Avaya Solution & Interoperability Test Lab

Application Notes for Windstream SIP Trunking Service (Sonus Platform) with Avaya Aura® Communication Manager Evolution Server Release 6.2, Avaya Aura® Session Manager Release 6.2 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) trunk between Windstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, 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....6
3. Reference Configuration....7
4. Equipment and Software Validated....8
5. Configure Avaya Aura® Communication Manager....10
  5.1. Licensing and Capacity....10
  5.2. System Features....11
  5.3. IP Node Names....12
  5.4. Codecs....12
  5.5. IP Network Region....13
  5.6. Signaling Group....16
  5.7. Trunk Group....17
  5.8. Calling Party Information....20
  5.9. Outbound Routing....20
  5.10. Incoming Call Handling....22
  5.11. Saving Communication Manager Configuration Changes....23
6. Configure Avaya Aura® Session Manager....23
  6.1. System Manager Login and Navigation....23
  6.2. Specify SIP Domain....25
  6.3. Add Location....25
  6.4. Add SIP Entities....27
  6.5. Add Entity Links....30
  6.6. Add Routing Policies....31
  6.7. Add Dial Patterns....33
  6.8. Add/View Session Manager....35
7. Configure Avaya Session Border Controller for Enterprise....36
  7.1. Avaya Session Border Controller for Enterprise Login....37
  7.2. Global Profiles....40
    7.2.1. Uniform Resource Identifier (URI) Groups....40
    7.2.2. Routing Profiles....41
    7.2.3. Topology Hiding....43
    7.2.4. Server Interworking....44
    7.2.5. Signaling Manipulation....50
    7.2.6. Server Configuration....51
  7.3. Domain Policies....54
    7.3.1. Application Rules....55
    7.3.2. Media Rules....56
    7.3.3. Signaling Rules....58
    7.3.4. Endpoint Policy Groups....62
    7.3.5. Session Policy....63
  7.4. Device Specific Settings....65

7.4.1. Network Management....65
7.4.2. Media Interface....66
7.4.3. Signaling Interface....67
7.4.4. End Point Flows - Server Flow....68
7.4.5. Session Flows....70
8. Windstream SIP Trunking Service Configuration....71
9. Verification and Troubleshooting....71
9.1. Verification Steps....72
9.2. Protocol Traces....72
9.3. Troubleshooting:....72
9.3.1. The Avaya SBCE....72
9.3.2. Communication Manager....75
10. Conclusion....75
11. References....75

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 6.2 configured as an Evolution Server, Avaya Aura® Session Manager 6.2, Avaya SBC 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 SIP, 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 SIP, 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. Both SIP and H.323 protocols are 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 codec negotiation with G.729 and G.711MU codecs.
- Early Media transmissions using G.729 and 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 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.
- T.38 fax is not supported.
- Off-net call forwarding using History-Info method is not supported.

2.2. Test Results

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

1. **Network Call Redirection fails with “302 Moved Temporarily”**. A vector DN is programmed to use “302 Moved Temporarily” to redirect an inbound call to PSTN before answering. Windstream does not properly support “302 Moved Temporarily” as it sent an ACK to the “302 Moved Temporarily” but did not redirect the call to PSTN party specified in the Contact header.

2. **The untrusted Calling Party Name (CPN) from Communication Manager is not examined**. In an outbound call scenario, PSTN displayed the original untrusted CPN from Communication Manager. Windstream does not examine the CPN before sending to PSTN. This is a known issue of Windstream SIP Trunking Service with no available resolution at this time.

3. **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.

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. The fax document was transmitted successfully with acceptable quality. **Note**: The codec set should have G.711MU codec as a first choice otherwise the fax call would not be successfully established since neither Communication Manager nor Windstream has the ability to switch the voice call using different codec .e.g. G/729 to G.711MU for the fax call

5. **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 “Sorry, your call cannot completed as dial, please check the number and dial again” and then followed by a regular busy tone. However, the call did not terminate properly as Windstream did not send out a CANCEL request. After the session provisioning timer expired, Communication Manager properly terminated the call and released the trunk. This is a known issue on Windstream SIP Trunking Service with no resolution available at this time.

6. **The Local Directory Assistance Call (411) does not terminate properly**. The outbound 411 call was successfully connected to an Interactive Voice Response (IVR) system at Windstream. The IVR was able to provide the correct requested directory number. However, the call did not terminate properly as Windstream did not send out a CANCEL request. After the session timer expired, Communication Manager properly terminated the call and released the trunk. This is a known issue on Windstream SIP Trunking Service with no resolution available at this time.

7. **When an inbound vector call is redirected to PSTN by a REFER, but the terminator PSTN party is busy, Windstream fails to disconnect the call**. After accepting the REFER by a “202 Accepted”, Windstream sends a “NOTIFY/Trying” to Communication Manager to indicate the transferred call is in progress. When the terminator PSTN party is busy, Windstream should be able to send regular busy tone to originator PSTN party. However, it did not send a “NOTIFY/486 User Busy” or a BYE request to disconnect the call. After the session timer expired, Communication Manager properly terminates the call and releases the trunk. This is a known issue on Windstream SIP Trunking Service with no resolution available at this time.

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 disguised in these Application Notes. Note: The IP addresses used in these Application Notes for the illustration purpose only.

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

- Avaya S8800 Servers running Avaya Aura® System Manager
- Avaya S8800 Servers running Avaya Aura® Session Manager
- Avaya S8800 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 (SIP and H.323)
- Avaya one-X® Communicator soft phones (SIP and 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 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 Session Manager is UDP, while TCP is used as the transport protocol between Session Manager and Communication Manager.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “ws.avaya.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.

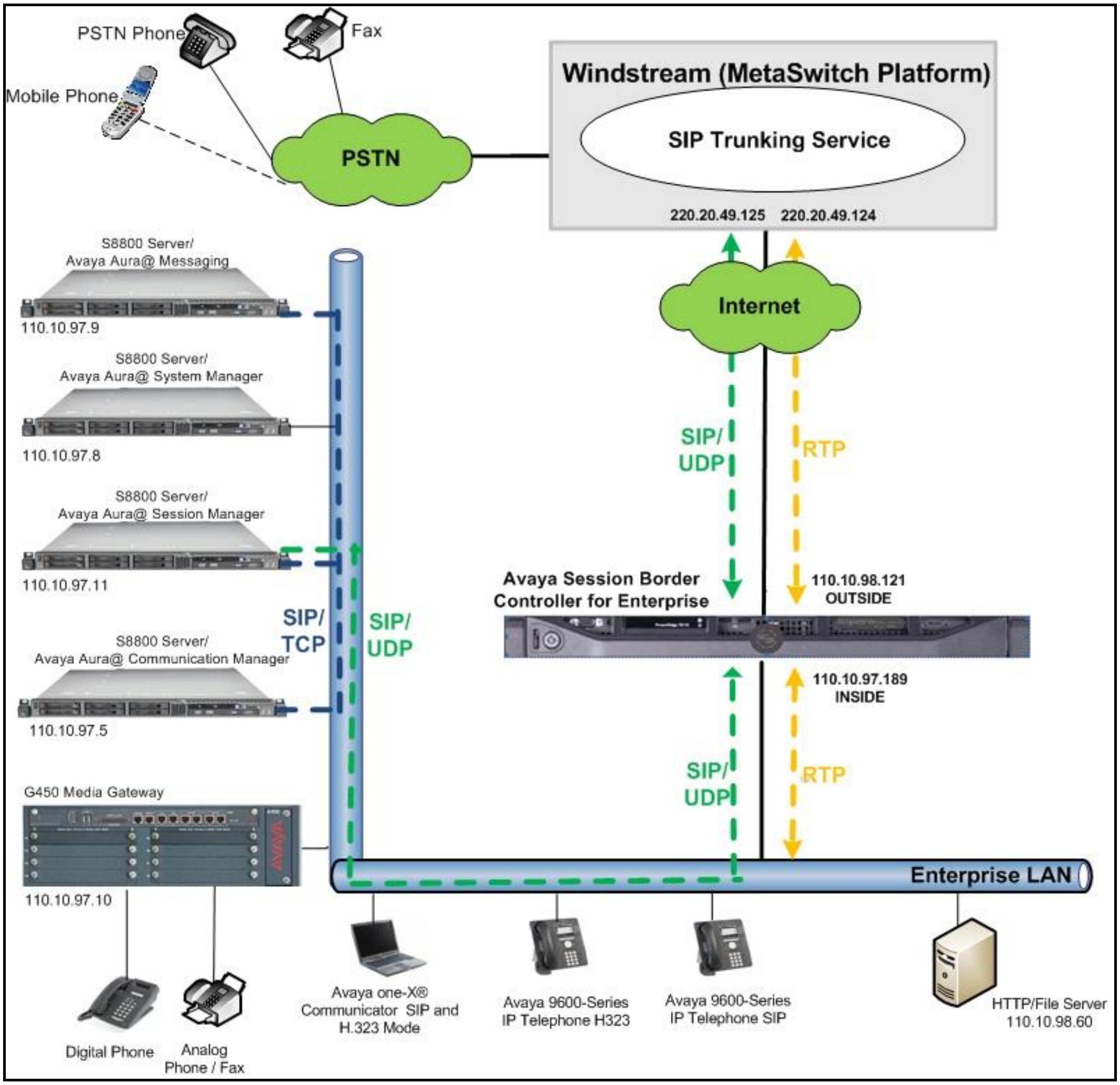


Figure 1: Avaya IP Telephony Network connecting to Windstream SIP Trunking Service

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 S8800 Server	6.2 (Avaya CM/R016x.02.0.823.0 with Service Pack 3 02.0.823.0-20001) (System Platform 6.2.1.0.9)

Avaya G450 Media Gateway	31.22.0
Avaya Aura® System Manager running on an Avaya S8800 Server	6.2.12.0 (Patch 6.2.12.202 Build Number 6.2.14.1.1925) (System Platform 6.2.1.0.9)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.2 (6.2.2.0.622005)
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 9640 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition R6_0_3-120511
Avaya one-X Communicator (SIP and 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 (Sonus Platform) Components	
Component	Release
Sonus NBS	Release V07.01.06 R002

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 Session Manager to carry traffic to and from service provider respectively. For inbound call, the call flows from Windstream to the Avaya SBCE to Communication Manager via Session 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 **24000** licenses are available and **96** 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 sales 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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 0
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 96
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   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  19
                            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.

```
display system-parameters features                              Page   9 of  19
                        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 Session Manager (**SM62**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM62                110.10.97.11
default             0.0.0.0
procr               110.10.97.5
procr6              ::
```

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 and G.729 with ptime 30ms. To use these codecs, enter G.711MU and G.729 in the **Audio Codec** column of the table in the order of preference, change the **Frames Per Pkt** to 3 to define the **Packet Size** as 30ms. Default values can be used for all other fields.

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

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

                          IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          3        30
 2: G.729            n          3        30
 3:
```

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.

Note: To successfully send and receive fax using G.711MU codec, the voice call has to be established with G.711MU codec. That means the codec profile should have G.711MU codec as a first choice and the Session Policy configuration on the Avaya SBCE in **Section 7.3.5** should prioritize G.711MU as the first choice in the prefer codec list.

```
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 calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance testing, **ip-network-region 1** was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name “ws.avaya.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 7.2.3** is used to convert this private domain name to the IP Address based URI-Host in the “From” and “PAI” headers to meet the requirement 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  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: ws.avaya.com
    Name: BVW
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
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, 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   4 of  20

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

Non-IP telephones (e.g., analog, digital) derive network region from the IP interface of the Avaya G450 Media Gateway which is the device connected to. 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, Session Manager 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 110.10.98.0/24 subnet.

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

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING

                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 110.10.97.0                                /24    3      n
   TO: 110.10.97.255
 FROM: 110.10.98.0                                /24    3      n
   TO: 110.10.98.255
 FROM:                                            /             n
   TO:
```

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   2
                                  IP INTERFACES


                  Type: procr
                                                       Target socket load: 19660

      Enable Interface? y                             Allow H.323 Endpoints? y
                                                       Allow H.248 Gateways? y
        Network Region: 1                              Gatekeeper Priority: 5


                                 IPV4 PARAMETERS
             Node Name: procr                     IP Address: 110.10.97.5


           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   2
                             MEDIA GATEWAY 1
                    Type: g450
                    Name: G450
               Serial No: 12N517873797
            Encrypt Link? y                  Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data: 1
           Recovery Rule: none

              Registered?  n
   FW Version/HW Vintage: 31 .22 .0  /1
        MGP IPV4 Address: 110.10.197.10
        MGP IPV6 Address:
   Controller IP Address:
             MAC Address: cc:f9:54:28:14:48
```

5.6. Signaling Group

Use the **add signaling-group** command to create two signaling groups between Communication Manager and Session Manager, 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 **SM**.
- 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 **SM62**. This node name maps to the IP address of Session Manager 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 **“ws.avaya.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 **y**. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- 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   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM62
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

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

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   2
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM62
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain: ws.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? 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 5.6**. 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 5.6**. 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: Public_Inbound              COR: 1        TN: 1        TAC: *001
   Direction: incoming      Outgoing Display? y
 Dial Access? n                                 Night Service:

Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       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** for the private inbound calls. 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
                                                UUI 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.
- Set the **Convert 180 to 183 for Early Media** field to **y**.

```
add trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? y
                 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


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

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: Public_outbound             COR: 1        TN: 1        TAC: *002
   Direction: outgoing       Outgoing Display? y
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk
                                              Member Assignment Method: auto
                                                       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 45 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 864263 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  45             1-2        864263           10    Total Administered: 2
                                                       Maximum Entries: 540
```

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

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 2
 4  45            1-2       864263          10       Maximum Entries: 9999
```

5.9. Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route an 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   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   45          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  10
                               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: *010
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *000
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2: 6
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        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           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    0                     1    28    2        op            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: WindstreamSonus
                             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 864263 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  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 864263           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 Aura® Session Manager

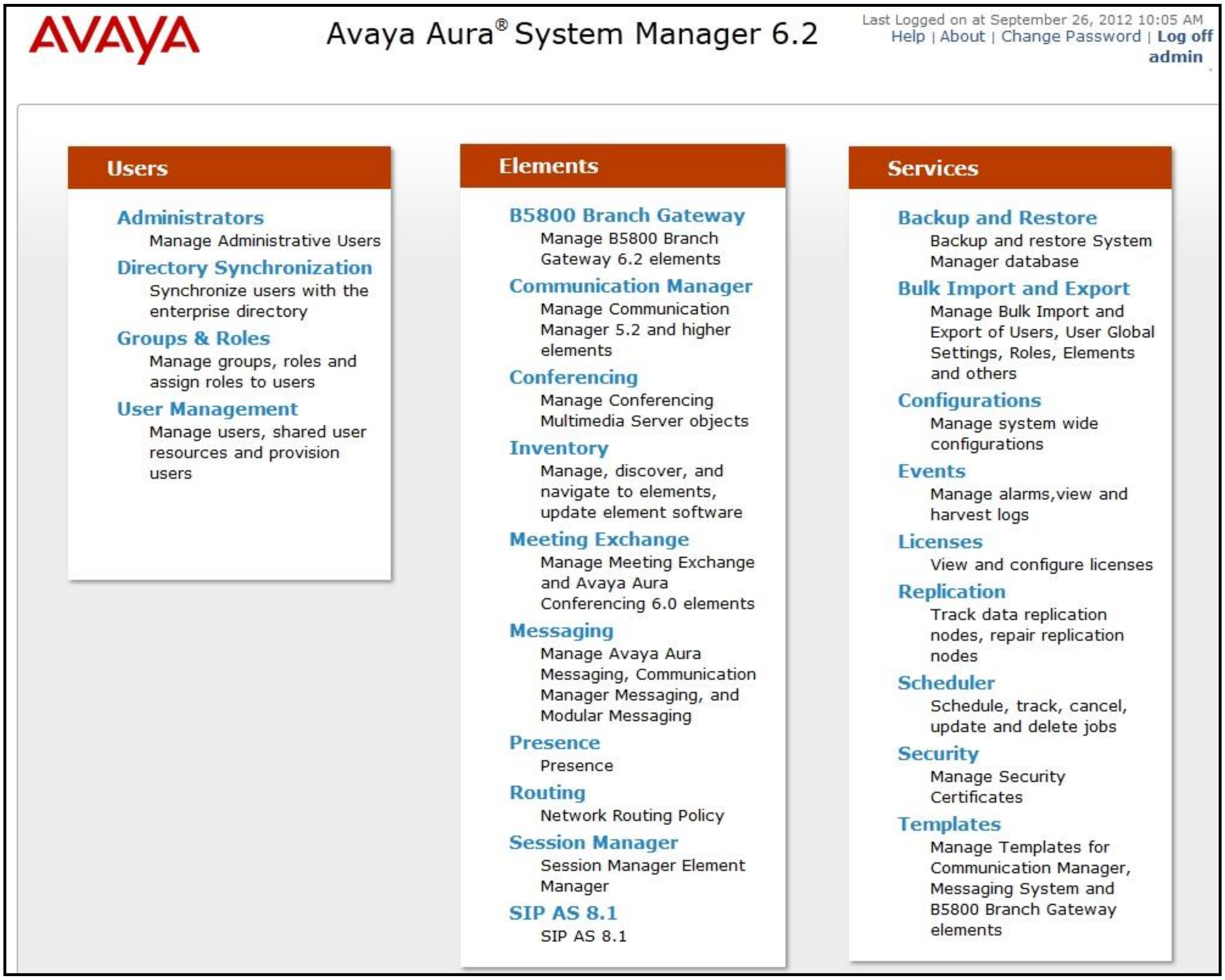
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



Avaya Aura® System Manager 6.2

Last Logged on at September 26, 2012 10:05 AM

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

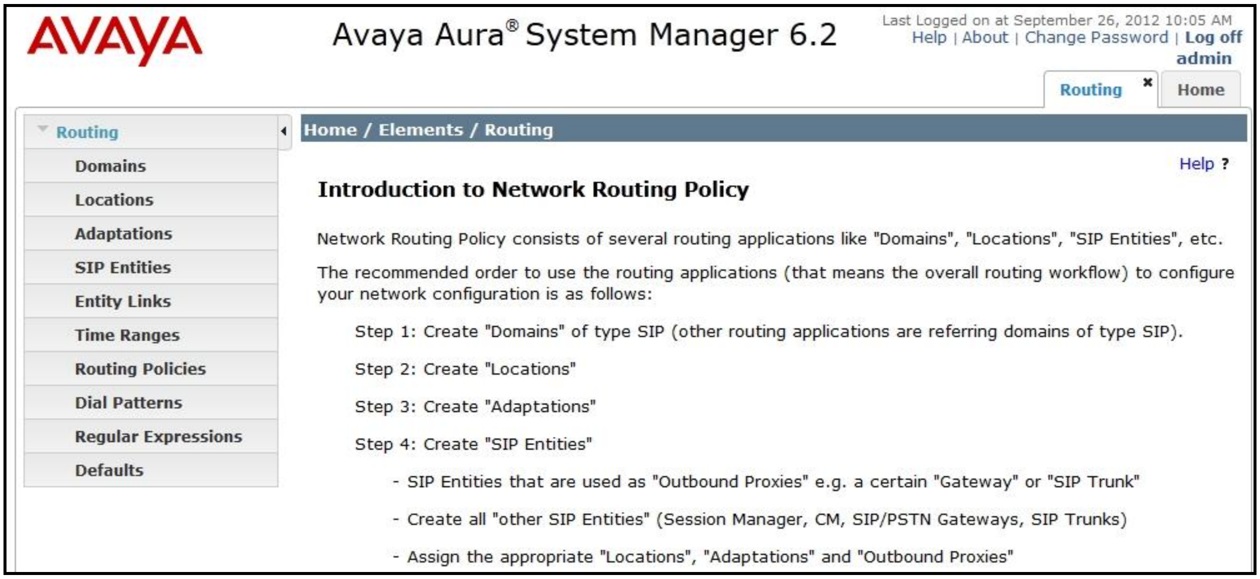
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway elements

Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

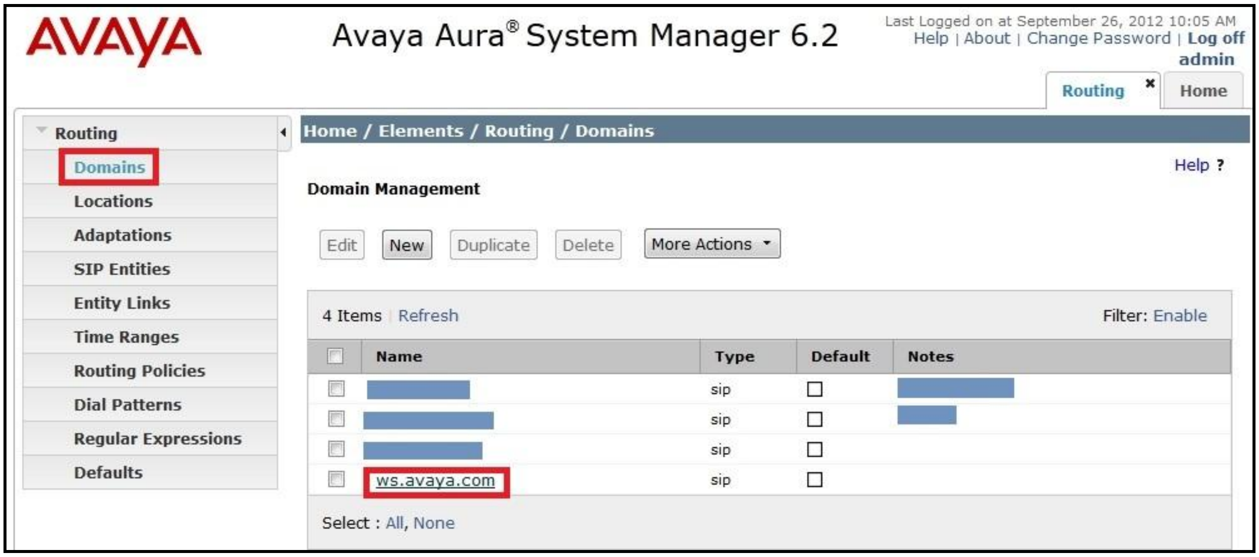
Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

6.2. Specify SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain "ws.avaya.com" was already being created for communication Session Manager and Communication Manager. The domain "ws.avaya.com" is not known to the Windstream. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Windstream.



Domain Management

☐	Name	Type	Default	Notes
☐	[redacted]	sip	☐	[redacted]
☐	[redacted]	sip	☐	[redacted]
☐	[redacted]	sip	☐	
☐	ws.avaya.com	sip	☐	

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for bandwidth management and call admission control purposes. To add a location, navigate to

Routing →Locations in the left-hand navigation pane and click the **New** button in the right pane (not shown).

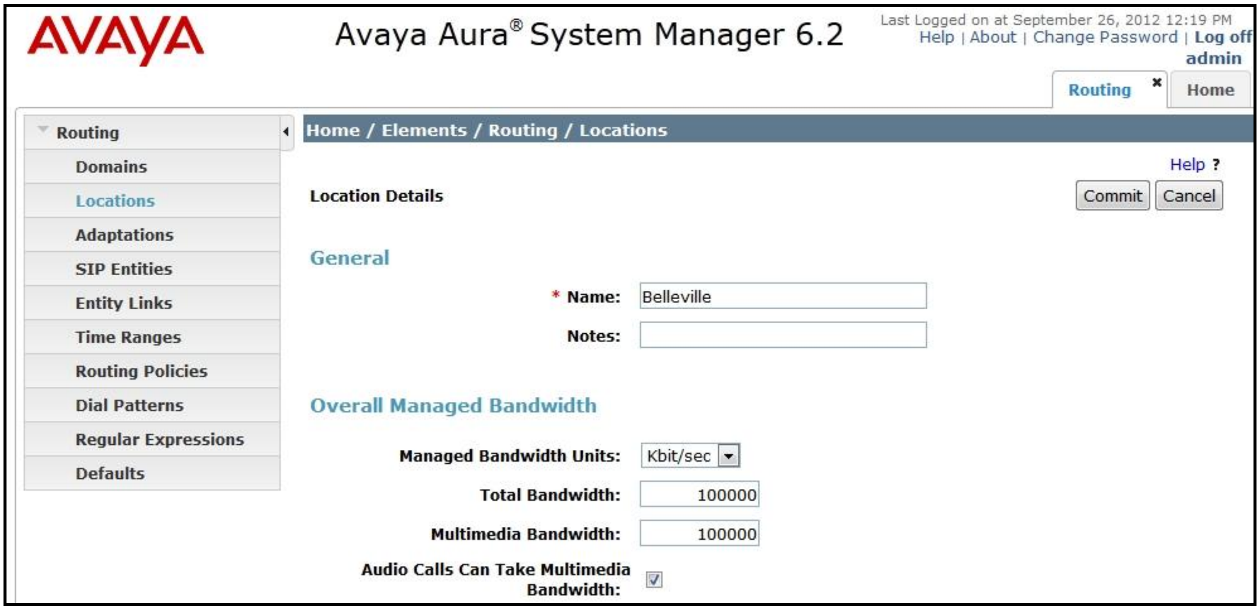
In the **General** section, enter the following values:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern** section (see the screen below), click **Add** and enter the following values:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Displayed below are the screenshots for location **Belleville**, which includes all equipment on the **110.10.x.x** subnet including Communication Manager, Session Manager and the Avaya SBCE. Click **Commit** to save.



Location Details

General

* Name: Belleville

Notes:

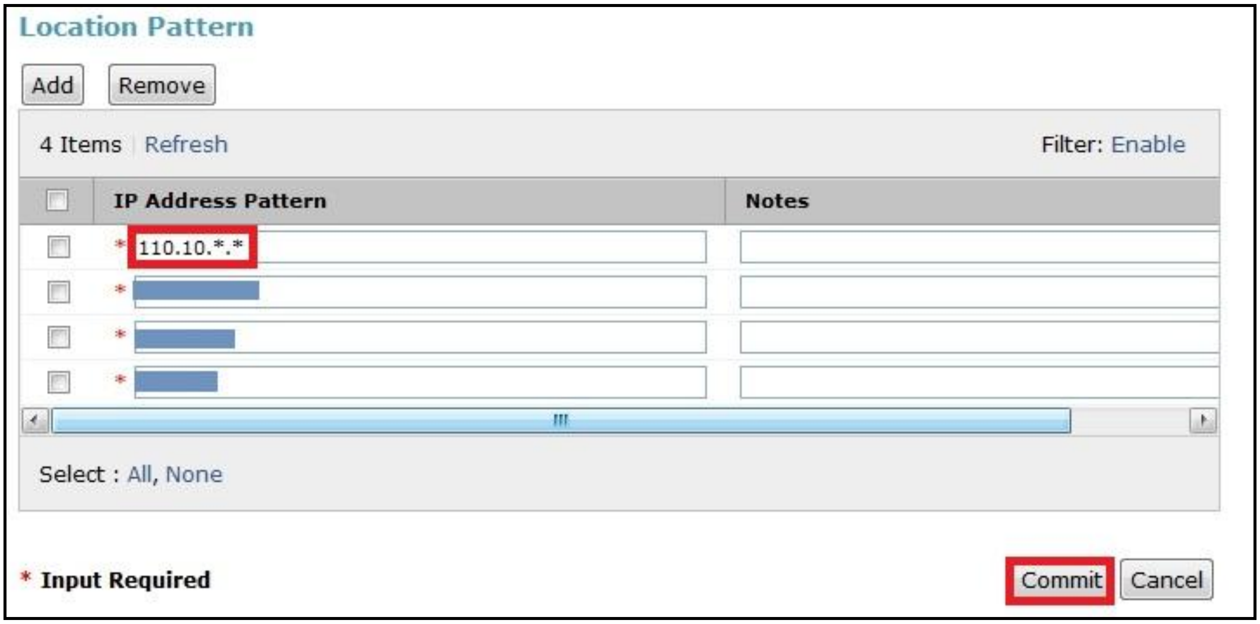
Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 100000

Multimedia Bandwidth: 100000

Audio Calls Can Take Multimedia Bandwidth: ☑



☐	IP Address Pattern	Notes
☐	* 110.10.*.*	
☐	* [redacted]	
☐	* [redacted]	
☐	* [redacted]	

* **Input Required**

6.4. Add SIP Entities

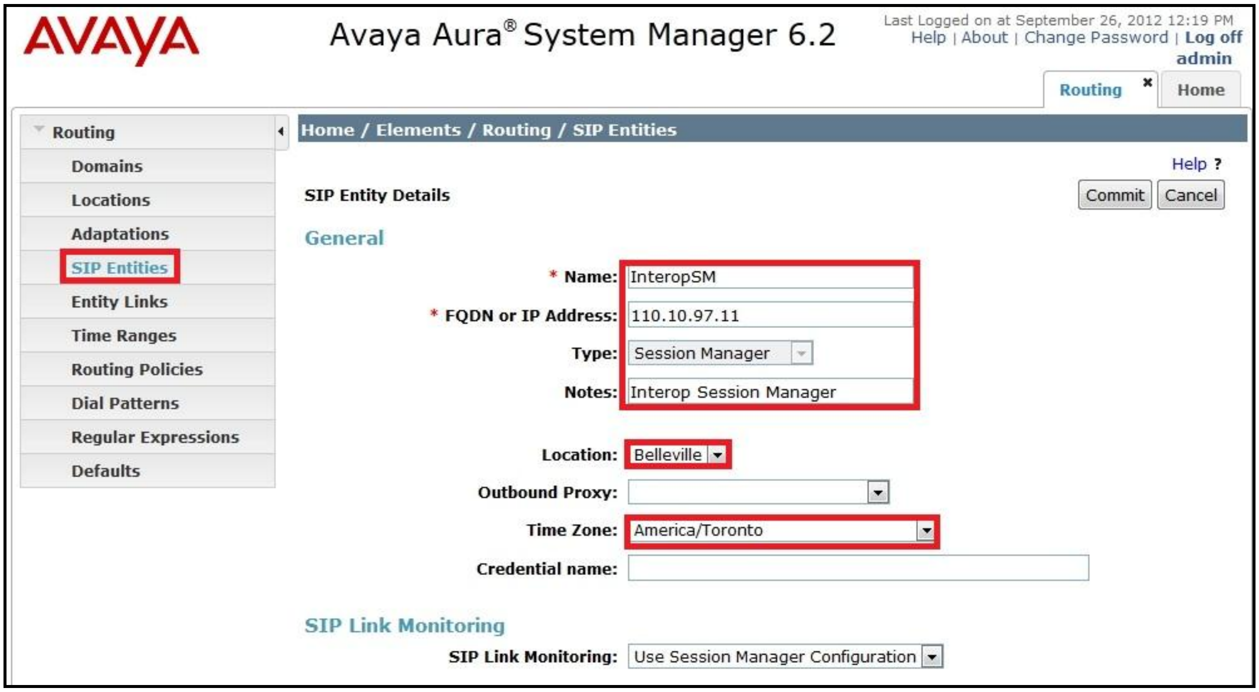
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and the Avaya SBCE.

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the Avaya SBCE.
- **Location:** Select one of the locations defined previously in **Section 6.3**.
- **Time Zone**: Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



SIP Entity Details

General

* Name: InteropSM

* FQDN or IP Address: 110.10.97.11

Type: Session Manager

Notes: Interop Session Manager

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

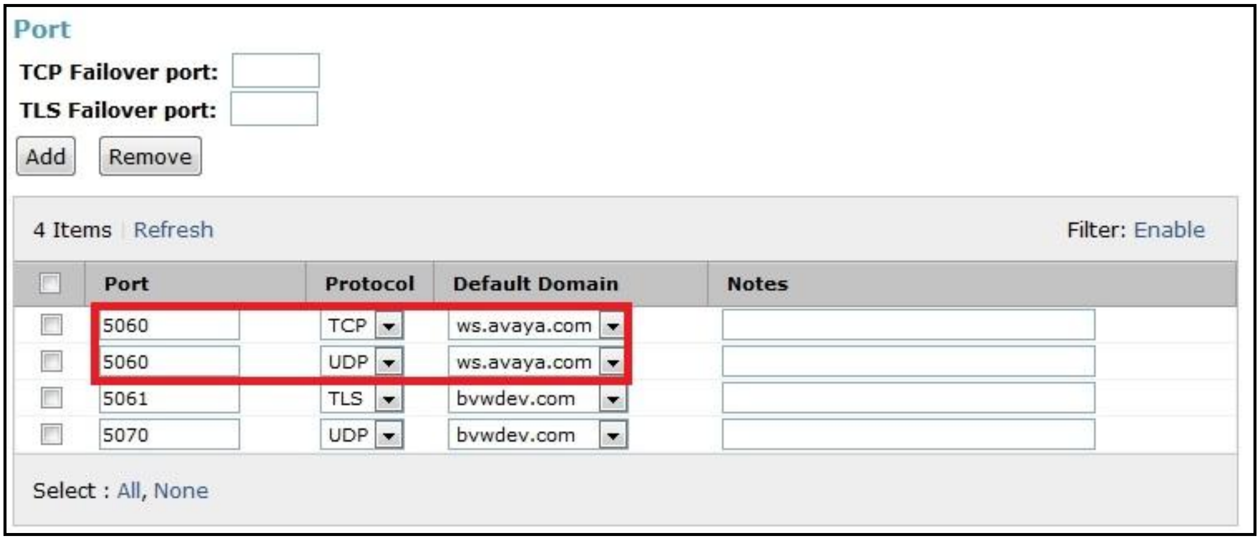
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Port** entry **5060** with **TCP** for connecting to Communication Manager and **Port** entry **5060** with **UDP** for connecting to the Avaya SBCE.



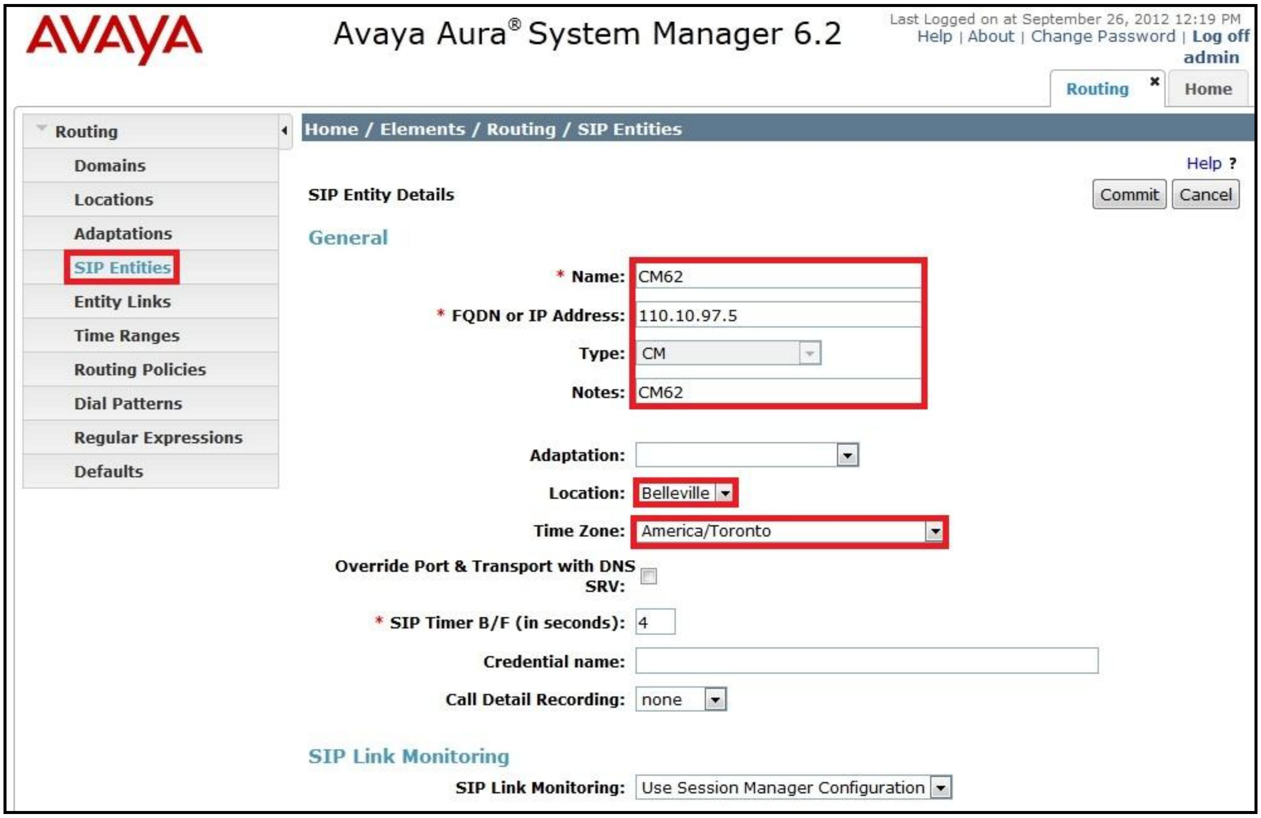
TCP Failover port:

TLS Failover port:

4 Items | Refresh | Filter: Enable

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	ws.avaya.com	
☐	5060	UDP	ws.avaya.com	
☐	5061	TLS	bvwdev.com	
☐	5070	UDP	bvwdev.com	

The following screen shows the addition of Communication Manager SIP Entities. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 26, 2012 12:19 PM
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / SIP Entities
Help ?
Commit
Cancel

SIP Entity Details

General

* Name: CM62

* FQDN or IP Address: 110.10.97.5

Type: CM

Notes: CM62

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

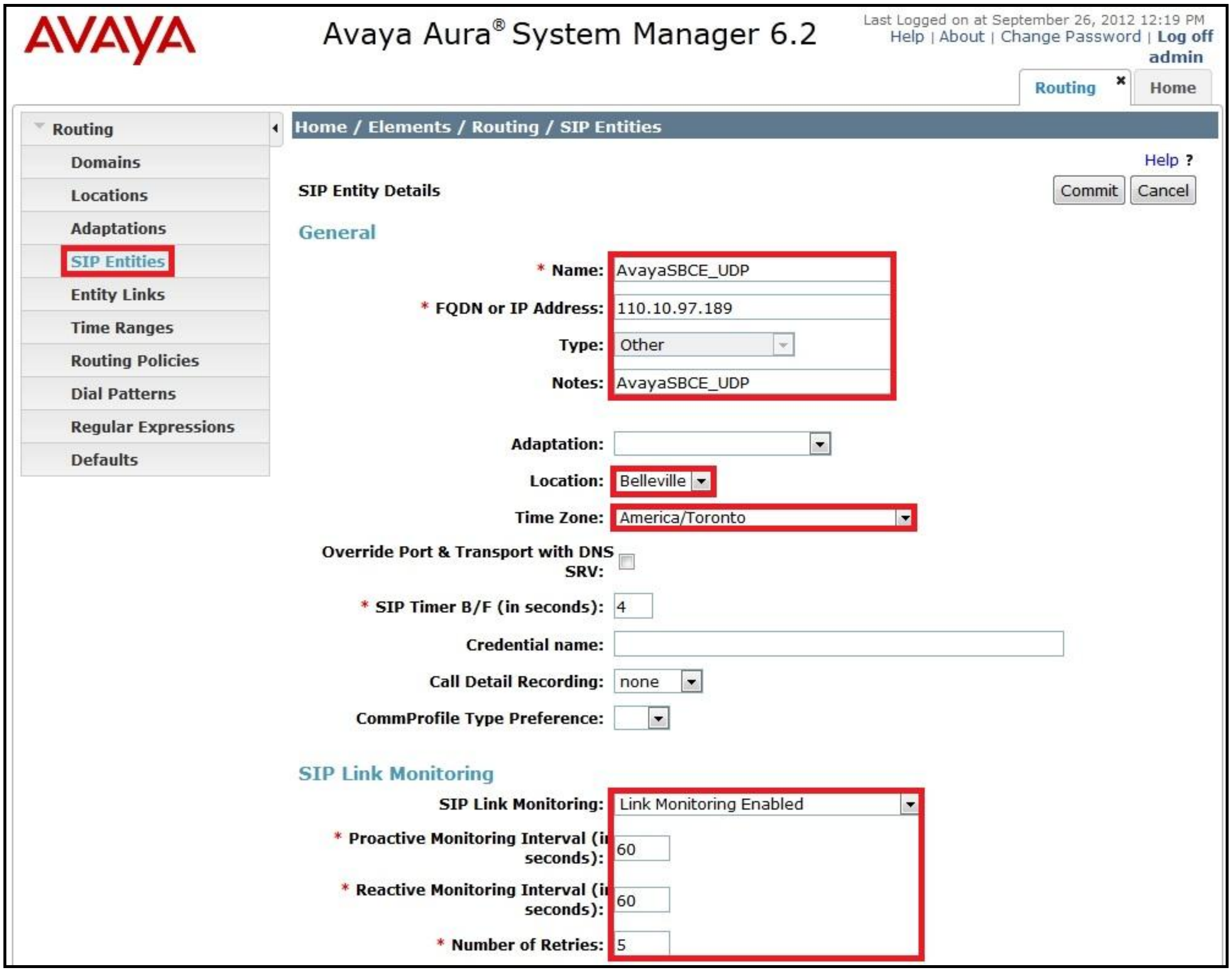
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select

Type as **Other**. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of 60 seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat in every 60 seconds to service provider (which is forwarded by the Avaya SBCE) to query for the status of the SIP trunk connecting to service provider.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 26, 2012 12:19 PM
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / SIP Entities
Help ?
Commit
Cancel

SIP Entity Details

General

* Name: AvayaSBCE_UDP

* FQDN or IP Address: 110.10.97.189

Type: Other

Notes: AvayaSBCE_UDP

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (i seconds): 60

* Reactive Monitoring Interval (i seconds): 60

* Number of Retries: 5

6.5. Add Entity Links

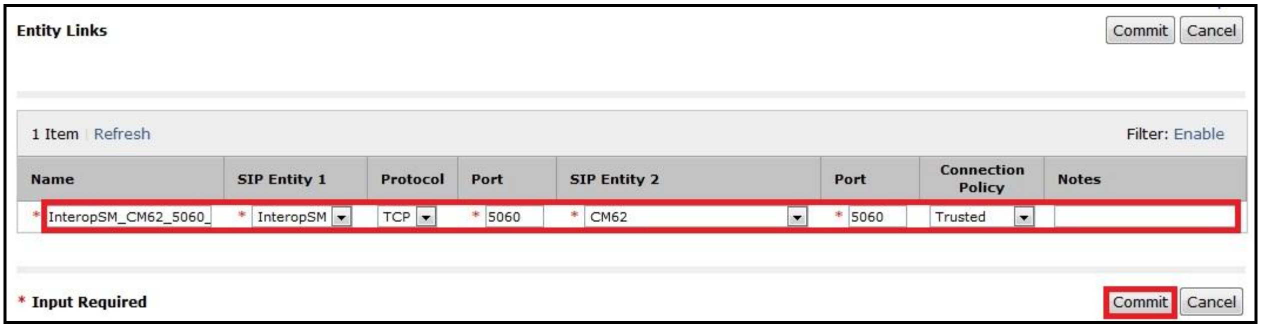
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and the other for the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link, TCP for the Entity Link to Communication Manager and UDP for the Entity Link to the Avaya SBCE.

- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**. For the Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note**: If this is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and the Avaya SBCE.

Entity Link to Communication Manager:



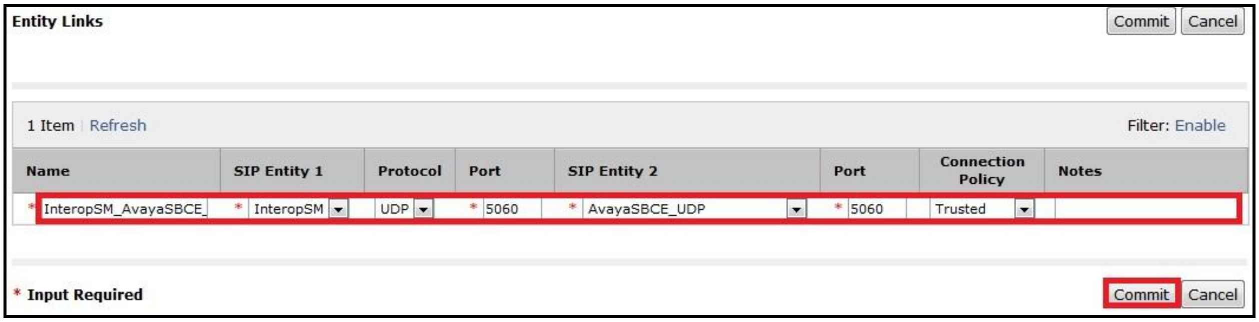
Entity Links

1 Item

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* InteropSM_CM62_5060_	* InteropSM	TCP	* 5060	* CM62	* 5060	Trusted	

* Input Required

Entity Link to the Avaya SBCE:



Entity Links

1 Item

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* InteropSM_AvayaSBCE_	* InteropSM	UDP	* 5060	* AvayaSBCE_UDP	* 5060	Trusted	

* Input Required

6.6. Add Routing Policies

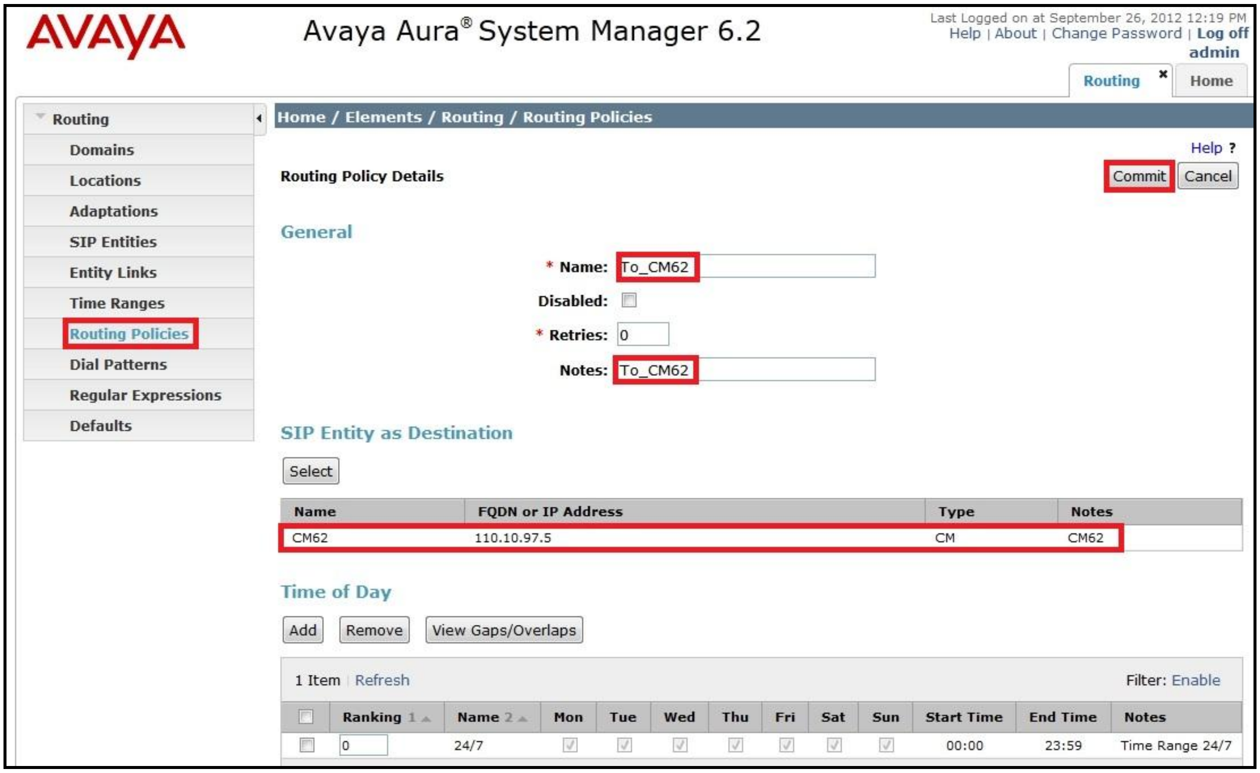
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies were added, one for Communication Manager and the other for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

In the **General** section, enter the following values:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies **To_CM62** for Communication Manager.



Routing Policy Details

General

* Name: To_CM62

Disabled: ☐

* Retries: 0

Notes: To_CM62

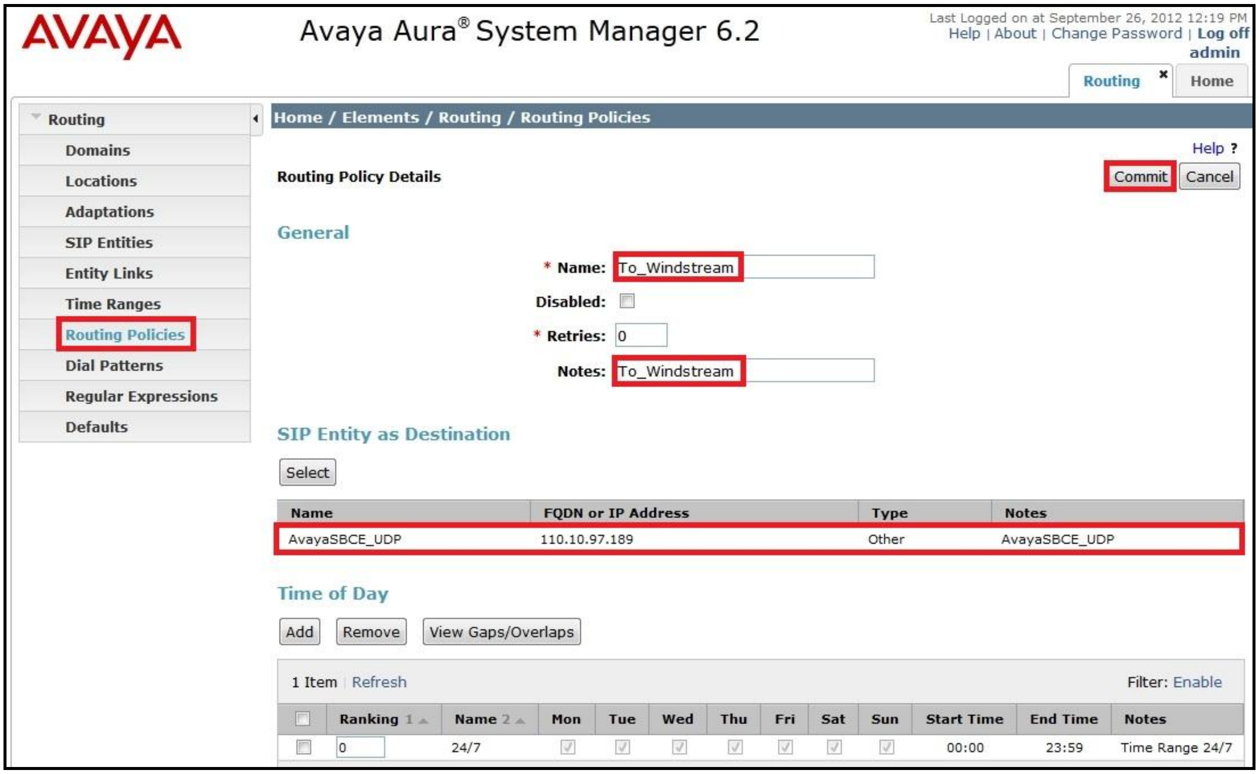
SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM62	110.10.97.5	CM	CM62

Time of Day

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

The following screens show the Routing Policies **To_Windstream** for the Avaya SBCE.



Routing Policy Details

General

* Name: To_Windstream

Disabled: ☐

* Retries: 0

Notes: To_Windstream

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AvayaSBCE_UDP	110.10.97.189	Other	AvayaSBCE_UDP

Time of Day

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Windstream and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values:

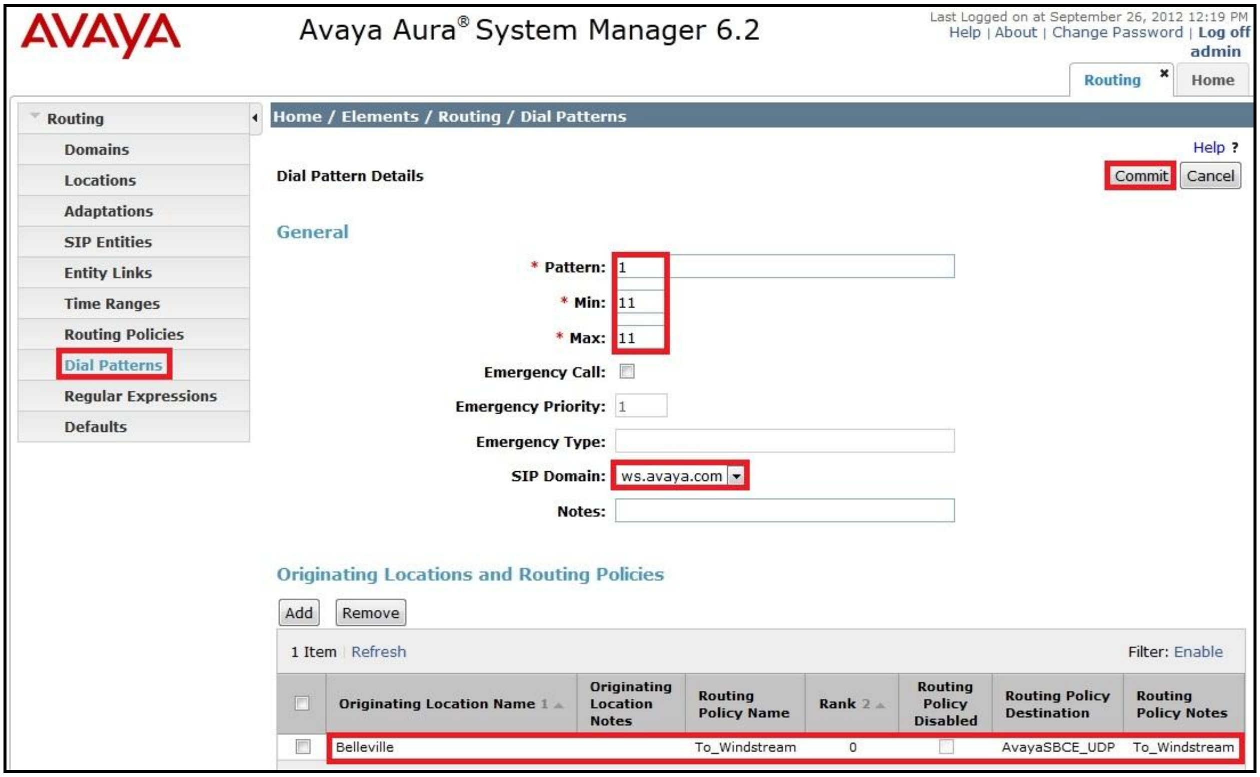
- **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls etc.) are similarly defined.

The first example shows that 11-digit dialed numbers that begin with 1 and has a destination domain of “ws.avaya.com” uses route policy **To_Windstream** as defined in **Section 6.6**.



Dial Pattern Details

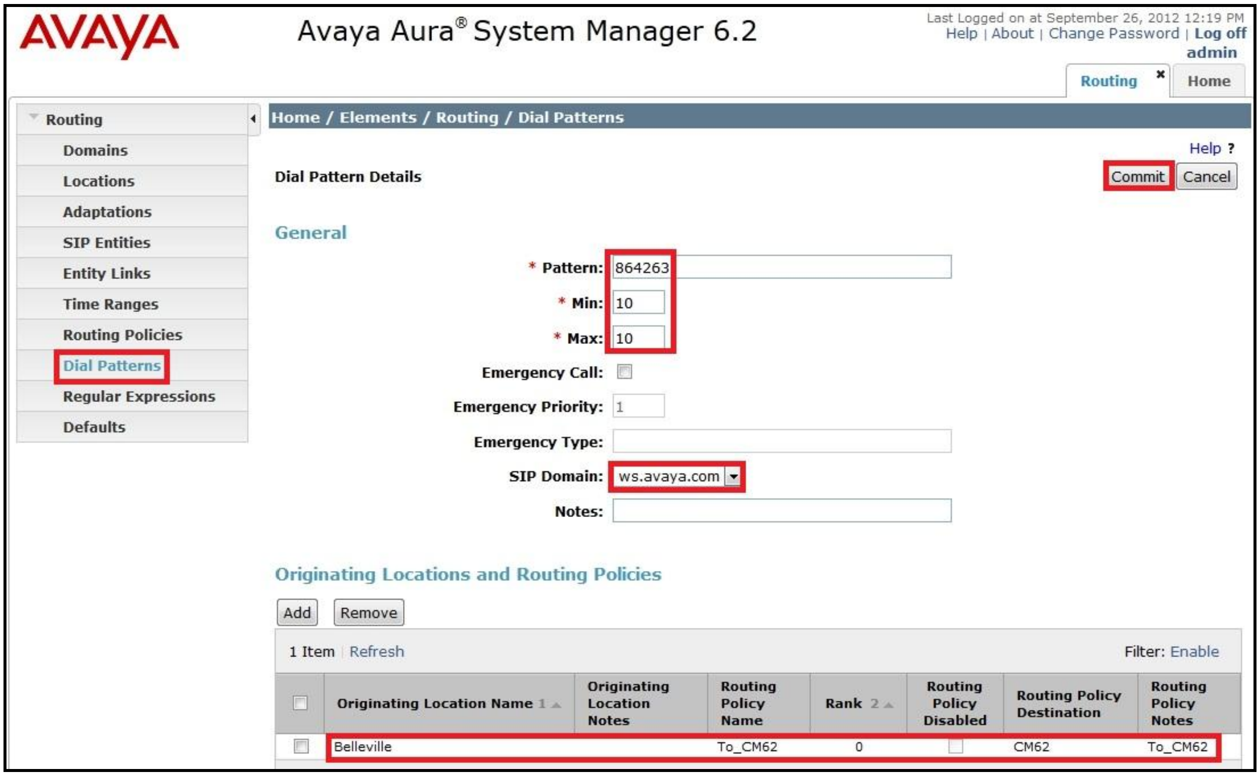
General

* Pattern: 1
* Min: 11
* Max: 11
Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: ws.avaya.com
Notes:

Originating Locations and Routing Policies

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Belleville		To_Windstream	0	☐	AvayaSBCE_UDP	To_Windstream

The second example shows that inbound 10-digit numbers that start with 864263 to domain “ws.avaya.com” uses route policy **To_CM** as defined in **Section 6.6**. These are the DID numbers assigned to the enterprise by Windstream.



Dial Pattern Details

General

* Pattern: 864263
* Min: 10
* Max: 10
Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: ws.avaya.com
Notes:

Originating Locations and Routing Policies

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Belleville		To_CM62	0	☐	CM62	To_CM62

6.8. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

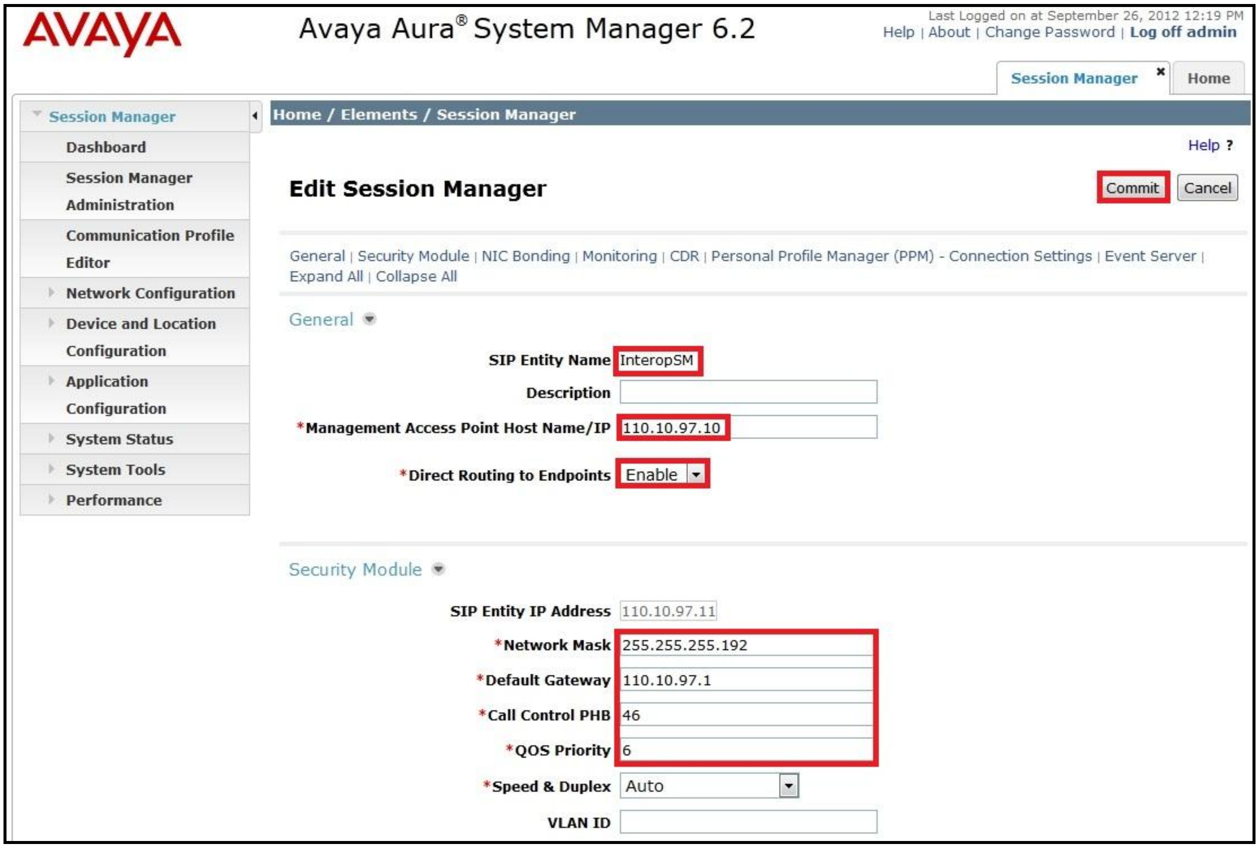
In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints**: Enabled, to enable call routing on the Session Manager.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.
- Use default values for the remaining fields. Click **Commit** to save (not shown).

The screen below shows the Session Manager values used for the compliance testing.


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at September 26, 2012 12:19 PM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager
Help ?
Edit Session Manager
Commit
Cancel
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All
General
Security Module

SIP Entity Name InteropSM
Description
***Management Access Point Host Name/IP** 110.10.97.10
***Direct Routing to Endpoints** Enable

SIP Entity IP Address 110.10.97.11
***Network Mask** 255.255.255.192
***Default Gateway** 110.10.97.1
***Call Control PHB** 46
***QOS Priority** 6
***Speed & Duplex** Auto
VLAN ID

7. 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 [**15**] and [**16**].

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

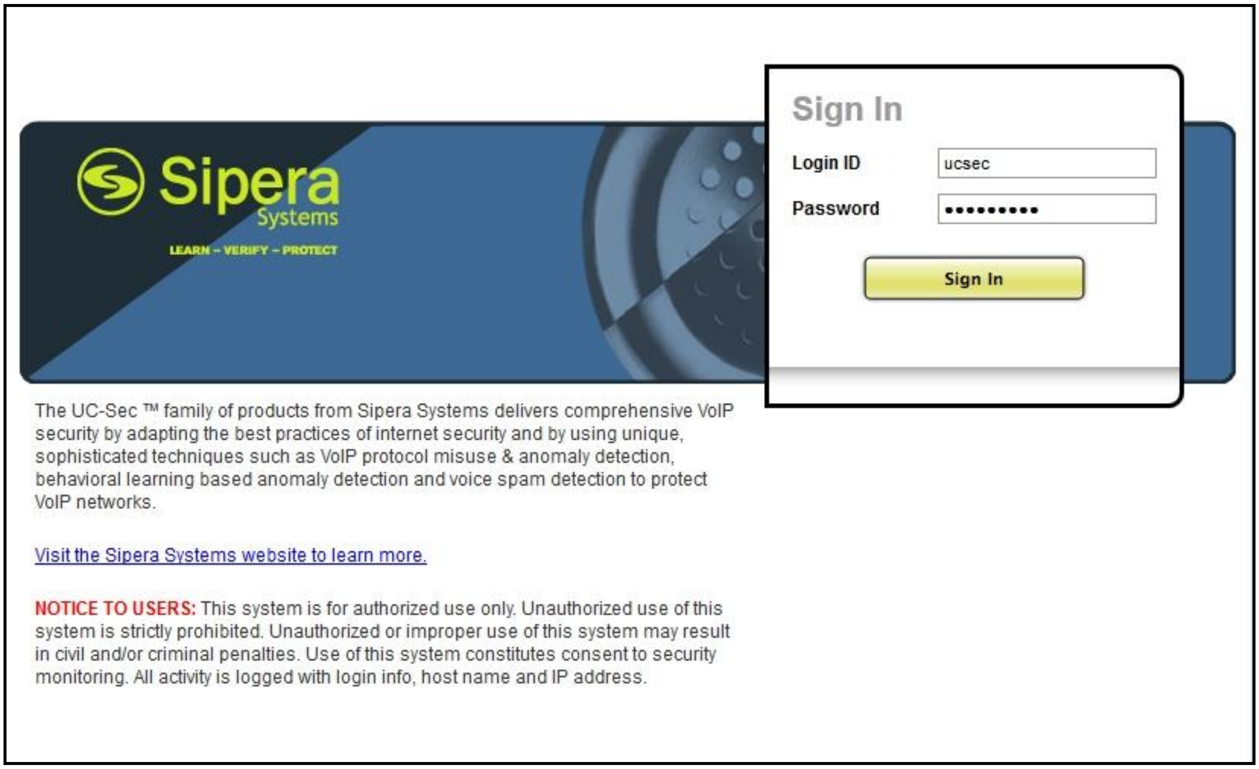
Call server configuration elements for the enterprise - Session Manager:

- 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

7.1. 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***.



Login ID: ucsec

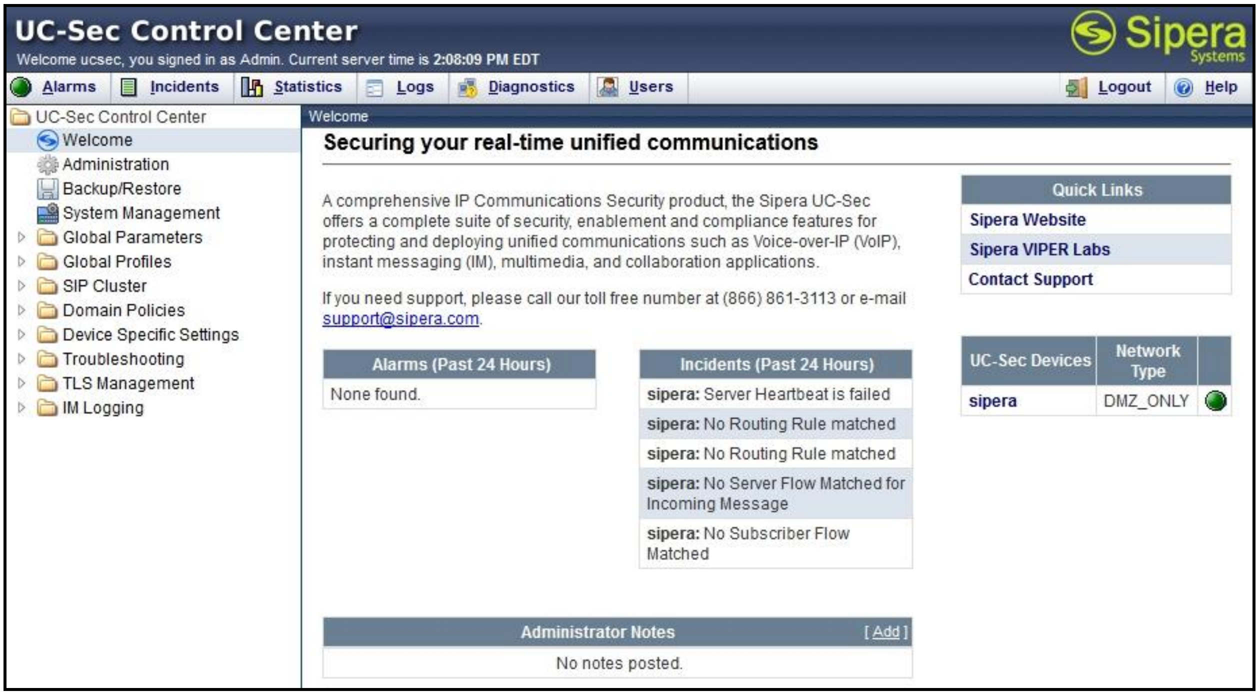
Password: ••••••••••

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.



Welcome ucsec, you signed in as Admin. Current server time is 2:08:09 PM EDT

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.

Quick Links
Sipera Website
Sipera VIPER Labs
Contact Support

Alarms (Past 24 Hours)
None found.

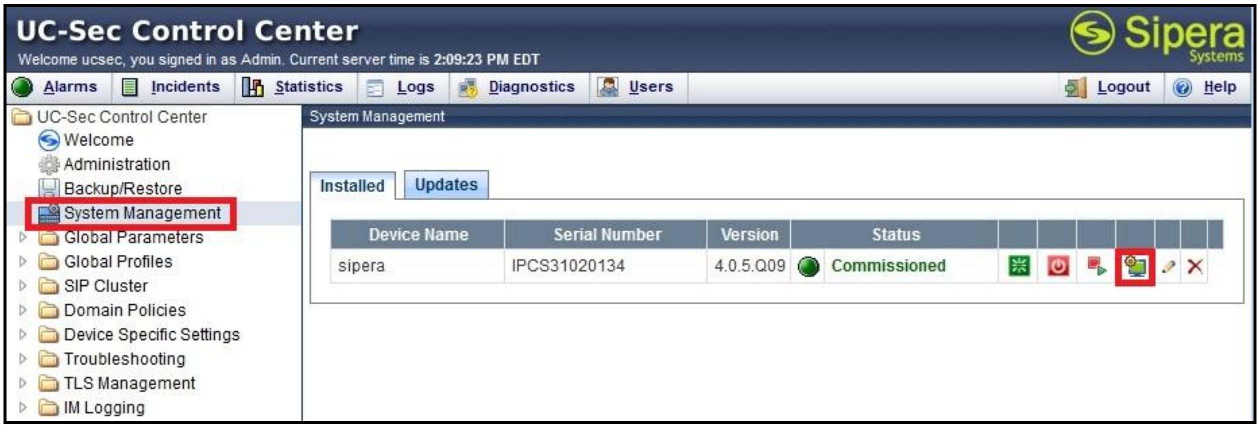
Incidents (Past 24 Hours)
sipera: Server Heartbeat is failed
sipera: No Routing Rule matched
sipera: No Routing Rule matched
sipera: No Server Flow Matched for Incoming Message
sipera: No Subscriber Flow Matched

UC-Sec Devices	Network Type	
sipera	DMZ_ONLY	●

Administrator Notes [Add]
No notes posted.

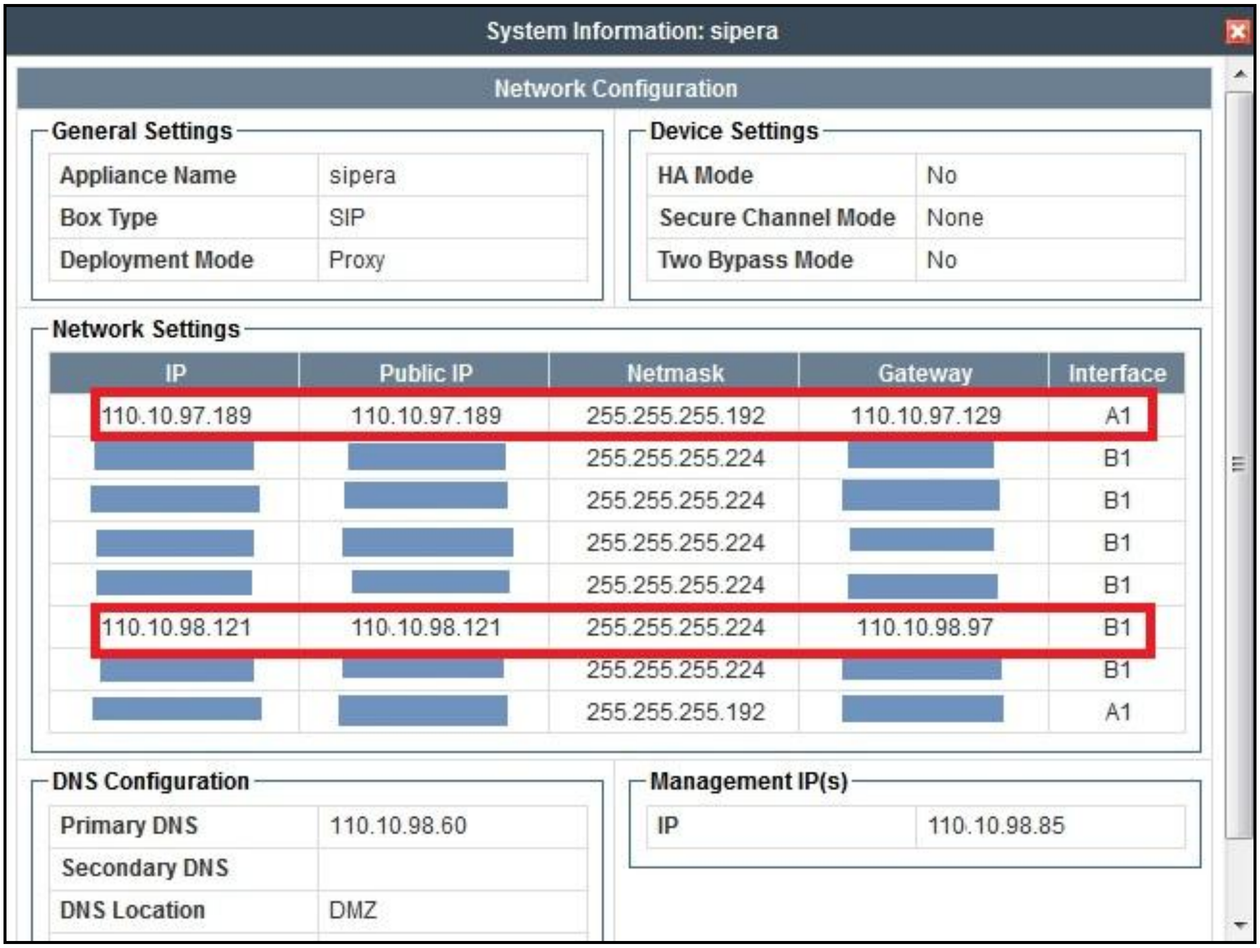
To view system information that has been configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane.

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.



Device Name	Serial Number	Version	Status
sipera	IPCS31020134	4.0.5.Q09	● Commissioned

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



General Settings

Appliance Name	sipera
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
110.10.97.189	110.10.97.189	255.255.255.192	110.10.97.129	A1
[redacted]	[redacted]	255.255.255.224	[redacted]	B1
[redacted]	[redacted]	255.255.255.224	[redacted]	B1
[redacted]	[redacted]	255.255.255.224	[redacted]	B1
[redacted]	[redacted]	255.255.255.224	[redacted]	B1
110.10.98.121	110.10.98.121	255.255.255.224	110.10.98.97	B1
[redacted]	[redacted]	255.255.255.224	[redacted]	B1
[redacted]	[redacted]	255.255.255.192	[redacted]	A1

DNS Configuration

Primary DNS	110.10.98.60
Secondary DNS	
DNS Location	DMZ

Management IP(s)

IP	110.10.98.85

7.2. Global Profiles

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

7.2.1. 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).

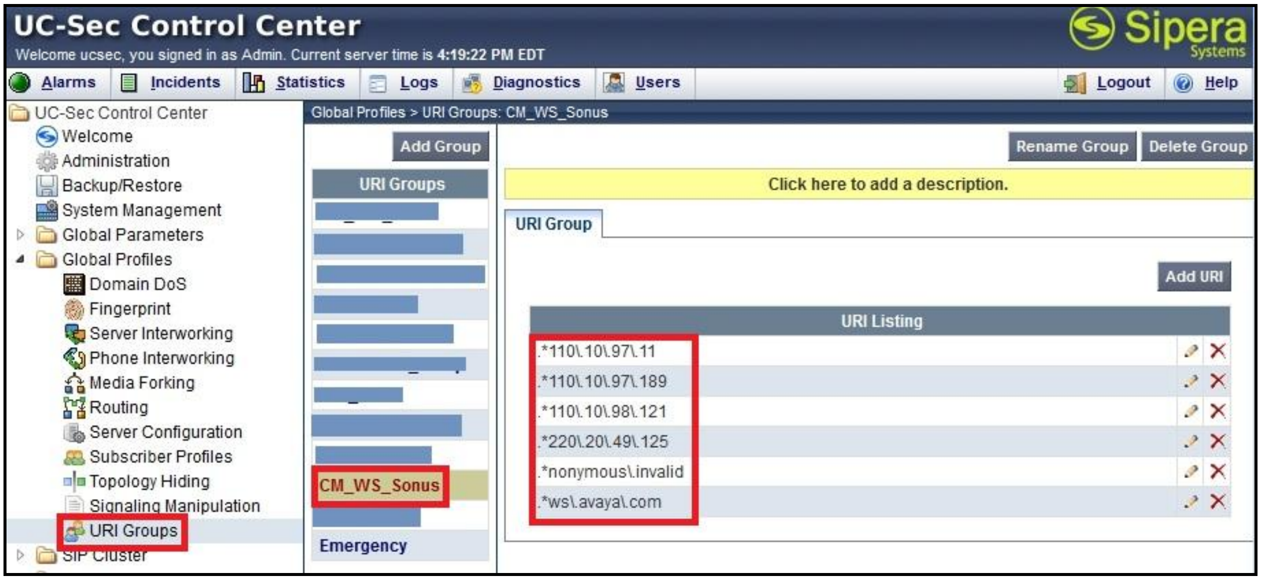
In the compliance testing, a URI Group named **CM_WS_Sonus** was added with URI type Regular Expression (not shown) and consists of:

- ".*ws\.avaya\.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 5.6**) and Session Manager (see **Section 6.2**).
- ".*nonymous\.invalid": enterprise domain, defined to support private call.

- ".*110\.10\.98\.121", ".*220\.20\.49\.125": IP address based URI-Host, used for public calls to/from the service provider. The Avaya SBCE public IP address "110.10.98.121" is set as URI-Host of the "From", "PAI" and "Diversion" headers while the public IP address of Windstream "220.20.49.125" is set as URI-Host of "Request-URI" and "To" headers.
- ".*110\.10\.97\.11", ".*110\.10\.97\.189": IP address based URI-Host, defined to support routing for the outbound OPTIONS heartbeat originated by Session Manager on the Entity Link to the Avaya SBCE (see **Section 6.5**). The OPTIONS will be forwarded by the Avaya SBCE to the service provider for response to confirm the status of the SIP trunk.

This URI-Group is used to match the "From" and "To" headers in a SIP call dialog received from both Session 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 7.2.2** and **Section 7.4.4**.

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



.*110\.10\.97\.11
.*110\.10\.97\.189
.*110\.10\.98\.121
.*220\.20\.49\.125
.*nonymous\.invalid
.*ws\.avaya\.com

7.2.2. 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.

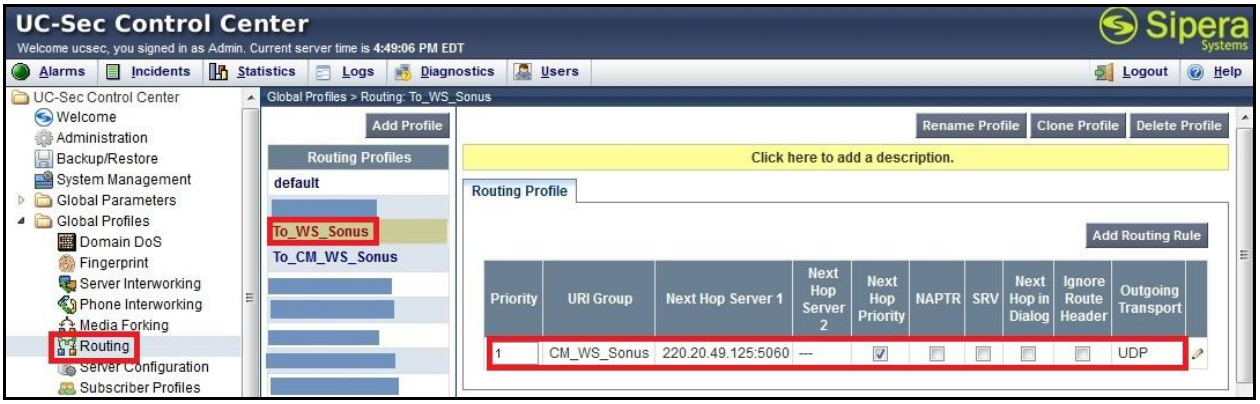
To create a Routing Profile, select **UC-Sec Control Center → Global Profiles → Routing**. Click on **Add Profile** (not shown).

In the compliance testing, a Routing Profile named **To_WS_Sonus** was created to use in conjunction with the server flow defined for Session 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_Sonus** 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.

7.2.2.1 Routing Profile for Windstream

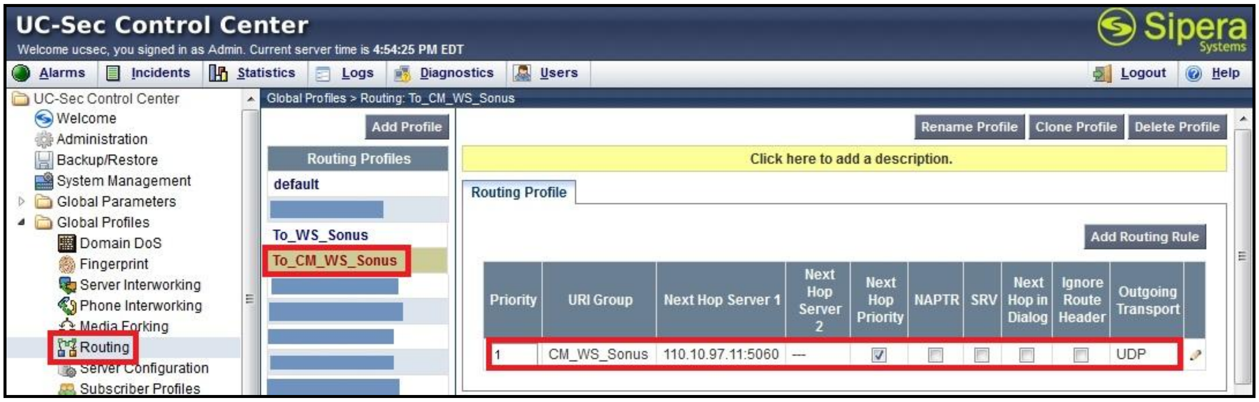
The screenshot below illustrates the **UC-Sec Control Center → Global Profiles → Routing**: **To_WS_Sonus**. As shown in **Figure 1**, Windstream SIP trunk is connected with transportation protocol UDP. If there is a match in the "To" header with the URI Group **CM_WS_Sonus** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of Windstream SIP trunk on port 5060.



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_WS_Sonus	220.20.49.125:5060	---	☑	☐	☐	☐	☐	UDP

7.2.2.2 Routing Profile for Session Manager

The Routing Profile **To_CM_WS_Sonus** was defined to route call where the "To" header matches the URI Group **CM_WS_Sonus** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, SIP trunk between Session Manager and the Avaya SBCE is connected with transportation protocol UDP.



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_WS_Sonus	110.10.97.11:5060	---	☑	☐	☐	☐	☐	UDP

7.2.3. 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_Sonus** and **To_CM_WS_Sonus** were created.

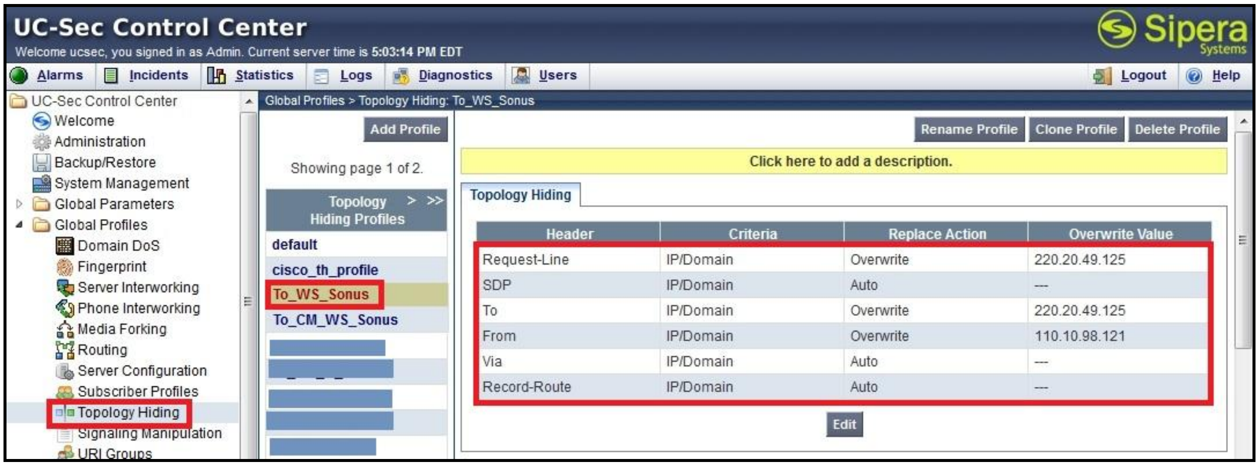
7.2.3.1 Topology Hiding Profile for Windstream

Profile **To_WS_Sonus** was defined to mask the enterprise SIP domain “ws.avaya.com” in “Request-URI” and “To” headers to IP “220.20.49.125” (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 “ws.avaya.com” in the “From” and “PAI” headers to IP “110.10.98.121” (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_Sonus**.



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	220.20.49.125
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	220.20.49.125
From	IP/Domain	Overwrite	110.10.98.121
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

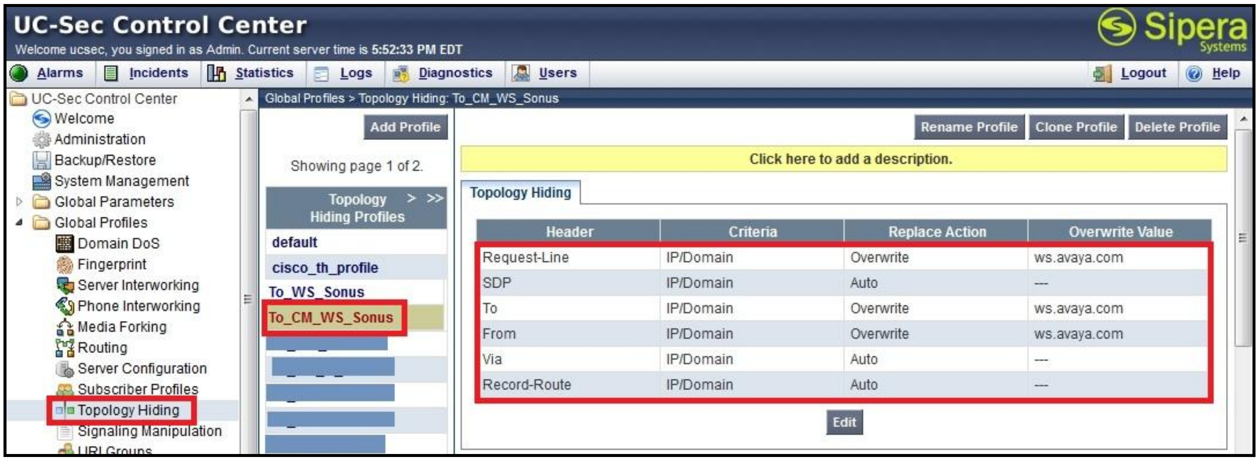
7.2.3.2 Topology Hiding Profile for Communication Manager

Profile **To_CM_WS_Sonus** was also created to mask Windstream URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain “ws.avaya.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_Sonus**.



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

7.2.4. 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.

7.2.4.1 Server Interworking profile for Windstream

Profile **WS_Sonus** 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:

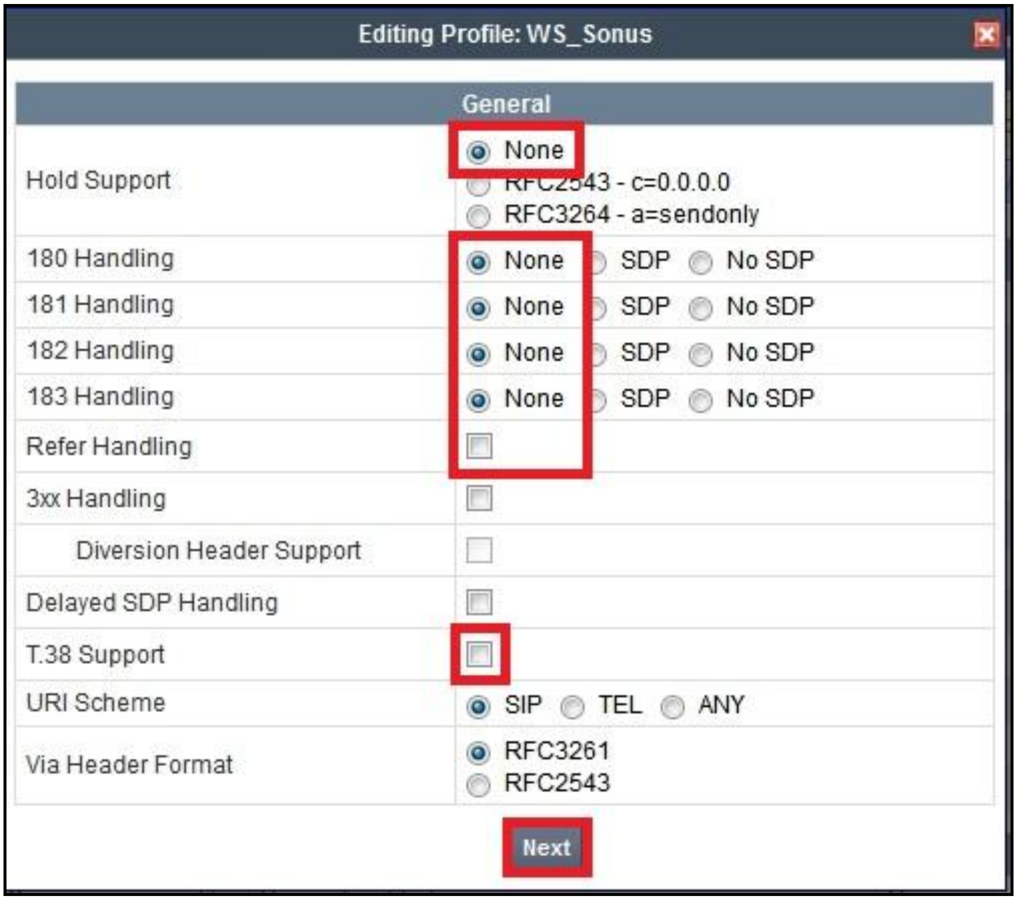
- Hold Support = None. The Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to Windstream.

- 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.

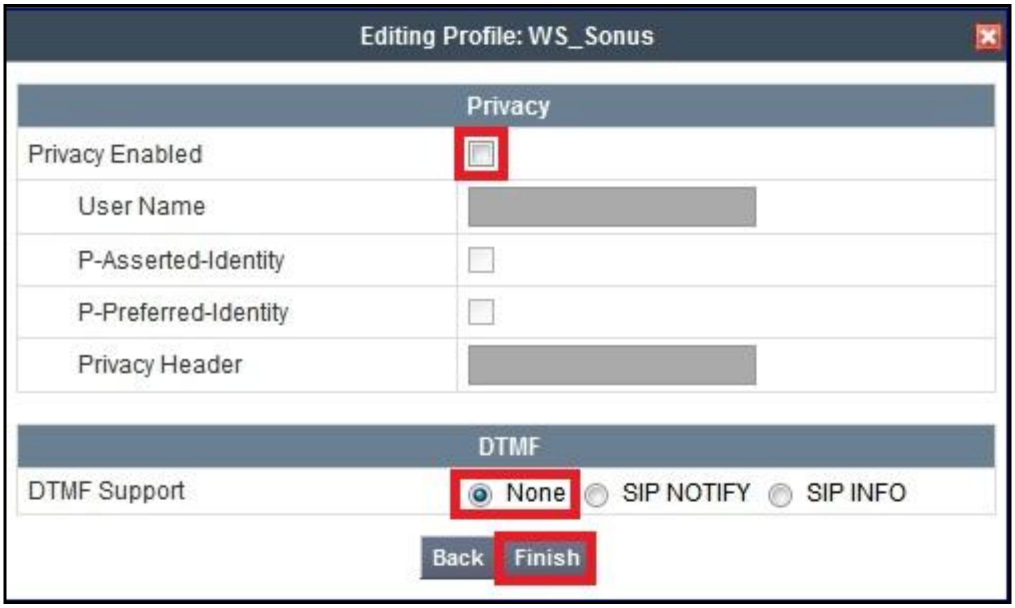
The screenshots below illustrate the Server Interworking profile **WS_Sonus**.



Editing Profile: WS_Sonus

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
T.38 Support	☐
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



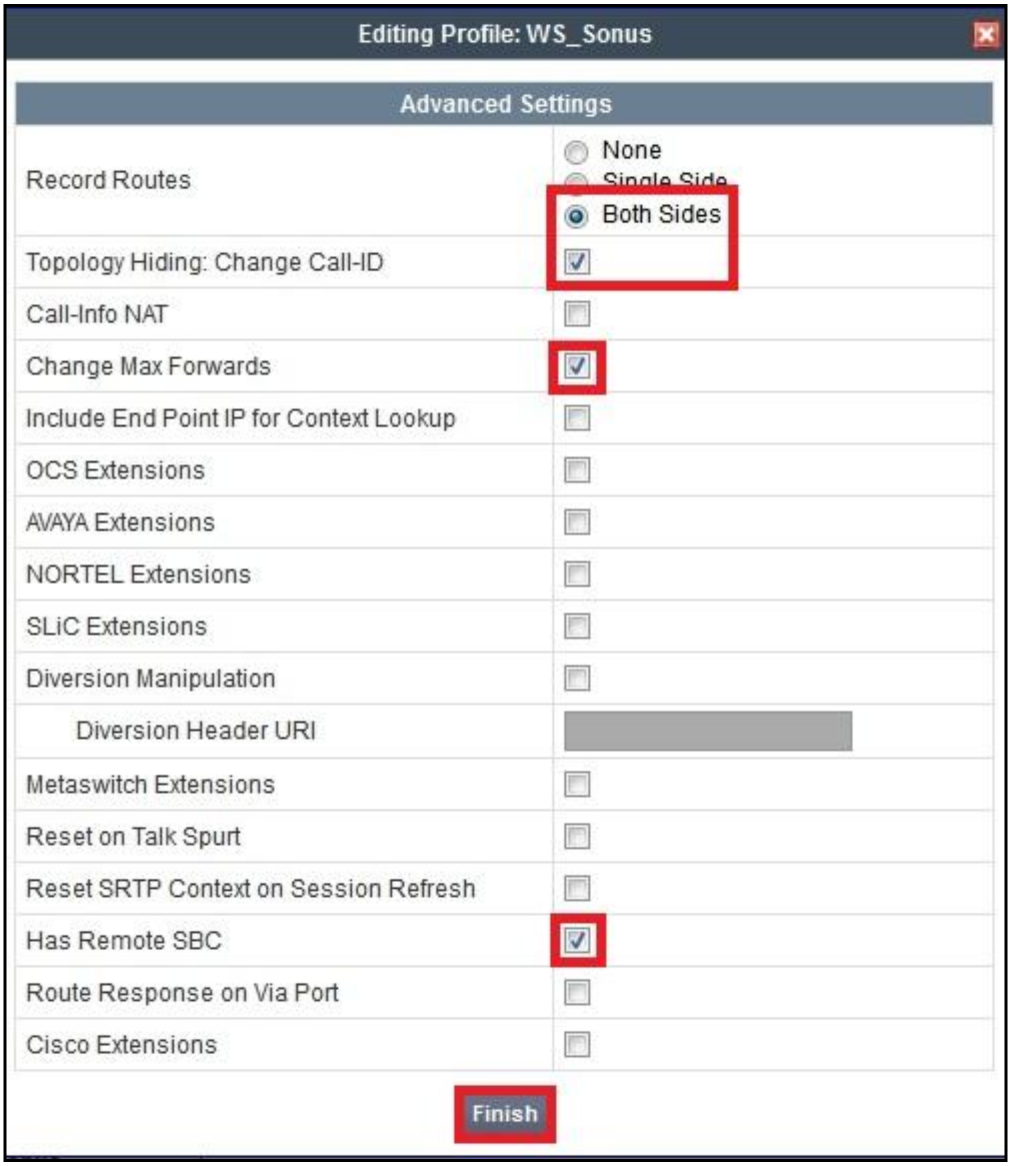
Editing Profile: WS_Sonus

Privacy

Privacy Enabled	☐
User Name	
P-Asserted-Identity	☐
P-Preferred-Identity	☐
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO



Editing Profile: WS_Sonus

Advanced Settings

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	☐
Change Max Forwards	☑
Include End Point IP for Context Lookup	☐
OCS Extensions	☐
AVAYA Extensions	☐
NORTEL Extensions	☐
SLiC Extensions	☐
Diversion Manipulation	☐
Diversion Header URI	
Metaswitch Extensions	☐
Reset on Talk Spurt	☐
Reset SRTP Context on Session Refresh	☐
Has Remote SBC	☑
Route Response on Via Port	☐
Cisco Extensions	☐

7.2.4.2 Server Interworking profile for Session Manager

Profile **CM_WS_Sonus** 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:

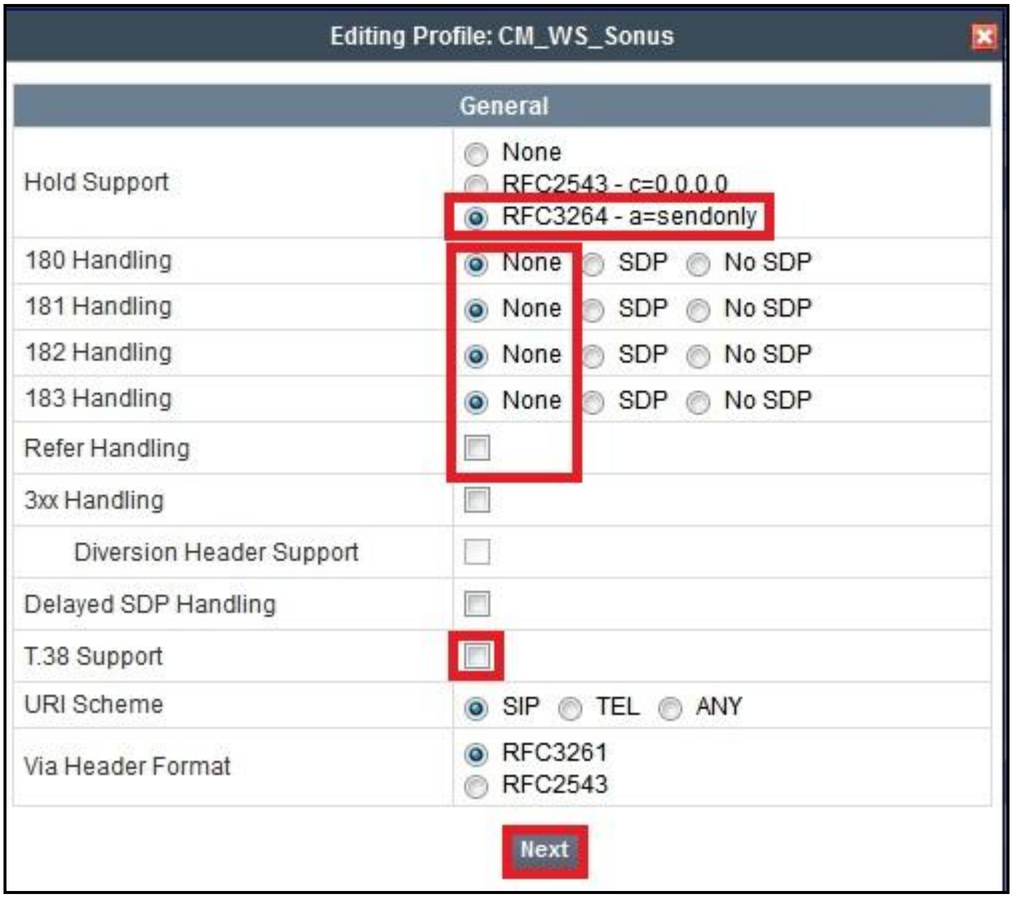
- Hold Support = RFC3264. Communication Manager supports hold/ resume as per RFC3264.
- 18X Handling = None. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from Windstream to Communication Manager.
- Refer Handling = Unchecked. The Avaya SBCE will not handle REFER, it will 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.

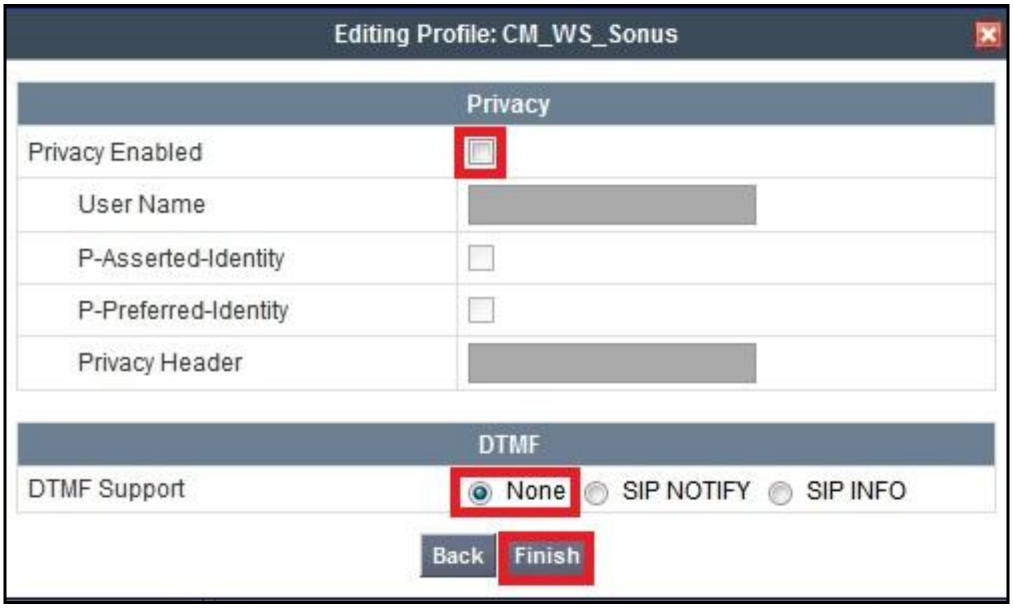
The screenshots below illustrate the Server Interworking profile **CM_WS_Sonus**.



Editing Profile: CM_WS_Sonus

General

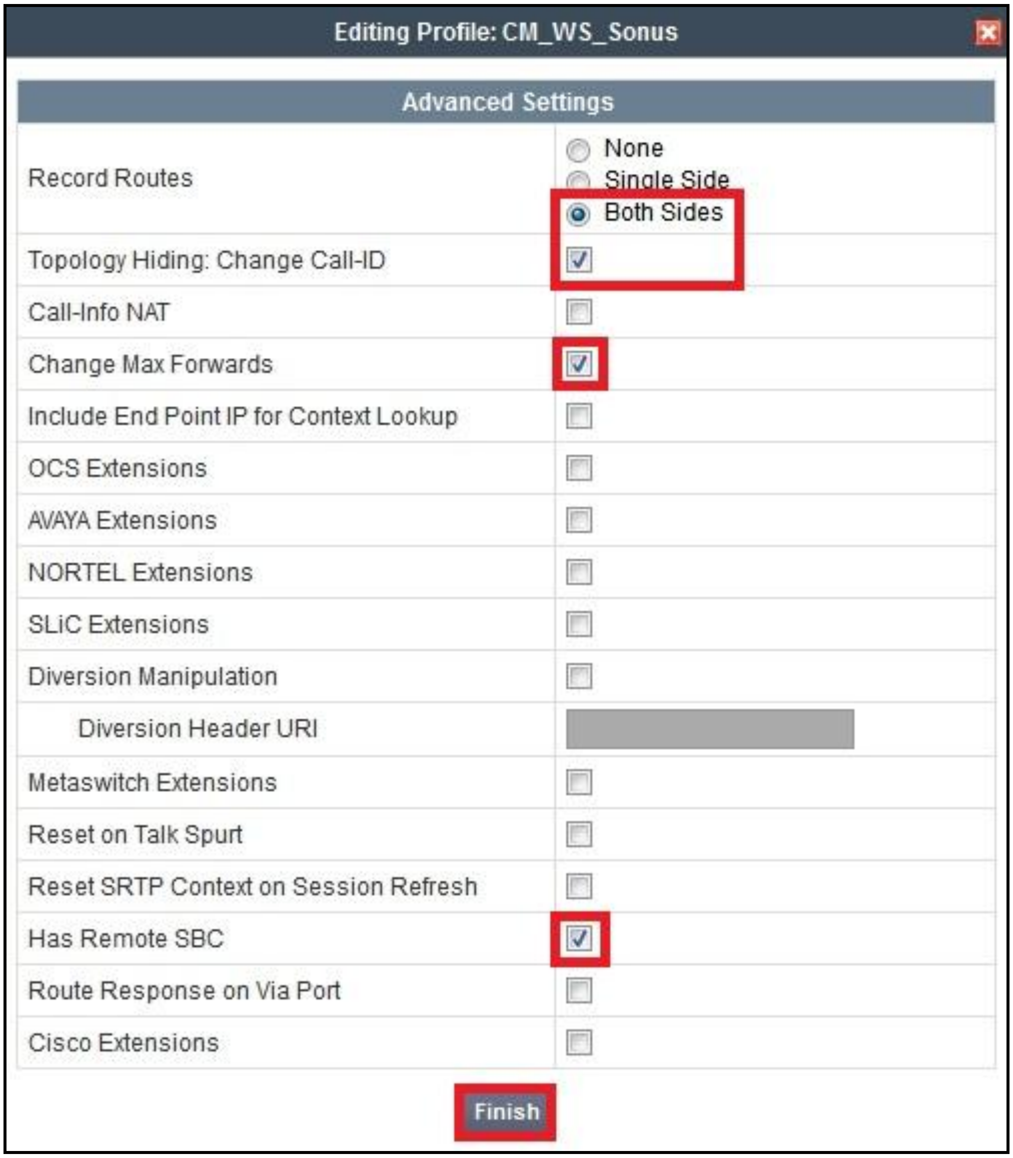
Hold Support	○ None ○ RFC2543 - c=0.0.0.0 ● RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
T.38 Support	☐
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



Editing Profile: CM_WS_Sonus

Privacy	
Privacy Enabled	☐
User Name	
P-Asserted-Identity	☐
P-Preferred-Identity	☐
Privacy Header	

DTMF	
DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO



Editing Profile: CM_WS_Sonus

Advanced Settings	
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	☐
Change Max Forwards	☑
Include End Point IP for Context Lookup	☐
OCS Extensions	☐
AVAYA Extensions	☐
NORTEL Extensions	☐
SLiC Extensions	☐
Diversion Manipulation	☐
Diversion Header URI	
Metaswitch Extensions	☐
Reset on Talk Spurt	☐
Reset SRTP Context on Session Refresh	☐
Has Remote SBC	☑
Route Response on Via Port	☐
Cisco Extensions	☐

7.2.5. 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_Sonus** 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= "110.10.98.121";
}
}
```

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.

The Topology-Hiding profile **To_WS_Sonus** 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 "ws.avaya.com". Thus, a SigMa rule is used to correct the URI-Host of "P-Asserted-Identity" header.

7.2.6. Server Configuration

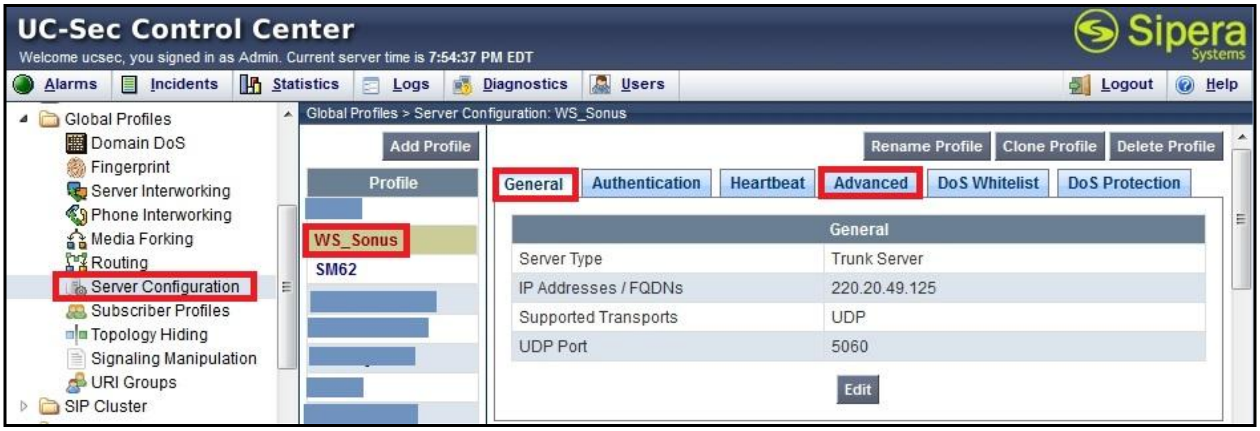
Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted 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_Sonus** for Windstream and server entry **SM62** for Session Manager.

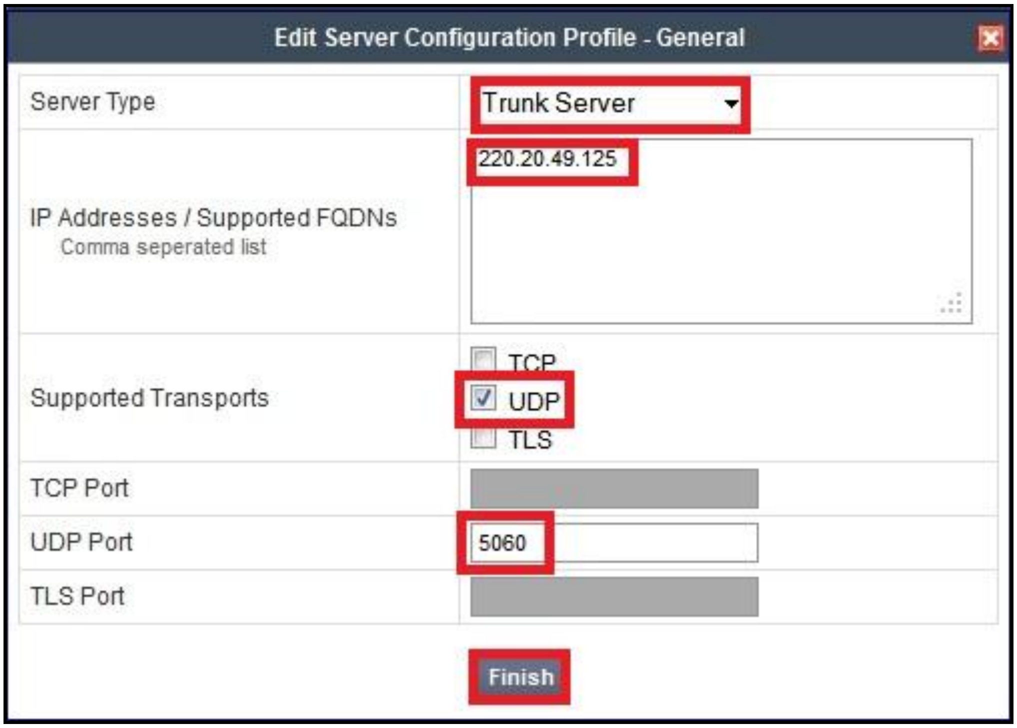
7.2.6.1 Server Configuration for Windstream

Server Configuration named **WS_Sonus** was created for Windstream, it will be discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as Windstream does not implement authentication on the SIP trunk. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Session Manager to Windstream to query the status of 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.



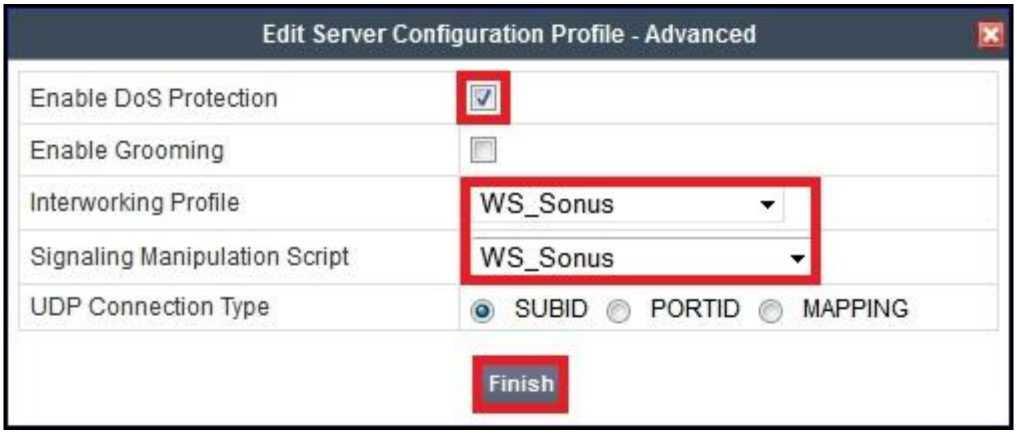
General	
Server Type	Trunk Server
IP Addresses / FQDNs	220.20.49.125
Supported Transports	UDP
UDP Port	5060

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



Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	220.20.49.125
Supported Transports	☐ TCP ☑ UDP ☐ TLS
TCP Port	
UDP Port	5060
TLS Port	

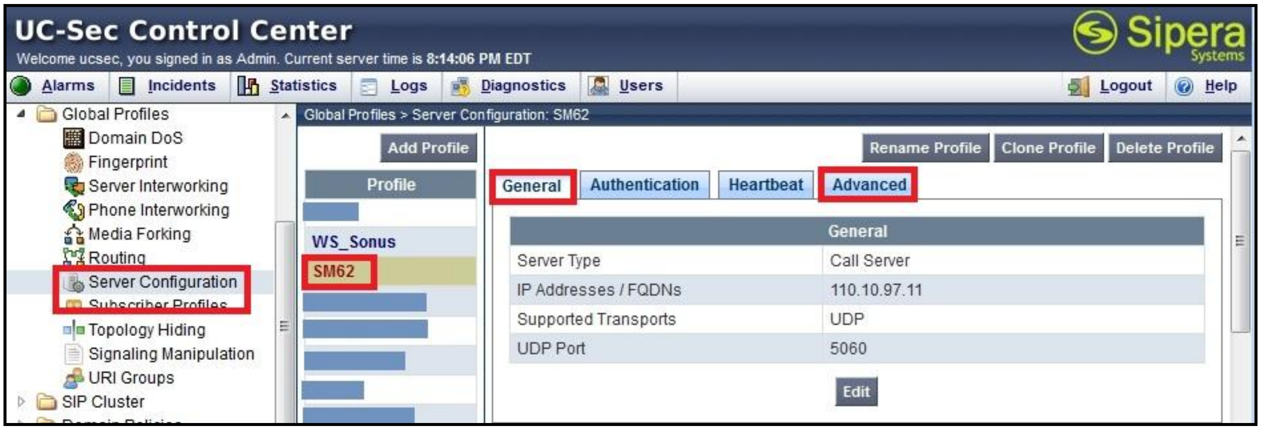
Under **Advanced** tab, check on **Enable DoS Protection**. For **Interworking Profile** drop down list, select **WS_Sonus** as defined in **Section 7.2.4** and for **Signaling Manipulation Script** drop down list select **WS_Sonus** as defined in **Section 7.2.5**. These configurations apply the specific SIP profile and SigMa rules to the Windstream traffic. The other settings are kept as default.


Edit Server Configuration Profile - Advanced

Enable DoS Protection	☑
Enable Grooming	☐
Interworking Profile	WS_Sonus
Signaling Manipulation Script	WS_Sonus
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

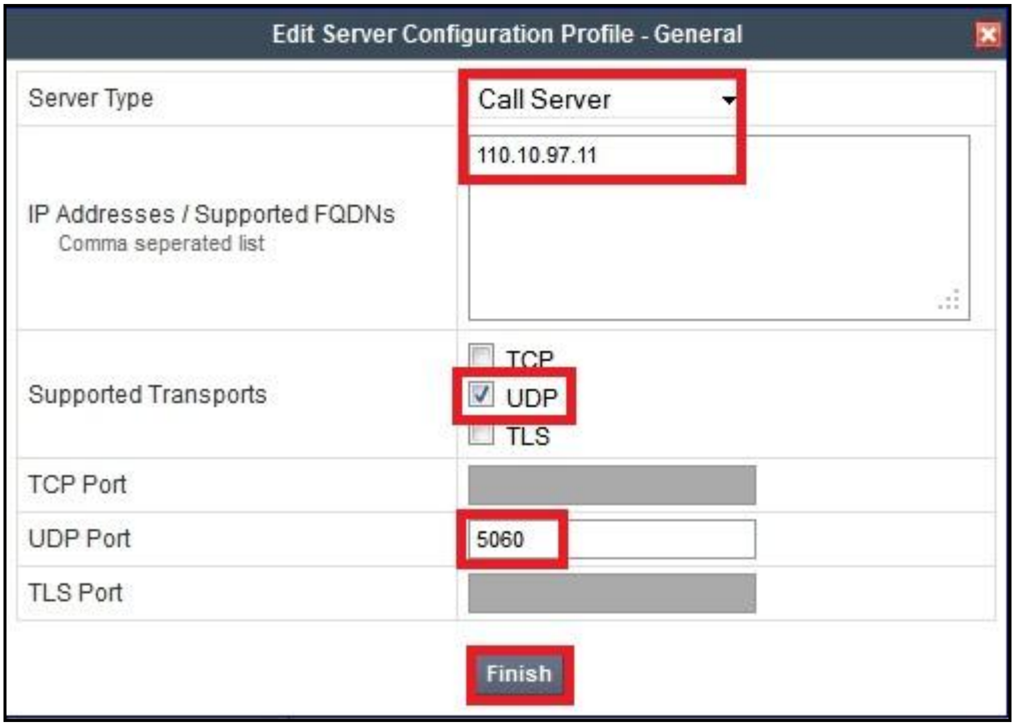
7.2.6.2 Server Configuration for Session Manager

Server Configuration named **SM62** was created for Session 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 Session Manager to query the status of the SIP trunk.



General	
Server Type	Call Server
IP Addresses / FQDNs	110.10.97.11
Supported Transports	UDP
UDP Port	5060

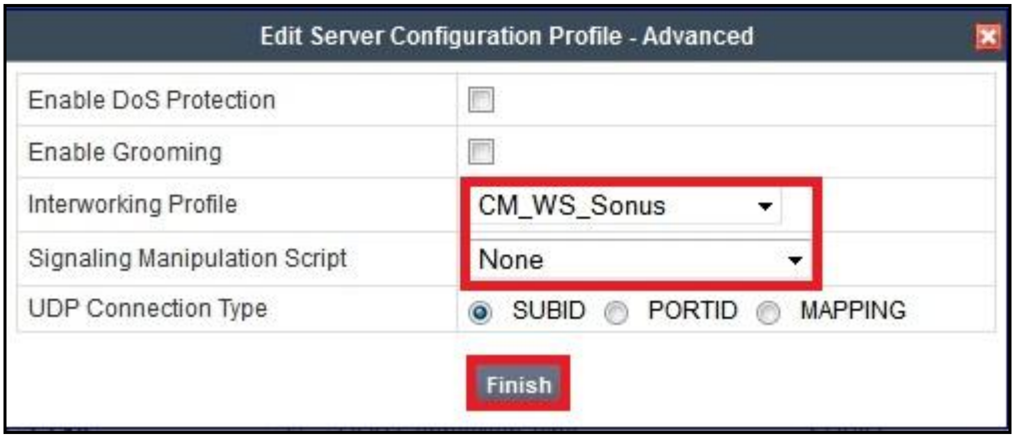
In the **General** tab, specify **Server Type** for Session Manager as **Call Server**. In the compliance testing, the link between the Avaya SBCE and Session Manager was UDP and Session Manager listens on port 5060.



Edit Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	110.10.97.11
Supported Transports	☐ TCP ☑ UDP ☐ TLS
TCP Port	
UDP Port	5060
TLS Port	

Under **Advanced** tab, for **Interworking Profile** drop down list select **CM_WS_Sonus** as defined in **Section 7.2.4** 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	☐
Enable Grooming	☐
Interworking Profile	CM_WS_Sonus
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.3. 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.

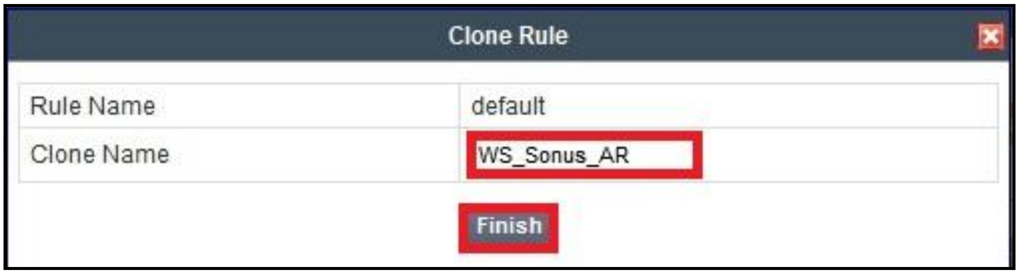
7.3.1. Application Rules

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

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

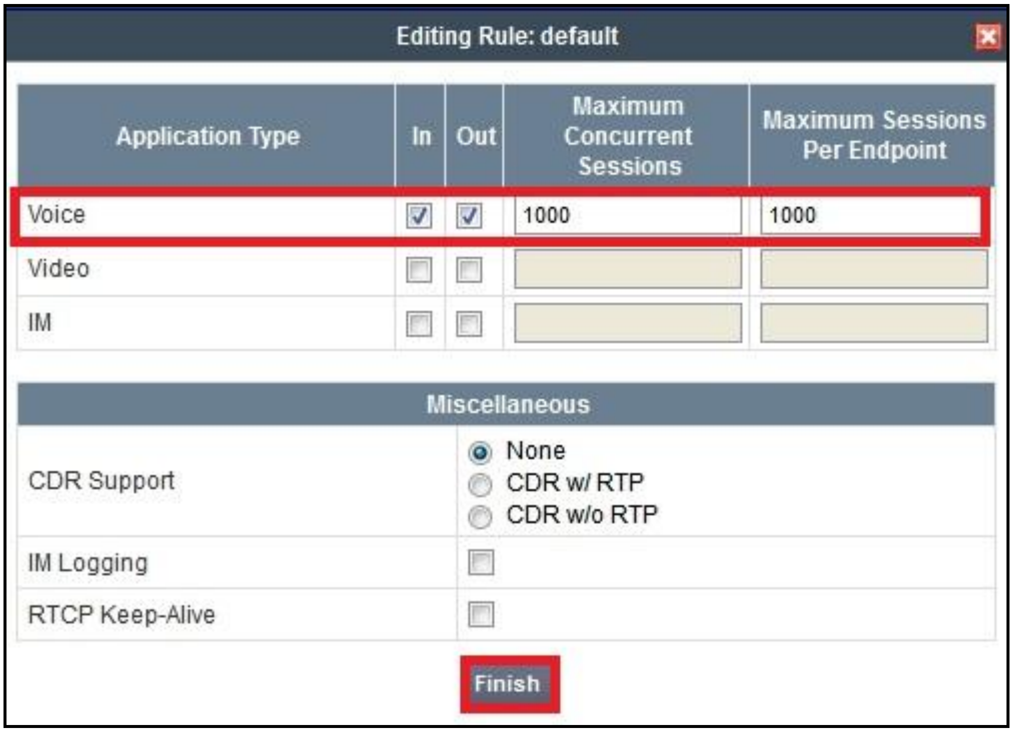
To clone an Application Rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the default rule chosen, click on **Clone Rule** (not shown).

Enter a rule with a descriptive name **WS_Sonus _AR** and click **Finish**.



Rule Name	default
Clone Name	WS_Sonus_AR

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_Sonus_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	☑	☑	1000	1000
Video	☐	☐		
IM	☐	☐		

Miscellaneous

CDR Support	● None ○ CDR w/ RTP ○ CDR w/o RTP
IM Logging	☐
RTCP Keep-Alive	☐

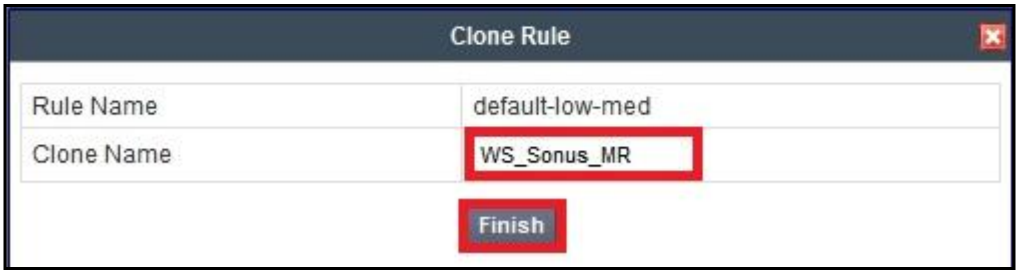
7.3.2. Media Rules

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_Sonus_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_Sonus_MR** and click **Finish**.



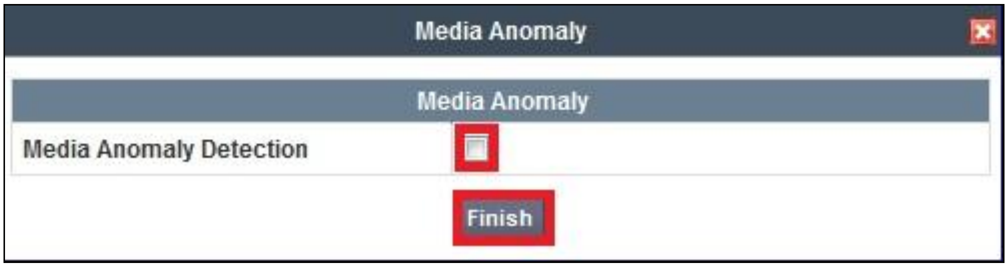
Clone Rule

Rule Name	default-low-med
Clone Name	WS_Sonus_MR

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**.

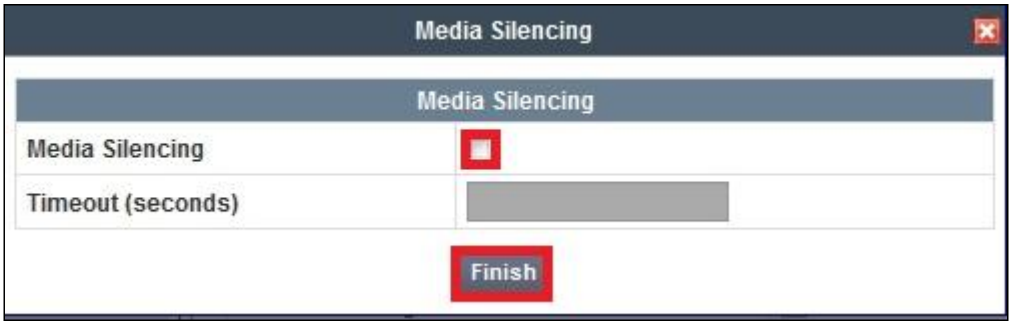


Media Anomaly

Media Anomaly	
Media Anomaly Detection	☐

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 being disconnected due to a RTP packet lost on public Internet.

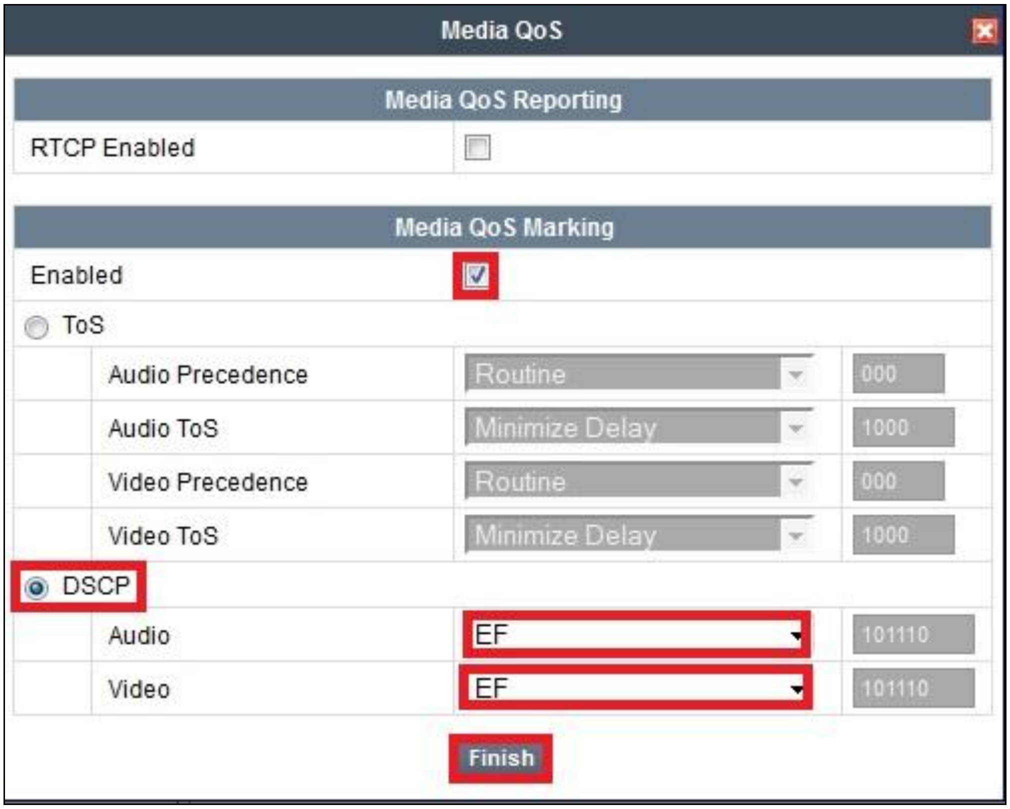
To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.



Media Silencing

Media Silencing	
Media Silencing	☐
Timeout (seconds)	

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.



RTCP Enabled	☐	
Enabled	☑	
○ ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
● DSCP		
Audio	EF	101110
Video	EF	101110

7.3.3. Signaling Rules

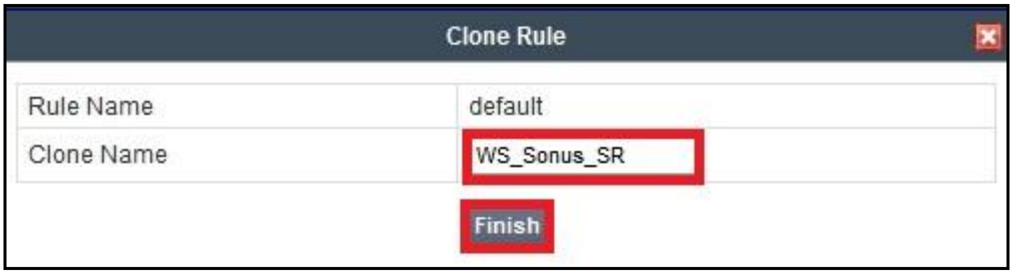
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined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

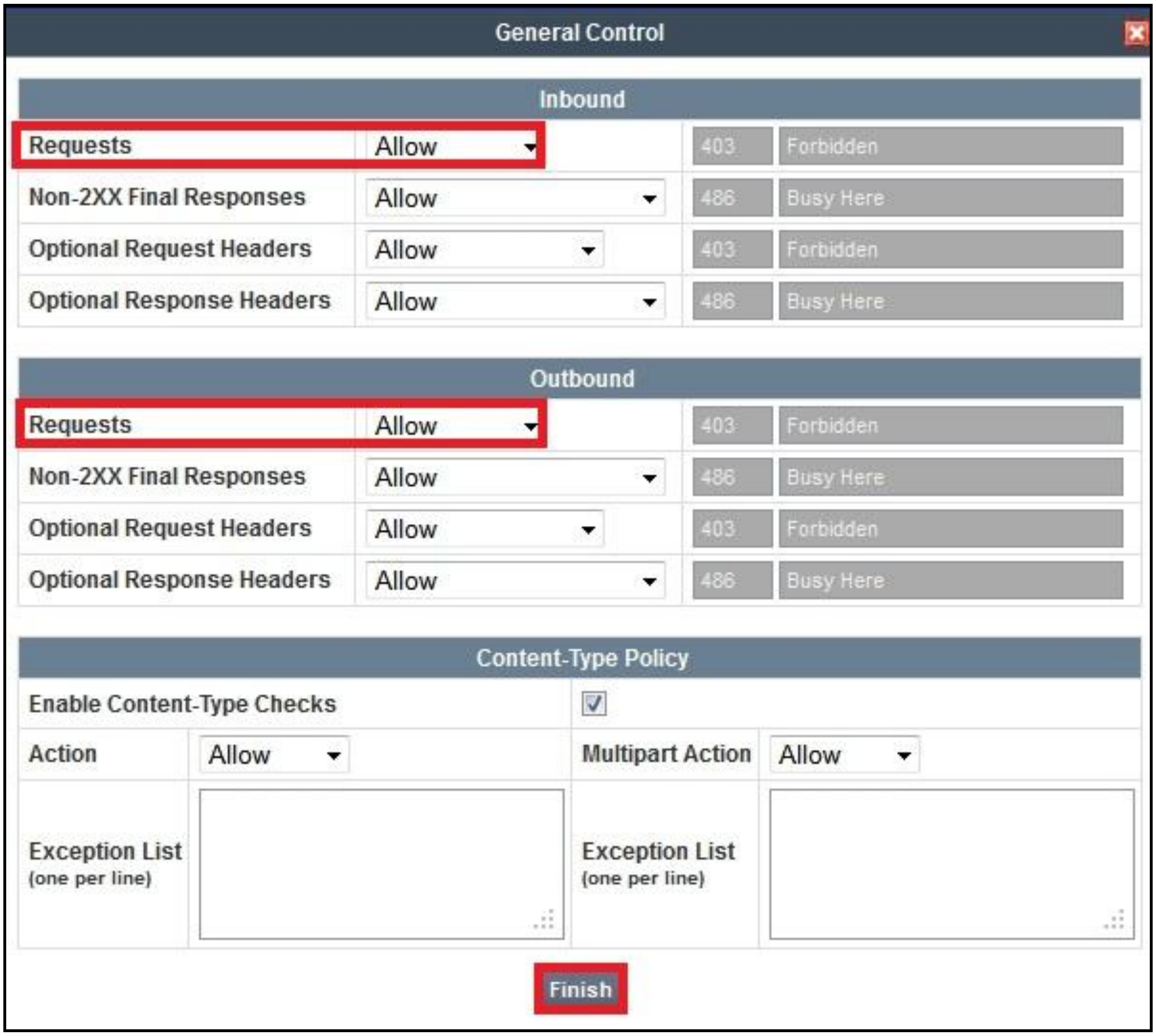
7.3.3.1 Signaling Rule for Windstream

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



Rule Name	default
Clone Name	WS_Sonus_SR

The **WS_Sonus_SR** was configured to allow Windstream to accept inbound and outbound call requests. Being cloned from the Signaling Rule **default**, the **WS_Sonus_SR** will block all requests with 403 Forbidden. To start accepting calls, go to **General** tab, click on **Edit**. Then change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.

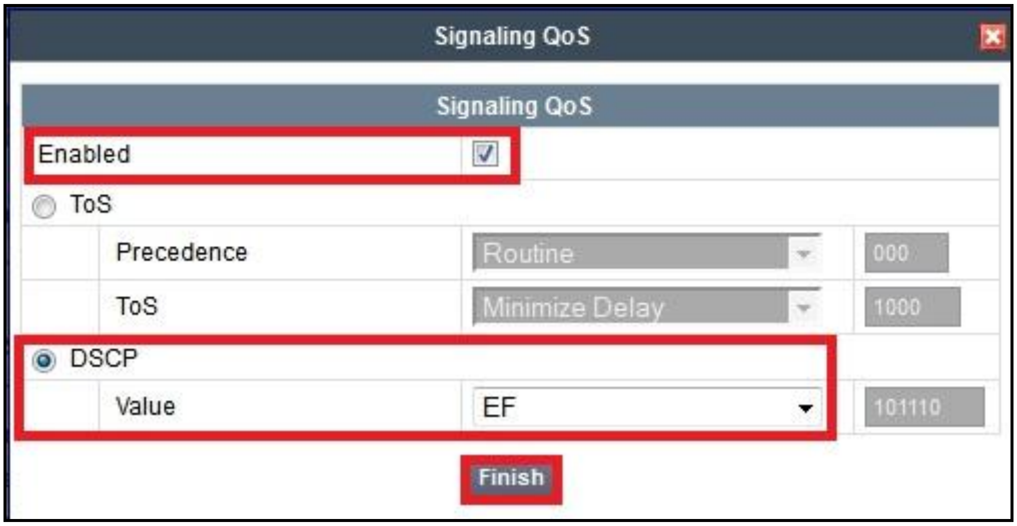


Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

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)	

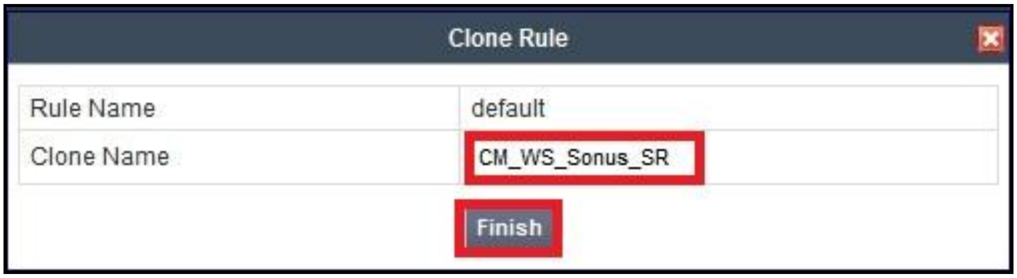
On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for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



Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	EF	101110

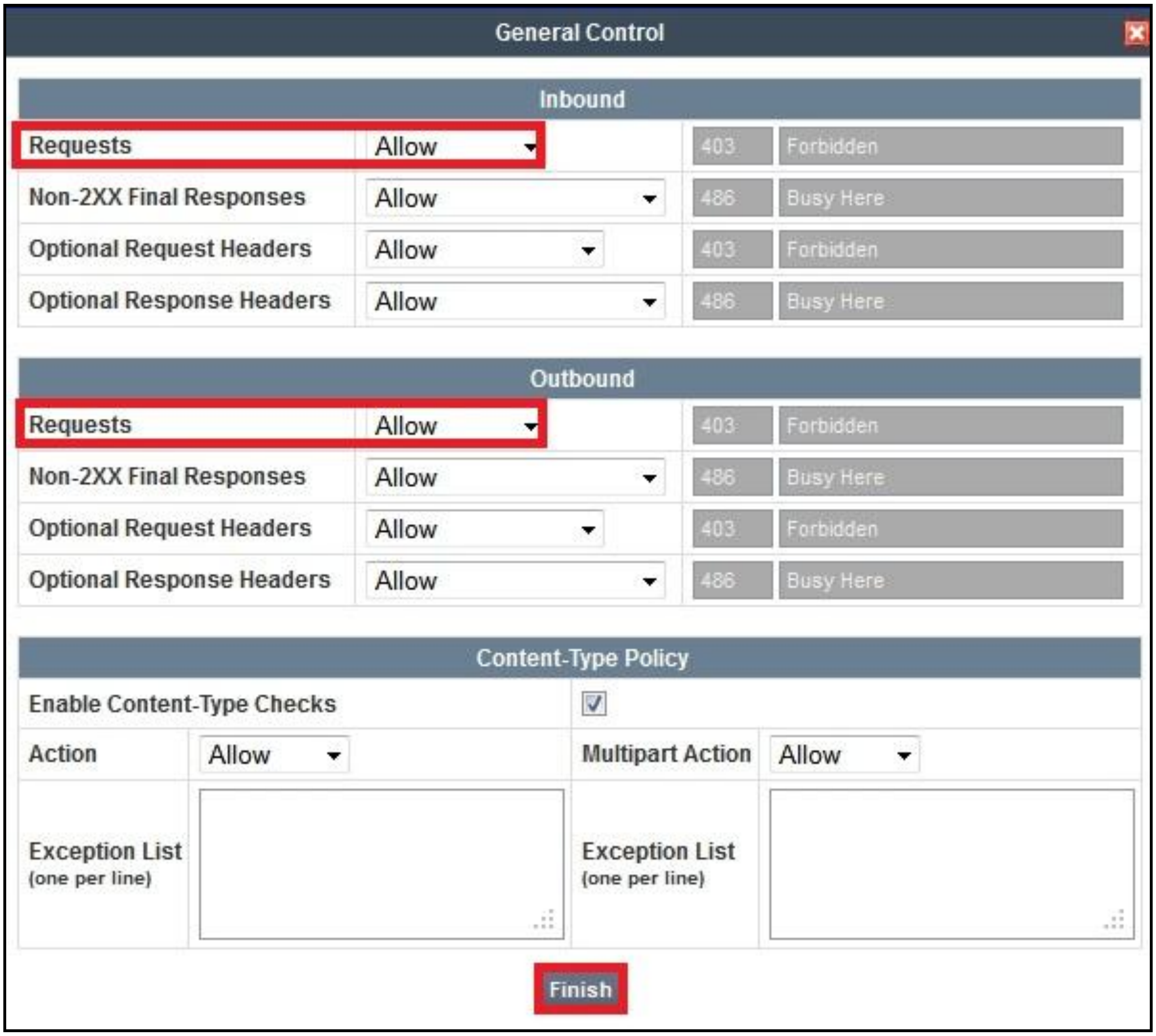
7.3.3.2 Signaling Rule for Session Manager

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



Rule Name	default
Clone Name	CM_WS_Sonus_SR

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



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

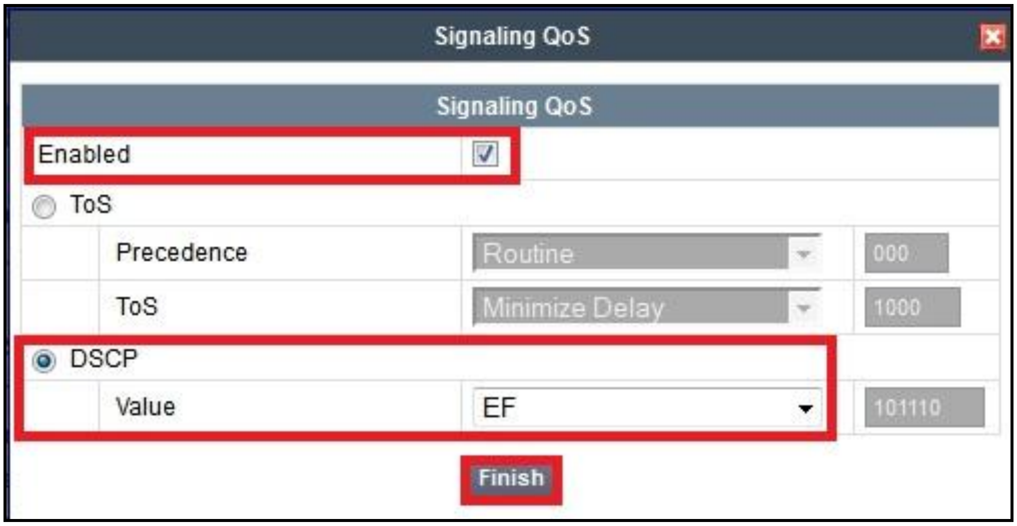
Outbound

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)	

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.



Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	EF	101110

7.3.4. 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**.**

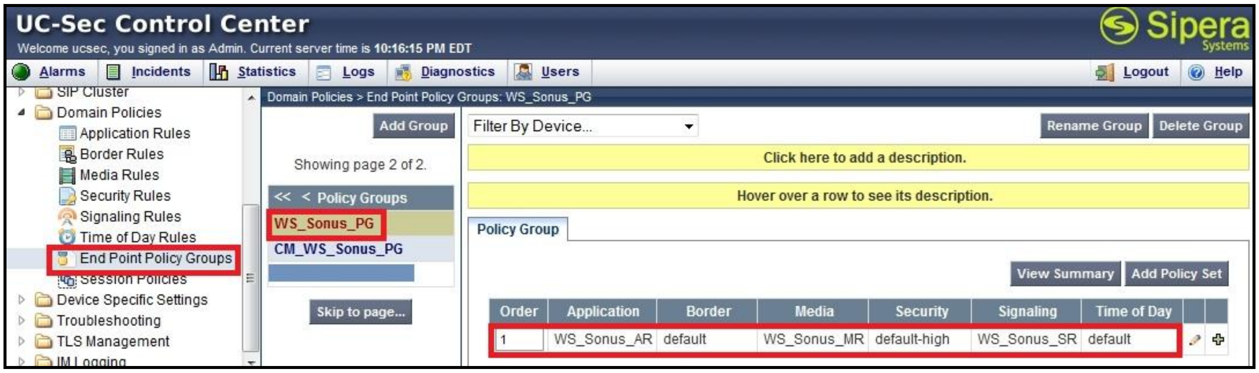
Endpoint Policy Groups were created for the Session Manager and the Windstream.

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

7.3.4.1 Endpoint Policy Group for Windstream

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

- Set Application Rule to **WS_Sonus_AR** as created in **Section 7.3.1**.
- Set Media Rule to **WS_Sonus_MR** as created **Section 7.3.2**.
- Set Signaling Rule to **WS_Sonus_SR** as created in **Section 7.3.3.1**.
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-high**.



Welcome ucsec, you signed in as Admin. Current server time is 10:16:15 PM EDT

Domain Policies > End Point Policy Groups: WS_Sonus_PG

Showing page 2 of 2.

Click here to add a description.

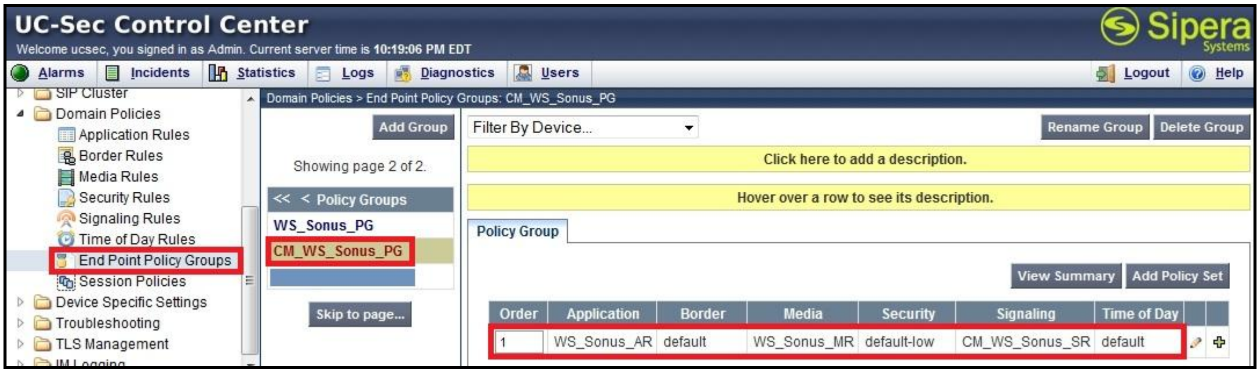
Hover over a row to see its description.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	WS_Sonus_AR	default	WS_Sonus_MR	default-high	WS_Sonus_SR	default

7.3.4.2 Endpoint Policy Group for Session Manager

The following screen shows **CM_WS_Sonus_PG** created for Session Manager:

- Set Application Rule to **WS_Sonus_AR** as created in **Section 7.3.1**.
- Set Media Rule to **WS_Sonus_MR** as created **Section 7.3.2**.
- Set Signaling Rule to **CM_WS_Sonus_SR** as created in **Section 7.3.3.2**.
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-low**.



Order	Application	Border	Media	Security	Signaling	Time of Day
1	WS_Sonus_AR	default	WS_Sonus_MR	default-low	CM_WS_Sonus_SR	default

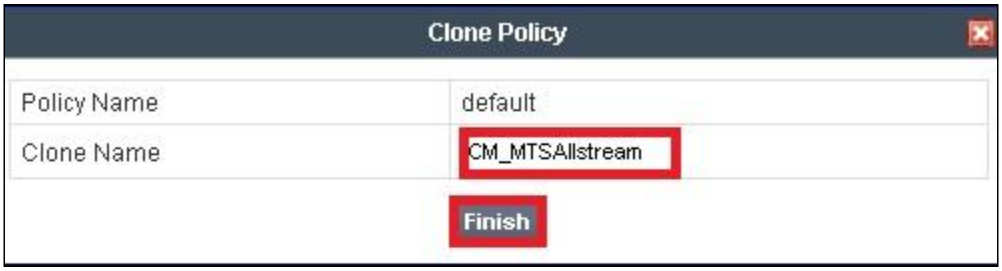
7.3.5. Session Policy

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 7.2.1**.

In the compliance testing, a Session Policy named **CM_WS_Sonus** 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 e→ Session Policies**. With the **default** rule chosen, click on **Clone Rule** (not shown).

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

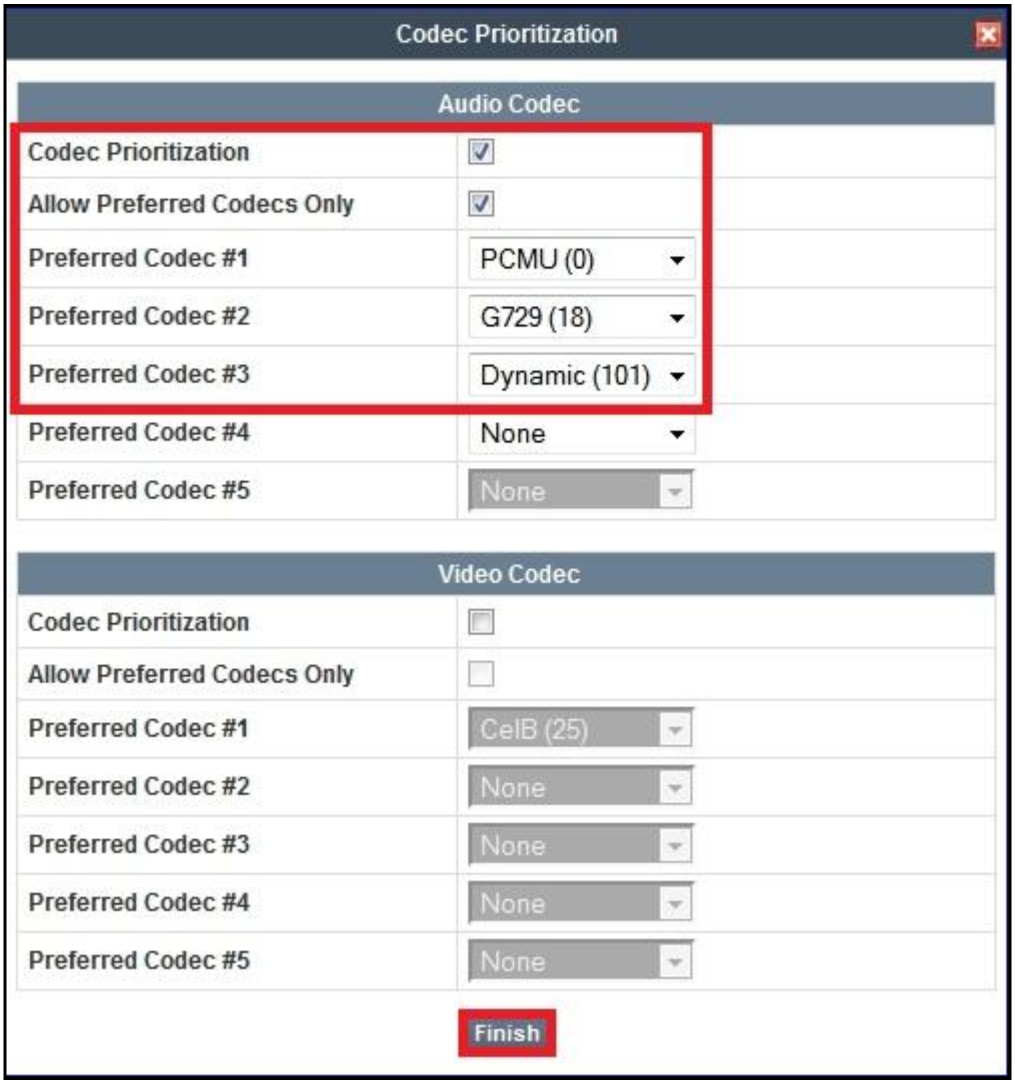


Policy Name	default
Clone Name	CM_MTSAllstream

Windstream supports voice codec G.729 and G.711MU in prioritized order with payload 101 for RFC2833/DTMF. To define **Codec Prioritization** for Audio Codec, select the profile

CM_WS_Sonus created above, click on **Edit** (not shown). Select **Preferred Codec #1** as G.711MU, **Preferred Codec #2** as G.729 and **Preferred Codec #3** as Dynamic (101) for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Note: T.38 fax is not yet supported by Windstream. This Session Policy prioritizes voice codec G.711MU to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both Communication Manager and Windstream cannot switch the voice call using different codec .e.g. G/729 to G.711MU for the fax call. Therefore, the Preferred Codec #1 has to be selected as G.711MU.



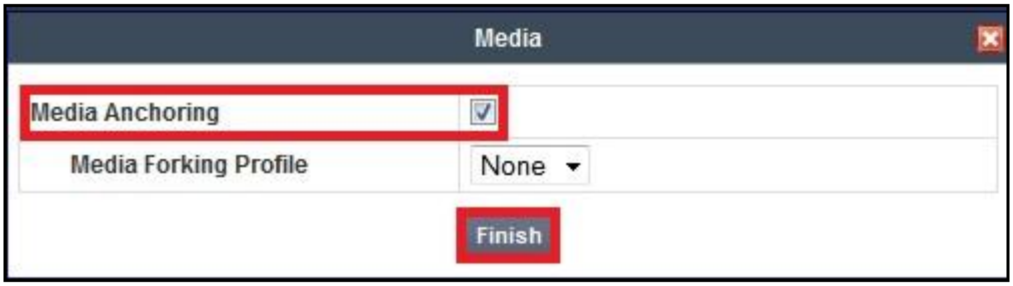
Audio Codec

Codec Prioritization	☑
Allow Preferred Codecs Only	☑
Preferred Codec #1	PCMU (0)
Preferred Codec #2	G729 (18)
Preferred Codec #3	Dynamic (101)
Preferred Codec #4	None
Preferred Codec #5	None

Video Codec

Codec Prioritization	☐
Allow Preferred Codecs Only	☐
Preferred Codec #1	CelB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None

To administer the **Media Anchoring** on the Avaya SBCE, select Session Policy **CM_WS_Sonus** created above then select tab **Media**, click **Edit** (not shown). Check to enable the **Media Anchoring**.



Media Anchoring ☑

Media Forking Profile None

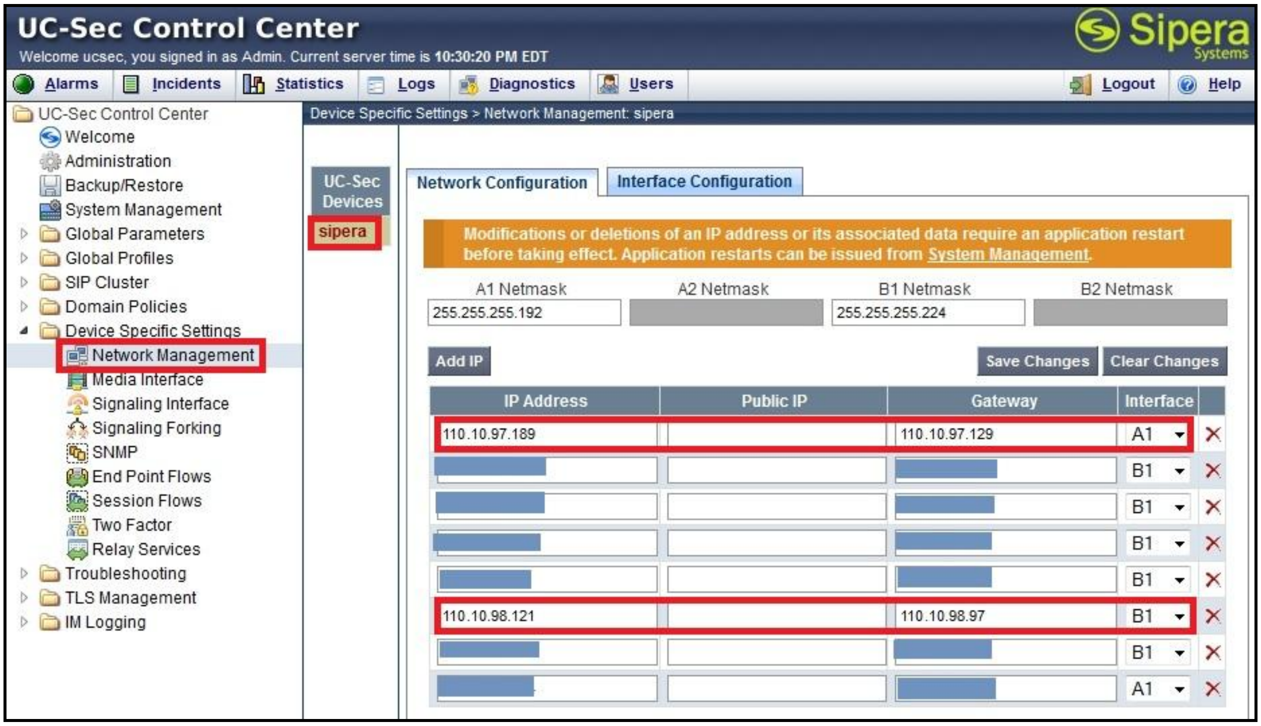
7.4. Device Specific Settings

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.

7.4.1. 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**.



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

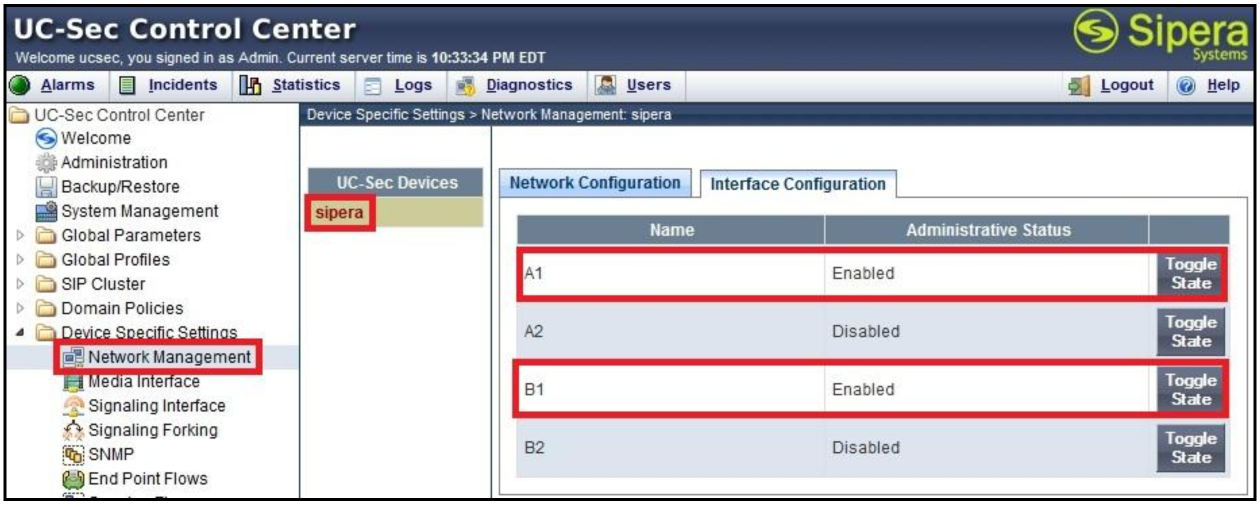
Device Specific Settings > Network Management: sipera

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	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface
110.10.97.189		110.10.97.129	A1
[redacted]		[redacted]	B1
[redacted]		[redacted]	B1
[redacted]		[redacted]	B1
[redacted]		[redacted]	B1
110.10.98.121		110.10.98.97	B1
[redacted]		[redacted]	B1
[redacted]		[redacted]	A1

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.



Welcome ucsec, you signed in as Admin. Current server time is 10:33:34 PM EDT

Device Specific Settings > Network Management: sipera

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

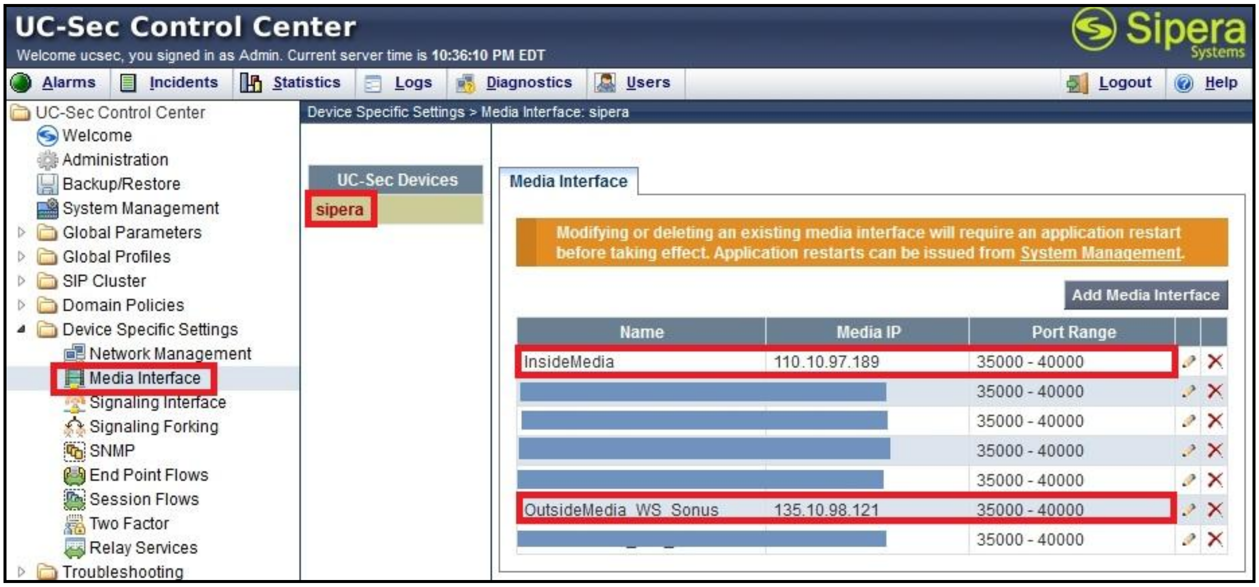
7.4.2. Media Interface

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.



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

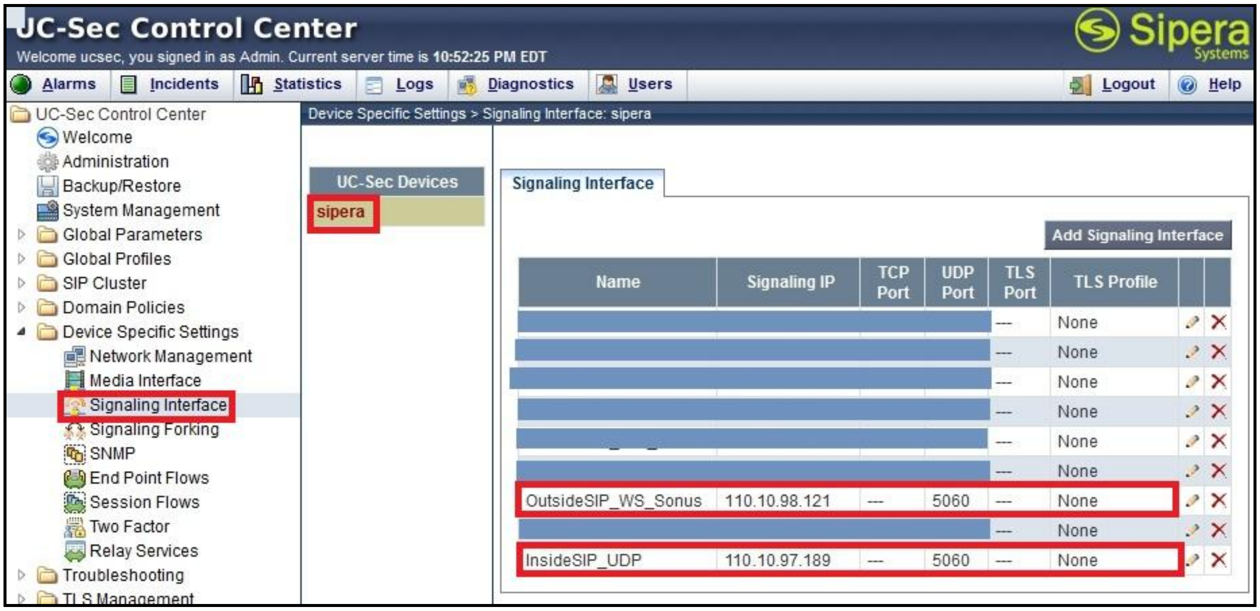
Name	Media IP	Port Range
InsideMedia	110.10.97.189	35000 - 40000
[redacted]	[redacted]	35000 - 40000
[redacted]	[redacted]	35000 - 40000
[redacted]	[redacted]	35000 - 40000
[redacted]	[redacted]	35000 - 40000
OutsideMedia_WS_Sonus	135.10.98.121	35000 - 40000
[redacted]	[redacted]	35000 - 40000

7.4.3. 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).

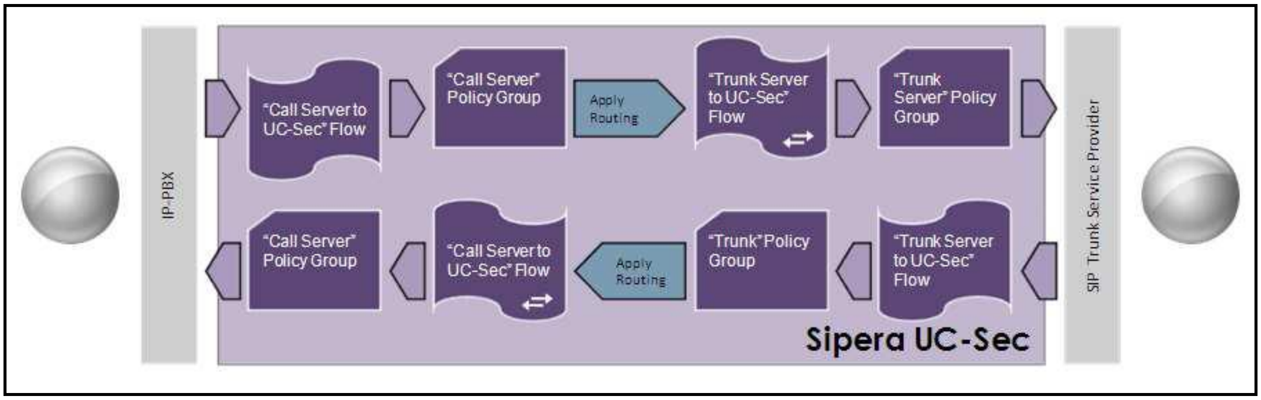
Separate Signaling Interfaces were created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
[redacted]	[redacted]	[redacted]	[redacted]	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
OutsideSIP_WS_Sonus	110.10.98.121	---	5060	---	None
[redacted]	[redacted]	[redacted]	[redacted]	---	None
InsideSIP_UDP	110.10.97.189	---	5060	---	None

7.4.4. 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.

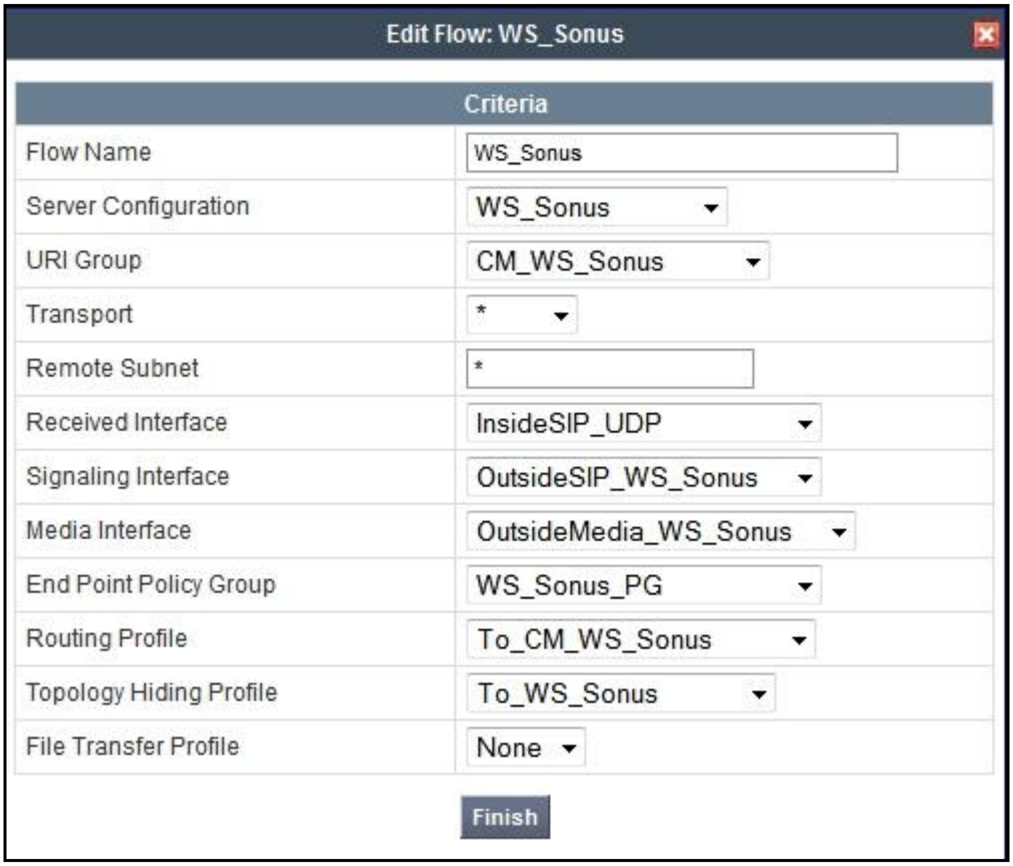

IP-PBX
"Call Server to UC-Sec" Flow
"Call Server" Policy Group
Apply Routing
"Trunk Server to UC-Sec" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to UC-Sec" Flow
Apply Routing
"Trunk" Policy Group
"Trunk Server to UC-Sec" Flow
Sipera UC-Sec
SIP Trunk Service Provider

In the compliance testing, separate Server Flows were created for Windstream and Session 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 7.2.6** to assign to the Flow.

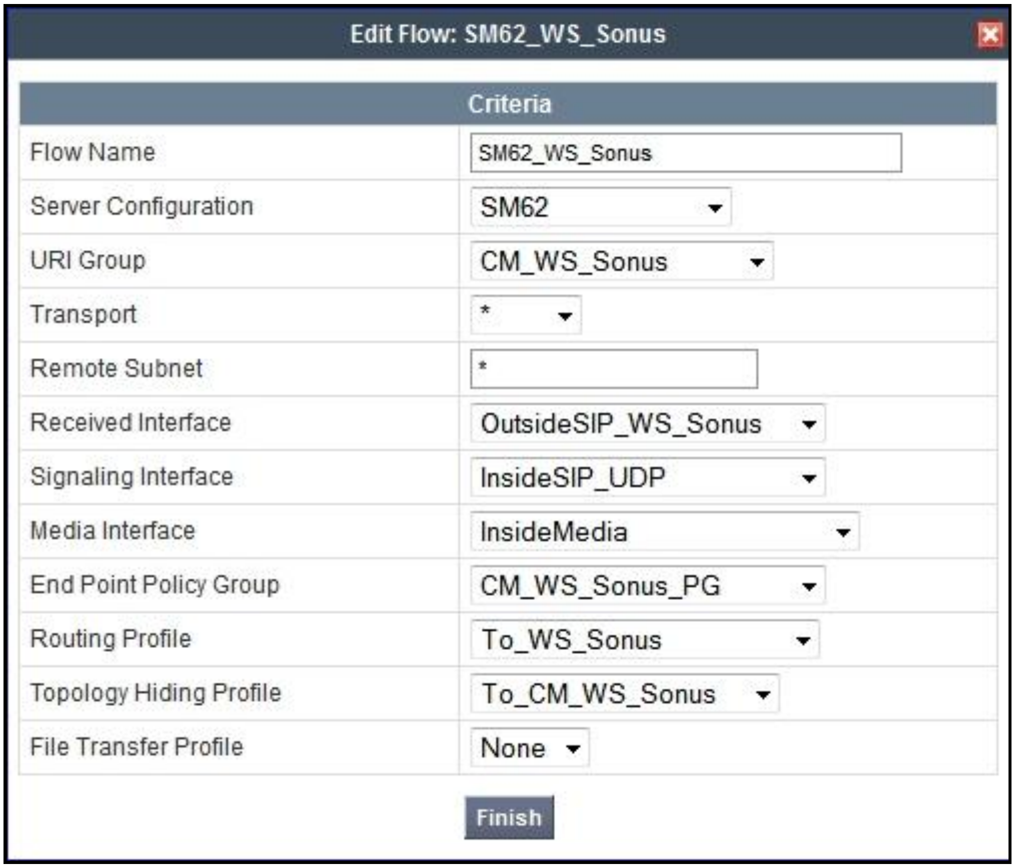
- **URI Group**: Select the URI Group created in **Section 7.2.1** to assign to the Flow.
- **Received Interface**: Select the Signaling Interface created in **Section 7.4.3** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface**: Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 7.3.4** to assign to the Server Configuration.
- **Routing Profile**: Select the Routing Profile created in **Section 7.2.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile**: Select the Topology-Hiding profile created in **Section 7.2.3** to apply to the Server Configuration.
- Click **Finish**.

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



Criteria	
Flow Name	WS_Sonus
Server Configuration	WS_Sonus
URI Group	CM_WS_Sonus
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_WS_Sonus
Media Interface	OutsideMedia_WS_Sonus
End Point Policy Group	WS_Sonus_PG
Routing Profile	To_CM_WS_Sonus
Topology Hiding Profile	To_WS_Sonus
File Transfer Profile	None

The following screen shows the Server Flow **SM62_WS_Sonus** configured for Session Manager.



Criteria	
Flow Name	SM62_WS_Sonus
Server Configuration	SM62
URI Group	CM_WS_Sonus
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_WS_Sonus
Signaling Interface	InsideSIP_UDP
Media Interface	InsideMedia
End Point Policy Group	CM_WS_Sonus_PG
Routing Profile	To_WS_Sonus
Topology Hiding Profile	To_CM_WS_Sonus
File Transfer Profile	None

7.4.5. 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 profile 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).

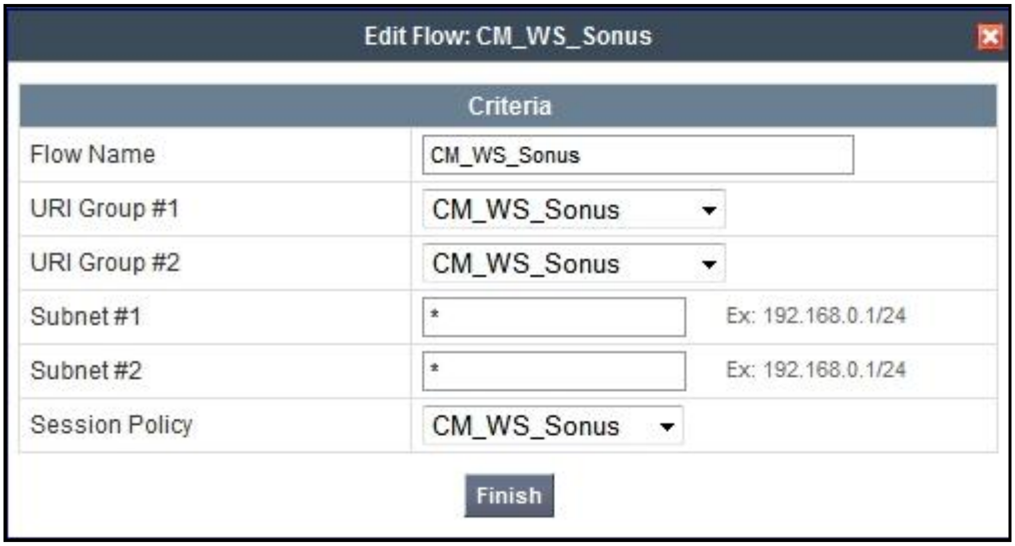
A common Session Flow was created for both Windstream and Communication Manager. In the new window that appears, enter the following values. Use default values for the remaining fields:

- **Flow Name**: Enter a descriptive name.
- **URI Group #1**: Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2**: Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the destination URI Group.
- **Session Policy**: Select the session policy created in **Section 7.3.5** 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_Sonus** was created.



Edit Flow: CM_WS_Sonus

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

8. 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 through security devices (if any).
- IP address and port number used for media through security devices (if any).
- 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.

9. 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.

9.1. 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 to 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.

9.2. Protocol Traces

The following SIP headers were 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 were 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.

9.3. Troubleshooting:

9.3.1. The 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:8642634500@110.10.98.121:5060 SIP/2.0
Via: SIP/2.0/UDP 220.20.49.125:5060;branch=z9hG4bK0dB77261396432a92b4
From: "BELLEVILLE   ON"
<sip:6139675279@220.20.49.125:5060;otg=LAB2PROD>;tag=gK0d0a9541
To: <sip:8642634500@110.10.98.121:5060>
Call-ID: 671951159_25488777@220.20.49.125
CSeq: 17229 INVITE
Max-Forwards: 19
Allow:
```

```
INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIONS
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay,
multipart/mixed
Contact: "BELLEVILLE   ON" <sip:6139675279@220.20.49.125:5060>
P-Charge-Info: sip:6139687508@220.20.49.125:5060
Supported: timer,100rel
Session-Expires: 1800
Min-SE: 90
Content-Length:  370
Content-Disposition: session; handling=required
Content-Type: application/sdp

v=0
o=Sonus_UAC 17091 28558 IN IP4 220.20.49.125
s=SIP Media Capabilities
c=IN IP4 220.20.49.124
t=0 0
m=audio 6554 RTP/AVP 18 0 4 2 101 19
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no;bitrate=6.3
a=rtpmap:2 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:19 CN/8000
a=sendrecv
a=maxptime:30
```

- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: "BELLEVILLE   ON"
<sip:6139675279@220.20.49.125:5060;otg=LAB2PROD>;tag=gK0d0a9541
To: <sip:8642634500@110.10.98.121:5060>;tag=8074a62fc8bee1192d4feeec9800
CSeq: 17229 INVITE
Call-ID: 671951159_25488777@220.20.49.125
Contact: "Windstream x4500"
<sip:8642634500@110.10.98.121:5060;transport=udp;user=phone>
Record-Route: <sip:110.10.98.121:5060;ipcs-line=174;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,join,replaces,sdp-anat,timer
Via: SIP/2.0/UDP 220.20.49.125:5060;branch=z9hG4bK0dB77261396432a92b4
Accept-Language: en
Require: timer
Server: Avaya CM/R016x.02.0.823.0 AVAYA-SM-6.2.1.0.621009
P-Asserted-Identity: "Windstream x4500" <sip:8642634500@110.10.98.121;user=phone>
Session-Expires: 1800;refresher=uas
Content-Type: application/sdp
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville"
;termlocname="Belleville";termsiglocname="Belleville"
Content-Length: 175

v=0
o=- 1340644683 2 IN IP4 110.10.98.121
s=-
c=IN IP4 110.10.98.121
b=AS:64
t=0 0
m=audio 35004 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:16132422192@220.20.49.125 SIP/2.0
From: "Windstream x4500"
<sip:8642634500@110.10.98.121>;tag=80b216d03cae21d30506996d800
To: <sip:16132422192@220.20.49.125>
CSeq: 1 INVITE
Call-ID: 05371a56a6731a3b9cffe94c9a22562a
Contact: "Windstream x4500" <sip:8642634500@110.10.98.121:5060>
Record-Route: <sip:110.10.98.121:5060;ipcs-line=158;lr;transport=udp>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, SUBSCRIBE, NOTIFY, REFER, INFO, PRACK,
PUBLISH, UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent:  Avaya CM/R016x.02.0.823.0 AVAYA-SM-6.2.2.0.622005
Max-Forwards: 66
Via: SIP/2.0/UDP 110.10.98.121:5060;branch=z9hG4bK-s1632-000101876877-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@ws.avaya.com>;avaya-cm-alert-type=internal
P-Asserted-Identity: "Windstream x4500" <sip:8642634500@110.10.98.121>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Content-Type: application/sdp
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville"
;termlocname="Belleville";termsiglocname="Belleville"
P-Charging-Vector: icid-value="AAS:6-d016b2801e20a3c695000d2d896"
Content-Length: 269

v=0
o=- 1347558711 1 IN IP4 110.10.98.121
s=-
c=IN IP4 110.10.98.121
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35006 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=ptime:30
```

- 200OK/SDP response by Windstream:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.121:5060;branch=z9hG4bK-s1632-000101876877-1--s1632-
From: "Windstream x4500"
<sip:8642634500@110.10.98.121>;tag=80b216d03cae21d30506996d800
To: <sip:16132422192@220.20.49.125>;tag=gK0aa2e2f9
Call-ID: 05371a56a6731a3b9cffe94c9a22562a
CSeq: 1 INVITE
Record-Route: <sip:110.10.98.121:5060;ipcs-line=158;lr;transport=udp>
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay,
multipart/mixed
Contact: <sip:16132422192@220.20.49.125:5060>
Allow:
INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIONS
P-Charging-Vector: icid-value="AAS:6-d016b2801e20a3c695000d2d896";term-ioi=6121
Require: timer
Supported: timer
Session-Expires: 1200;refresher=uac
Content-Length:  235
Content-Disposition: session; handling=required
Content-Type: application/sdp

v=0
o=Sonus_UAC 1791 5057 IN IP4 220.20.49.125
s=SIP Media Capabilities
c=IN IP4 220.20.49.124
t=0 0
m=audio 5316 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=maxptime:20
```

9.3.2. 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.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 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 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5.

11. References

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

Avaya product documentation is available at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.1, July 2012.
[2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.
[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, July 2012, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.2, July 2012, Document Number 555-245-205.
[5] *Implementing Avaya Aura® System Manager*, Release 6.2, July 2012.
[6] *Upgrading Avaya Aura® System Manager to 6.2*, Release 6.2, July 2012.
[7] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012.
[8] *Implementing Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603473.
[9] *Upgrading Avaya Aura® System Manager*, Release 6.2, July 2012, Document Number 03-603518.
[10] *Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603324.
[11] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* Release 3.1, November 2009, Document Number 16-300698.
[12] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
[13] *Administering Avaya one-X® Communicator*, April 2011.
[14] *Using Avaya one-X® Communicator*, April 2011.
[15] *UC-Sec Install Guide (*102-5224-400v1.01*)*
[16] *UC-Sec Administration Guide (*010-5423-400v106*)*
[17] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/
[18] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/
[19] *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.

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.