



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise 4.0.5 with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, and various Avaya endpoints.

CenturyLink 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 was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing CenturyLink SIP Trunk Services.

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	5
3.	Reference Configuration	6
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager.....	7
5.1.	Licensing and Capacity	8
5.2.	System Features.....	9
5.3.	IP Node Names.....	10
5.4.	Codecs	10
5.5.	IP Interface for procr	11
5.6.	IP Network Region.....	11
5.7.	Signaling Group	13
5.8.	Trunk Group.....	15
5.9.	Inbound Routing.....	17
5.10.	Calling Party Information	18
5.11.	Outbound Routing	19
5.12.	Saving Communication Manager Configuration Changes	22
6.	Configure Avaya Aura® Session Manager	23
6.1.	Avaya Aura® System Manager Login and Navigation	23
6.2.	Specify SIP Domain	24
6.3.	Add Location.....	25
6.4.	Add SIP Entities	28
6.5.	Add Entity Links	32
6.6.	Add Routing Policies	33
6.7.	Add Dial Patterns	34
6.8.	Verify Avaya Aura® Session Manager Instance	37
7.	Configure Avaya Session Border Controller for Enterprise	39
7.1.	Global Profiles.....	42
7.1.1.	Routing Profile.....	42
7.1.2.	Topology Hiding Profile	44
7.1.3.	Server Interworking Profile	47
7.1.4.	Signaling Manipulation.....	57
7.1.5.	Server Configuration.....	59
7.2.	Domain Policies	69
7.2.1.	Media Rule.....	69
7.2.2.	Signaling Rule.....	71
7.2.3.	Application Rule	75

7.2.4.	Endpoint Policy Group	76
7.3.	Device Specific Settings.....	78
7.3.1.	Network Management.....	78
7.3.2.	Signaling Interface	80
7.3.3.	Media Interface	80
7.3.4.	End Point Flows - Server Flow	81
8.	CenturyLink SIP Trunk Service Configuration	85
9.	Verification and Troubleshooting	85
9.1.	Verification.....	85
9.2.	Troubleshooting	86
10.	Conclusion	89
11.	Additional References.....	90

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.0.1, Session Manager 6.1, and Avaya Session Border Controller for Enterprise 4.0.5 integration with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6.

In the sample configuration, the Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Avaya SBCE performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

Communication Manager and Session Manager are connected using two Communication Manager SIP trunk groups. One trunk group is used for internal SIP traffic including SIP phones and Aura® Messaging, while the other is used for external SIP traffic. Session Manager then has one connection to Avaya SBCE for CenturyLink SIP traffic.

CenturyLink SIP Trunk is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

CenturyLink SIP Trunk will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

CenturyLink SIP Trunk (Legacy Qwest) Service passed compliance testing.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.

- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Inbound toll-free calls.
- Codecs G.729A, G.729AB and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Network Call Redirection using the SIP REFER method or a 302 response is not supported by CenturyLink.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.

2.3. Support

For technical support on the CenturyLink SIP Trunk Service, contact CenturyLink using the Customer Care links at www.centurylink.com

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, Avaya SBCE provides NAT functionality and SIP header manipulation. Avaya SBCE receives traffic from CenturyLink SIP Trunk on port 5060 and sends traffic to the CenturyLink SIP Trunk using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been either replaced with private IP addresses or have been blocked out. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

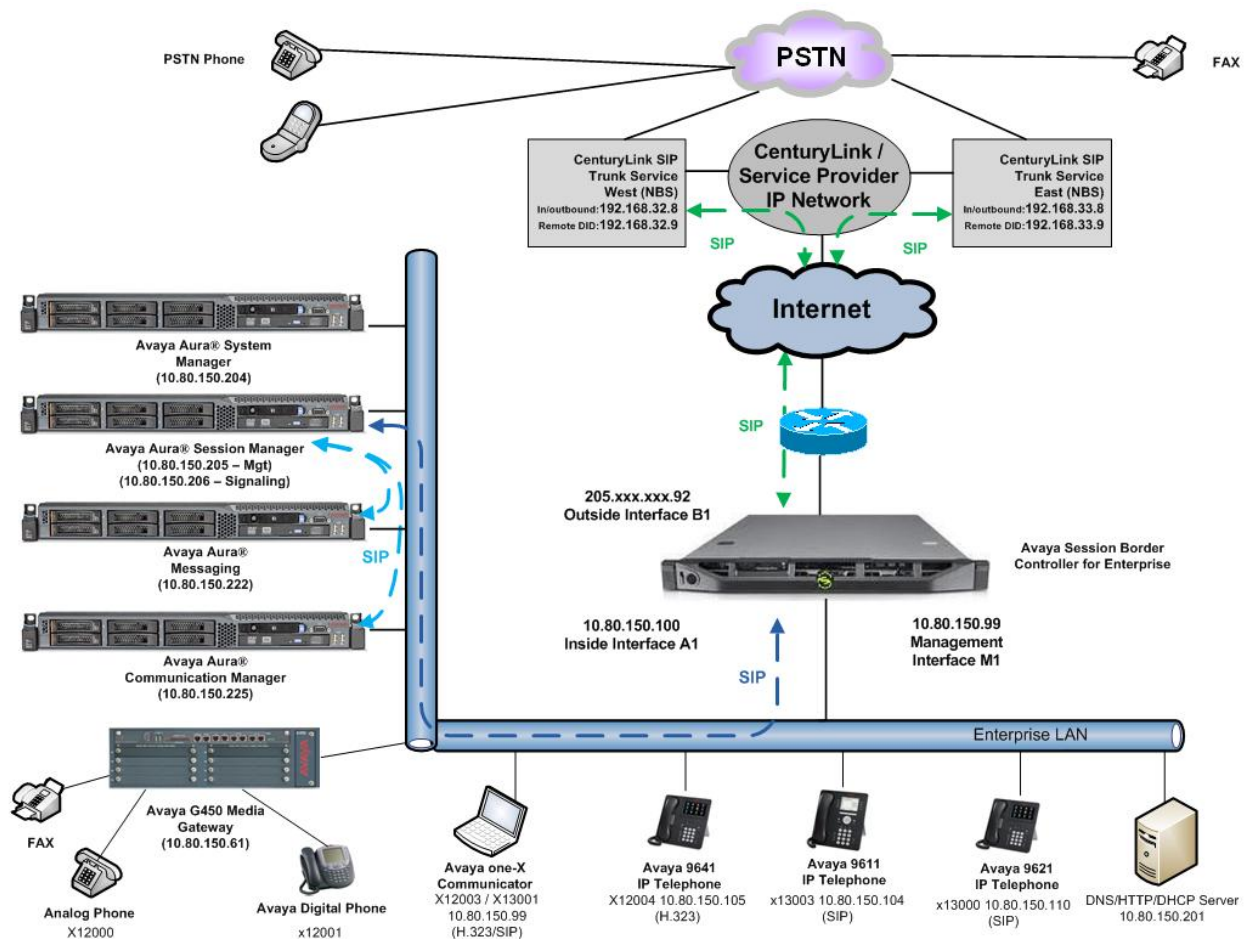


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manger	R016x.00.1.510.1-19303 (SP 5)
Avaya Aura® Messaging	R016x.00.1.510.1-004_0302 (SP 3)
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.115
Avaya Aura® Session Manager	6.1.4.0.614005
Avaya Session Boarder Controller for Enterprise	4.0.5
Avaya G450 Media Gateway	31.18.1
Avaya 9641 IP Telephone (H.323)	Avaya one-X Deskphone Edition 6.0.1
Avaya 9621 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0.1
Avaya 9611 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0.1
Avaya one-X Communicator (H.323 and SIP)	6.1.0.12
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus Network Border Switch (NBS)	07.03.05 R006

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for CenturyLink SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from CenturyLink. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

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

Note: IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

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 the service provider. The example shows that **12000** licenses are available and **275** 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 additional capacity.

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	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		128	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	0	
Maximum Video Capable IP Softphones:		18000	1	
Maximum Administered SIP Trunks:		12000	275	
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		10	0	
Maximum Media Gateway VAL Sources:		250	1	
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	

Figure 2: System Parameters Customer Options Page 2

5.2. System Features

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

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      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
```

Figure 3: System Parameters Feature Page 1

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **Anonymous** for both types of calls.

```
display system-parameters features                             Page 9 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: Anonymous
      CPN/ANI/ICLID Replacement for Unavailable Calls: Anonymous

      DISPLAY TEXT
      Identity When Bridging: principal
      User Guidance Display? n
      Extension only label for Team button on 96xx H.323 terminals? n

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code: 1
      International Access Code: 011

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

Figure 4: System Parameters Feature Page 9

5.3. IP Node Names

Use the **display node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

display node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SM	10.80.150.206	
default	0.0.0.0	
procr	10.80.150.225	
procr6	::	

Figure 5: Node Names IP

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. The CenturyLink SIP Trunk Service supports G.729A, G.729AB and G.711MU. During compliance testing each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first choice. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** were entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

Figure 6: IP Codec Set 2 Page 1

On **Page 2**, set the **Fax Mode** to **T.38-standard**.

change ip-codec-set 2			Page 2 of 2
IP Codec Set			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	
FAX	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	

Figure 7: IP Codec Set 2 Page 2

5.5. IP Interface for procr

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 1700	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.80.150.225	
Subnet Mask: /24		

Figure 8: IP Interface procr

5.6. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Location** field to match the enterprise location for this SIP trunk.

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. To enable shuffling, set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Set the **UDP Port Min** and **UDP Port Max** fields to a range suitable for RTP traffic.
- Default values can be used for all other fields.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2		
Location: 1	Authoritative Domain: avayalab.com	
Name: SIP Trunks		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 2	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		

Figure 9: IP Network Region 2 Page 1

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 2										Page	4	of	20
Source Region: 2 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	2	y	NoLimit								n		t
2	2												
3													
4													

Figure 10: IP Network Region 2 Page 4

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer Server** field will initially be set to **Others** and cannot be changed via administration. The Peer Server field will automatically change to **SM** once Communication Manager detected a Session Manager peer.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. 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 defined for the service provider in **Section 5.6**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.

- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5081	Far-end Listen Port: 5081	
	Far-end Network Region: 2	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Figure 11: Signaling Group 2

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- 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 **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
  Group Name: SIP SP 2                             COR: 1                TN: 1          TAC: *02
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: public-ntwrk                       Auth Code? n
                                                  Member Assignment Method: auto
                                                  Signaling Group: 2
                                                  Number of Members: 10
```

Figure 12: Trunk Group 2 Page 1

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

```
add trunk-group 2                                     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 Out? y
```

Figure 13: Trunk Group 2 Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Set **Modify Tandem Calling Number** to **tandem-cpn-form**. Default values were used for all other fields.

add trunk-group 2

Page 3 of 21

TRUNK FEATURES

ACA Assignment? nMeasured: none

Maintenance Tests? y

Numbering Format: public

UI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: tandem-cpn-form

Show ANSWERED BY on Display? y

Figure 14: Trunk Group 2 Page 3

On **Page 4**, set the **Network Call Redirection** field to **n**. This disables the unsupported Refer and 302 Moved Temporarily features. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. Set the **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **100**, the value preferred by CenturyLink.

add trunk-group 2

Page 4 of 21

PROTOCOL VARIATIONS

Mark Users as Phone? n

Prepend '+' to Calling Number? n

Send Transferring Party Information? n

Network Call Redirection? n

Send Diversion Header? y

Support Request History? n

Telephone Event Payload Type: 100

Convert 180 to 183 for Early Media? n

Always Use re-INVITE for Display Updates? n

Identity for Calling Party Display: P-Asserted-Identity

Figure 15: Trunk Group 2 Page 4

5.9. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via Communication Manager incoming call handling table may not be necessary. If the DID number sent by CenturyLink is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group.

Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **3035557104** to extension **12004**.

change inc-call-handling-trmt trunk-group 2					Page 1 of 30	
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	10	3035557104	10	12004		
public-ntwrk	10	3035557105	10	12005		
public-ntwrk	10	3035557106	10	13000		
public-ntwrk	10	3035557107	10	13001		
public-ntwrk	10	3035557108	10	13002		
public-ntwrk	10	3035557127	10	13003		
public-ntwrk	10	6145555714	10	13004		
public-ntwrk	10	6145555715	10	12000		

Figure 16: Incoming Call Handling Treatment

5.10. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the bolded row shown in the example abridged output below, a specific Communication Manager extension (x12004) is mapped to a DID number that is known to CenturyLink for this SIP Trunk connection (3035557104), when the call uses trunk group 2.

change public-unknown-numbering 5 ext-digits 12000 trunk-group 2					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12000	2	6145555715	10	Total Administered: 22
5	12001	2	6145555716	10	Maximum Entries: 9999
5	12004	2	3035557104	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
5	12005	2	3035557105	10	
5	13000	2	3035557106	10	
5	13001	2	3035557107	10	
5	13002	2	3035557108	10	
5	13003	2	3035557127	10	
5	13004	2	6145555714	10	

Figure 17: Public Unknown Numbering

Use the **change tandem-calling-party-num** command, to define the calling party number to send to the PSTN for tandem calls from SIP users.

In the example shown below, calls originating from extension 13001 and routed to trunk group 2 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case **pub-unk**.

change tandem-calling-party-num					Page 1 of 8
CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS					
CPN Len	CPN Prefix	Trk Grp(s)	Delete	Insert	Number Format
5	13001	2	5	3035557107	pub-unk
5	13002	2	5	3035557108	pub-unk
5	13003	2	5	3035557127	pub-unk
5	13004	2	5	6145555714	pub-unk

Figure 18: Tandem Calling Party Number

5.11. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an outside line. This common configuration is illustrated below. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
2	5	ext							
3	5	ext							
4	5	ext							
5	5	ext							
6	5	ext							
7	5	ext							
8	5	ext							
9	1	fac							
*	3	dac							
#	3	dac							

Figure 19: Dialplan Analysis

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)			Page 1 of 10
Abbreviated Dialing List1 Access Code: *10						
Abbreviated Dialing List2 Access Code: *12						
Abbreviated Dialing List3 Access Code: *13						
Abbreviated Dial - Prgm Group List Access Code: *14						
Announcement Access Code: *19						
Answer Back Access Code:						
Auto Alternate Routing (AAR) Access Code: *00						
Auto Route Selection (ARS) – Access Code 1: 9			Access Code 2:			
Automatic Callback Activation: *33			Deactivation: #33			
Call Forwarding Activation Busy/DA: *30 All: *31			Deactivation: #30			
Call Forwarding Enhanced Status:			Act:			
			Deactivation:			

Figure 20: Feature Access Codes

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., **1303**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., **11**) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., **1**) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type:** **fnpa** the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. For 411 and 911 calls use **svcl** and **emer** respectively. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1. For more information and a complete list of Communication Manager call types, refer to [3] and [4].

The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 1							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
1303	11	11	1	fnpa		n	
1502	11	11	1	fnpa		n	
1720	11	11	1	fnpa		n	
1800	11	11	1	fnpa		n	
1866	11	11	1	fnpa		n	
1877	11	11	1	fnpa		n	
1888	11	11	1	fnpa		n	
1908	11	11	1	fnpa		n	
2	10	10	1	hnpa		n	
3	10	10	1	hnpa		n	
4	10	10	1	hnpa		n	
411	3	3	1	svcl		n	
5	10	10	1	hnpa		n	
555	7	7	deny	hnpa		n	
6	10	10	1	hnpa		n	

Figure 21: ARS Analysis

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **2** 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.
- **Pfx Mrk: 1** The prefix mark (**Pfx Mrk**) of 1 will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

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

Figure 22: Route Pattern 1

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by CenturyLink being converted to 5 digit extensions.

change ars digit-conversion 0					Page 1 of 2			
ARS DIGIT CONVERSION TABLE					Percent Full: 0			
Location: all								
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI	Req
3035557104	10	10	10	12004	ext	y	n	
3035557105	10	10	10	12005	ext	y	n	
3035557106	10	10	10	10000	ext	y	n	
3035557107	10	10	10	13004	ext	y	n	
3035557108	10	10	10	13002	ext	y	n	
3035557109	10	10	10	13001	ext	y	n	
3035557127	10	10	10	13003	ext	y	n	
6145555686	10	10	10	13000	ext	y	n	
6145555711	10	10	10	13003	ext	y	n	
6145555714	10	10	10	13004	ext	y	n	
6145555715	10	10	10	12000	ext	y	n	

Figure 23: ARS Digit Conversion

5.12. Saving Communication Manager Configuration Changes

The command **save translation all** can be used to save the configuration.

save translation all	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

Figure 24: Save Translation All

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, Avaya SBCE and Session Manager
- 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 Instance, corresponding to the Session Manager server to be administered in 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. Avaya Aura® System Manager Login and Navigation

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

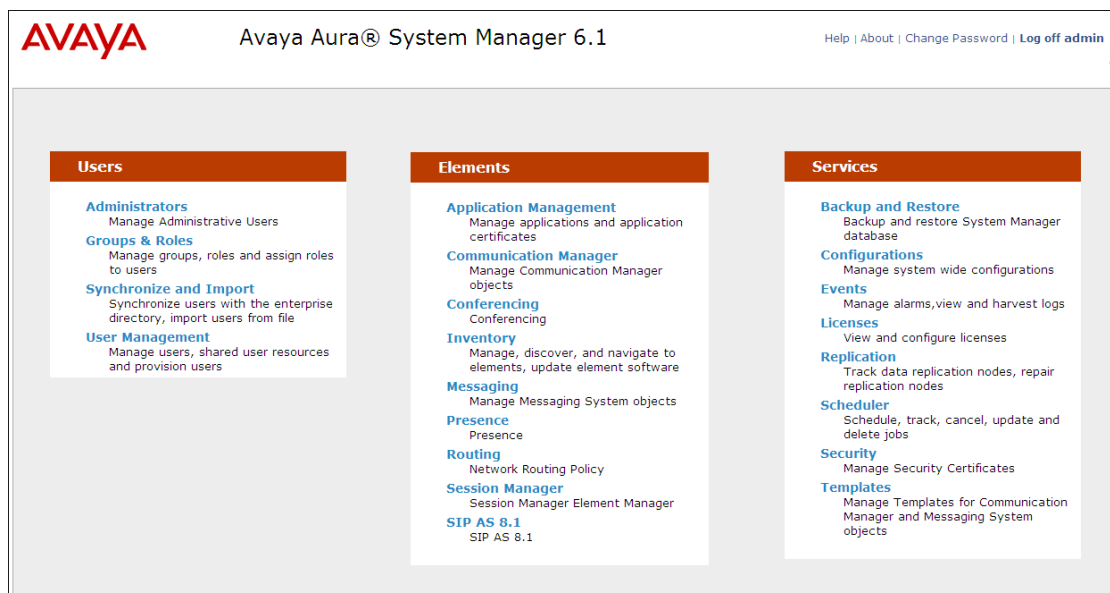


Figure 25: System Manger Main Menu

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

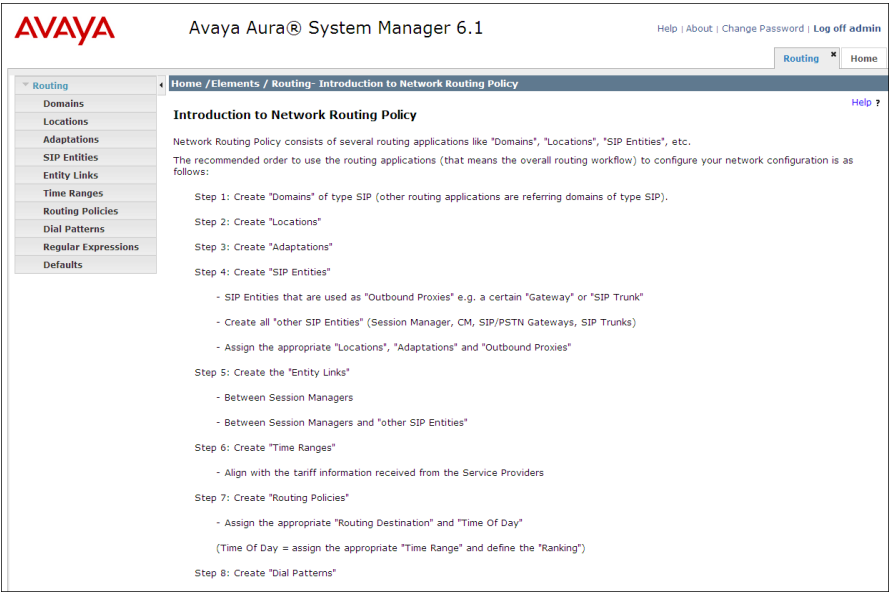


Figure 26: System Manger Routing Menu

6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing** → **Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The following screen shows the entry for the **avayalab.com** domain.

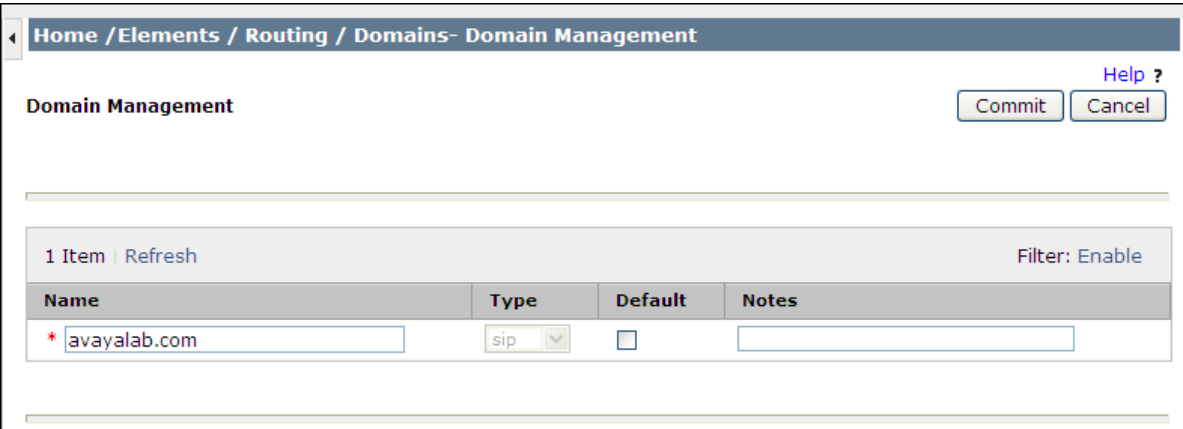


Figure 27: SIP Domain in Session Manager

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. 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. Use default values for all remaining fields:

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

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.4**), so it was not necessary to add a pattern.

The following screen shows the addition of **Location_150_SM**, this location will be used for Session Manager. Click **Commit** to save.

Home / Elements / Routing / Locations - Location Details

Location Details [Help ?](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

0 Items | [Refresh](#) Filter: [Enable](#)

IP Address Pattern	Notes
--------------------	-------

Figure 28: Creating a Location for Session Manger

Note: Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for Communication Manager and Avaya SBCE. Displayed below is the screen for **Location_150_CM** used for Communication Manager.

The screenshot shows a web-based configuration interface for a location. The breadcrumb trail at the top is 'Home / Elements / Routing / Locations - Location Details'. The page title is 'Location Details'. There are 'Commit' and 'Cancel' buttons in the top right corner, along with a 'Help ?' link. A message states: 'Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting'.

The 'General' section contains a required field for 'Name' with the value 'Location_150_CM' and a 'Notes' field with the value 'Communication Manager'.

The 'Overall Managed Bandwidth' section has a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec' and an empty 'Total Bandwidth' input field.

The 'Per-Call Bandwidth Parameters' section has a required field for 'Default Audio Bandwidth' set to '80' with a 'Kbit/sec' dropdown.

The 'Location Pattern' section has 'Add' and 'Remove' buttons. Below them is a table with 0 items, a 'Refresh' button, and a 'Filter: Enable' link. The table has two columns: 'IP Address Pattern' and 'Notes'.

At the bottom, there is a red asterisk indicating 'Input Required' and 'Commit' and 'Cancel' buttons.

Figure 29: Creating a Location for Communication Manger

Below is the screen for **AvayaSBCE-LOC150** used for Avaya SBCE.

Home / Elements / Routing / Locations - Location Details

Location Details

Help ?

Commit Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

ASBCE-LOC150

Notes:

Avaya SBC-E Location 150

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

Add Remove

0 Items | Refresh

Filter: Enable

	IP Address Pattern	Notes
--	--------------------	-------

* Input Required

Commit Cancel

Figure 30: Creating a Location for Avaya SBCE

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP server connected to it, which includes Communication Manager and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand 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 **SIP Trunk** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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

The screenshot shows a web interface for configuring a SIP Entity. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities - SIP Entity Details". The page title is "SIP Entity Details". There are "Commit" and "Cancel" buttons in the top right corner, along with a "Help ?" link. The "General" section is active and contains the following fields: "Name" (required, value: ASM), "FQDN or IP Address" (required, value: 10.80.150.206), "Type" (dropdown menu, value: Session Manager), "Notes" (text area, value: Session Manager), "Location" (dropdown menu, value: Location_150_SM), "Outbound Proxy" (dropdown menu, empty), "Time Zone" (dropdown menu, value: America/Denver), and "Credential name" (text area, empty). The "SIP Link Monitoring" section contains a "SIP Link Monitoring" dropdown menu with the value "Use Session Manager Configuration".

Figure 31: Creating a SIP Entity for Session Manger

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 **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

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

- **Port:** Port number on which Session Manager can listen for 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.

For the compliance test, six **Port** entries were added. Although UDP was added for SIP clients, only the TCP and TLS ports were used by Session Manager in the reference configuration.

Port

6 Items | [Refresh](#)
Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avayalab.com	
<input type="checkbox"/>	5060	TCP	avayalab.com	
<input type="checkbox"/>	5061	TLS	avayalab.com	
<input type="checkbox"/>	5070	TCP	avayalab.com	
<input type="checkbox"/>	5080	TCP	avayalab.com	
<input type="checkbox"/>	5081	TLS	avayalab.com	

Select : [All](#), [None](#)

* **Input Required**

Figure 32: Session Manager Ports

The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, a new SIP entity is created separate from the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the processor interface on Communication Manager defined in **Section 5.3**.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Help ?](#)

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Figure 33: Creating a SIP Entity for Communication Manger Trunk Group 2

The following screen shows the addition of **ASBCE-150** SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Avaya SBCE in **Section 6.3**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details Help ? Commit Cancel

General

* Name: ASBCE-150

* FQDN or IP Address: 10.80.150.100

Type: SIP Trunk

Notes: Avaya SBC-E Location 150

Adaptation:

Location: ASBCE-LOC150

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Figure 34: Creating a SIP Entity for Avaya SBCE

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand 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 SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **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 5.7**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Connection Policy:** Select **Trusted**.

Note: If the Connection Policy is not trusted, 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 Avaya SBCE. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Commit Cancel Help ?

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM_CM601-TG2-Loc150	* ASM	TLS	* 5081	* CM601-TG2-Loc150	* 5081	Trusted	

* Input Required Commit Cancel

Figure 35: Creating an Entity Link for Communication Manager

Entity Link to Avaya SBCE:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links [Help ?](#)

1 Item | [Refresh](#) Filter: [Enable](#)

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* ASM_ASBCE-150_50	* ASM	TCP	* 5060	* ASBCE-150	* 5060	Trusted

* Input Required

Figure 36: Creating an Entity Link for Avaya SBCE

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 must be added; one for Communication Manager Trunk Group 2 and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand 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. Use default values for all remaining fields:

- **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** (not shown). The selected SIP Entity displays on 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 for Communication Manager trunk group 2 and Avaya SBCE.

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-CM601-TG2-LOC150'. The page has a breadcrumb trail: 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. There are 'Commit' and 'Cancel' buttons in the top right, along with a 'Help ?' link. The 'General' section contains the following fields:

- Name:** To-CM601-TG2-LOC150
- Disabled:** ☐
- Notes:** Trunk Group 2 for SIP SP#2

 Below the 'General' section is the 'SIP Entity as Destination' section, which includes a 'Select' button. At the bottom, there is a table with the following data:

Name	FQDN or IP Address	Type	Notes
CM601-TG2-Loc150	10.80.150.225	CM	Trunk Group 2 for SP 2

Figure 37: Routing Policy to Communication Manager Trunk Group 2

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-ASBCE-LOC150'. The page has a breadcrumb trail: 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. There are 'Commit' and 'Cancel' buttons in the top right, along with a 'Help ?' link. The 'General' section contains the following fields:

- Name:** To-ASBCE-LOC150
- Disabled:** ☐
- Notes:** To Avaya SBCE Location 150

 Below the 'General' section is the 'SIP Entity as Destination' section, which includes a 'Select' button. At the bottom, there is a table with the following data:

Name	FQDN or IP Address	Type	Notes
ASBCE-150	10.80.150.100	SIP Trunk	Avaya SBC-E Location 150

Figure 38: Routing Policy to Avaya SBCE

6.7. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to CenturyLink 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-hand 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. Use default values for all remaining fields:

- **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:** Select 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 test are shown below. This Session Manager is shared between two test environments. The first example shows that **11** digit dialed numbers that begin with **1** to domain **avayalab.com** and originating from **Location_150_CM** uses route policy **To-ASBCE-LOC150**.

Dial Pattern Details

General

* **Pattern:** 1

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: 1+ OUTBOUND

Originating Locations and Routing Policies

Add **Remove**

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Location_140_CM	Subnet 140	To VZ_Acme	0	<input type="checkbox"/>	VZ_Acme	
<input type="checkbox"/>	Location_150_CM	Communication Manager	To-ASBCE-LOC150	0	<input type="checkbox"/>	ASBCE-150	To Avaya SBCE Location 150

Select : All, None

Figure 39: Outbound Dial Pattern Example

The second example shows that a **10** digit number starting with **303555** to domain **avayalab.com** and originating from **ASBCE-LOC150** uses route policy **To-CM601-TG2-LOC150**. This will allow DID numbers assigned to the enterprise from CenturyLink to route to Communication Manager using trunk group 2. CenturyLink did not assign every number that starts with 303555 to the enterprise. So to properly route any number that is not a DID starting with 303555 dialed from Communication Manager, **Location_150_CM** was added to use route policy **To-ASBCE-LOC150**.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details
[Help ?](#)

Dial Pattern Details
[Commit](#) [Cancel](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

2 Items | [Refresh](#)
Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	ASBCE-LOC150	Avaya SBC-E Location 150	To-CM601-TG2-LOC150	0	<input type="checkbox"/>	CM601-TG2-Loc150	Trunk Group 2 for SIP SP#2
<input type="checkbox"/>	Location_150_CM	Communication Manager	To-ASBCE-LOC150	0	<input type="checkbox"/>	ASBCE-150	To Avaya SBCE Location 150

Select : All, None

Figure 40: Inbound Dial Pattern Example

6.8. Verify Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **new** button in the right pane (not shown). If the Session Manager instance 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.

The following screen shows the Session Manager values used for the compliance test.



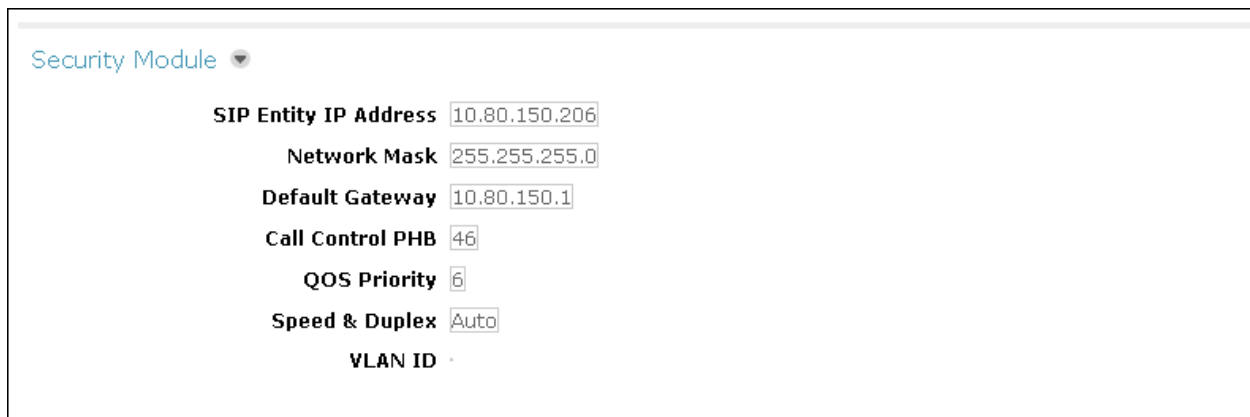
The screenshot displays the 'View Session Manager' configuration page. The breadcrumb trail at the top reads: 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. A 'Help ?' link is in the top right corner. The main title is 'View Session Manager' with a 'Return' button. Below the title is a horizontal menu with options: 'General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |'. Below this menu are 'Expand All' and 'Collapse All' links. The 'General' section is expanded, showing the following fields: 'SIP Entity Name' with the value 'ASM', 'Description' (empty), 'Management Access Point Host Name/IP' with the value '10.80.150.205', and 'Direct Routing to Endpoints' with the value 'Enable'.

Figure 41: Session Manager Administration

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **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 **Save** (not shown) to add this Session Manager. The following screen shows the remaining Session Manager values used for the compliance test.



The screenshot displays a configuration window titled "Security Module" with a dropdown arrow. Below the title, several configuration fields are listed with their corresponding values entered in text boxes:

- SIP Entity IP Address:** 10.80.150.206
- Network Mask:** 255.255.255.0
- Default Gateway:** 10.80.150.1
- Call Control PHB:** 46
- QOS Priority:** 6
- Speed & Duplex:** Auto
- VLAN ID:** (field is empty)

Figure 42: Session Manager Security Module

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [13] and [14].

A pictorial view of this configuration is shown below. It is separated into two sections representing the values for the Avaya enterprise site and CenturyLink. It shows the components needed for the compliance test. Each of these components is defined in the Avaya SBCE web configuration as described in the following sections.

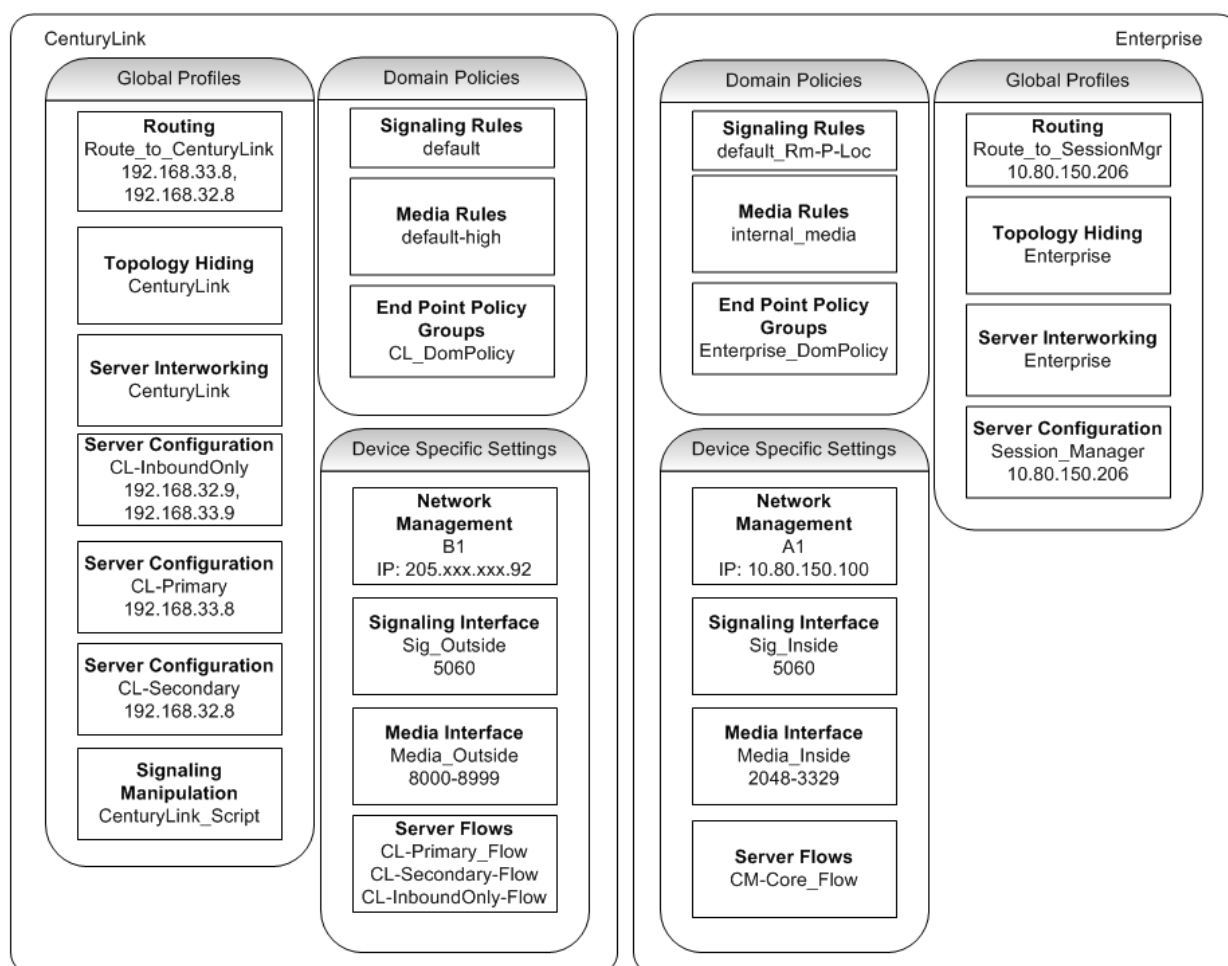


Figure 43: Pictorial View of Configuration

Use a WEB browser to access the Avaya SBCE web interface, enter <https://<ip-addr>/ucsec> in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

Log in with the appropriate credentials. Click **Sign In**.

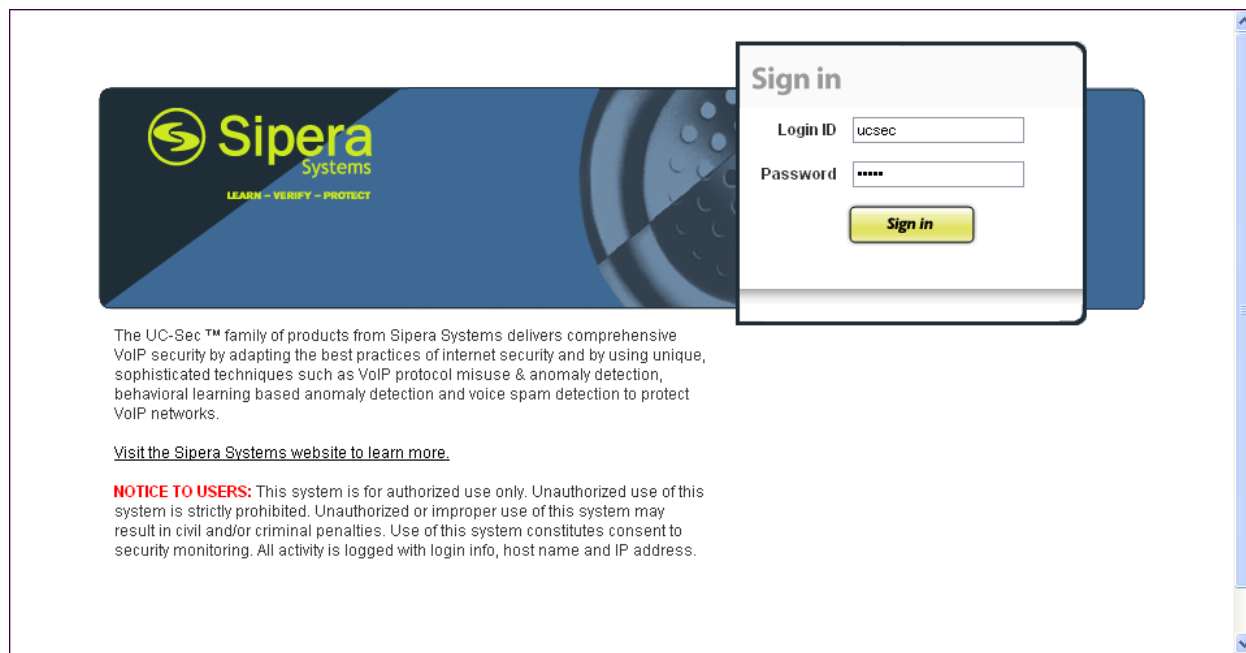


Figure 44: Avaya SBCE Web Page Login

The main page of the UC-Sec Control Center will appear.

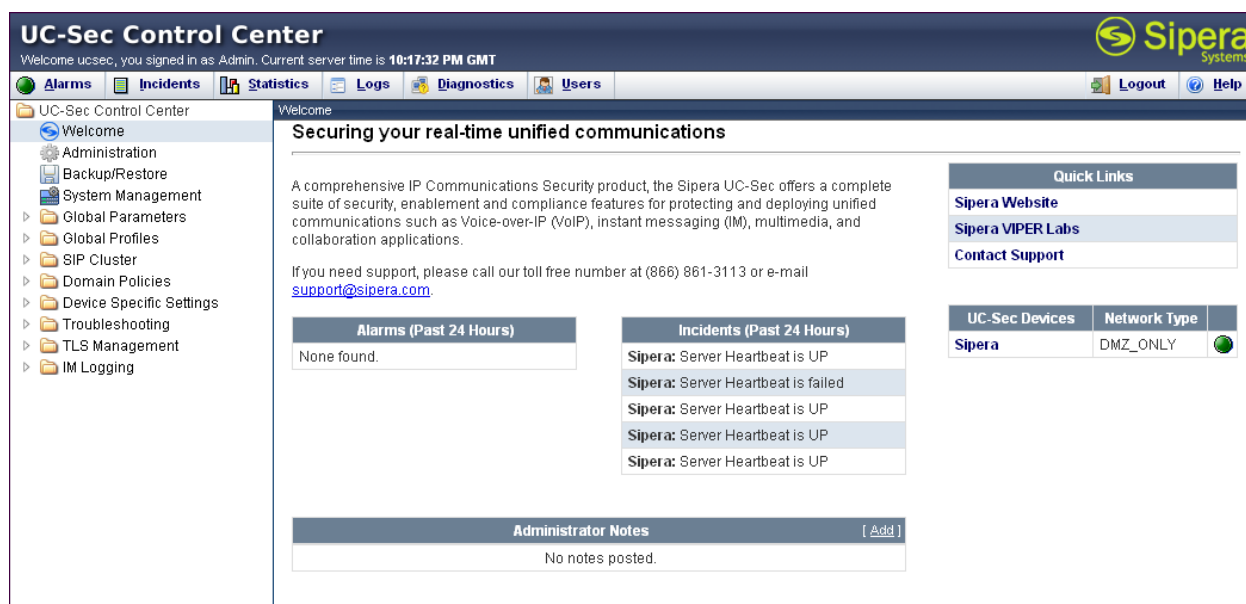


Figure 45: UC-Sec Main Page

To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **Sipera** is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).

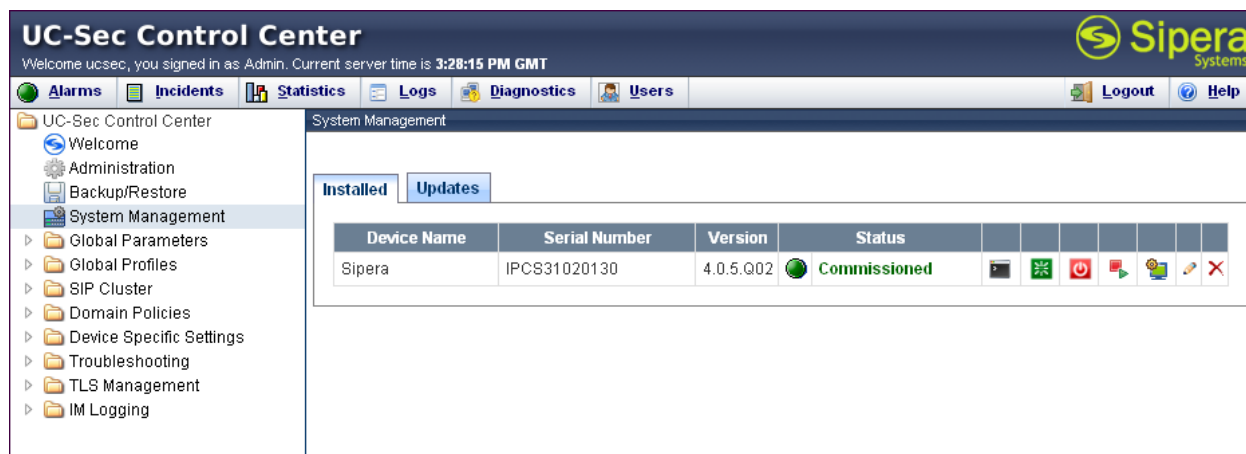


Figure 46: System Management

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

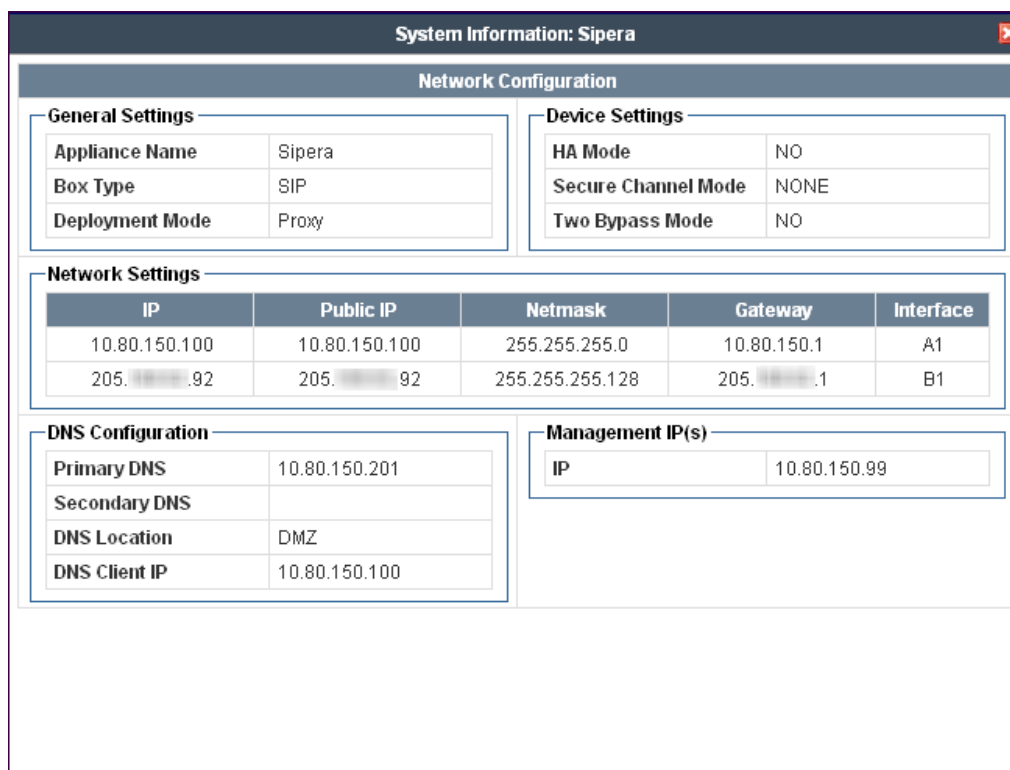


Figure 47: System Information

7.1. Global Profiles

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

7.1.1. Routing Profile

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.

Create a Routing Profile for Session Manager and CenturyLink SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

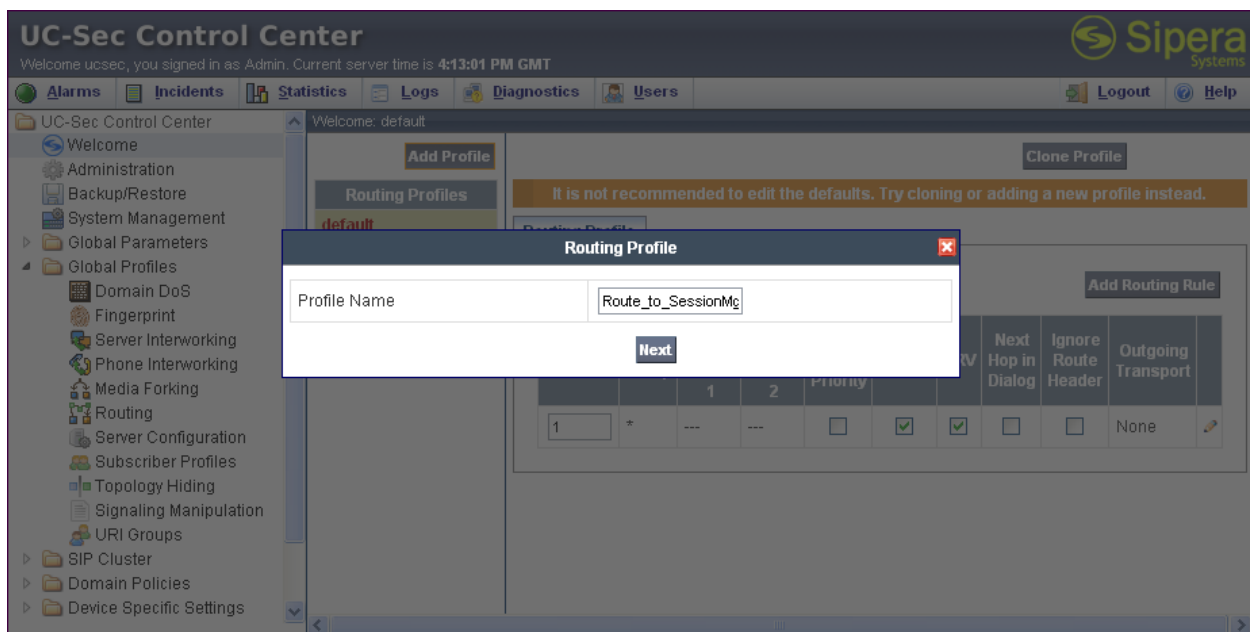


Figure 48: Adding Routing Profile – Profile Name

In the new window that appears, enter the following values (not shown). Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server:** Checked.
- **Use Next Hop for In-Dialog Messages:** Unchecked.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module in **Section 6.8**. The Outgoing Transport and port number must match the Avaya SBCE Entity Link created on Session Manager in **Section 6.5**.

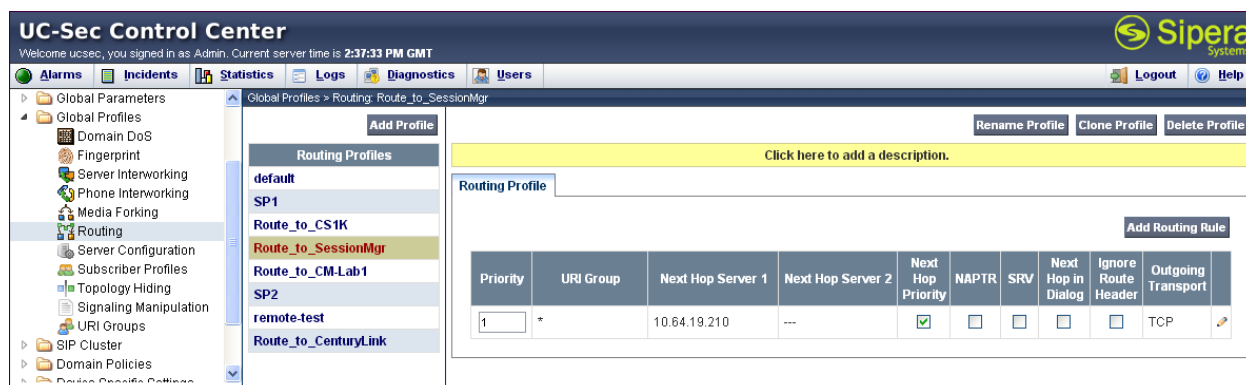


Figure 49: Routing Profile to Session Manager

The following screen shows the Routing Profile to CenturyLink. For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two SIP servers allocated for outbound traffic were added to the Routing Profile.

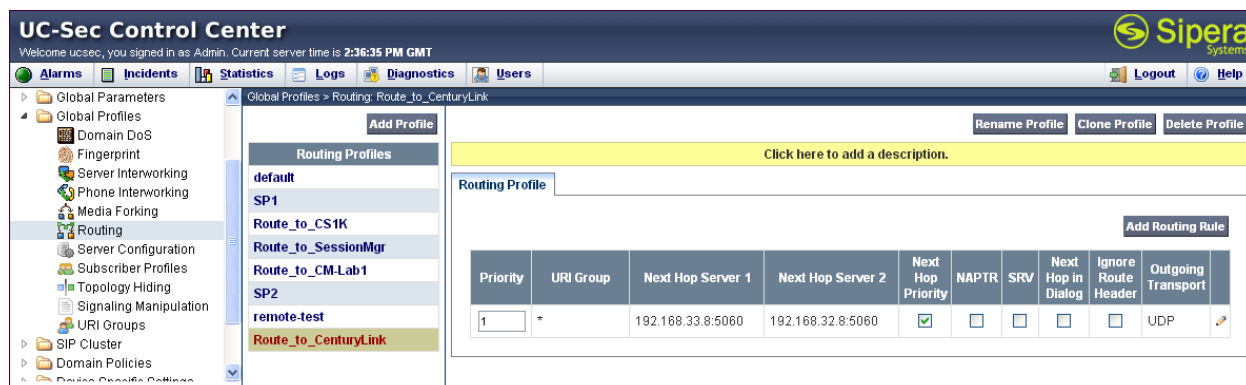


Figure 50: Routing Profile to CenturyLink

7.1.2. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Create a Topology Hiding Profile for the enterprise and CenturyLink SIP Trunk. In the sample configuration, the **Enterprise** and **CenturyLink** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center** → **Global Profiles** → **Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown in Figure 51.

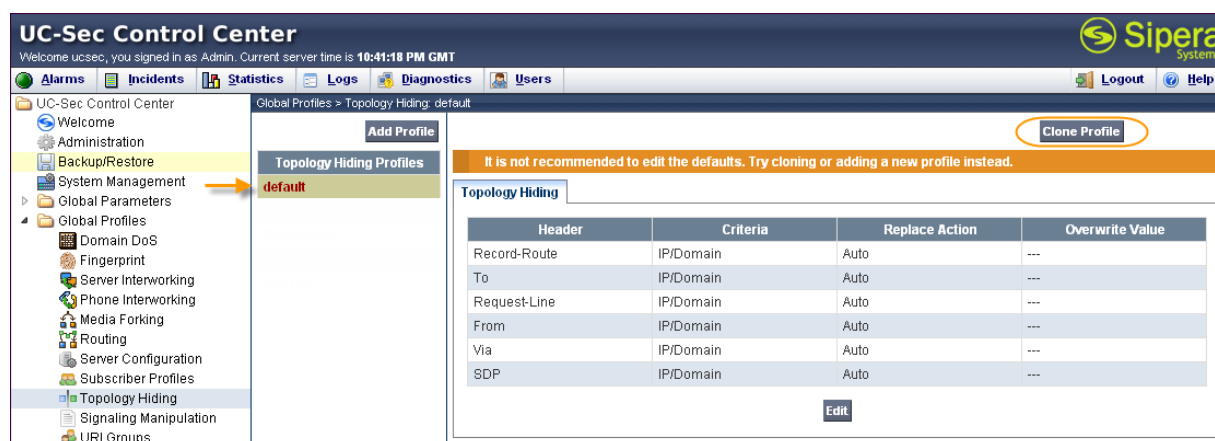
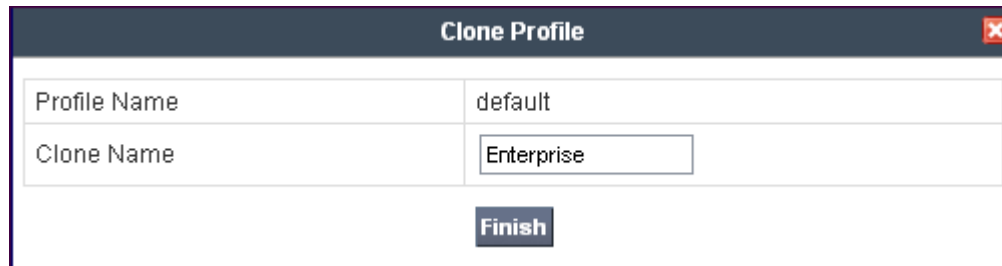


Figure 51: Topology Hiding – Clone Profile

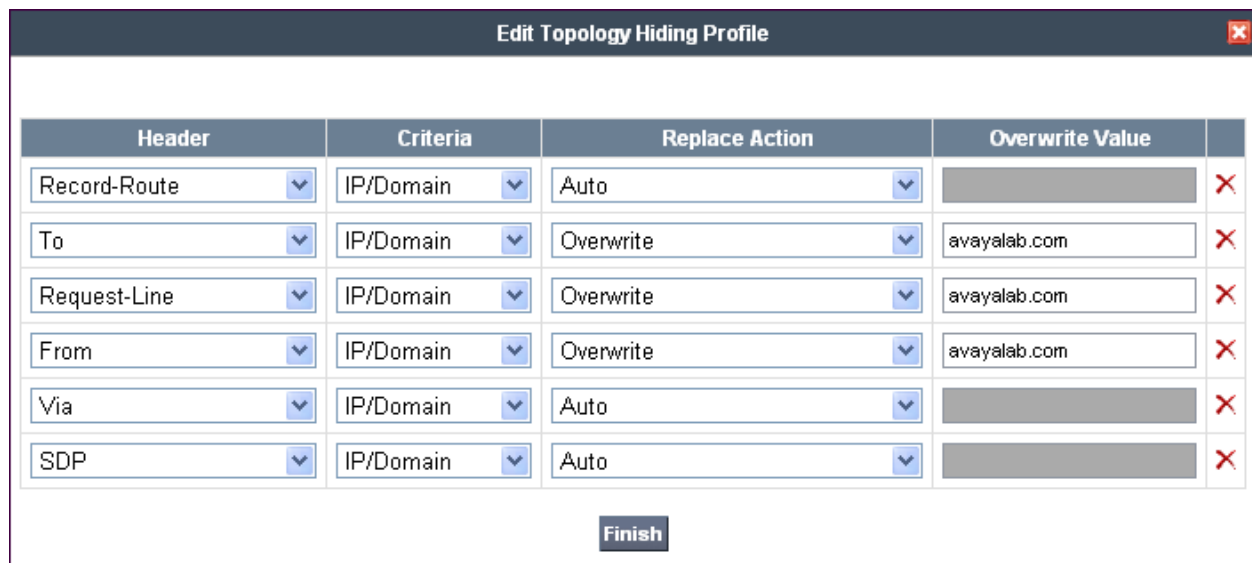
Enter a descriptive name for the new profile and click **Finish**.



The 'Clone Profile' dialog box has a title bar with a close button. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Enterprise'. Below these fields is a 'Finish' button.

Figure 52: Creating a Topology Hiding Profile for Enterprise

Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.2**) and the Communication Manager signaling group Far-end Domain (**Section 5.6**). Click **Finish** to save the changes.



The 'Edit Topology Hiding Profile' dialog box contains a table with the following data:

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

Below the table is a 'Finish' button.

Figure 53: Topology Hiding for Enterprise

It is not necessary to modify the **CenturyLink** profile from the default values. The following screen shows the Topology Hiding Policy created for CenturyLink.

[Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

CenturyLink

Topology Hiding

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

[Edit](#)

Figure 54: Topology Hiding for CenturyLink

When creating or editing Topology Hiding Profiles, there are six types of headers available for selection in the Header drop-down list to choose from. In addition to the six headers, there are additional headers not listed that are affected when either of two types of listed headers (e.g., **To Header** and **From Header**) are selected in the **Header** drop-down list. **Table 2** lists the six headers along with all of the other affected headers in three header categories (e.g., **Source Headers**, **Destination Headers**, and **SDP Headers**).

Topology Hiding Headers	
Main Header Names	Header(s) Affected by Main Header
Source Headers	
Record-Route	
From	(1) Referred-By (2) P-Asserted Identity
Via	
Destination Headers	
To	(1) ReferTo
Request-Line	
SDP Headers	
Origin Header	

Table 2: Topology Hiding Headers

7.1.3. Server Interworking Profile

The Server Interworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for **Enterprise** and **CenturyLink**.

7.1.3.1 Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown in **Figure 55**.



Figure 55: Server Interworking – Add Profile for Enterprise

Enter a descriptive name for the new profile and click **Next** to continue.

The screenshot shows a dialog box titled 'Interworking Profile'. It contains a 'Profile Name' text field with the value 'Enterprise' entered. Below the field is a 'Next' button.

Figure 56: Server Interworking – Profile Name for Enterprise

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Hold Support:** Select **RFC3264**.
- **T.38 Support:** Checked.

Click **Next** to continue.

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

Back **Next**

Figure 57: Server Interworking Enterprise - General

Default values can be used for the next window that appears. Click **Next** to continue.

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

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

Back **Next**

Figure 58: Server Interworking Enterprise - Privacy

Default values can be used for the next window that appears. Click **Next** to continue.

SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]

Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]

Back **Next**

Figure 59: Server Interworking Enterprise – SIP Timers

On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**
- **Has Remote SBC**

Click **Finish** to save changes.

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

Back **Finish**

Figure 60: Server Interworking Enterprise – Advanced Settings

7.1.3.2 Server Interworking Profile – CenturyLink

To create a new Server Interworking Profile for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown in **Figure 61**.

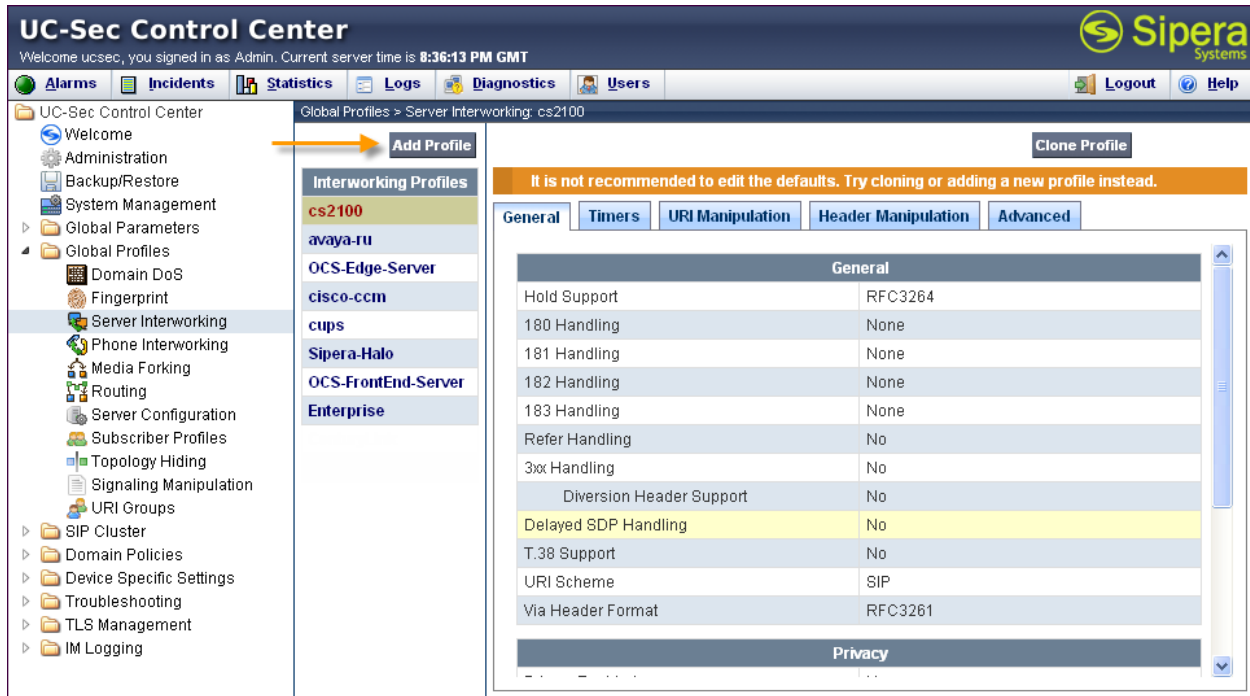


Figure 61: Server Interworking – Add Profile for CenturyLink

Enter a descriptive name for the new profile and click **Next** to continue.

The screenshot shows a dialog box titled 'Interworking Profile'. It has a 'Profile Name' label and a text input field containing 'CenturyLink'. Below the input field is a 'Next' button.

Figure 62: Server Interworking – Profile Name for CenturyLink

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Hold Support:** Select **RFC3264 - a=sendonly**.
- **T.38 Support:** Checked.

Click **Next** to continue.

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

Back **Next**

Figure 63: Server Interworking CenturyLink - General

Default values can be used for the next window that appears. Click **Next** to continue.

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

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

Back **Next**

Figure 64: Server Interworking CenturyLink - Privacy

Default values can be used for the next window that appears. Click **Next** to continue.

Configuration is not required. All fields are optional.

SIP Timers	
Min-SE	seconds, [90 - 86400]
Init Timer	milliseconds, [50 - 1000]
Max Timer	milliseconds, [200 - 8000]
Trans Expire	seconds, [1 - 64]
Invite Expire	seconds, [180 - 300]

Transport Timers	
TCP Connection Inactive Timer	seconds, [600 - 3600]

Back **Next**

Figure 65: Server Interworking CenturyLink – SIP Timers

On the **Advanced Settings** the default values can be used. Click **Finish** to save changes.

Interworking Profile

Advanced Settings

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

Back

Finish

Figure 66: Server Interworking CenturyLink – Advanced Settings

Create a URI Manipulation to remove the plus sign (+) Communication Manager places in the FROM, CONTACT, and P-Asserted Identity headers. Within the **CenturyLink** Profile, select the **URI Manipulation** tab and click **Add Regex**.

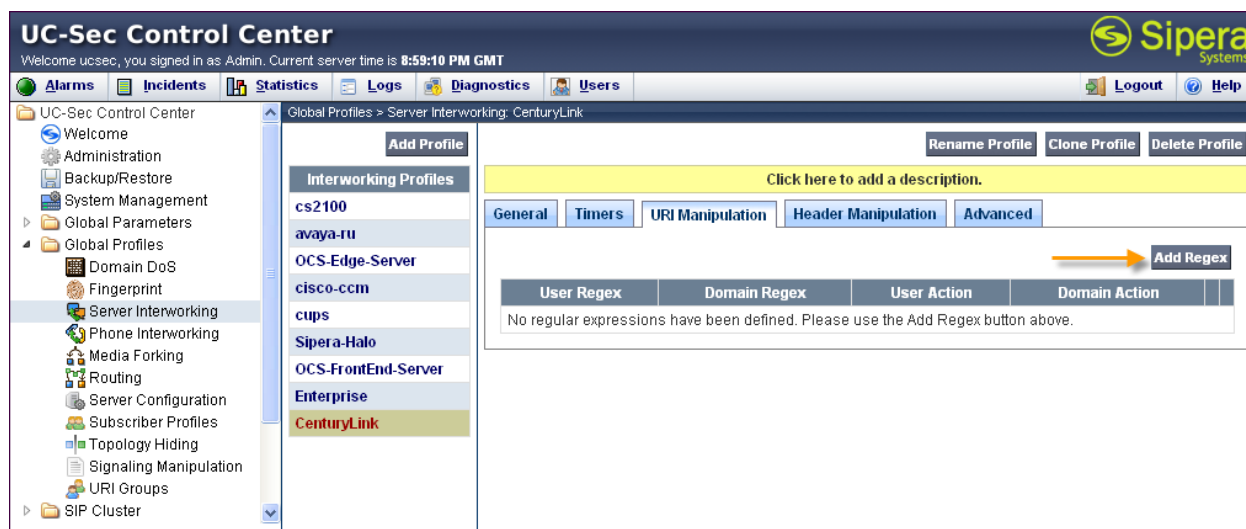


Figure 67: Server Interworking CenturyLink – Add Regex

The following screen is presented. In the **User Regex** field, enter a regular expression to match. In the sample configuration `\+.*` was entered. In this expression the backslash is used to escape the special meaning of “+” in a regular expression. The expression “`.*`” will match anything after the plus sign.

In the **User Action** field, select **Remove prefix [Value]**. In the **User Values** field enter `+`. Click **Finish** to save the configuration.

Add Regex ✕

URI Manipulation

Invalid or incorrectly entered regular expressions may cause unexpected results.

 Ex: [0-9]{3,5}\\\\user, (simple|advanced)\\\\-user[A-Z]{3}

When a URI [user@domain] matches the following:

User Regex	<input style="width: 90%;" type="text" value="\\+.*"/> <small>(Blank is wildcard)</small>
Domain Regex	<input style="width: 90%;" type="text"/> <small>(Blank is wildcard)</small>

Do this with the user section:

User Action	<input style="width: 90%;" type="text" value="Remove prefix [Value]"/>
User Values	<input style="width: 30%;" type="text" value="+"/> <input style="width: 60%;" type="text"/>

Do this with the domain section:

Domain Action	<input style="width: 90%;" type="text" value="None"/>
Domain Values	<input style="width: 30%;" type="text"/> <input style="width: 60%;" type="text"/>

Figure 68: Server Interworking CenturyLink – URI Manipulation

The following screen shows the completed URI Manipulation for CenturyLink.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 5:20:36 PM GMT

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

[Logout](#) [Help](#)

- UC-Sec Control Center
- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Subscriber Profiles
 - Topology Hiding
 - Signaling Manipulation
 - URI Groups

Global Profiles > Server Interworking: CenturyLink

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

User Regex	Domain Regex	User Action	Domain Action
\\+.*		Remove prefix +	None

Figure 69: Server Interworking CenturyLink – URI Manipulation Completed

DDT; Reviewed:
SPOC 5/6/2013

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

56 of 91
CLCM601SM61Sipe

7.1.4. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a 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 E-SBC. Using this language, a script can be written and tied to a given flow through the Element Management System (EMS) GUI. The E-SBC appliance then interprets this script at the given entry point or “hook point”.

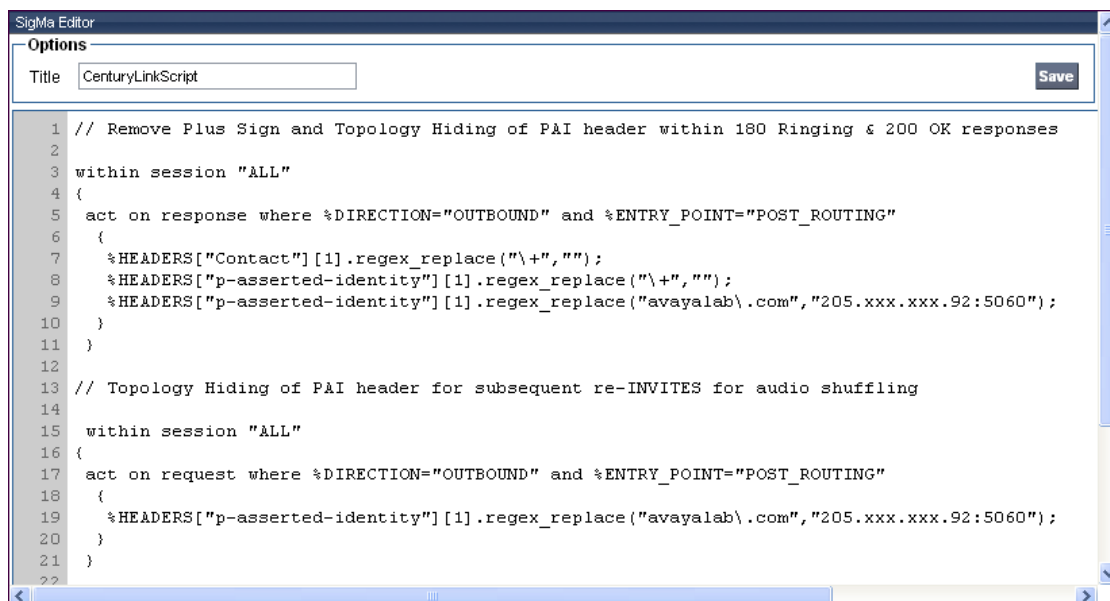
These application notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and the removal of the plus sign (+) added by Communication Manager in SIP response messages. Although an URI Manipulation was created in the Interworking Profiles for CenturyLink to remove the plus sign (**Figure 67**), the plus sign was not removed from response messages. This did not affect interoperability with Centurylink, however a script was added to remove the plus sign to keep the response SIP messages consistent with requests.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will pop up.

The following sample script is written in two sections. Each section begins with a comment describing what will take place in that portion of the script. The first section will act on the response of an inbound call from CenturyLink (e.g., 180 Ringing and 200 OK) while the second acts on the request of an outbound call to CenturyLink (e.g., re-INVITE messages from Communication Manager for audio shuffling). The script is further broken down as follows:

- **within session “ALL”** Transformations applied to all SIP sessions.
- **act on response** Actions to be taken to the response of an INVITE (e.g., 180 Ringing and 200 OK).
- **%DIRECTION=“OUTBOUND”** Applied to a messages leaving the Avaya SBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has routed through Avaya SBCE.
- **%HEADERS[“Contact”][1]** Used to retrieve an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.
- **.regex_replace(“\+”,“”);** An action to replace a given match with the provide string (e.g., find “+” and replace it with nothing).

The Contact and P-Asserted Identity (PAI) headers will be modified by replacing the plus sign (+) with nothing. The PAI header will be further modified by replacing the domain “avayalab.com” with the external IP address of the Avaya SBCE and the SIP port of 5060 in both the response and request sessions.



```

1 // Remove Plus Sign and Topology Hiding of PAI header within 180 Ringing & 200 OK responses
2
3 within session "ALL"
4 {
5   act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
6   {
7     %HEADERS["Contact"][1].regex_replace("\+", "");
8     %HEADERS["p-asserted-identity"][1].regex_replace("\+", "");
9     %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com", "205.xxx.xxx.92:5060");
10  }
11 }
12
13 // Topology Hiding of PAI header for subsequent re-INVITES for audio shuffling
14
15 within session "ALL"
16 {
17   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
18   {
19     %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com", "205.xxx.xxx.92:5060");
20   }
21 }
22

```

Figure 70: SigMa Editor

The following screen shows the finished Signaling Manipulation Script **CenturyLinkScript**.

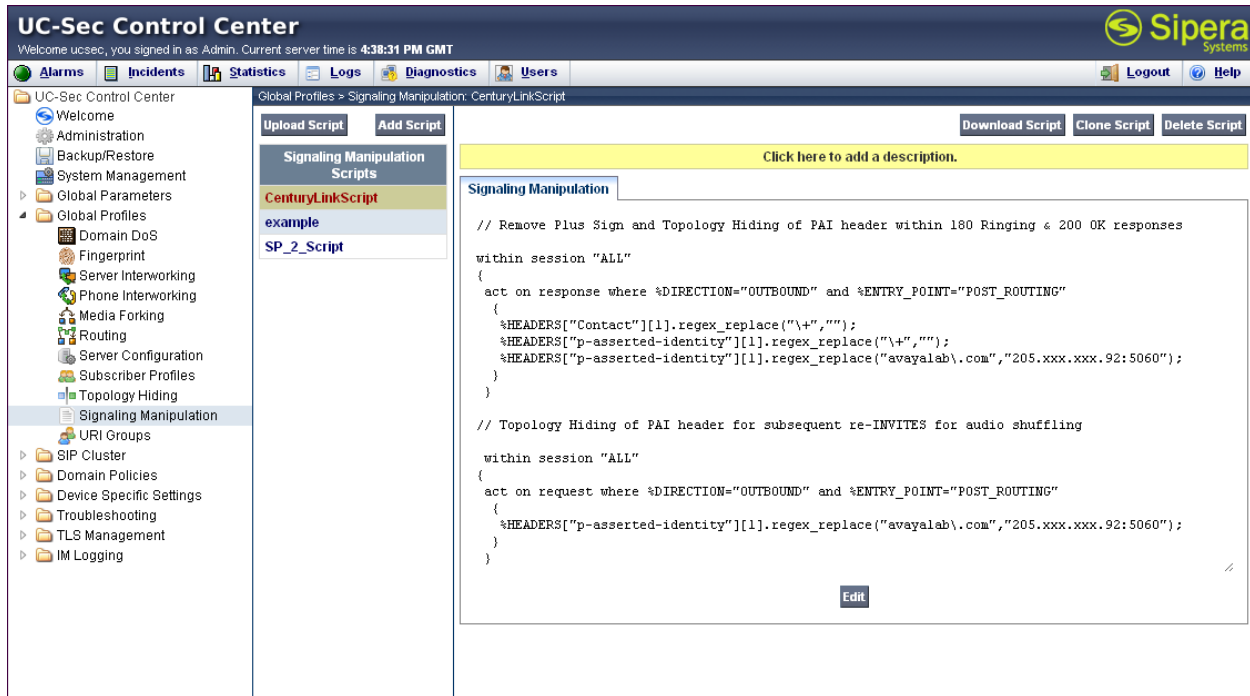


Figure 71: CenturyLink Signaling Manipulation Script

7.1.5. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs 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.

In the sample configuration, separate Server Configurations were created for **Session_Manager** and **CenturyLink**.

7.1.5.1 Server Configuration – Session_Manager

To add a Server Configuration Profile for Session Manger navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** as shown in **Figure 72**.

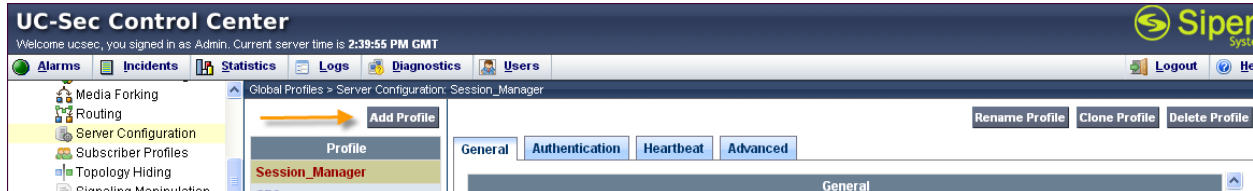


Figure 72: Server Configuration Add Profile

Enter a descriptive name for the new profile and click **Next**.

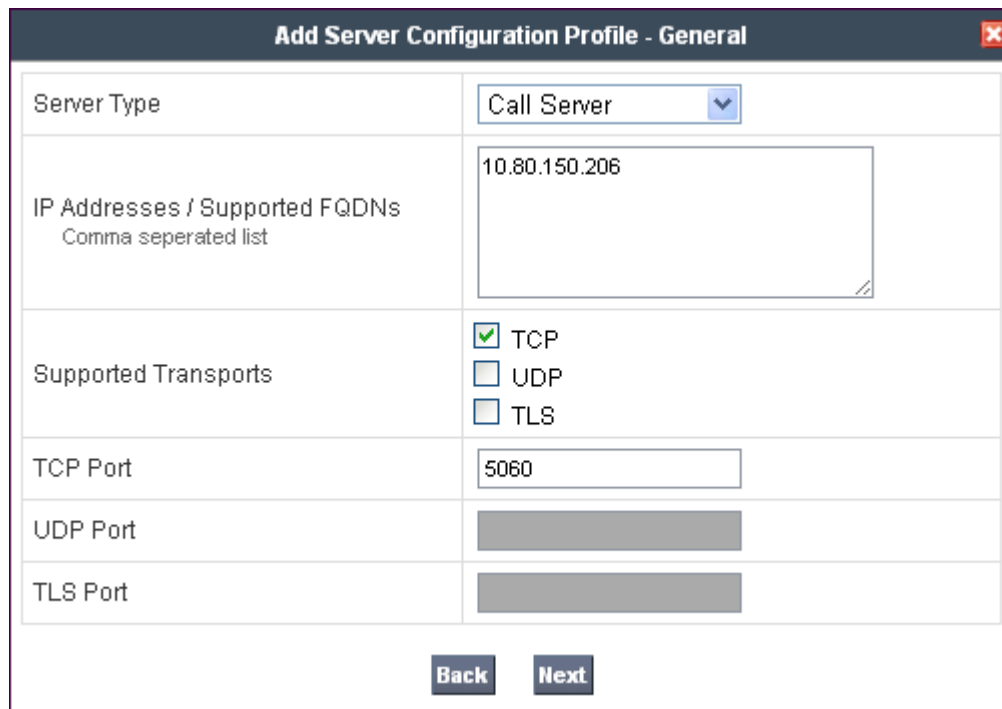
The screenshot shows a modal dialog box titled 'Add Server Configuration Profile'. It contains a text input field labeled 'Profile Name' with the text 'Session_Manager' entered. Below the input field is a 'Next' button.

Figure 73: Server Configuration – Profile Name Session Manager

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module in **Section 6.8**.
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link on Session Manager in **Section 6.5**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link on Session Manager in **Section 6.5**.

Click **Next** to continue.



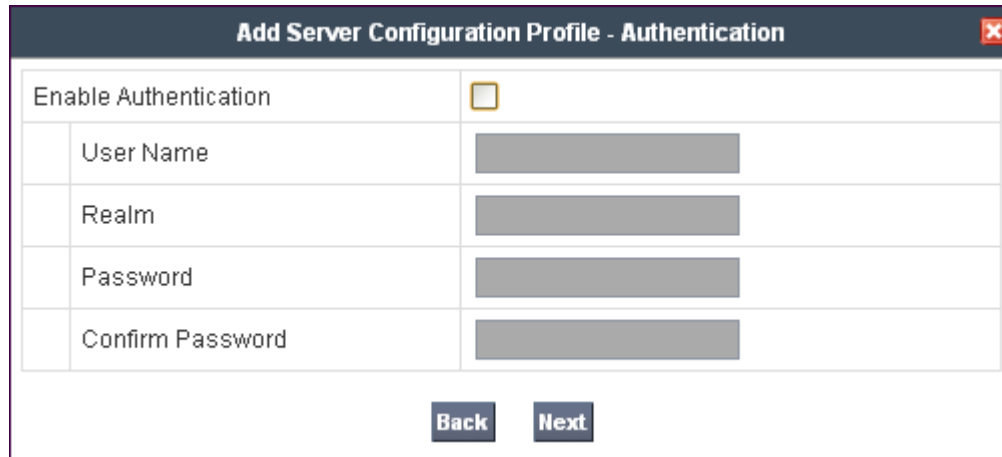
The screenshot shows a window titled "Add Server Configuration Profile - General". It contains the following fields and controls:

Server Type	Call Server (dropdown)
IP Addresses / Supported FQDNs <small>Comma seperated list</small>	10.80.150.206
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	(disabled field)
TLS Port	(disabled field)

At the bottom are "Back" and "Next" buttons.

Figure 74: Server Configuration –Session Manager General

Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.



Add Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

Back Next

Figure 75: Server Configuration – Session Manager Authentication

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Figure 76: Server Configuration – Session Manager Heartbeat

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.1.3.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.

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

Figure 77: Server Configuration – Session Manager Advanced

7.1.5.2 Server Configuration - CenturyLink

For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound. Separate Server Configuration Profiles were created for the Primary and Secondary inbound and outbound IP addresses. A third Server Configuration Profile was created for the inbound only IP addresses.

To add Server Configuration Profiles for CenturyLink navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** as shown in **Figure 72**. Enter a descriptive name for the new profile and click **Next**.

Add Server Configuration Profile

Profile Name: CL-Primary

Next

Figure 78: Server Configuration – Profile Name CL-Primary

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the SIP proxy of the service provider. In the sample configuration, this is 192.168.33.8 for the Primary server and 192.168.32.8 for the Secondary server. This will associate the inbound SIP messages from CenturyLink's SIP server to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and CenturyLink.
- **TCP Port:** Enter the port number that CenturyLink uses to send SIP traffic.

Click **Next** to continue.

Add Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Comma seperated list: 192.168.33.8

Supported Transports: ☐ TCP, ☒ UDP, ☐ TLS

TCP Port: [Empty field]

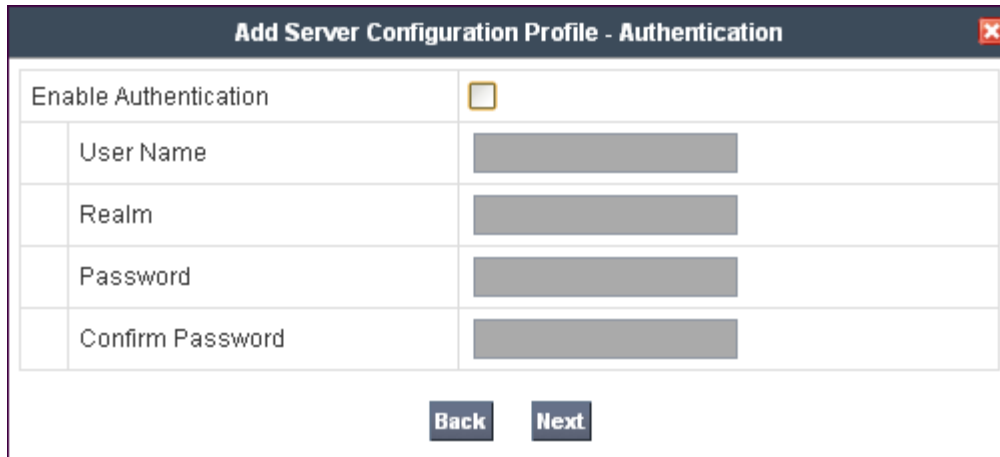
UDP Port: 5060

TLS Port: [Empty field]

Back Next

Figure 79: Server Configuration – CL-Primary General

Verify **Enable Authentication** is unchecked as CenturyLink does not require authentication. Click **Next** to continue.



Add Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

Back Next

Figure 80: Server Configuration – CL-Primary Authentication

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

The SIP OPTIONS are sent to the SIP server entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile** as show previously in **Figure 79**. The URI of PING@centurylink.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. CenturyLink does not look at the From and To headers when replying to SIP OPTIONS so any URI can be used as long as it is in the proper format (USER@DOMAIN).

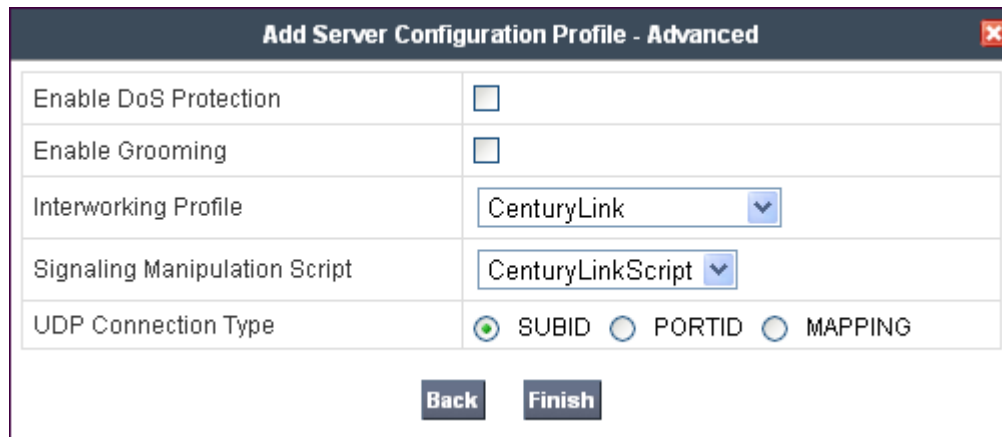
Add Server Configuration Profile - Heartbeat

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS <input type="button" value="v"/>
Frequency	60 seconds
From URI	PING@centurylink.com
To URI	PING@centurylink.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Back
Next

Figure 81: Server Configuration – CL-Primary Heartbeat

In the new window that appears, select the Interworking Profile created for CenturyLink in **Section 7.1.3.2**. Select the Signaling Manipulation Script created in **Section 7.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration.



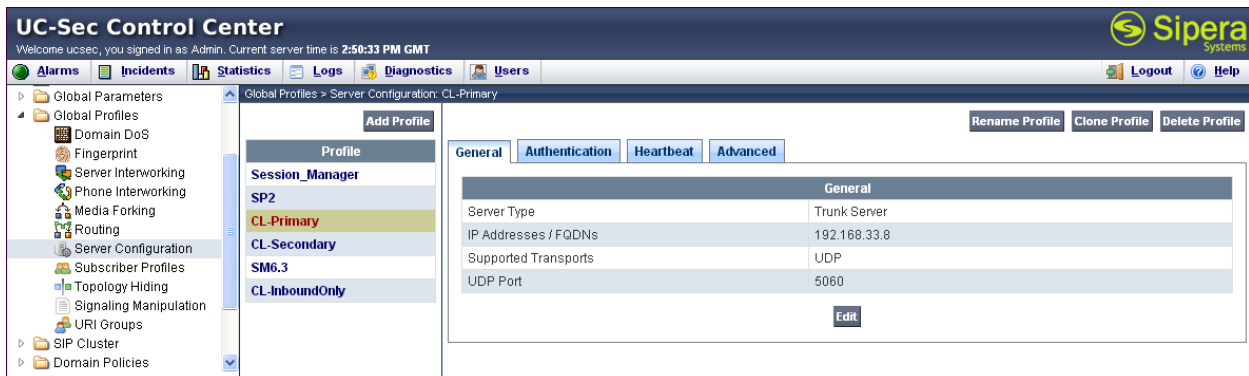
The dialog box titled "Add Server Configuration Profile - Advanced" contains the following fields:

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

At the bottom are "Back" and "Finish" buttons.

Figure 82: Server Configuration – CL-Primary Advanced

Once configuration is completed, the **CL-Primary** server configuration profile will appear as follows.



The UC-Sec Control Center interface shows the "Global Profiles > Server Configuration: CL-Primary" page. The left sidebar lists various configuration categories, with "Server Configuration" selected. The main area displays the "CL-Primary" profile under the "Session_Manager" section. The "General" tab is active, showing the following details:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.33.8
Supported Transports	UDP
UDP Port	5060

Buttons for "Add Profile", "Rename Profile", "Clone Profile", "Delete Profile", and "Edit" are visible.

Figure 83: Server Configuration – CL-Primary Complete

Repeat these procedures to create a separate server configuration for the secondary IP address for CenturyLink. Once configuration is completed, the **CL-Secondary** server configuration profile will appear as follows.

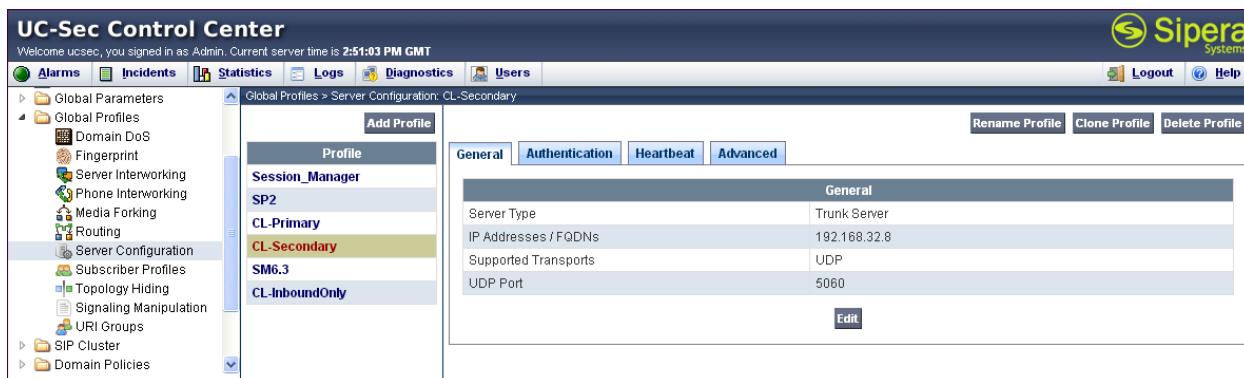


Figure 84: Server Configuration – CL-Secondary Complete

The inbound only IP addresses can be placed into one server configuration profile with the Heartbeat disabled as shown in **Figure 85** and **Figure 86**.

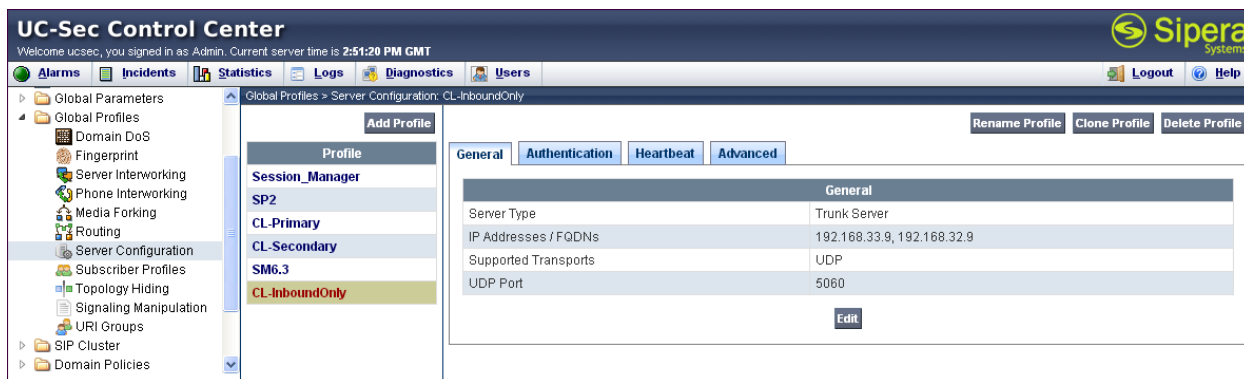


Figure 85: Server Configuration – CL-InboundOnly General

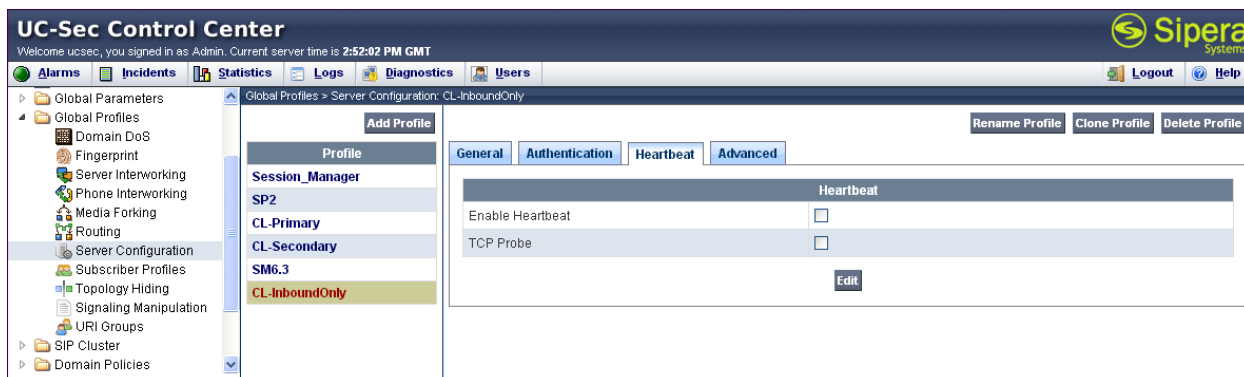


Figure 86: Server Configuration – CL-InboundOnly Heartbeat

7.2. Domain Policies

The Domain Policies feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in 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 flows. There are default policies available to use, or a custom domain policy can be created.

7.2.1. Media Rule

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 packets matching these criteria will be handled by the UC-Sec security product.

Create a custom Media Rule to set the Quality of Service and Media Anomaly Detection. The sample configuration shows a default Media Rule was used for CenturyLink and a custom Media Rule **Internal-media** was created for the enterprise.

To create a custom Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown in **Figure 87**.

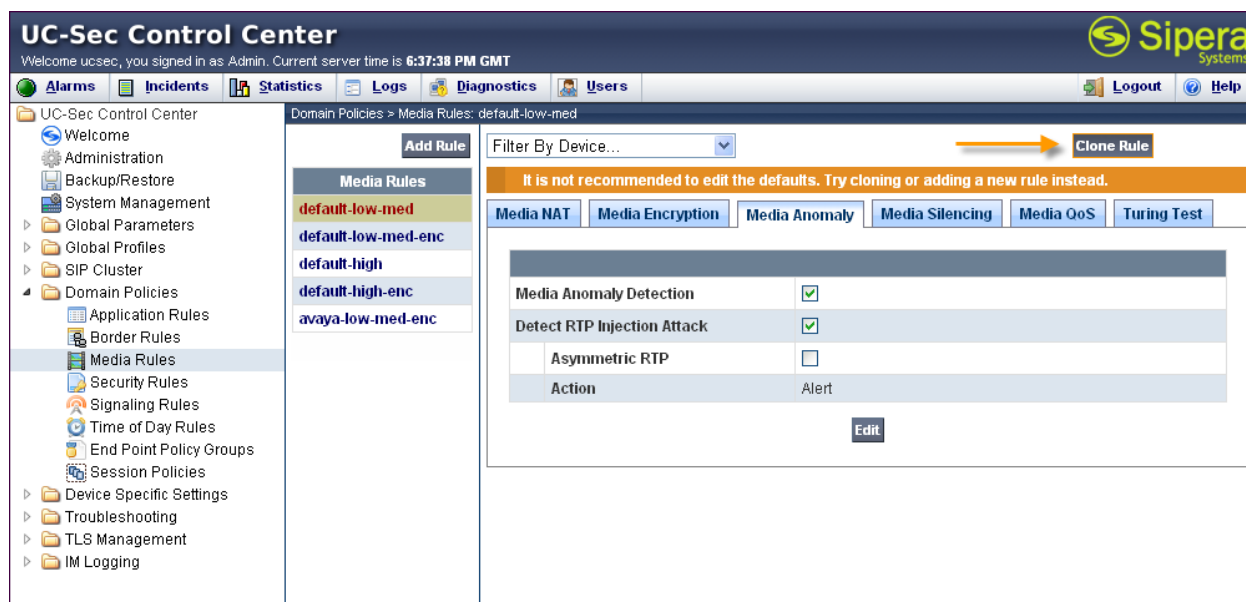
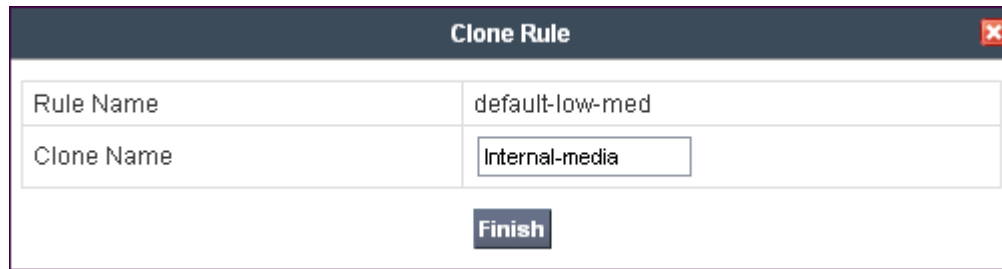


Figure 87: Media Rule Clone Rule

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



A dialog box titled "Clone Rule" with a close button (X) in the top right corner. It contains two input fields: "Rule Name" with the value "default-low-med" and "Clone Name" with the value "Internal-media". Below the fields is a "Finish" button.

Figure 88: Creating a Media Rule

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the RTP Injection Attack alerts from being created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**. Uncheck **Media Anomaly Detection** and click **Finish** (not shown).

The following screen shows the **Internal-media** rule with **Media Anomaly Detection** disabled.

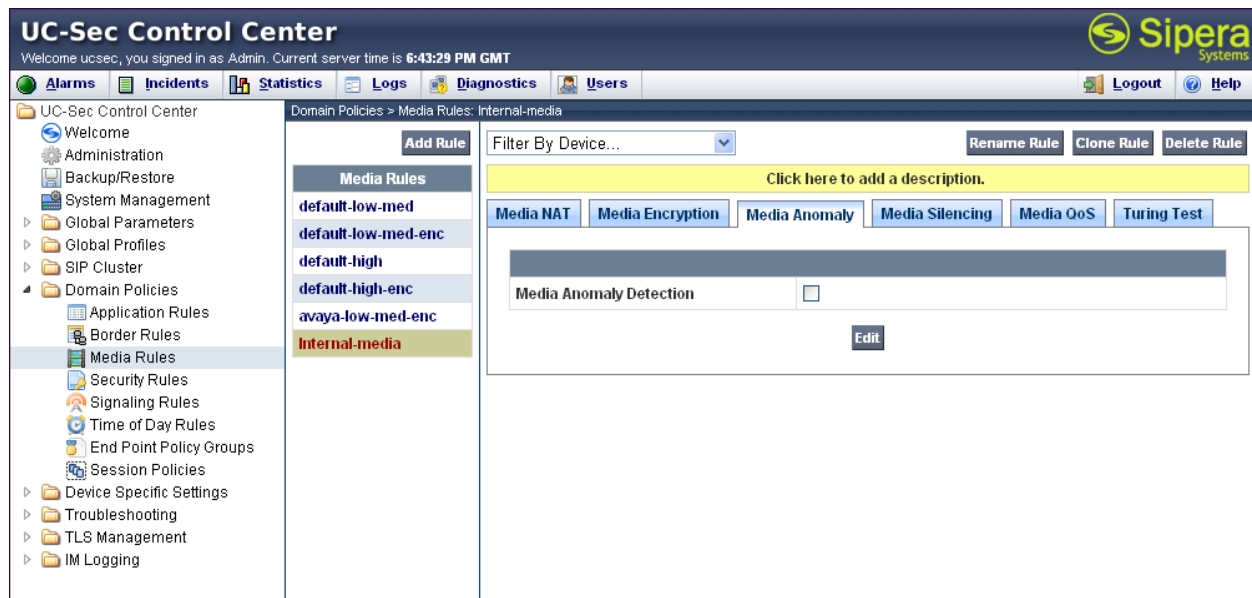


Figure 89: Internal Media Rule Media Anomaly

On the **Media 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 the media. The following screen shows the QoS values used for compliance testing.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Domain Policies' expanded and 'Media Rules' selected. The main content area shows the configuration for the 'Internal-media' rule. The 'Media QoS' tab is active, showing settings for Media QoS Reporting, Media QoS Marking, Audio QoS, and Video QoS.

Media QoS Reporting	
RTCP Enabled	<input type="checkbox"/>

Media QoS Marking	
Enabled	<input checked="" type="checkbox"/>
QoS Type	DSCP

Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF

[Edit](#)

Figure 90: Internal Media Rule QoS

7.2.2. Signaling Rule

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.

Clone and modify the default signaling rule to strip the P-Location and Alert Info headers from the SIP message before it is sent to the CenturyLink SIP Trunk. To clone a signaling rule, navigate to **UC-Sec Control Center** → **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown **Figure 91**.

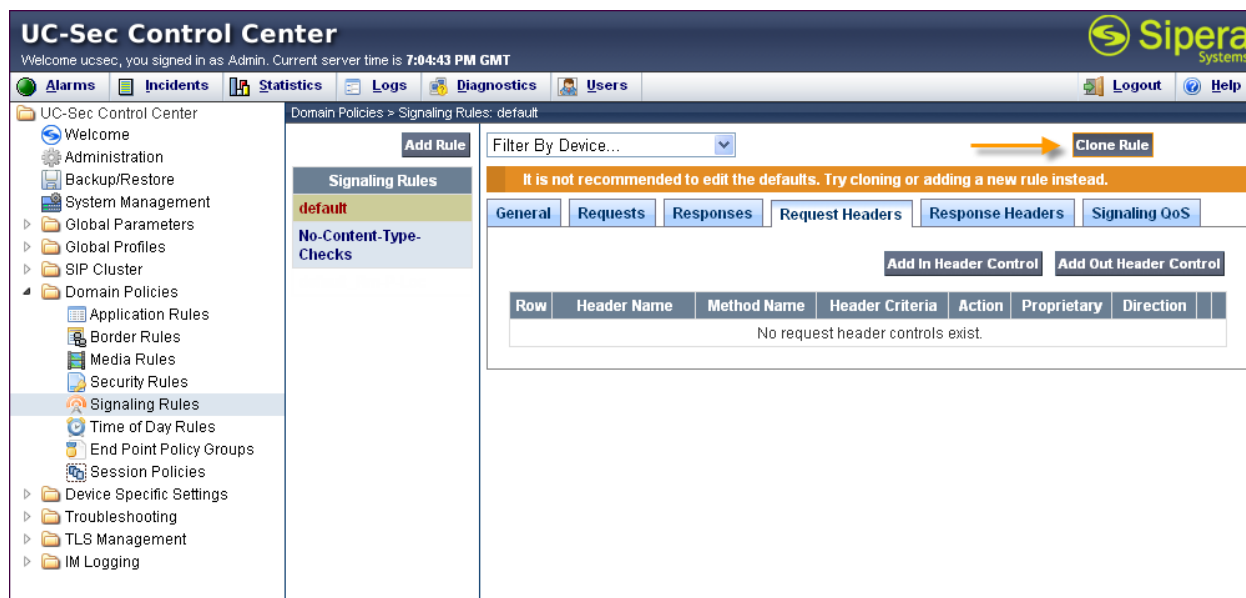


Figure 91: Signaling Rule Clone Rule

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

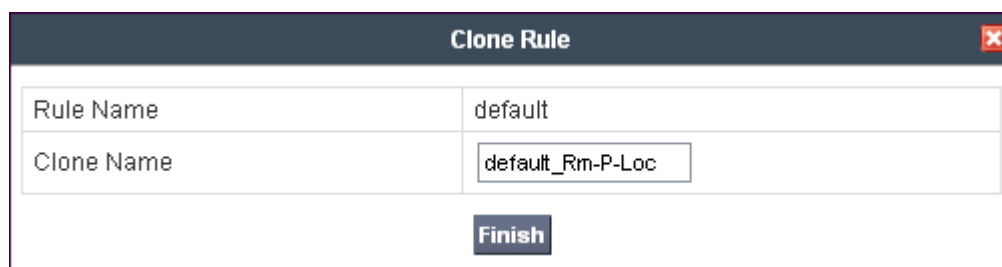


Figure 92: Creating a Signaling Rule

Select the **Request Headers** tab and click **Add In Header Control** (not shown). In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Proprietary Request Header?:** Checked.
- **Header Name:** Enter **P-Location**.
- **Method Name:** Select **INVITE** from the drop-down box.
- **Header Criteria:** Select **Forbidden**.
- **Presence Action:** Select **Remove header** from the drop-down box.

Click **Finish** to save the configuration

Edit Header Control

Proprietary Request Header? ☒

Header Name: P-Location

Method Name: INVITE

Header Criteria: ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action: Remove header 486 Busy Here

Finish

Figure 93: Editing a Signaling Rule

Next, remove the header in the **Response Headers** tab. Repeat these steps for the **Alert-Info** and other headers wished to be removed. The following screen shows the **default_Rm-P-Loc** rule used in the sample configuration with the **P-Location** and **Alert-Info** headers configured to be removed.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 7:13:51 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Domain Policies > Signaling Rules: default_Rm-P-Loc

Add Rule

Filter By Device...

Signaling Rules

default

No-Content-Type-Checks

default_Rm-P-Loc

Click here to add a description.

General Requests Responses Request Headers Response Headers Signaling QoS

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	INVITE	Forbidden	Remove Header	No	IN		
2	P-Location	INVITE	Forbidden	Remove Header	Yes	IN		

Figure 94: Signaling Rule Request Headers

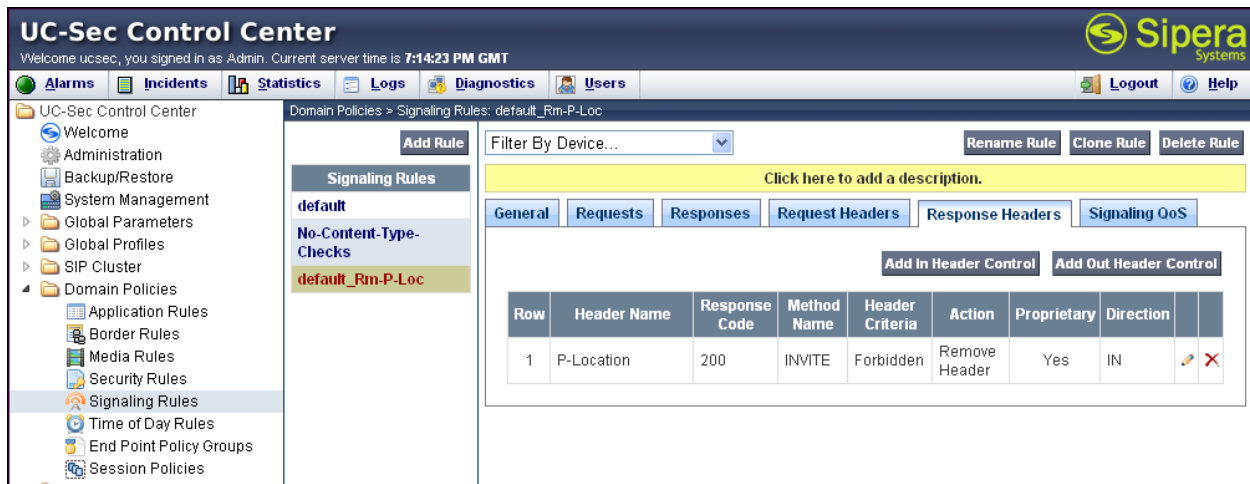


Figure 95: Signaling Rule Response Headers

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 values used for compliance testing.

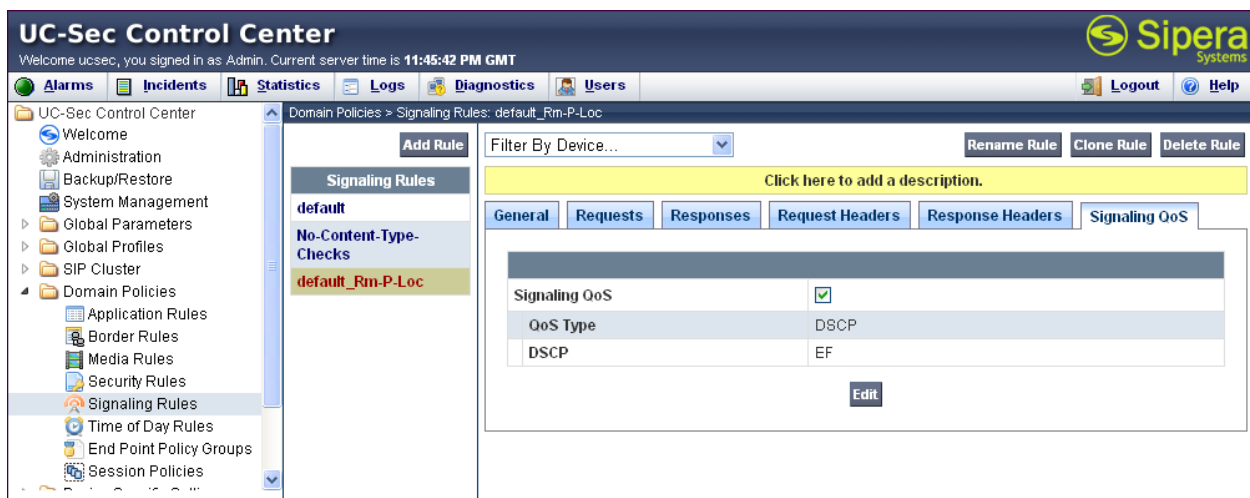


Figure 96: Signaling Rule QoS

7.2.3. Application Rule

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, one can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Create an Application Rule to increase the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Sessions** 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** as shown in **Figure 97**.

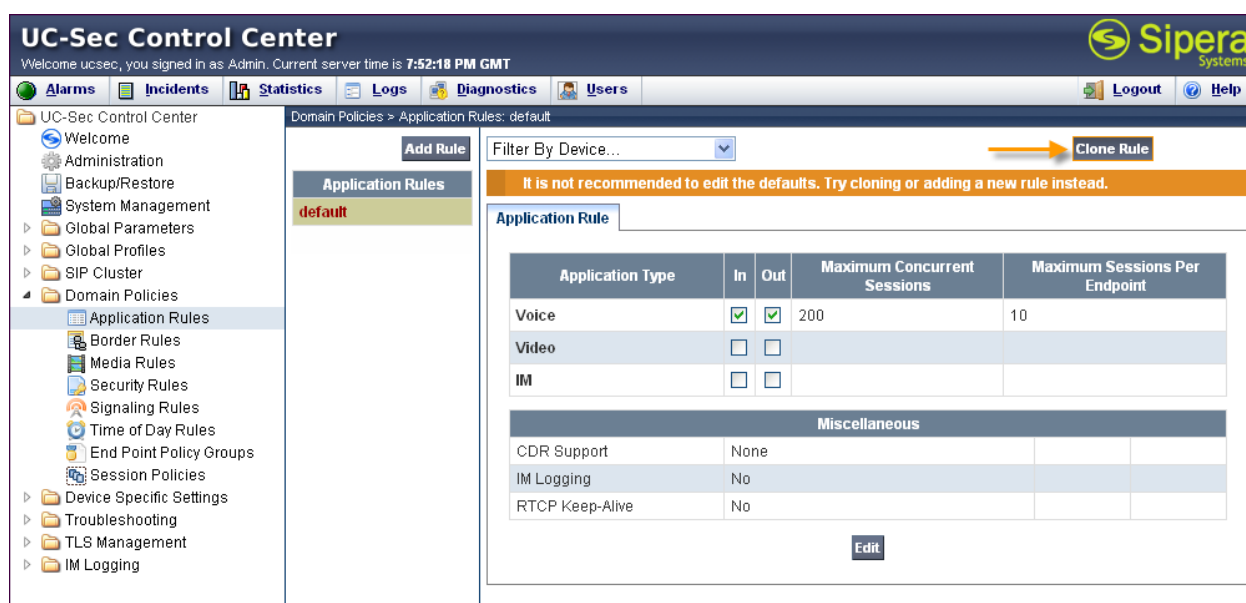


Figure 97: Application Rule Clone Rule

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

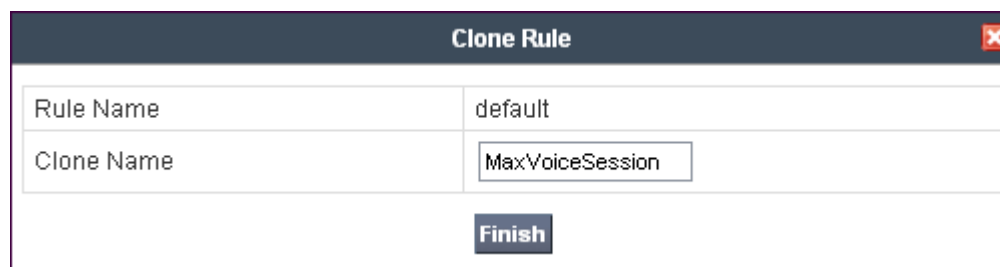


Figure 98: Creating an Application Rule

Edit the rule by clicking the **Edit** button as shown in **Figure 99**. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. Set the values high enough for the amount of traffic the network is able process. Keep in mind the Avaya SBCE takes 30 seconds for sessions to be cleared after disconnect.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, SIP Cluster, and Domain Policies. The 'Domain Policies' section is expanded, showing 'Application Rules' as the selected item. The main content area displays the configuration for the 'MaxVoiceSession' rule. At the top, there are buttons for 'Add Rule', 'Filter By Device...', 'Rename Rule', 'Clone Rule', and 'Delete Rule'. Below these is a yellow box with the text 'Click here to add a description.' The main configuration area is titled 'Application Rule' and contains a table with columns for 'Application Type', 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The table has three rows: 'Voice', 'Video', and 'IM'. The 'Voice' row has checkboxes for 'In' and 'Out' both checked, and values of 2000 for both session limits. The 'Video' and 'IM' rows have unchecked checkboxes and empty session limit fields. Below the table is a 'Miscellaneous' section with a table for 'CDR Support', 'IM Logging', and 'RTCP Keep-Alive'. The 'CDR Support' row has a value of 'None'. The 'IM Logging' and 'RTCP Keep-Alive' rows have a value of 'No'. An 'Edit' button is located at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous			
CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

Figure 99: Application Rule

7.2.4. Endpoint Policy Group

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 in **Section 7.3.4**. Create a separate Endpoint Policy Group for the enterprise and the CenturyLink SIP Trunk.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → End Point Policy Groups** and click on **Add Group** as shown in **Figure 100**.

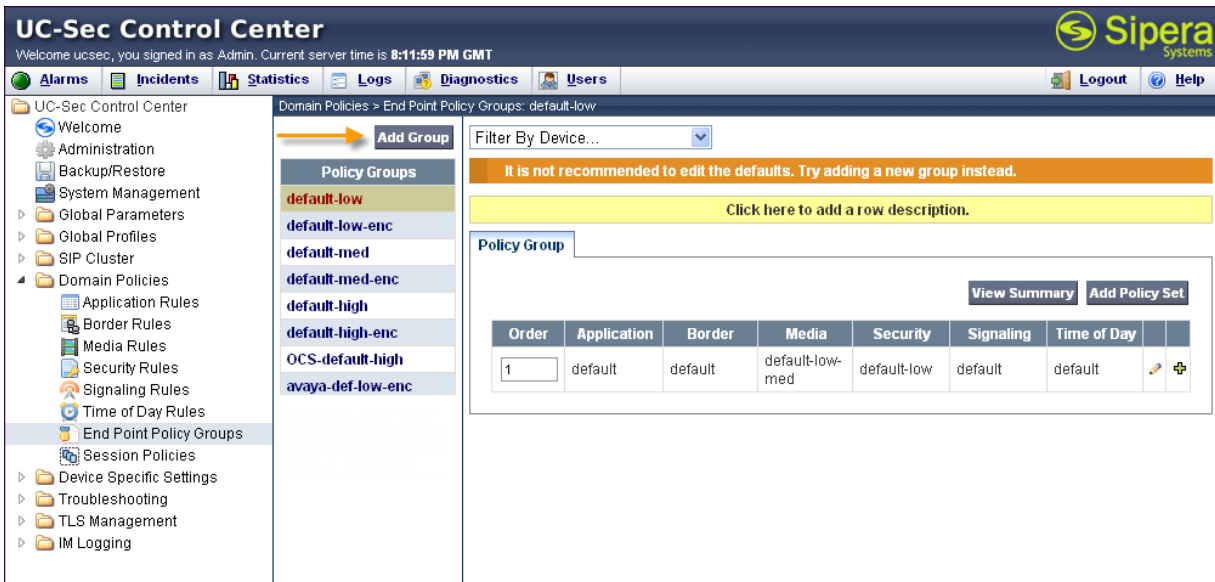


Figure 100: End Point Policy Group Add Group

The following screen shows **Enterprise_DomPolicy** created for the enterprise. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, **Security** and **Time of Day** rules to **default** or **default-low**.

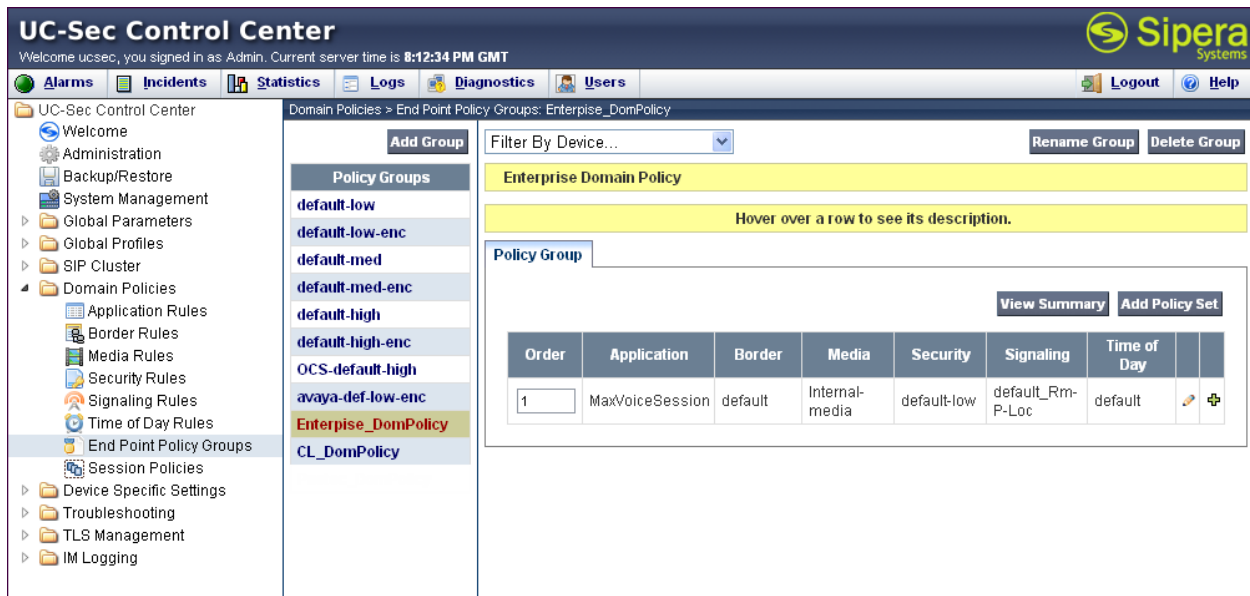


Figure 101: End Point Policy Group for Enterprise

The following screen shows **CL_DomPolicy** created for CenturyLink SIP Trunk. Set the **Application** rule to the one previously created. Set the **Border**, **Media**, **Security**, **Signaling** and **Time of Day** rules to **default** or **default-high**.

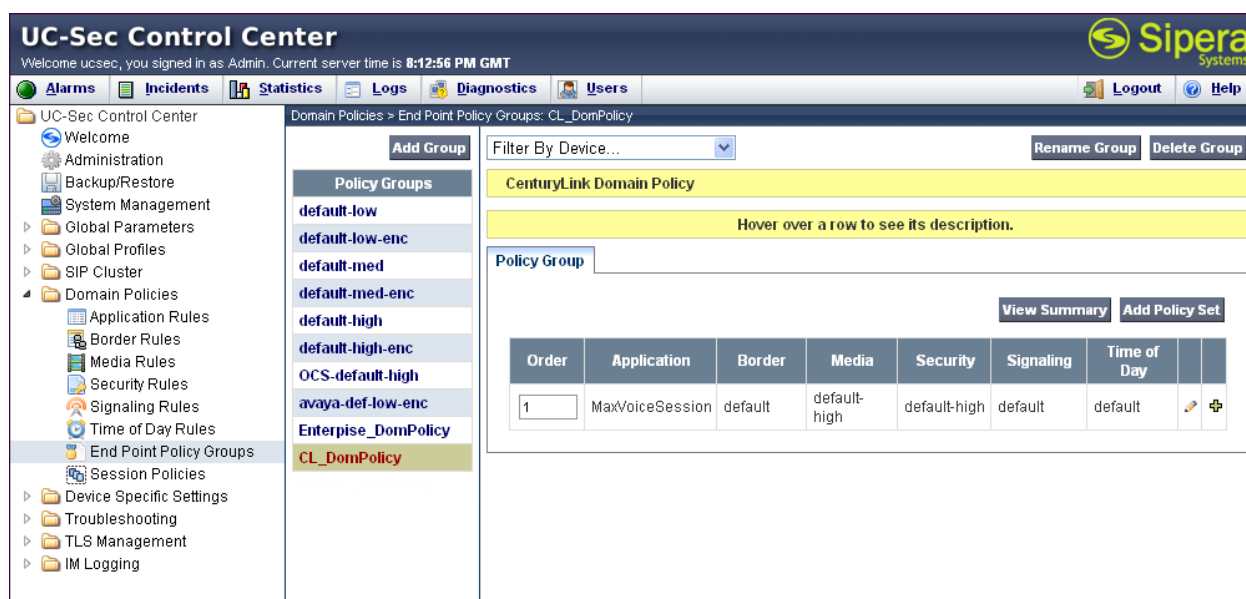


Figure 102: End Point Policy Group for CenturyLink

7.3. Device Specific Settings

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

7.3.1. Network Management

The 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 is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Network Management** and 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 external interface is assigned to **B1**.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 8:22:48 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

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

Device Specific Settings > Network Management: Sipera

UC-Sec Devices
Sipera

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.128 B2 Netmask

Add IP Changes will not take effect until the interface is updated. Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
10.80.150.100		10.80.150.1	A1
205.xxx.xxx.92		205.xxx.xxx.1	B1

Figure 103: Network Management Network Configuration

The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click its **Toggle State** button.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 8:23:21 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

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

Device Specific Settings > Network Management: Sipera

UC-Sec Devices
Sipera

Network Configuration Interface Configuration

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

Figure 104: Network Management Interface Configuration

7.3.2. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Signaling Interface** and click **Add Signaling Interface**.

The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

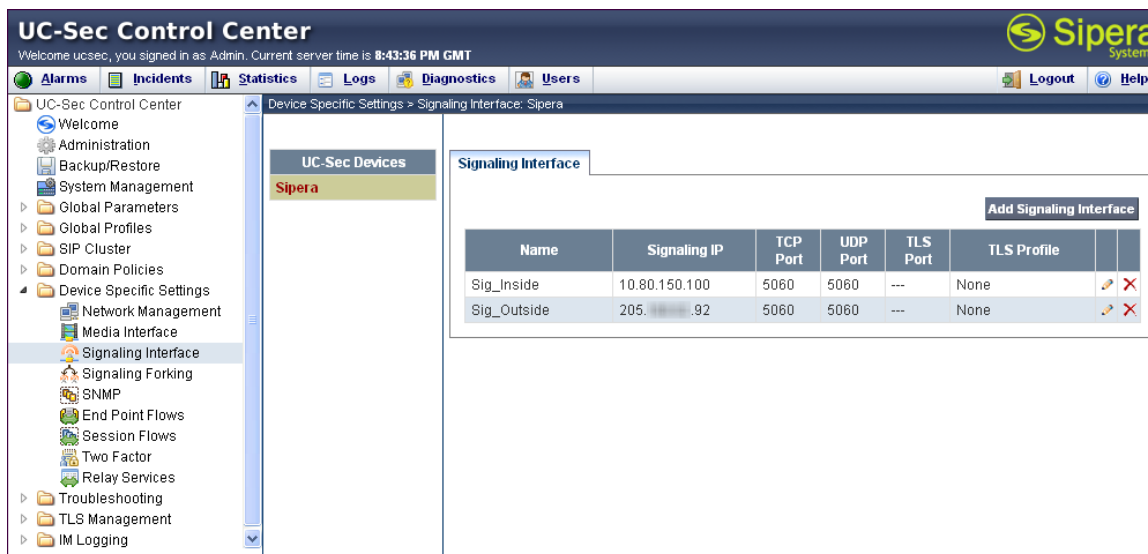


Figure 105: Signaling Interfaces

7.3.3. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will listen for SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces. The inside port range needs to match the **UDP Port Min** and **UDP Port Max** fields in the Communication Manager IP network Region created in **Section 5.6**. The outside port range should match the RTP port range provided by CenturyLink.

To create a new Signaling Interface, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Media Interface** and click **Add Media Interface**.

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces. After the media interfaces are created, an application restart is necessary before the changes will take effect.

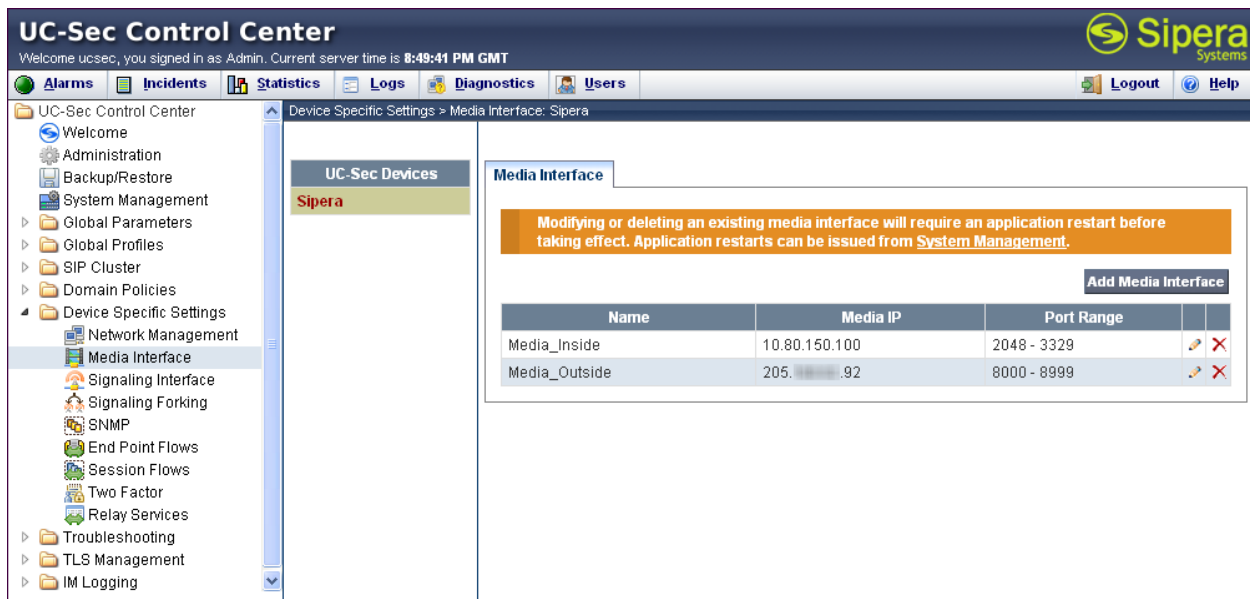


Figure 106: Media Interface

7.3.4. 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.

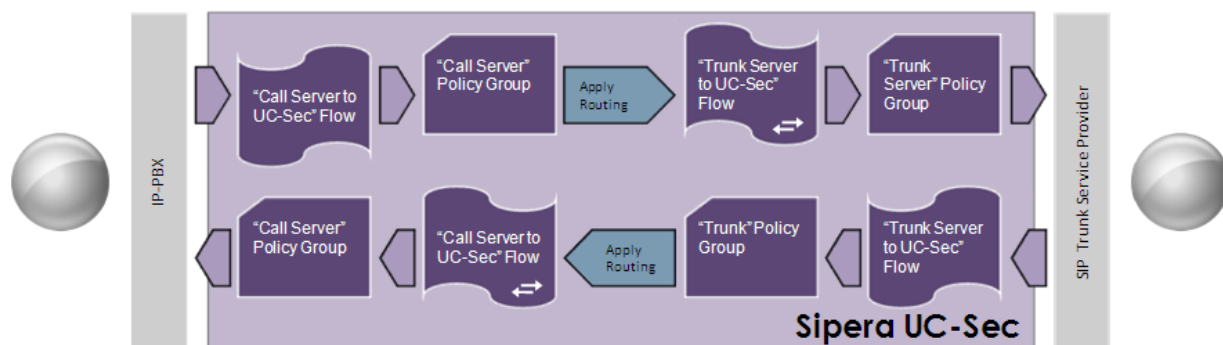


Figure 107: Avaya SBCE Call Flow

Create a Server Flow for Session Manager and the Centurylink SIP Trunk. 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** as shown in **Figure 108**.

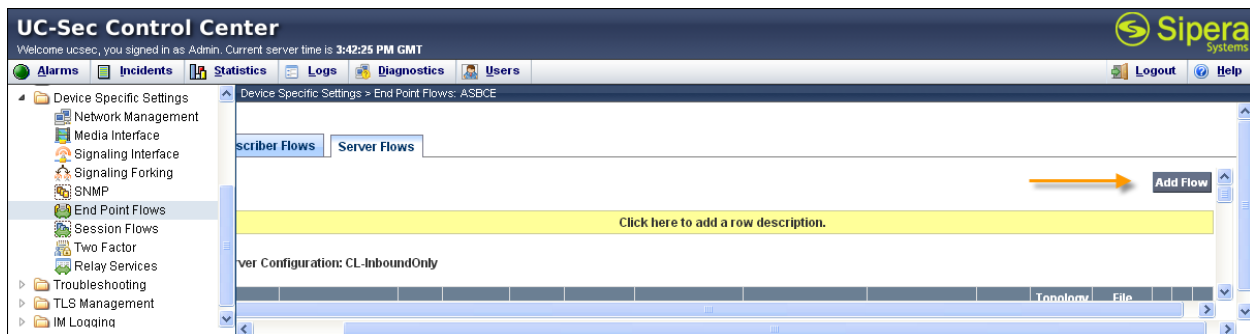


Figure 108: Add a Server Flow

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.1.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the Server Flow for CL-Primary:

The screenshot shows a window titled "Edit Flow: CenturyLink_Flow" with a "Criteria" section. The criteria are as follows:

Criteria	
Flow Name	CL-Primary-Flow
Server Configuration	CL-Primary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_SessionMgr
Topology Hiding Profile	CenturyLink
File Transfer Profile	None

At the bottom of the criteria section is a "Finish" button.

Figure 109: Server Flow for CL-Primary

The following screen shows the Server Flow for CL-Secondary:

The screenshot shows a window titled "Edit Flow: CenturyLink_Flow" with a "Criteria" section. The criteria are as follows:

Criteria	
Flow Name	CL-Secondary-Flow
Server Configuration	CL-Secondary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_SessionMgr
Topology Hiding Profile	CenturyLink
File Transfer Profile	None

At the bottom of the criteria section is a "Finish" button.

Figure 110: Server Flow for CL-Secondary

The following screen shows the Server Flow for CL-InboundOnly-Flow:

Criteria	
Flow Name	CL-InboundOnly-Flow
Server Configuration	CL-InboundOnly
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_SessionMgr
Topology Hiding Profile	CenturyLink
File Transfer Profile	None

Finish

Figure 111: Server Flow for CL-Secondary

The following screen shows the Server Flow for Session Manager:

Criteria	
Flow Name	Session_Manager_Flow
Server Configuration	Session_Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside
Signaling Interface	Sig_Inside
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy
Routing Profile	Route_to_CenturyLink
Topology Hiding Profile	Enterprise
File Transfer Profile	None

Finish

Figure 112: Server Flow for Session Manager

8. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk Service, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at www.centurylink.com and requesting information via the online sales links or telephone numbers.

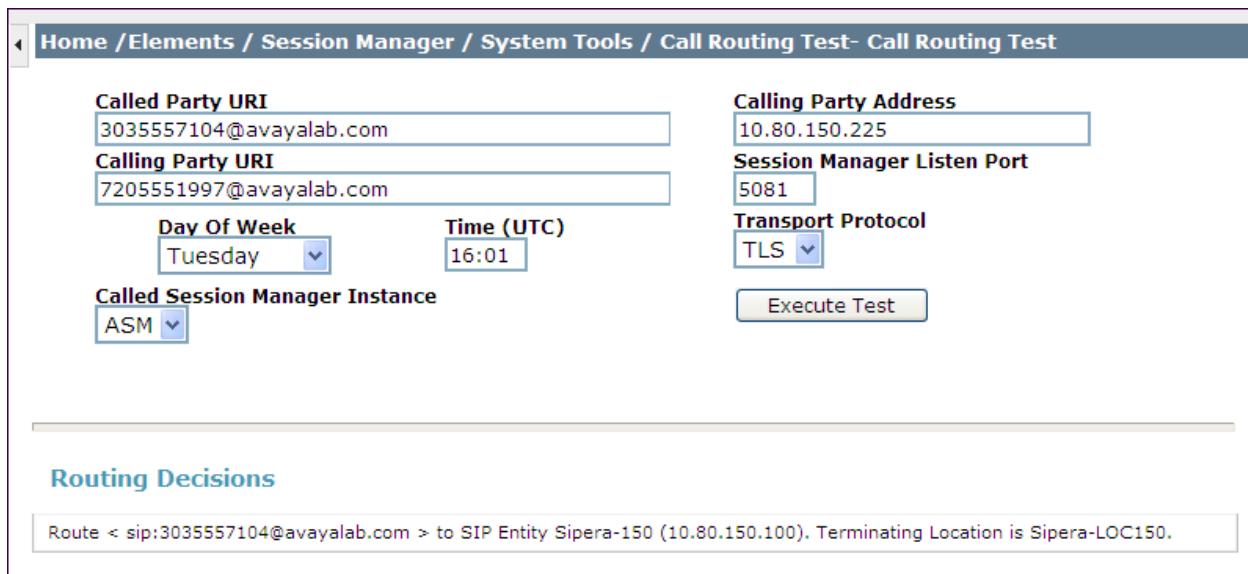
9. Verification and Troubleshooting

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 that can be used to troubleshoot the solution.

9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows a call routing test for an outbound call to PSTN via CenturyLink. Under **Routing Decisions**, observe the call will rout via Avaya SBCE to CenturyLink. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



Home / Elements / Session Manager / System Tools / Call Routing Test- Call Routing Test

Called Party URI
3035557104@avayalab.com

Calling Party URI
7205551997@avayalab.com

Day Of Week
Tuesday

Time (UTC)
16:01

Calling Party Address
10.80.150.225

Session Manager Listen Port
5081

Transport Protocol
TLS

Called Session Manager Instance
ASM

Execute Test

Routing Decisions

Route < sip:3035557104@avayalab.com > to SIP Entity Sipera-150 (10.80.150.100). Terminating Location is Sipera-LOC150.

Figure 113: Call Routing Test

2. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
3. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.

4. Verify that the user on the PSTN can end an active call by hanging up.
5. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Use the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended. Where **n** is the trunk group number used for CenturyLink SIP Trunk Service defined in **Section 5.8**.

Below is an example of an active call.

```
status trunk 1
```

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/active	no	S00000
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

Figure 114: Status Trunk Active

Verify the port returns to **in-service/idle** after the call has ended.

```
status trunk 1
```

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/idle	no	
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

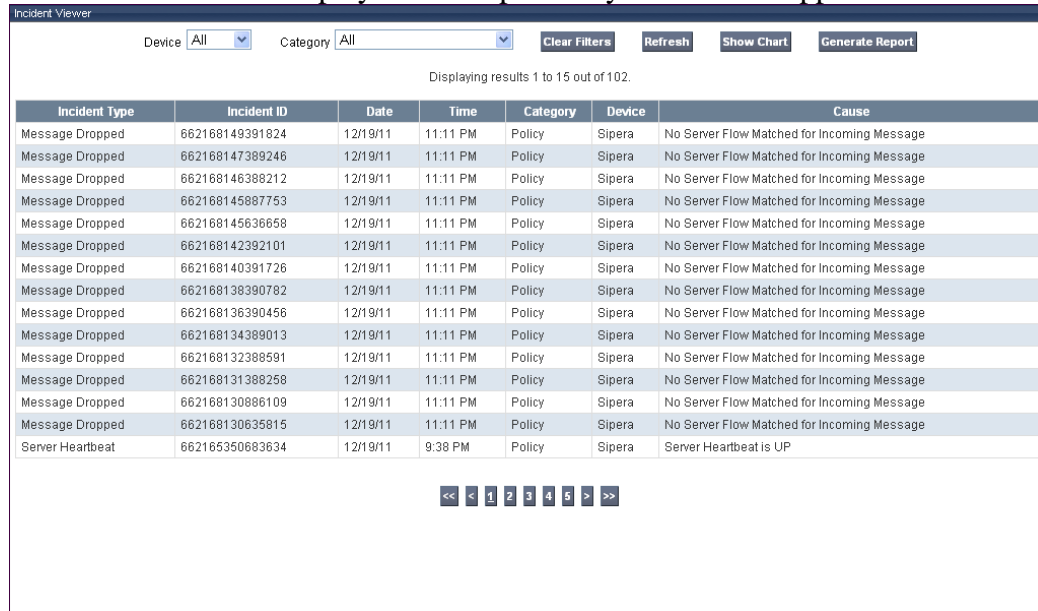
Figure 115: Status Trunk Idle

9.2. Troubleshooting

1. Communication Manager:
 - **list trace station** <extension number> - Trace calls to and from a specific station.
 - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
 - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
 - **status trunk** <trunk access code number> - Displays trunk group information.
2. Session Manager: **traceSM -x -uni** – Session Manager command line tool for traffic analysis. Log in to the Session Manager management interface to run this command.

3. Avaya Session Border Controller for Enterprise:

- **Incidences** – Displays alerts captured by the UC-Sec appliance.



The Incident Viewer interface displays a table of incidents. At the top, there are filters for Device (All) and Category (All), along with buttons for Clear Filters, Refresh, Show Chart, and Generate Report. Below the filters, it states "Displaying results 1 to 15 out of 102." The table has columns for Incident Type, Incident ID, Date, Time, Category, Device, and Cause. The incidents listed are all "Message Dropped" events, except for the last one which is a "Server Heartbeat".

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145887753	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145636658	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168142392101	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168140391726	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168138390782	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168136390456	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168134389013	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168132388591	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168131388258	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130886109	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130635815	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Server Heartbeat	662165350683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

Figure 116: Incident Viewer

- **Diagnostics** – Allows for PING tests and displays application and protocol use.

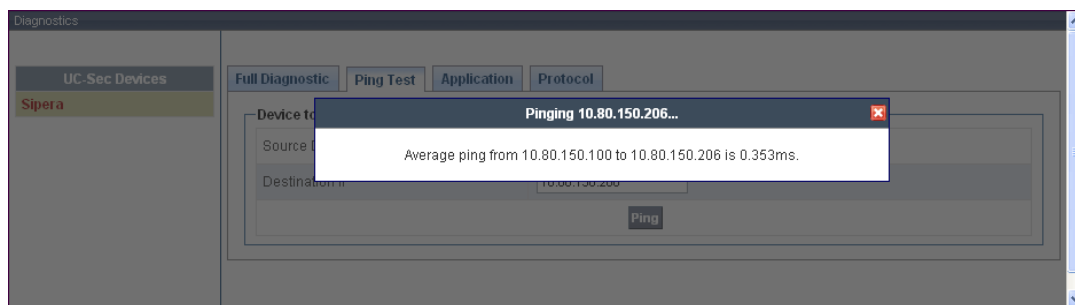


Figure 117: Diagnostics

- **Troubleshooting → Trace Settings** – Configure and display call traces and packet captures for the UC-Sec appliance.

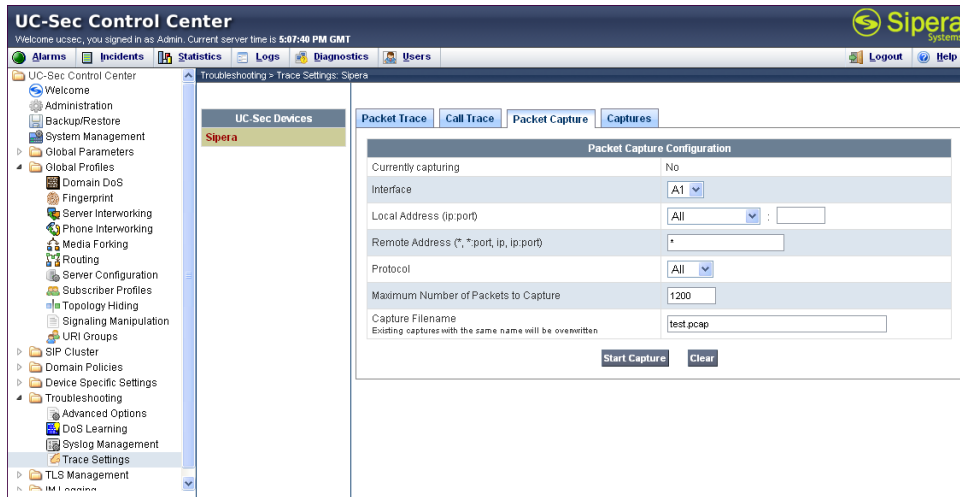


Figure 118: Packet Capture

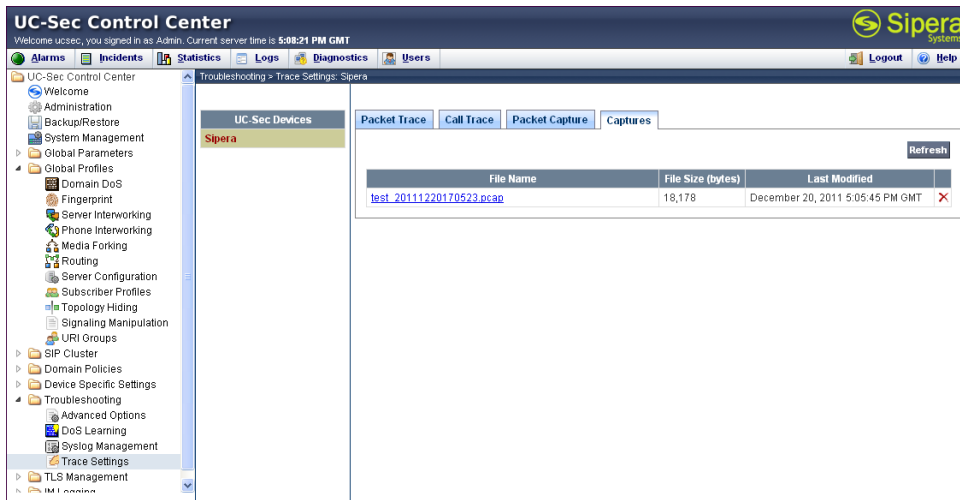


Figure 119: Packet Capture Download

The packet capture file can be downloaded and viewed using a Network Protocol Analyzer like Wireshark:

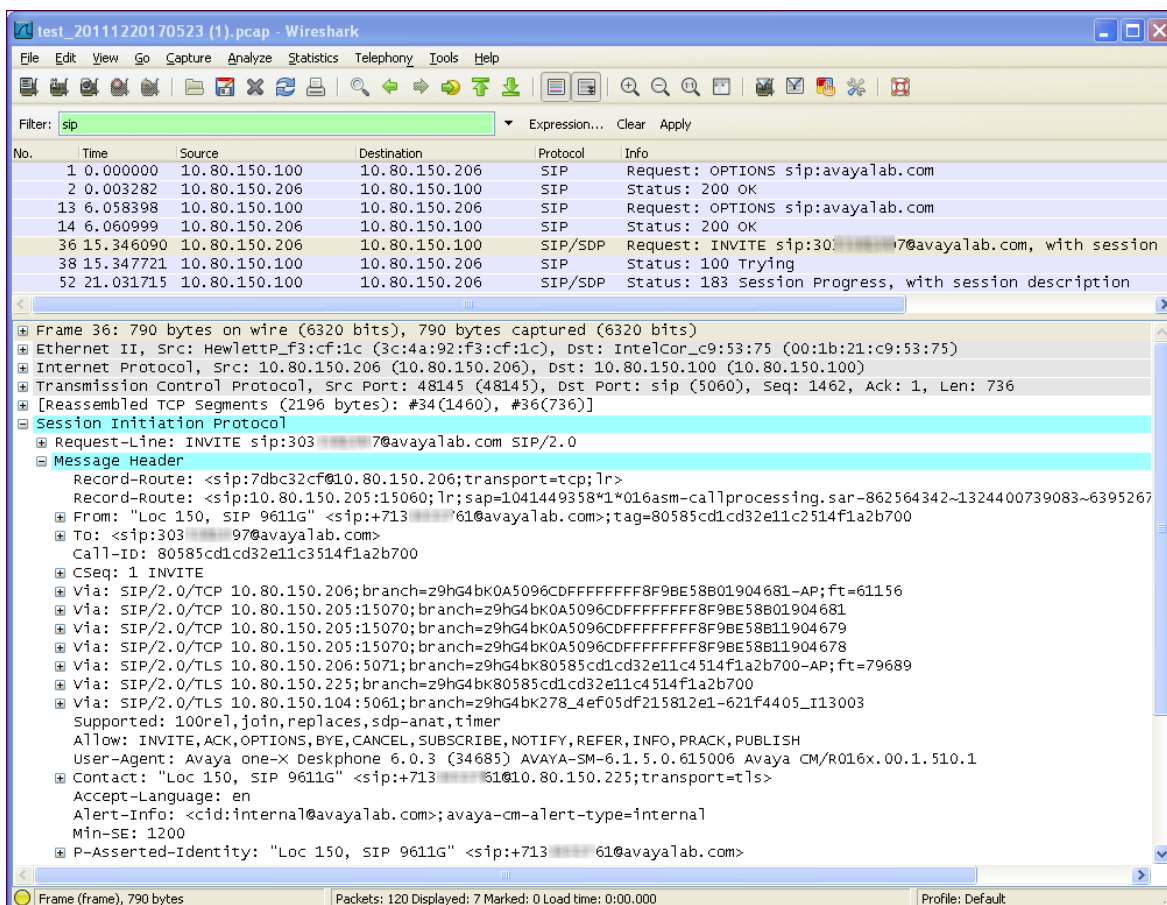


Figure 120: Packet Capture Viewer

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager Evolution Server to the CenturyLink SIP Trunk (Legacy Qwest) Service. The CenturyLink SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. Additional 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 6.0.3, February 2011.*
- [2] *Administering Avaya Aura® System Platform, Release 6.0.3, February 2011.*
- [3] *Administering Avaya Aura® Communication Manager, June 2010, Document Number 03-300509.*
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation, June 2010, Document Number 555-245-205.*
- [5] *Installing and Upgrading Avaya Aura® System Manager 6.1 GA Version, November 2010.*
- [6] *Installing and Configuring Avaya Aura® Session Manager, April 2011, Document Number 03-603473.*
- [7] *Administering Avaya Aura® Session Manager, November 2010, Document Number 03-603324.*
- [8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x, April 2010, Document Number 16-601443.*
- [9] *4600 Series IP Telephone LAN Administrator Guide, July 2008, Document Number 555-233-507.*
- [10] *Avaya one-X Deskphone H.323 Administrator Guide, May 2011, Document Number 16-300698.*
- [11] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1, December 2010, Document Number 16-603838.*
- [12] *Administering Avaya one-X Communicator, July 2011.*
- [13] *UC-Sec Install Guide (102-5224-400v1.01)*
- [14] *UC-Sec Administration Guide (010-5423-400v106)*

©2013 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.