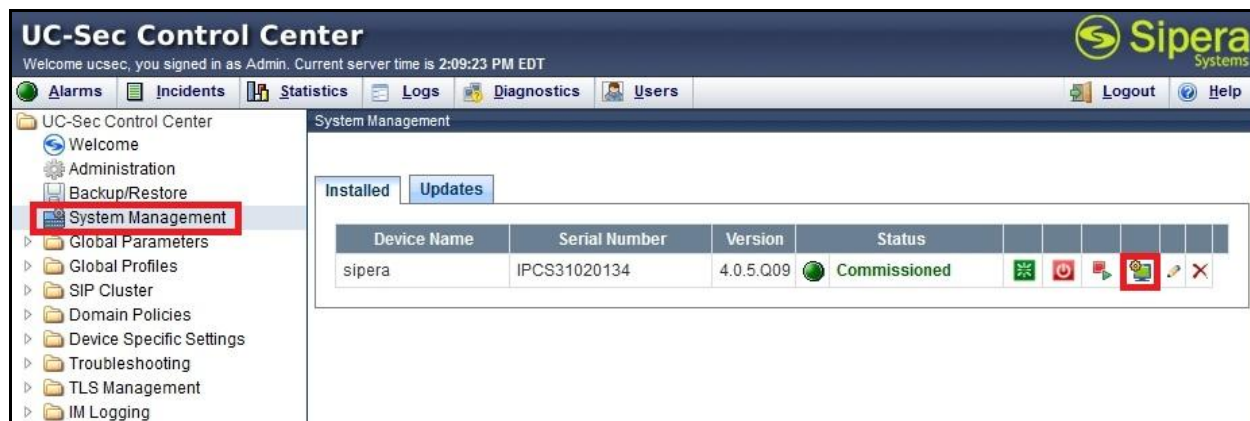
UC-Sec Devices

UC-Sec Devices	Network Type
sipera	DMZ_ONLY

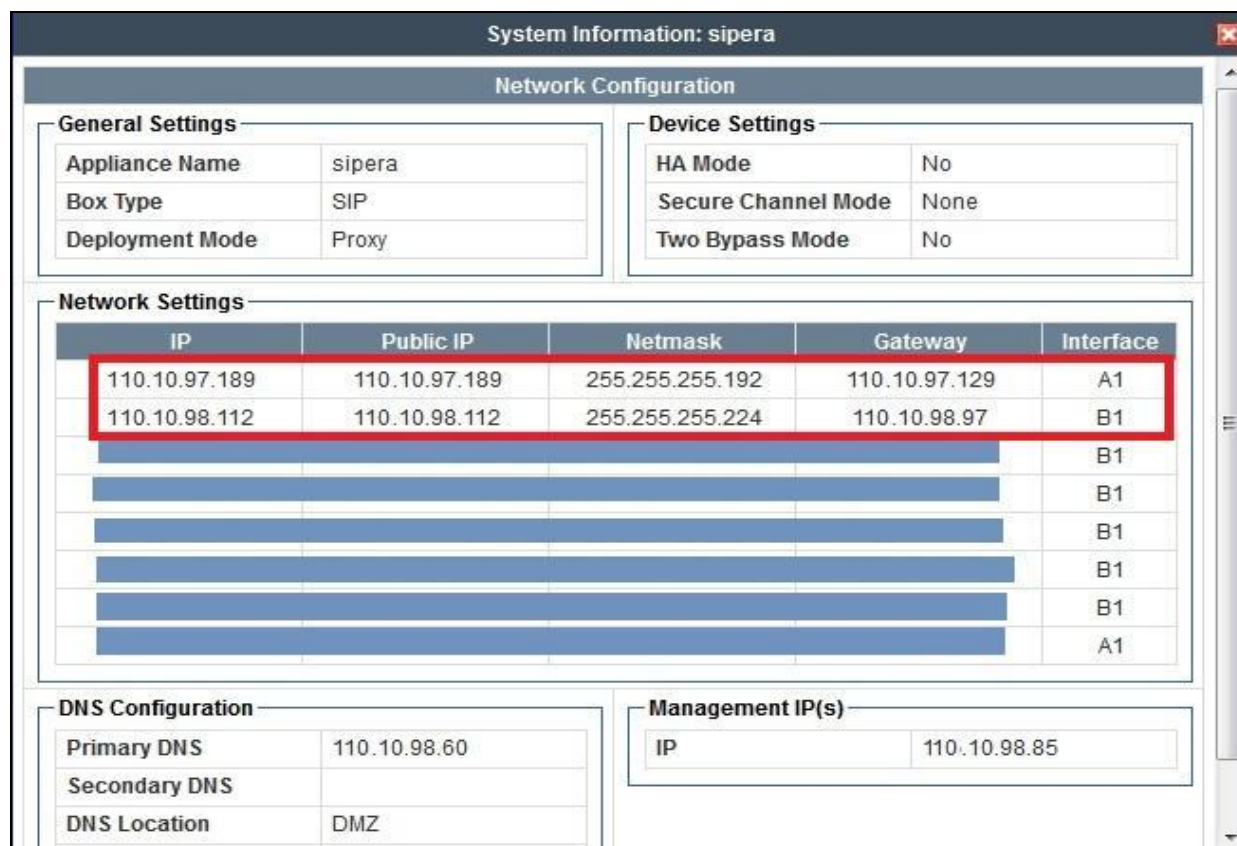
Administrator Notes [\[Add \]](#)

No notes posted.

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 testing, a single device named **sipera** was added. To view the configuration of this device, click the **View Config** icon (the third icon from the right) as shown below.



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.



6.2. Global Profiles

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

6.2.1. Uniform Resource Identifier (URI) Groups

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.

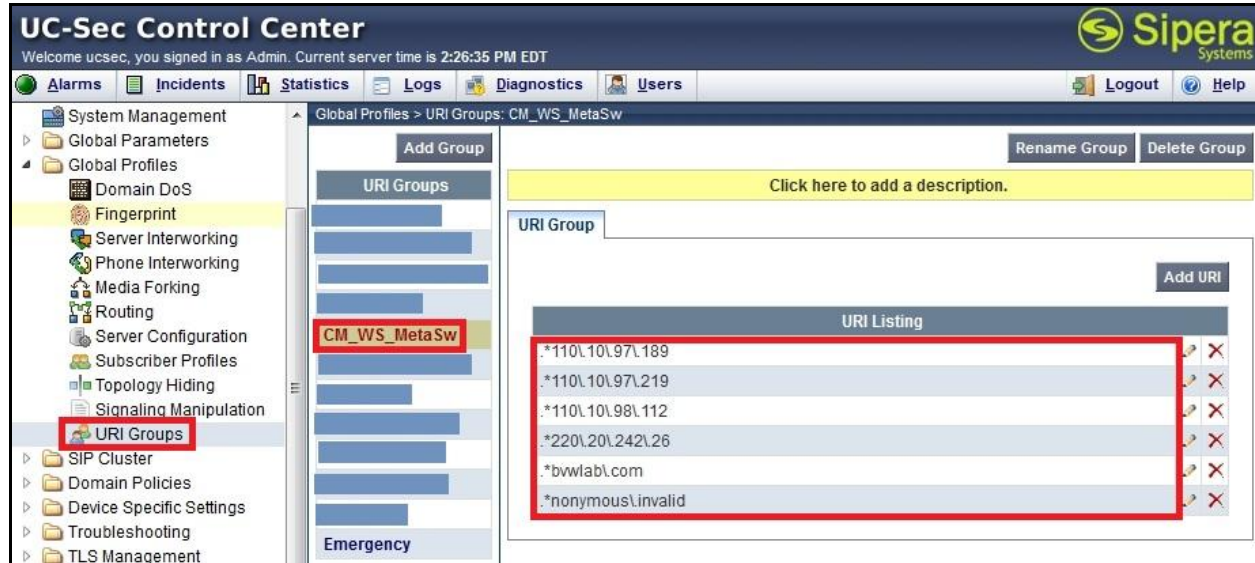
To add an URI Group, select **UC-Sec Control Center → Global Profiles → URI Groups**. Click on **Add Group** (not shown).

In the compliance testing, a URI Group named **CM_WS_MetaSw** was added with URI type Regular Expression (not shown) and consists of:

- “*.bvwnlab.com”: enterprise domain, used for calls across the enterprise networks. This domain matches the domain configured for Communication Manager (see **Section 5.5** and **Section 0**).
- “*.nonyomous.invalid”: enterprise domain, defined to support private call.
- “*.110.10.98.112”, “*.220.20.242.26”: IP address based URI-Host, used for public calls to/from the service provider. The Avaya SBCE public IP address “110.10.98.112” is set as URI-Host of the “From”, “PAI” and “Diversion” headers while the public IP address of Windstream “220.20.242.26” is set as URI-Host of “Request-URI” and “To” headers.
- “*.110.10.97.219”, “*.110.10.97.189”: IP address based URI-Host, defined to support routing PRACK from Communication Manager to Windstream in an outbound call since the PRACK has the URI-Host as the IP address of the Avaya SBC .i.e. “110.10.97.189” instead of the enterprise domain .i.e. “bvwndev.com”.

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

The screenshot below illustrates the URI listing for URI Group **CM_WS_MetaSw**.



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 testing, a Routing Profile named **To_WS_MetaSw** was created to use in conjunction with the server flow defined for Communication Manager. This entry is to route the outbound call from the enterprise to Windstream.

In the opposite direction, a Routing Profile named **To_CM_WS_MetaSw** was created to be used in conjunction with the server flow defined for Windstream. This entry is to route the inbound call from Windstream to the enterprise.

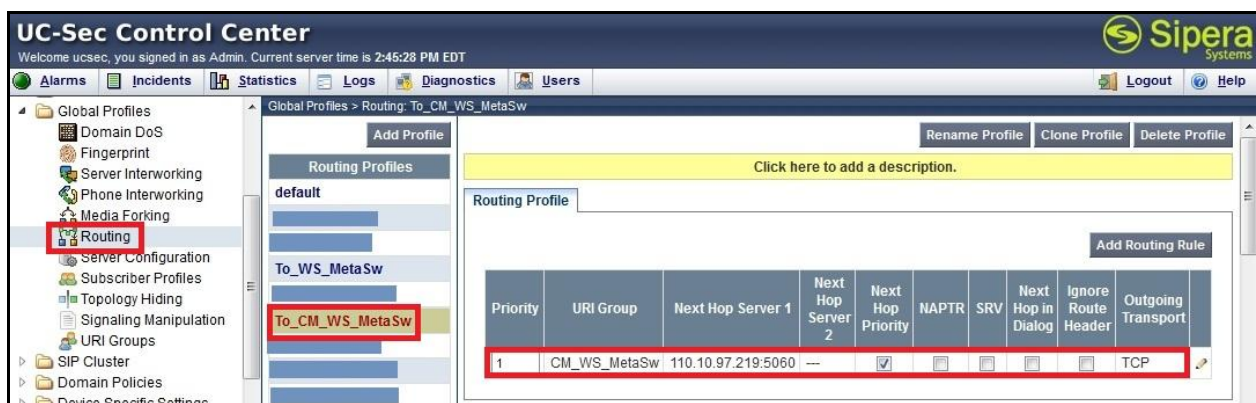
6.2.2.1 Routing Profile for Windstream

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



6.2.2.2 Routing Profile for Session Manager

The Routing Profile To_CM_WS_MetaSw was defined to route call where the “To” header matches the URI Group CM_WS_MetaSw 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 the 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 the compliance testing, two Topology Hiding profiles **To_WS_MetaSw** and **To_CM_WS_MetaSw** were created.

6.2.3.1 Topology Hiding Profile for Windstream

Profile **To_WS_MetaSw** was defined to mask the enterprise SIP domain "bvwnlab.com" in "Request-URI" and "To" headers to IP "220.20.242.26" (the IP address Windstream uses as URI-Host portion for "Request-URI" and "To" headers to meet the SIP specification requirement of Windstream); mask the enterprise SIP domain "bvwnlab.com" in the "From" and "PAI" headers to IP "110.10.98.112" (the Avaya SBCE public IP address); and replace Record-Route, Via headers and SDP (originated from Communication Manager) by external IP address known to Windstream. It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

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 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.

The screenshots below illustrate the Topology Hiding profile **To_WS_MetaSw**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a tree view of configuration categories, with 'Topology Hiding' highlighted. The main content area shows the configuration for the 'To_WS_MetaSw' profile. A table lists the headers, criteria, replace actions, and overwrite values for this profile.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	220.20.242.26
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	220.20.242.26
From	IP/Domain	Overwrite	110.10.98.112
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

6.2.3.2 Topology Hiding Profile for Communication Manager

Profile **To_CM_WS_MetaSw** was also created to mask Windstream URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain “bvwlab.com”, replace Record-Route, Via headers and SDP added by Windstream by internal IP address known to Communication Manager.

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in 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.

The screenshots below illustrate the Topology Hiding profile **To_CM_WS_MetaSw**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a tree view of configuration categories, with 'Topology Hiding' selected and highlighted with a red box. The main content area shows the configuration for the 'To_CM_WS_MetaSw' profile, which is also highlighted with a red box in the profile list. A table titled 'Topology Hiding' lists the headers and their corresponding actions and values.

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

6.2.4. Server Interworking

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

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

In the compliance testing, two Server Interworking profiles were created for Windstream and Session Manager respectively.

6.2.4.1 Server Interworking profile for Windstream

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

General settings:

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

Advanced settings:

- Record Routes = Both Sides. The Avaya SBCE will send “Record-Route” header to both call and trunk servers.
- Topology Hiding: Change Call-ID = Checked. The Avaya SBCE will modify “Call-ID” header for the call toward Windstream.
- Change Max Forwards: Checked. The Avaya SBCE will adjust the original Max-Forwards value from Communication Manager to Windstream by reducing the intermediate hops involving in the call flow.
- Has Remote SBC: Checked. Windstream has SBC which interfaces its Central Office (CO) which interfaces to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from Windstream for the media.

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

Editing Profile: WS_MetaSw

General

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 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: WS_MetaSw

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

Editing Profile: WS_MetaSw

Advanced Settings

Record Routes	<div><div><input type="radio"/> None</div><div><input type="radio"/> Single Side</div><div><input checked="" type="radio"/> Both Sides</div></div>
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

6.2.4.2 Server Interworking profile for Communication Manager

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

General settings:

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

Advanced settings:

- Record Routes = Both Sides. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- Topology Hiding: Change Call-ID = Checked. The Avaya SBCE will modify “Call-ID” header for the call toward Communication Manager.
- Change Max Forwards: Checked. The Avaya SBCE will adjust the original Max-Forwards value from Windstream to Communication Manager by reducing the intermediate hops involving in the call flow.
- Has Remote SBC: Checked. This setting allows the Avaya SBCE to always use the SDP received from Communication Manager for the media.

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

Editing Profile: CM_WS_MetaSw

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: CM_WS_MetaSw

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

Editing Profile: CM_WS_MetaSw

Advanced Settings

Record Routes	<div><div><input type="radio"/> None</div><div><input type="radio"/> Single Side</div><div><input checked="" type="radio"/> Both Sides</div></div>
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

6.2.5. Signaling Manipulation

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 UC-Sec 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 **WS_MetaSw** was created for Server Configuration for Windstream 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"
  {
    remove(%HEADERS["Allow-Events"][1]);
    remove(%HEADERS["Organization"][1]);
  }
}
```

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 to Windstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

For the outbound SIP traffic, the Topology-Hiding profile **To_WS_MetaSw** could properly mask the URI-Host of “P-Asserted-Identity” header in request messages. However, as a limitation, the “P-Asserted-Identity” header in response messages still has the private enterprise domain “bvwlabs.com”. Thus, a SigMa rule is used to correct the URI-Host of “P-Asserted-Identity” header. The rule is shown in the following screenshot.

```
%HEADERS["P-Asserted-Identity"][1].URI.HOST= "110.10.98.112";
```

The statement `act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"` is to specify the script will take effect on all type of SIP messages for inbound calls from Windstream and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

For the inbound SIP traffic, the INVITE from Windstream contains “Allow-Events” and “Organization” headers which are not currently supported by the Avaya Aura ® Messaging. For more information, see **Section 2.2**, observation #10. Therefore, two rules are used to delete these headers. The rules are shown in the following screenshot.

```
remove(%HEADERS["Allow-Events"][1]);
remove(%HEADERS["Organization"][1]);
```

6.2.6. Server Configuration

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 were created, server entry **WS_MetaSw** for Windstream and server entry **CM_WS_MetaSw** for Communication Manager.

6.2.6.1 Server Configuration for Windstream

Server Configuration named **WS_MetaSw** was created for Windstream, it will be discussed in detail as below. **General**, **Heartbeat** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as Windstream does not implement authentication on the SIP trunk. The additional **DoS Whitelist** and **DoS Protection** tabs are displayed after DoS Protection is enabled under **Advanced** tab, the settings for these tabs are kept as default.



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

Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Comma seperated list</small>	220.20.242.26
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
Finish	

In the **Heartbeat** tab, check **Enable Heartbeat**, select **Method** as **OPTIONS** and **Frequency** as **60** to allow the Avaya SBCE to send OPTIONS heartbeat to Windstream in every 60 seconds. Windstream requires the presence of the subscribed DID number in the “From” header in order to accept OPTIONS with a “200 OK”, otherwise the OPTIONS will be rejected. Thus, in the “From URI”, enter URI-User as a subscribed DID number and URI-Host as the Avaya SBC public IP address .e.g. “5012871130@110.10.98.112”. The same example applies to the “To URI”, however, the “To URI” will have URI-Host as the IP address of Windstream interface .e.g. “5012871130@220.20.242.26”. For more info, see **Section 2.2**, observation #9.

Edit Server Configuration Profile - Heartbeat

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	5012871130@110.10.98.112
To URI	5012871130@220.20.242.26
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
Finish	

Under **Advanced** tab, check on **Enable DoS Protection**. For **Interworking Profile** drop down list, select **WS_MetaSw** as defined in **Section 6.2.4** and for **Signaling Manipulation Script** drop down list select **WS_MetaSw** as defined in **Section 6.2.5**. These configurations apply the specific SIP profile and SigMa rules to the Windstream traffic. The other settings are kept as default.

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	WS_MetaSw
Signaling Manipulation Script	WS_MetaSw
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 Session Manager

Server Configuration named **CM_WS_MetaSw** was created for Communication Manager is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Windstream to Communication Manager to query the status of the SIP trunk.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:00:49 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Server Configuration: CM_WS_MetaSw

General	
Server Type	Call Server
IP Addresses / FQDNs	110.10.97.219
Supported Transports	TCP
TCP Port	5060
<input type="button" value="Edit"/>	

In the **General** tab, specify **Server Type** for Communication Manager as **Call Server**. In the compliance testing, the link between the Avaya SBCE and Communication Manager was 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	

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

Edit Server Configuration Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CM_WS_MetaSw
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
Finish	

6.3. Domain Policies

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. These criteria 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.

Application Rule is created to set the number of concurrent voice traffic. The sample configuration is cloned and modified 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 **WS_MetaSw_AR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	WS_MetaSw_AR
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 testing, 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 **WS_MetaSw_AR** are set high enough to be considered non-blocking.

Editing Rule: default ✕

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 **CM_WS_MetaSw_MR** used for both the enterprise and Windstream.

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 **WS_MetaSw_MR** and click **Finish**.



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

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, the 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, the Avaya SBCE generates alert in the **Incidents Log**. In the compliance testing, the **Media Silencing** detection was disabled to prevent the call from unexpectedly disconnected due to a RTP packet lost on public Internet.

To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.

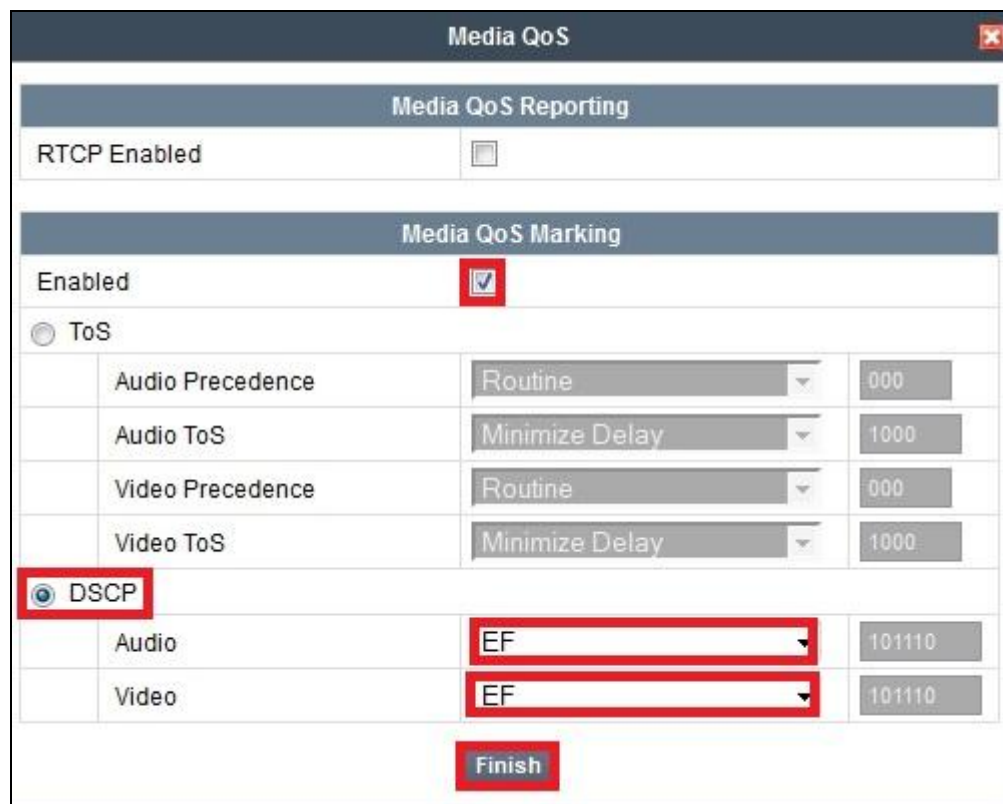


The screenshot shows a 'Media Silencing' configuration window. It has a title bar with a close button. Below the title bar is a section header 'Media Silencing'. Under this header, there are two rows: 'Media Silencing' with an unchecked checkbox, and 'Timeout (seconds)' with a text input field. At the bottom of the window is a 'Finish' button.

Media Silencing	
Media Silencing	<input type="checkbox"/>
Timeout (seconds)	

Finish

Select the **Media QoS** tab and click **Edit** to configure the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for the compliance testing.



The screenshot shows a 'Media QoS' configuration window. It has a title bar with a close button. Below the title bar is a section header 'Media QoS Reporting'. Under this header, there is a row: 'RTCP Enabled' with an unchecked checkbox. Below this is another section header 'Media QoS Marking'. Under this header, there is a row: 'Enabled' with a checked checkbox. Below this is a radio button group with 'ToS' selected. Below the radio button group is a table with four rows: 'Audio Precedence', 'Audio ToS', 'Video Precedence', and 'Video ToS'. Each row has a dropdown menu and a text input field. Below the table is a radio button group with 'DSCP' selected. Below the radio button group is a table with two rows: 'Audio' and 'Video'. Each row has a dropdown menu and a text input field. At the bottom of the window is a 'Finish' button.

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

Finish

6.3.3. Signaling Rules

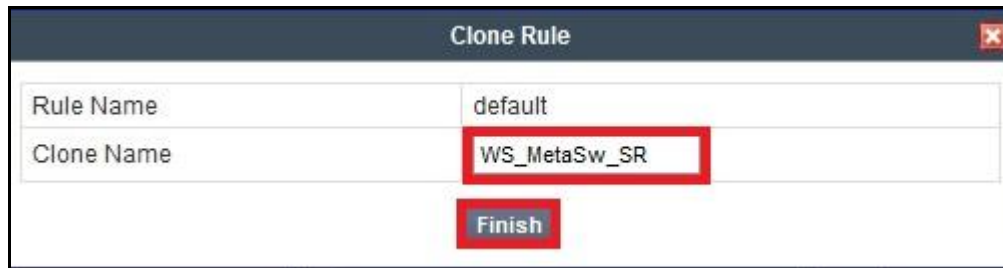
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined 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 the compliance testing, two Signaling Rules were created for Windstream and Communication Manager.

6.3.3.1 Signaling Rule for Windstream

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



Clone Rule	
Rule Name	default
Clone Name	WS_MetaSw_SR
Finish	

The **WS_MetaSw_SR** was configured to allow Windstream to accept inbound and outbound call requests. Being cloned from the Signaling Rule **default**, the **WS_MetaSw_SR** will block all requests with a “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.

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)	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div>	Exception List (one per line)	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div>

Finish

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The 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 testing.



The image shows a 'Signaling QoS' configuration window. It has a title bar with the text 'Signaling QoS' and a close button. Below the title bar is a section header 'Signaling QoS'. There are three main sections: 'Enabled' with a checked checkbox, 'ToS' with radio buttons and dropdowns, and 'DSCP' with a radio button and a dropdown. The 'DSCP' section is highlighted with a red box. The 'Value' dropdown is set to 'EF'. There is a 'Finish' button at the bottom.

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			

6.3.3.2 Signaling Rule for Session Manager

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



The image shows a 'Clone Rule' window. It has a title bar with the text 'Clone Rule' and a close button. Below the title bar is a table with two rows: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'CM_WS_MetaSw_SR'. The 'Clone Name' field is highlighted with a red box. There is a 'Finish' button at the bottom.

Clone Rule	
Rule Name	default
Clone Name	CM_WS_MetaSw_SR
Finish	

This **CM_WS_MetaSw_SR** was configured to allow Communication Manager to accept inbound and outbound call requests. Being cloned from the Signaling Rule **default**, the **CM_WS_MetaSw_SR** will block all requests with a “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

☒

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). The 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 testing.

The screenshot shows a configuration window titled "Signaling QoS". Inside, there is a sub-header "Signaling QoS". Below this, the "Enabled" checkbox is checked. There are two radio buttons: "ToS" and "DSCP". The "DSCP" radio button is selected. Below the "DSCP" radio button, there is a "Value" dropdown menu set to "EF". To the right of the "Value" dropdown, there is a text box showing "101110". At the bottom of the window, there is a "Finish" button.

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 were created for the Communication Manager and the Windstream.

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 Windstream

The following screen shows **WS_MetaSw_PG** created for Windstream:

- Set Application Rule to **WS_MetaSw_AR** as created in **Section 6.3.1**.
- Set Media Rule to **WS_MetaSw_MR** as created **Section 6.3.2**.
- Set Signaling Rule to **WS_MetaSw_SR** as created in **Section 6.3.3.1**.
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-high**.

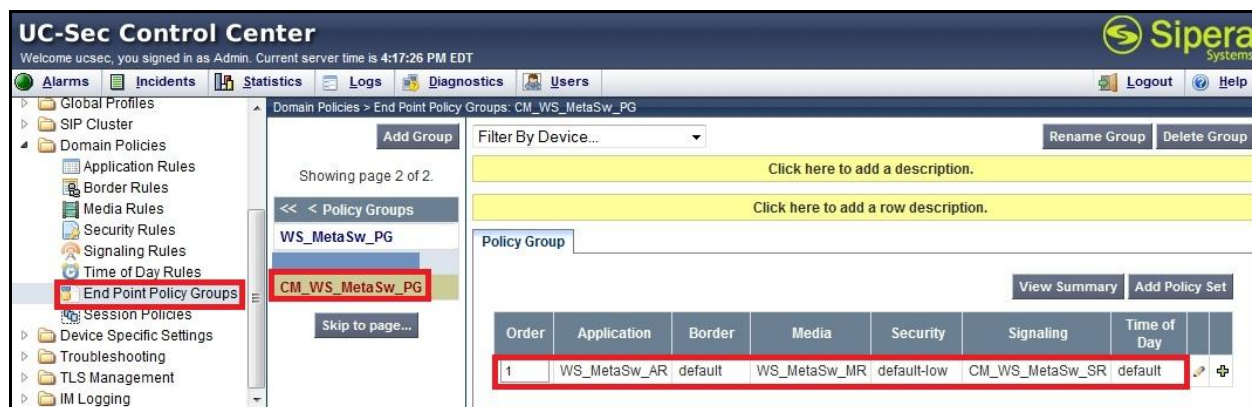
The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'End Point Policy Groups' highlighted. The main content area shows the configuration for 'WS_MetaSw_PG'. A table lists the policy group's rules, with the first row highlighted in red:

Order	Application	Border	Media	Security	Signaling	Time of Day
1	WS_MetaSw_AR	default	WS_MetaSw_MR	default-high	WS_MetaSw_SR	default

6.3.4.2 Endpoint Policy Group for Session Manager

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

- Set Application Rule to **WS_MetaSw_AR** as created in **Section 6.3.1**.
- Set Media Rule to **WS_MetaSw_MR** as created **Section 6.3.2**.
- Set Signaling Rule to **CM_WS_MetaSw_SR** as created in **Section 6.3.3.2**.
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-low**.



6.3.5. Session Policy

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 testing, a Session Policy named **CM_WS_MetaSw** was created to match the codec configuration on Windstream. The policy also allows the Avaya SBCE to anchor media in off-net call forward or off-net call transfer scenarios. It is applied to both Server Configurations for Communication Manager and Windstream.

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 **CM_WS_MetaSw** for the new policy and click **Finish**.

The screenshot shows a 'Clone Policy' dialog box with the following fields and buttons:

Policy Name	default
Clone Name	CM_WS_MetaSw

Finish

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

Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0) ▼
Preferred Codec #2	Dynamic (101) ▼
Preferred Codec #3	None ▼
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 administer the **Media Anchoring** on the Avaya SBCE, select Session Policy **CM_WS_MetaSw** created above then select tab **Media**, click **Edit** (not shown). Check to enable the **Media Anchoring**.

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

Finish

6.4. Device Specific Settings

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

Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was 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, 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**.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 10:30:20 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- 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

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](#).

A1 Netmask 255.255.255.192 A2 Netmask B1 Netmask 255.255.255.224 B2 Netmask

Add IP Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface	
110.10.97.189		110.10.97.129	A1	X
			B1	X
			B1	X
			B1	X
			B1	X
110.10.98.112		110.10.98.97	B1	X
			B1	X
			A1	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 10:33:34 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - SNMP
 - End Point Flows

Device Specific Settings > Network Management: sipera

UC-Sec Devices

sipera

Network Configuration Interface Configuration

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

6.4.2. Media Interface

Media Interface screen is where the media ports are defined. The 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).

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

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 10:36:10 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - SNMP
 - End Point Flows
 - Session Flows
 - Two Factor
 - Relay Services
 - Troubleshooting

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		X
		35000 - 40000		X
		35000 - 40000		X
		35000 - 40000		X
		35000 - 40000		X
OutsideMedia_WS_MetaSw	110.10.98.112	35000 - 40000		X
		35000 - 40000		X

6.4.3. Signaling Interface

Signaling Interface screen is where the SIP signaling port is defined. The 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).

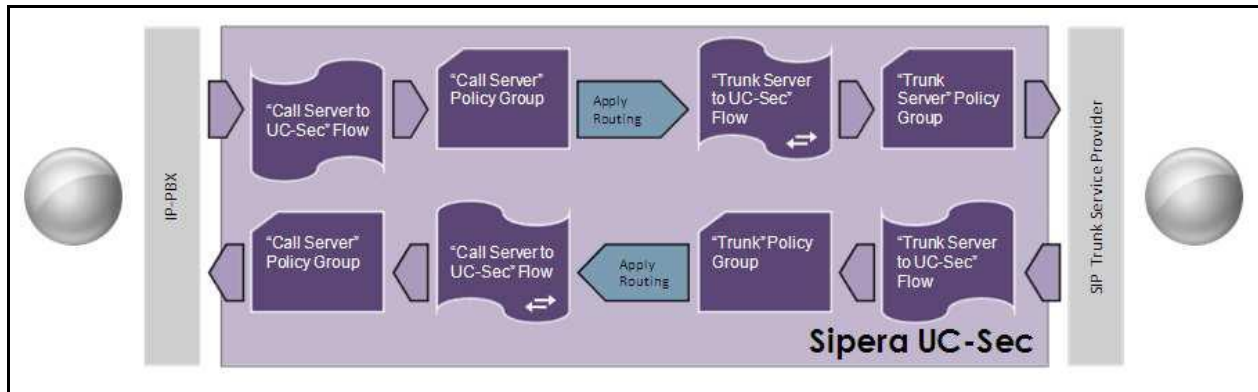
Separate Signaling Interfaces were created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060.

The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a navigation tree with 'Signaling Interface' selected. The main content area shows the 'Signaling Interface' configuration for the 'sipera' device. A table lists the configured interfaces:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP_TCP	110.10.97.189	5060	---	---	None	
OutsideSIP_WS_MetaSw	110.10.98.112	---	5060	---	None	
				---	None	
				---	None	
				---	None	
				---	None	
				---	None	
				---	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 the Avaya SBCE to secure a SIP Trunk call.



In the compliance testing, separate Server Flows were created for Windstream 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, 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 created in **Section 6.4.3** 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** to assign 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 to the Server Configuration.
- Click **Finish**.


The following screen shows the Server Flow **WS_MetaSw** configured for Windstream.

Edit Flow: WS_MetaSw

Criteria	
Flow Name	WS_MetaSw
Server Configuration	WS_MetaSw
URI Group	CM_WS_MetaSw
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_TCP
Signaling Interface	OutsideSIP_WS_MetaSw
Media Interface	OutsideMedia_WS_MetaSw
End Point Policy Group	WS_MetaSw_PG
Routing Profile	To_CM_WS_MetaSw
Topology Hiding Profile	To_WS_MetaSw
File Transfer Profile	None

Finish

The following screen shows the Server Flow **CM_WS_MetaSw** configured for Communication Manager.



Criteria	
Flow Name	CM_WS_MetaSw
Server Configuration	CM_WS_MetaSw
URI Group	CM_WS_MetaSw
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_WS_MetaSw
Signaling Interface	InsideSIP_TCP
Media Interface	InsideMedia
End Point Policy Group	CM_WS_MetaSw_PG
Routing Profile	To_WS_MetaSw
Topology Hiding Profile	To_CM_WS_MetaSw
File Transfer Profile	None

Finish

6.4.5. Session Flows

Session Flows feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or 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 was created for both Windstream and Communication Manager. 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 created in **Section 6.2.1** 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**.

Note: 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 **CM_WS_MetaSw** was created.

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

Finish

7. Windstream SIP Trunking Service Configuration

Windstream 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. Windstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the Windstream. The information provided by Windstream includes:

- IP address and port number used for signaling traffic.
- IP address and port number used for media traffic.
- Windstream SIP domain. In the compliance testing, Windstream preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, Windstream preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between Windstream and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either Windstream 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.

8.1. Verification Steps

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

8.2. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

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

- 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.

8.3. Troubleshooting

This section describes steps to troubleshooting the calls at the enterprise networks. The sample commands or procedures may be implemented in the field to confirm the configurations are provisioned properly.

8.3.1. Troubleshooting Avaya SBCE

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

Following is an example inbound call from Windstream to the enterprise.

- Inbound INVITE request from Windstream:

```
INVITE sip:5012871130@110.10.98.112:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 220.20.242.26:5060;branch=z9hG4bKiqoen42088j00es2a641.1
Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info, as-
feature-event
Max-Forwards: 69
Call-ID: 6234AD19@75.89.98.228
From: <sip:16139675258@220.20.242.26:5060>;tag=75.89.98.228+1+f703f+c561294b;isup-
oli=00
To: <sip:5012871130@110.10.98.112>
CSeq: 232278149 INVITE
Expires: 180
Organization:
Supported: 100rel, resource-priority
Content-Length: 179
Content-Type: application/sdp
Contact: <sip:16139675258@220.20.242.26:5060;transport=udp>;isup-oli=00
P-Asserted-Identity: <sip:16139675258@75.89.98.228:5060>

v=0
o=- 3859176134 3859176134 IN IP4 220.20.242.26
s=-
c=IN IP4 220.20.242.26
t=0 0
m=audio 10404 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: <sip:16139675258@220.20.242.26:5060>;tag=75.89.98.228+1+f703f+c561294b;isup-
oli=00
To: <sip:5012871130@110.10.98.112>;tag=800be36eae216825069cc4200
CSeq: 232278149 INVITE
Call-ID: 6234AD19@75.89.98.228
Contact: <sip:110.10.98.112:5060;transport=udp>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=815;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 220.20.242.26:5060;branch=z9hG4bKiqoen42088j00es2a641.1
Accept-Language: en
```



```
Server: Avaya CM/R015x.02.1.016.4
Session-Expires: 1200;refresher=uas
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 35000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

Following is an example outbound call from the enterprise to Windstream.

- Outbound INVITE request from the enterprise:

```
INVITE sip:16139675258@220.20.242.26 SIP/2.0
From: "WS x1130" <sip:5012871130@110.10.98.112>;tag=804e30576eae217325069cc4200
To: sip:16139675258@220.20.242.26
CSeq: 1 INVITE
Call-ID: cd22983a44b7e22a5c90a72385a9d163
Contact: "WS x1130" <sip:5012871130@110.10.98.112:5060>
Record-Route: <sip:110.10.98.112:5060;ipcs-line=873;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-s1632-002037400263-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@bvwlabs.com>;avaya-cm-alert-type=internal
P-Asserted-Identity: "WS x1130" <sip:5012871130@110.10.98.112>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Content-Type: application/sdp
Content-Length: 166

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 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

- 200OK/SDP response by Windstream:

```
SIP/2.0 200 OK
From: "WS x1130" <sip:5012871130@220.20.242.26>;tag=804e30576eae217325069cc4200
To: <sip:16139675258@220.20.242.26>;tag=75.89.98.228+1+10bf3f+3a4c6798
CSeq: 1 INVITE
Call-ID: cd22983a44b7e22a5c90a72385a9d163
Via: SIP/2.0/UDP 110.10.98.112:5060;branch=z9hG4bK-s1632-002037400263-1--s1632-
Record-Route: <sip:110.10.98.112:5060;ipcs-line=873;lr;transport=udp>
```

```
Server: DC-SIP/2.0
Organization:
Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info, as-
feature-event
Supported: 100rel, resource-priority
Allow: INVITE, ACK, CANCEL, BYE, REGISTER, OPTIONS, PRACK, UPDATE, SUBSCRIBE, NOTIFY,
REFER, INFO, PUBLISH
Accept-Encoding: identity
Accept: application/sdp, application/simple-message-summary, message/sipfrag,
application/isup, application/x-simple-call-service-info, multipart/mixed,
application/broadsoft, application/vq-rtcpxr, application/media_control+xml,
application/dtmf-relay, text/plain, application/x-as-feature-event+xml
Contact: <sip:16139675258@220.20.242.26:5060;transport=udp>
Content-Length: 179
Content-Type: application/sdp

v=0
o=- 3859320654 3859320654 IN IP4 220.20.242.26
s=-
c=IN IP4 220.20.242.26
t=0 0
m=audio 10408 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

8.3.2. Troubleshooting Communication Manager

- **list trace station** <extension number>. Traces call to and from a specific station.
- **list trace tac** <trunk access code number>. Trace call 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 Windstream SIP Trunking Service. Windstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. Windstream 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 Windstream 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.*
- [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/>

Product documentation for Windstream SIP Trunking Service is available from Windstream.

©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.