



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Vodafone DE SIP Trunk Service with Avaya Aura[®] Communication Manager 7.1, Avaya Aura[®] Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Vodafone DE and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 7.1, Avaya Aura[®] Communication Manager 7.1, Avaya Session Border Controller for Enterprise 7.2 and various Avaya endpoints.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Vodafone DE 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 via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. INTRODUCTION.....	4
2. GENERAL TEST APPROACH AND TEST RESULTS	4
2.1. INTEROPERABILITY COMPLIANCE TESTING	5
2.2. TEST RESULTS	6
2.3. SUPPORT.....	6
3. REFERENCE CONFIGURATION	7
4. EQUIPMENT AND SOFTWARE VALIDATED.....	9
5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	11
5.1. LICENSING AND CAPACITY	11
5.2. SYSTEM FEATURES.....	13
5.3. IP NODE NAMES.....	14
5.4. CODECS.....	14
5.5. IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER	16
5.6. CONFIGURE IP INTERFACE FOR PROCR	19
5.7. SIGNALING GROUP	19
5.8. TRUNK GROUP	21
5.9. CALLING PARTY INFORMATION.....	25
5.10. OUTBOUND ROUTING	26
5.11. INCOMING CALL HANDLING TREATMENT	31
5.12. SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.....	31
6. CONFIGURE AVAYA AURA® SESSION MANAGER	32
6.1. AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	33
6.2. SPECIFY SIP DOMAIN.....	35
6.3. ADD LOCATION.....	36
6.4. ADD ADAPTATION.....	37
6.5. ADD SIP ENTITIES.....	40
6.5.1. <i>Configure Session Manager SIP Entity</i>	41
6.5.2. <i>Configure Communication Manager SIP Entity</i>	43
6.5.3. <i>Configure Avaya Session Border Controller for Enterprise SIP Entity</i>	44
6.6. ADD ENTITY LINKS	44
6.7. ADD ROUTING POLICIES.....	47
6.8. ADD DIAL PATTERNS	48
7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	51
7.1. LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	51
7.2. GLOBAL PROFILES.....	54
7.2.1. <i>Configure Server Interworking Profile - Avaya Site</i>	54
7.2.2. <i>Configure Server Interworking Profile – Vodafone DE SIP Trunk Site</i>	55
7.2.3. <i>Configure Server – Avaya Site</i>	56
7.2.4. <i>Configure Server – Vodafone DE SIP Trunk</i>	58
7.2.5. <i>Configure Routing – Avaya Site</i>	60
7.2.6. <i>Configure Routing – Vodafone DE SIP Trunk Site</i>	61
7.2.7. <i>Configure Topology Hiding – Avaya Site</i>	62
7.3. DOMAIN POLICIES	64
7.3.1. <i>Create Media Rules</i>	64
7.3.2. <i>Create Signaling Rules</i>	66
7.3.2.1 Signaling Rules – Session Manager.....	67
7.3.2.2 Signaling Rules – Vodafone DE	69

7.3.3. Create Endpoint Policy Groups	71
7.4. DEVICE SPECIFIC SETTINGS.....	72
7.4.1. Manage Network Settings.....	72
7.4.2. Create Media Interfaces.....	76
7.4.3. Create Signaling Interfaces.....	77
7.4.4. Configuration Server Flows.....	78
7.4.4.1 Create End Point Flows – SMVM Flow.....	78
7.4.4.2 Create End Point Flows – Vodafone DE SIP Trunk Flow.....	79
8. VODAFONE DE SIP TRUNK CONFIGURATION	80
9. VERIFICATION STEPS.....	80
10. CONCLUSION.....	81
11. REFERENCES.....	82

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Vodafone DE and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.1, Avaya Aura® Communication Manager 7.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.2 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Vodafone DE SIP Trunk are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Vodafone DE SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Vodafone DE SIP Trunk Service did not include use of any specific encryption features as requested by Vodafone DE.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog 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 Avaya deskphone types including H.323, SIP, digital, and analog 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 softphones. Two Avaya soft phones were used in testing: Avaya one-X[®] Communicator (1XC) and Avaya Equinox[®] for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Equinox[®] for Windows was used in testing as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060, between the Avaya enterprise and Vodafone DE
- Direct IP-to-IP Media (also known as “Shuffling”) over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server.
- Various call types including: local call, long distance, international, outbound toll-free, service
- Codec G.711A, G.729A
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura[®] Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite/Update in off-net call transfer
- SIP Diversion header in off-net call forward
- Call Center scenarios
- Fax using G.711 pass-through mode
- Mobility EC500
- DTMF - RFC2833
- Remote Worker

The following items are not supported or were not tested:

- Authentication and Registration were not supported by Vodafone DE
- Fax T.38 was not supported by Vodafone DE
- The REFER method was not supported by Vodafone DE

- Inbound toll-free call and Emergency call were not tested

2.2. Test Results

Interoperability testing of Vodafone DE SIP Trunk was completed successfully with the limitations listed below:

- **Outbound Caller ID** - On outbound calls, the calling party number is shown as the pilot/base number of the account and not the actual DDI sent by Avaya Aura Communication Manager. The trunk was configured by Vodafone DE with a length that was longer than the set of numbers provided for testing. In this case, it is expected behavior that the pilot/base number is used as the calling party
- **The Call Forward and Caller ID** - For inbound PSTN calls that are call forwarded to another PSTN endpoint, the forwarding party number is shown as the calling party instead of the original PSTN caller (forwarded party). This also impacts enterprise users with Twinning (mobility) enabled. These users have their inbound calls also ring a mobile phone. On the mobile phone, the enterprise host number is shown as the calling party instead of the original PSTN caller
- **The G.711 pass-through fax does not work** - The G.711 pass-through fax calls failed due to excessive jitter on the trunks used in the test environment
- **There is one-way or no audio in a number of different call scenarios of off-net call forward and call transfer** - This issue was addressed by both a configuration change in the Vodafone network and by removing the Referred-By header on the Avaya SBCE (See **Section 7.3.2.2** in details)
- **There is one-way or no audio in a number of different call scenarios of off-net call forward and call transfer** - This issue was addressed by a configuration change in both sides: To deactivate “symmetric latching” on Vodafone network and to remove the Referred-By header on the Avaya SBCE (See **Section 7.3.2.2**). Note: As Vodafone’s recommendation, if the “symmetric latching” is activated on Vodafone’s network, Vodafone will wait for a RTP package to open the forward ports. In this case, customer’s system needs to force open the forward ports on Vodafone by sending a silence RTP package

2.3. Support

For technical support on Vodafone DE products please visit the website at www.vodafone.de or contact an authorized Vodafone DE representative.

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

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Vodafone DE SIP Trunk. This is the configuration used for compliance testing.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Messaging
- Avaya 1600 Series IP Deskphones (H.323)
- Avaya 9600 Series IP Deskphones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya Equinox® for Windows

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in this document. Similarly, any references to real routable PSTN numbers have been replaced with numbers that cannot be routed over the PSTN.

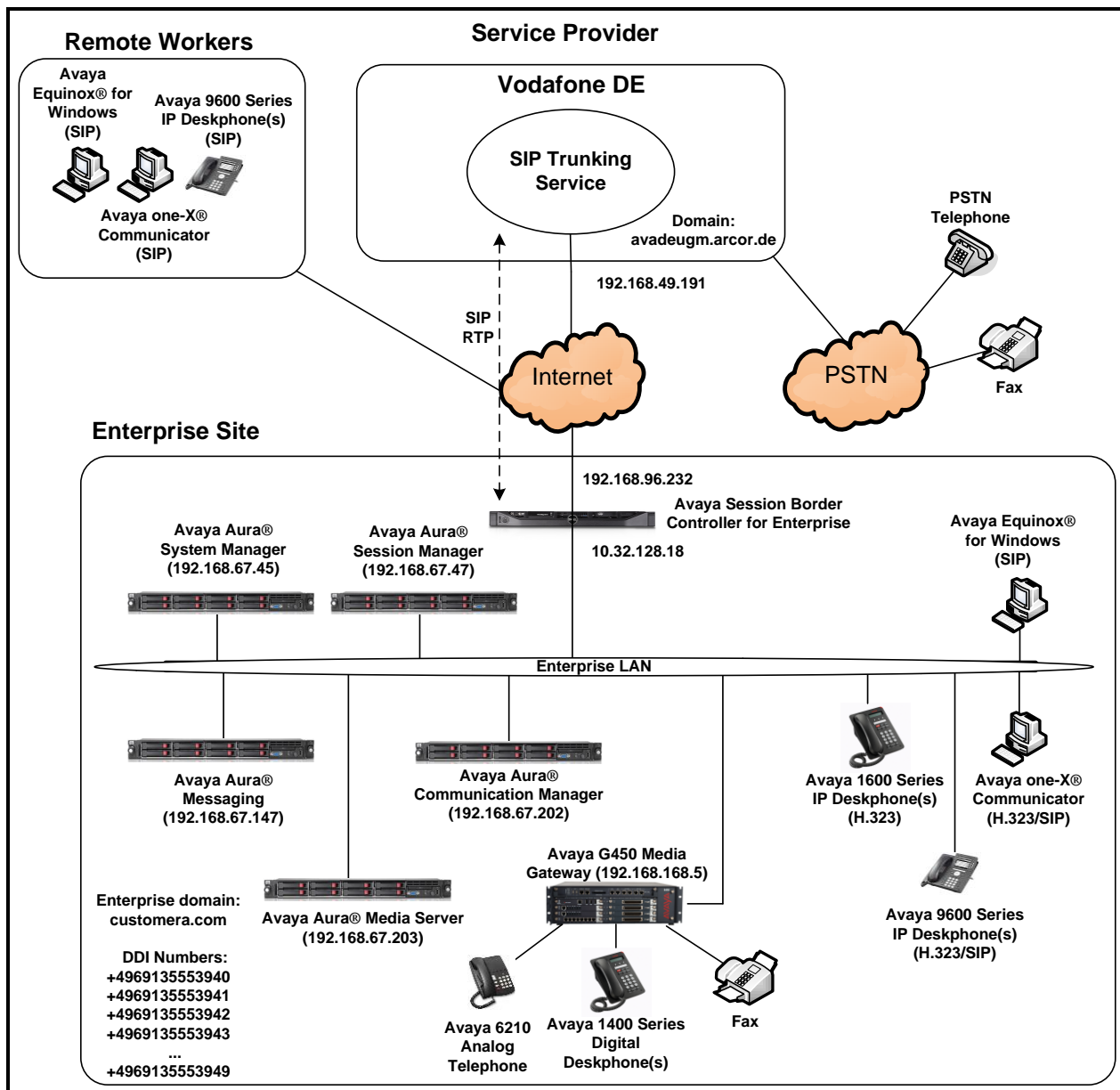


Figure 1: Avaya IP Telephony Network and Vodafone DE SIP Trunk

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® System Manager running in a virtualized environment on a HP ProLiant DL360 G7 Server	7.1 Patch1 (Software Update Revision 7.1.0.0.116823)
Avaya Aura® Session Manager running in a virtualized environment on a HP ProLiant DL360 G7 Server	7.1 (Build 7.1.0.0.710028)
Avaya Aura® Communication Manager running in a virtualized environment on a HP ProLiant DL360 G7 Server	7.1 (R017x.01.0.532.0)
Avaya Aura® Media Server running in a virtualized environment on a HP ProLiant DL360 G7 Server	7.8 (7.8.0.323)
Avaya G450 Media Gateway	38.18
Avaya Aura® Messaging running in a virtualized environment on a HP ProLiant DL360 G7 Server	7.0
Avaya Session Border Controller for Enterprise	7.2 (7.2.0.0-18-13712)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.4 (6.6401)
Avaya 9611 IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	7.1.0 (7.1.0.1.1)
Avaya one-X® Communicator (H.323 or SIP)	6.2 SP12 (Build 6.2.12.04-SP12)
Avaya Equinox® for Windows	3.2 (3.2.0.35)
Vodafone DE	
Oracle Session Border Controller	7.2
Italtel Softswitch	20.50.52

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

Note: From Release 7.0, Avaya uses the VMware®- based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer. Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7 (It was used for the compliance testing), and HP ProLiant DL360p G8.
- S8300D and S8300E.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications such as Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, and Avaya Aura® Media Server on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.

It is assumed the general installation of VMware®- based Avaya Appliance Virtualization Platform, Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, Avaya Aura® Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Vodafone DE SIP Trunk.

The 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.

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 4000 SIP trunks are available and 100 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:		4000	0
Maximum Concurrently Registered IP Stations:		2400	2
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	5
Maximum Administered SIP Trunks:		4000	100
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

Figure 2: System-Parameters Customer-Options Form – Page 2

On **Page 4**, verify that **ARS** is set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? Y		

Figure 3: System-Parameters Customer-Options Form – Page 4

On **Page 6**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

display system-parameters customer-options		Page 6 of 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n	System Management Data Transfer? n	
Personal Station Access (PSA)? y	Tenant Partitioning? y	
PNC Duplication? n	Terminal Trans. Init. (TTI)? y	
Port Network Support? n	Time of Day Routing? y	
Posted Messages? y	TN2501 VAL Maximum Capacity? y	
Private Networking? y	Uniform Dialing Plan? y	
Processor and System MSP? y	Usage Allocation Enhancements? y	
Processor Ethernet? y	Wideband Switching? y	
Remote Office? y	Wireless? n	
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

Figure 4: System-Parameters Customer-Options Form – Page 6

5.2. System Features

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

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

Figure 5: System-Parameters Features Form – 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 **restricted** and **unavailable** respectively (refer to **Section 5.8**).

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

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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:
  International Access Code:

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

Figure 6: System-Parameters Features Form – Page 9

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses as below:

- Session Manager: **Name: SM, IP Address: 192.168.67.47**
- Communication Manager: **Name: procr, IP Address: 192.168.67.202**

These node names will be needed for defining the service provider signaling group in **Section 5.7**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
AAM	192.168.67.147	
AMS	192.168.67.203	
SM	192.168.67.47	
default	0.0.0.0	
gateway	192.168.67.1	
procr	192.168.67.202	
procr6 ::		

Figure 7: Node-Names IP Form

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. In the compliance test, **ip-codec-set 2** was used for this purpose. Vodafone DE supports the **G.711A**, and **G.729A** codecs. Default values can be used for all other fields.

change ip-codec-set 2

Page1 of 2

IP CODEC SET

Codec Set: 2

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.711A	n	2	20
2: G.729A	n	2	20

Media EncryptionEncryption SRCTP: enforce-unenc-srtcp

1: 1-srtp-aescm128-hmac80

2: none

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **off**. Vodafone DE supports only Fax using G.711 pass-through mode.

change ip-codec-set 2		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	Packet Size (ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region for Media Gateway, Media Server

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. For the compliance test, IP network region **1** was chosen for the service provider trunk.

Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **customerera.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 G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **Section 5.7**
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**
- Default values can be used for all other fields

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: customerera.com	
Name: SP Region	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 2	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3329	IP Audio Hairpinning? n	
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 10: IP-Network-Region Form

The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (**192.168.67.202**), and that the gateway **MGP IPv4 Address** is **192.168.67.5**. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```

display media-gateway 1                                     Page 1 of 2
                                MEDIA GATEWAY 1

                                Type: g450
                                Name: g450
                                Serial No: 12TG18000244
                                Link Encryption Type: tls-only      Enable CF? n
                                Network Region: 1                  Location: 1
                                                                Site Data:

                                Recovery Rule: none

                                Registered? y
                                FW Version/HW Vintage: 38 .18 .0 /1
                                MGP IPV4 Address: 192.168.67.5
                                MGP IPV6 Address:
                                Controller IP Address: 192.168.67.202
                                MAC Address: 3c:3a:73:17:c5:a8

                                Mutual Authentication? optional

```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an **MM712** media module supporting Avaya digital phones in slot **V1**, an **MM711** supporting analog phones on slot **V2**, and the capability to provide announcements and music on hold via “**gateway-announcements**” in logical slot **V9**.

```

display media-gateway 1                                     Page 2 of 2
                                MEDIA GATEWAY 1

                                Type: g450

Slot  Module Type      Name      DSP Type  FW/HW version
V1:  MM712           DCP MM    MP80      153  7
V2:  MM711           ANA MM
V3:
V4:
V5:
V6:
V7:
V8:
V9:  gateway-announcements  ANN VMM

Max Survivable IP Ext: 8

```

Figure 12: Media Gateway – Page 2

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1

                                MEDIA SERVER

Media Server ID: 1

    Signaling Group: 11
Voip Channel License Limit: 10
Dedicated Voip Channel Licenses: 10

    Node Name: AMS
    Network Region: 1
                Location: 1
Announcement Storage Area:
```

Figure 13: Media Server

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

change ip-interface procr	
IP INTERFACES	
Type: PROCR	Target socket load: 4800
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: 192.168.67.202
Subnet Mask: /24	

Figure 14: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. For the compliance test, signaling group **1** was used for both outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- Set the **Group Type** field to **sip**
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and 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. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- 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 **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port for TLS, such as **5068**

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to **customera.com**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval
- Default values may be used for all other fields

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5068	Far-end Listen Port: 5068	
	Far-end Network Region: 1	
	Far-end Secondary Node Name:	
Far-end Domain: customera.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 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- 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 **AMS**. This node name maps to the IP address of Media Server as defined in **Section 5.3**
- Set the **Near-end Listen Port** to **9061** and **Far-end Listen Port** to a valid unused port for TLS, such as **5061**
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **192.168.67.203**

change signaling-group 11
Page 1 of 2

SIGNALING GROUP

Group Number: 11
Group Type: sip
Transport Method: tls

Peer Detection Enabled? n
Peer Server: AMS

Near-end Node Name: procr
Far-end Node Name: AMS
Near-end Listen Port: 9061
Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain: 192.168.67.203

Figure 16: Signaling-Group 11

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 **1** was used for both outbound and inbound calls to the service provider. It 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. (i.e. ***020**). Note: Refer to **Section 5.10** for adding * in dialing plan
- Set Class of Restriction (**COR**) to **1**
- Set **Direction** to **two-way** for trunk group **20**
- Set the **Service Type** field to **public-ntwrk**
- Set **Member Assignment Method** to **auto**
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group **1** was associated to signaling group **1**
- 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 1		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: SIP Trunks	COR: 1	TN: 1 TAC: *020
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0	Auth Code? n	
Service Type: public-ntwrk	Member Assignment Method: auto	
	Signaling Group: 1	
	Number of Members: 50	

Figure 17: Trunk-Group – Page 1

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.7**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that UPDATES must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

add trunk-group 1		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
Redirect On OPTIM Failure: 6000		
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval (sec): 600		
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n	

Figure 18: Trunk-Group – 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 (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **pub-unk** (see **Section 5.10**).

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 an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

add trunk-group 1

Page 3 of 21

TRUNK FEATURES

ACA Assignment? n

Measured: none

Maintenance Tests? y

Numbering Format: public

UI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Hold/Unhold Notifications? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** (default setting) so that the SIP Refer is not sent in redirected calls. Note: In the compliance test, Vodafone DE worked with SIP re-Invite/Update successfully in redirected calls, however Vodafone did not support the SIP REFER.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been redirected. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging. The **Diversion Header** is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	

Figure 20: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “P-Asserted-Identity” 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 numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and it is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public-unknown-numbering entry can be applied for all extensions. In the compliance test, all stations with a 5-digit extension beginning with **19** will send the calling party number as the **CPN Prefix** plus the extension number.

Note: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a ‘+’ in front of user number in From, P-Asserted-Identity, Contact, Diversion headers.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	19101	1	4969135553941	13	Total Administered: 13 Maximum Entries: 240
5	19102	1	4969135553942	13	
5	19103	1	4969135553943	13	
5	19105	1	4969135553946	13	
5	19106	1	4969135553945	13	
5	19107	1	4969135553946	13	
5	19110	1	4969135553947	13	
5	44002	1	4969135553947	13	
5	46053	1	4969135553947	13	

Figure 21: Public-Unknown-Numbering Form

5.10. 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 configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- **Dialed String** beginning with **9** for feature access code (**dac**)
- **Dialed String** beginning with ***** for Trunk Access Code (dac) defined on Trunk group 1 in **Section 5.8**

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext						
181	4	ext						
9	1	dac						
800	4	ext						
*	4	dac						

Figure 22: Dialplan–Analysis Form

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

change feature-access-codes		Page 1 of 11
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialin3g List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *111		
Answer Back Access Code:		
Attendant Access code:		
Auto Alternate Routing (AAR) Access Code:		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA:	All:	Deactivation:
Call Forwarding Enhanced Status:	Act:	Deactivation:
Call Park Access Code:		
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure	Open Code:	Close Code:

Figure 23: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 1** which contains the SIP trunk group to the service provider (as defined next).

change ars analysis 0						
ARS DIGIT ANALYSIS TABLE						
Location: all						
Percent Full: 1						
Dialed	Total		Route	Call	Node	ANI
String	Min	Max	Pattern	Type	Num	Reqd
00	13	15	1	intl		n
06913	11	15	1	natl		n
118	3	6	1	svcl		n

Figure 24: ARS–Analysis Form

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 in route pattern **1** for 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 **1** was used
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level
- **Numbering Format:** Set this field to **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

change route-pattern 1															Page 1 of 3		
Pattern Number: 1 Pattern Name: SP																	
SCCAN? n Secure SIP? n																	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits								QSIG		
															Intw		
1:	1	0								n						user	
2:										n						user	
3:										n						user	
4:										n						user	
5:										n						user	
6:										n						user	

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request		Dgts	Format	
								Subaddress		
1:	y	y	y	y	y	n	n	rest	pub-unk	none
2:	y	y	y	y	y	n	n	rest		none
3:	y	y	y	y	y	n	n	rest		none
4:	y	y	y	y	y	n	n	rest		none
5:	y	y	y	y	y	n	n	rest		none
6:	y	y	y	y	y	n	n	rest		none

Figure 25: Route–Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction: none**. This setting allows the outbound call using feature access code (fac) 6 over SIP trunks.

change cor 1		Page 1 of 23
CLASS OF RESTRICTION		
COR Number: 1		
COR Description:		
FRL: 0	APLT? y	
Can Be Service Observed? n	Calling Party Restriction: none	
Can Be A Service Observer? n	Called Party Restriction: none	
Time of Day Chart: 1	Forced Entry of Account Codes? n	
Priority Queuing? n	Direct Agent Calling? n	
Restriction Override: none	Facility Access Trunk Test? n	
Restricted Call List? n	Can Change Coverage? n	
Access to MCT? y	Fully Restricted Service? n	
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n	
Send ANI for MFE? n	Add/Remove Agent Skills? n	
MF ANI Prefix:	Automatic Charge Display? n	
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n	
	Can Be Picked Up By Directed Call Pickup? n	
	Can Use Directed Call Pickup? n	
	Group Controlled Restriction: inactive	

Figure 26: Class of Restriction Form

5.11. Incoming Call Handling Treatment

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, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. See **Section 6.4** for Session Manager Digit Conversion.

5.12. Save Avaya Aura[®] Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura[®] Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring 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 define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring 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 as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

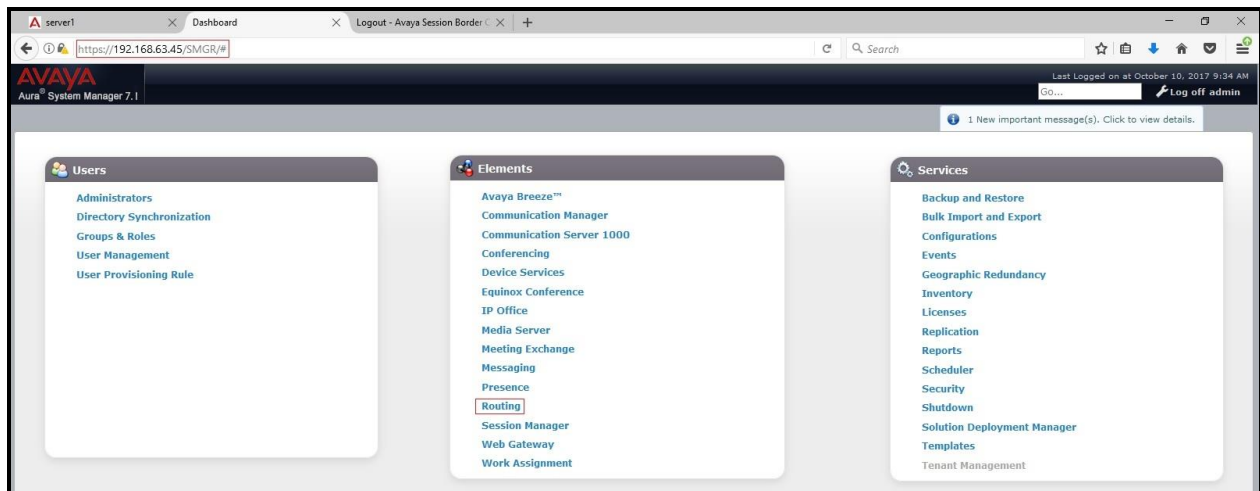


Figure 27: System Manager Home Screen

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

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

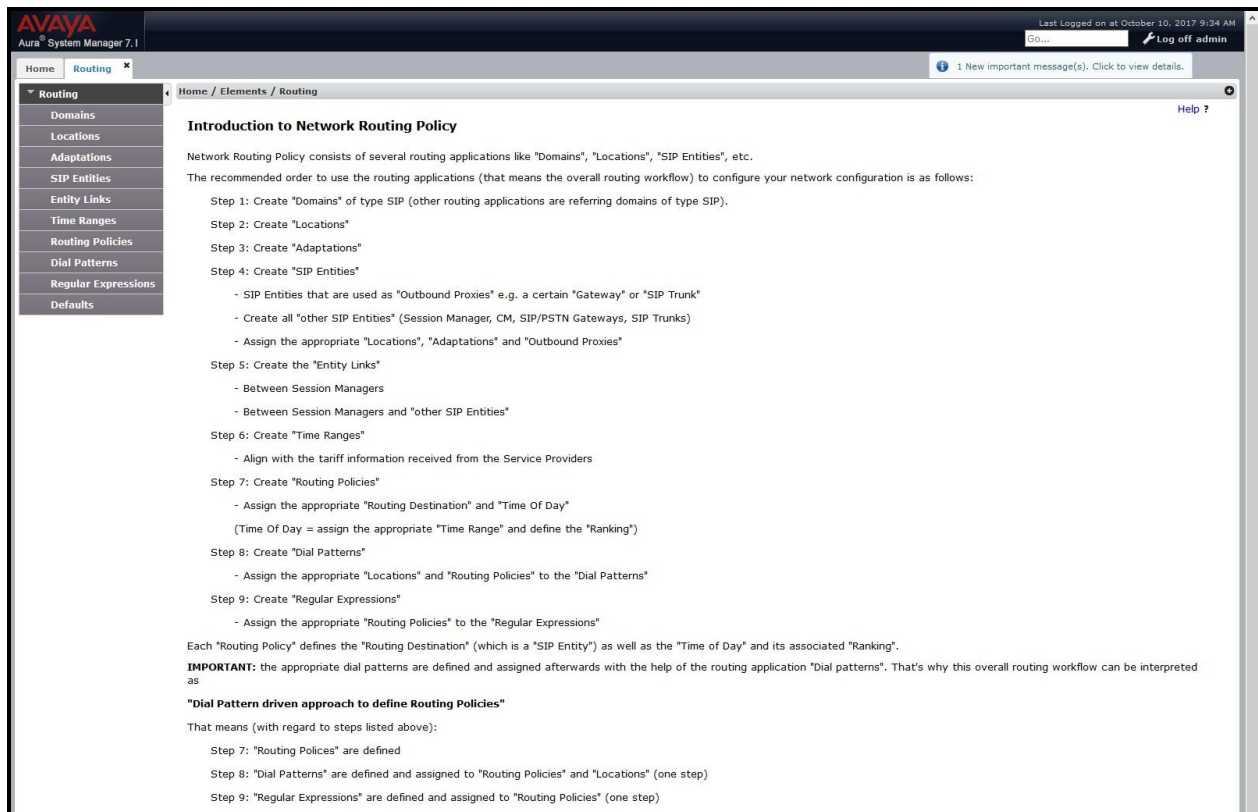


Figure 28: Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **customera.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), 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** to save.

The screen below shows the existing entry for the enterprise domain.



The screenshot displays the 'Domain Management' web interface. At the top, a breadcrumb trail reads 'Home / Elements / Routing / Domains'. The main title 'Domain Management' is on the left, and 'Help ?' is on the right. Below the title, there are 'Commit' and 'Cancel' buttons. A table below shows one item with the following details:

Name	Type	Notes
customera.com	sip	

Figure 29: Domain Management

6.3. Add Location

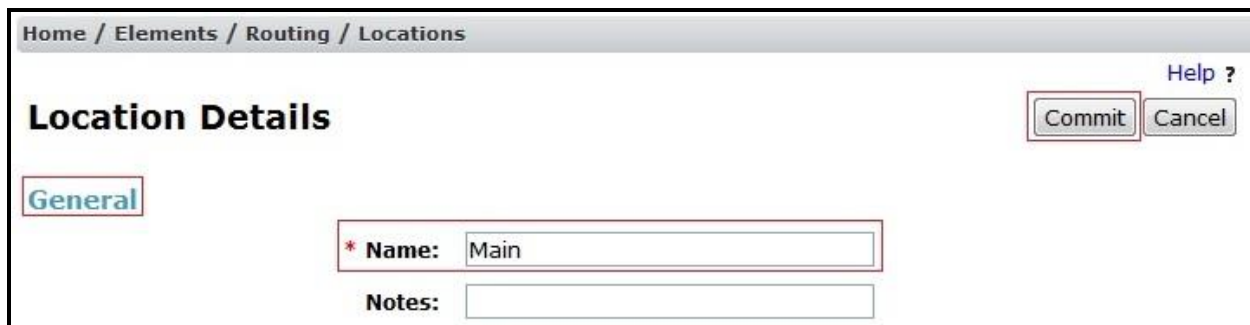
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Main**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

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 new right pane that appears (shown below), fill in the following:

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)

Click **Commit** to save



The screenshot displays a web application interface for configuring a location. At the top, a breadcrumb trail reads "Home / Elements / Routing / Locations". Below this, the title "Location Details" is shown on the left, and "Help ?" is on the right. In the top right corner, there are "Commit" and "Cancel" buttons. On the left side, a tab labeled "General" is selected. The main form area contains two fields: a required field labeled "* Name:" with the value "Main" entered, and an optional field labeled "Notes:" which is currently empty.

Figure 30: Location Configuration

6.4. Add Adaptation

Session Manager can be configured with adaptations that can modify SIP messages before or after routing decisions have been made or perform digit manipulation. The adaptation **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages.

For the compliance test, two adaptations were used. The first adaptation was applied to the Communication Manager SIP entity and performed the mapping of inbound DID numbers from Vodafone DE to local Communication Manager extensions. The second adaptation was applied to the Avaya SBCE SIP entity and performed to add a plus sign in From/PAI headers for the outbound INVITE using One-X Communicator in phone mode.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Adaptation Name:** Enter a descriptive name for the adaptation (e.g., **Map-MT-CM-DDIs**).
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu
- **Module Parameter Type:** Leave blank
- **Notes:** Enter a description (optional)

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane has 'Routing' selected, and the 'Adaptations' sub-menu is highlighted. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. The form contains the following fields:

- * Adaptation Name:** Map-MT-CM-DDIs
- * Module Name:** DigitConversionAdapter (selected from a dropdown menu)
- Module Parameter Type:** (empty dropdown menu)
- Egress URI Parameters:** (empty text field)
- Notes:** Map Inb DDIs

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

Figure 31: Adaptation for Mapping DID Numbers 1

To map inbound DID numbers from Vodafone DE to Communication Manager local extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID numbers
- **Min:** Enter a minimum dialed number length used in the match criteria
- **Max:** Enter a maximum dialed number length used in the match criteria
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number
- **Insert Digits:** Enter the digits to insert new local extensions
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number

Click **Commit** to save

Digit Conversion for Outgoing Calls from SM

Add Remove

7 Items
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+4969135553941	*14	*14		*14	19101	destination		
<input type="checkbox"/>	*+4969135553942	*14	*14		*14	19102	destination		
<input type="checkbox"/>	*+4969135553943	*14	*14		*14	19103	destination		
<input type="checkbox"/>	*+4969135553944	*14	*14		*14	46000	destination		
<input type="checkbox"/>	*+4969135553945	*14	*14		*14	19106	destination		
<input type="checkbox"/>	*+4969135553946	*14	*14		*14	19107	destination		
<input type="checkbox"/>	*+4969135553947	*14	*14		*14	20010	destination		

Select : All, None

Commit Cancel

Figure 32: Adaptation for Mapping DID Numbers 2

To create the adaptation that will be applied to the SBCE SIP entity, navigate to **Routing** → **Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Adaptation Name:** Enter a descriptive name for the adaptation (e.g., **Add + sign**)
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu
- **Module Parameter Type:** Select **Name-Value Parameter** from the drop-down menu
- Click **Add** button and enter the following values:
 - **Name:** **fromto**
 - **Value:** **true**
- Use default values for all remaining fields

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane has 'Routing' expanded, and 'Adaptations' is selected. The main area displays the 'Adaptation Details' form. The 'General' tab is active. The form contains the following fields:

- Adaptation Name:** Add + sign
- Module Name:** DigitConversionAdapter (selected from a dropdown)
- Module Parameter Type:** Name-Value Parameter (selected from a dropdown)

Below these fields is a table for parameters:

Add		Remove	
<input type="checkbox"/>	Name		Value
<input type="checkbox"/>	fromto		true

Below the table, there is a 'Select' dropdown set to 'All, None'. At the bottom, there are fields for 'Egress URI Parameters' and 'Notes'.

Figure 33: Adaptation for Adding + Sign 1

To add + sign, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for inserting a + sign. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number
- **Min:** Enter a minimum dialed number length used in the match criteria
- **Max:** Enter a maximum dialed number length used in the match criteria
- **Delete Digits** Enter 0
- **Insert Digits:** Enter +
- **Address to modify:** Select **origination** since this inserted digit only applies to the original number

Click **Commit** to save

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*49	12	15		0	+	origination		Add + for 1XC other phone mode

Figure 34: Adaptation for Adding + Sign 2

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, 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 new right pane that appears (shown on the next page), fill in the following:

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**. Adaptation modules were not used in this configuration
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Main**
- **Time Zone:** Select the time zone for the Location above

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.5.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **asm**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address** **192.168.67.47**. The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The left sidebar shows a navigation menu with 'Routing' selected, and 'SIP Entities' highlighted under the 'Routing' section. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration form contains the following fields:

- Name:** asm
- FQDN or IP Address:** 192.168.67.47
- Type:** Session Manager (dropdown menu)
- Notes:** Expressway
- Location:** Main (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New_York (dropdown menu)
- Minimum TLS Version:** Use Global Setting (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

Figure 35: Session Manager SIP Entity

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

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

- **Port:** Port number on which Session Manager listens for SIP requests
- **Protocol:** Transport protocol to be used with this port
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain

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

Multiple port entries are shown in the screenshot below. The first two are standard ports used for SIP traffic: port 5060 for TCP and port 5061 for TLS. These ports were provisioned as part of the Session Manager installation not covered by this document. In addition, port 5068 defined in **Section 5.7** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list and highlighted below.

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

5 Items [Filter: Enable](#)

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	customerera.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	customerera.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5062	TCP	customerera.com	<input type="checkbox"/>	
<input type="checkbox"/>	5068	TLS	customerera.com	<input type="checkbox"/>	

Figure 36: Session Manager SIP Entity Port

6.5.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **ACM_public**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager **192.168.67.202**. Note that **CM** was selected for **Type**. The **Adaptation** is set as **Map-MT-CM-DIDs** (Defined in **Section 6.4**). The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA
Aura® System Manager 7.1

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: ACM_public

* FQDN or IP Address: 192.168.67.202

Type: CM

Notes:

Adaptation: Map-MT-CM-DDIs

Location: Main

Time Zone: America/New_York

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection Mode: Off

SIP Link Monitoring: Use Session Manager Configuration

Loop Detection

Monitoring

Figure 37: Communication Manager SIP Entity

6.5.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **VNJ-SBCE1**. The **FQDN or IP Address** field is set to the IP address of the SBCE's private network interface **10.32.128.18**. Note that **SIP Trunk** was selected for **Type**. The Adaptation is set as **Add + sign** (Defined in **Section 6.4**). The user will need to select the specific values for the **Location** and **Time Zone**.

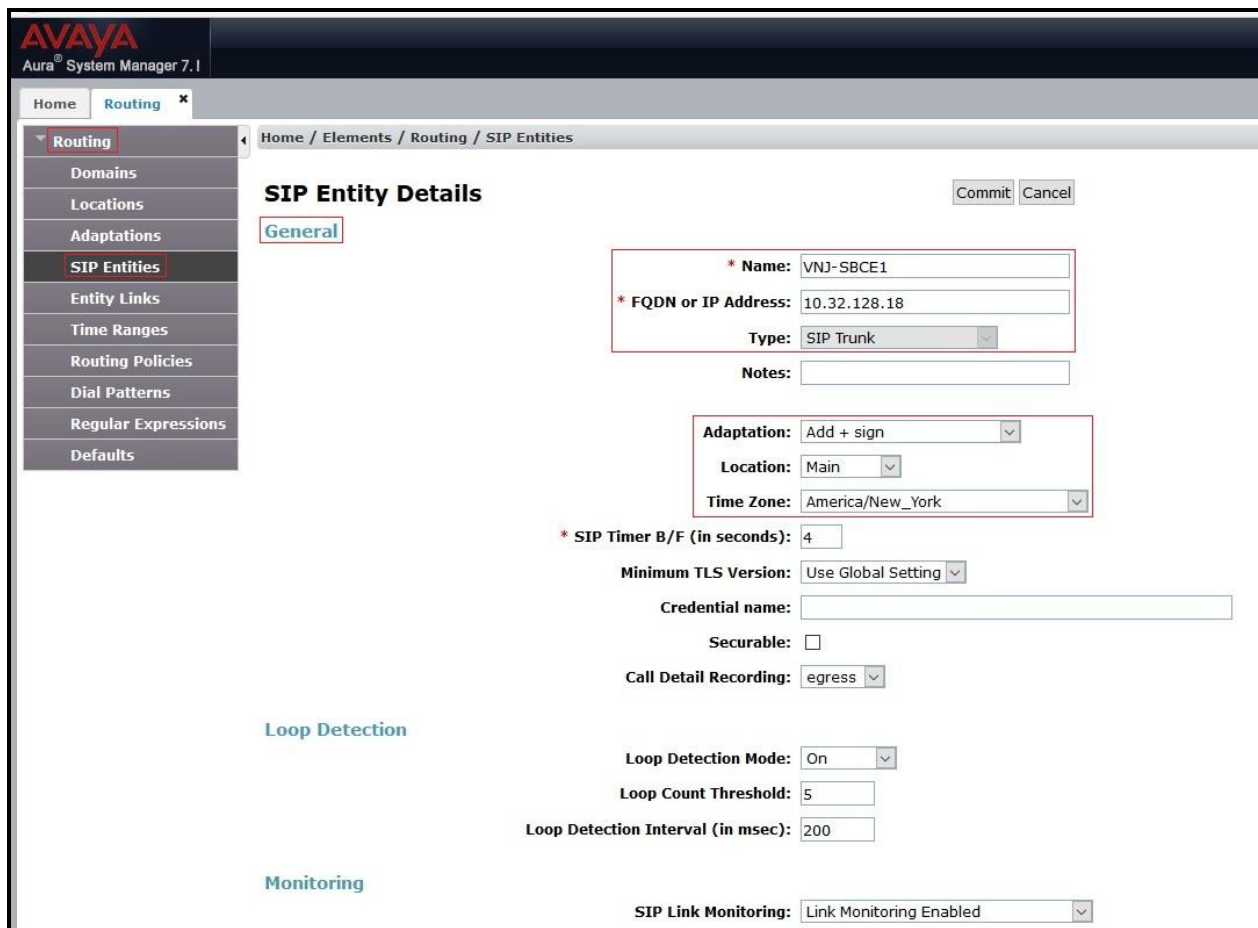


Figure 38: Avaya SBCE SIP Entity

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by the service provider traffic and one to the 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). In the new right pane that appears (shown on the next page), fill in the following:

- **Name:** Enter a descriptive name
- **SIP Entity 1:** Select the Session Manager being used
- **Protocol:** Select the transport protocol used for this link
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.5**
- **Port:** Port number on which the other system receives SIP requests from the Session Manager
- **Connection Policy:** Select **trusted**. **Note:** If **trusted** is not selected, calls from the associated SIP Entity specified in **Section 6.5** will be denied

Click **Commit** to save

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The item 'sm_ACM_public_5068_T' is selected, showing a link from 'Q.asm' to 'Q.ACM_public' using the 'TLS' protocol on port '5068'. The 'Connection Policy' is set to 'trusted'. There are 'Commit' and 'Cancel' buttons at the top right of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
* sm_ACM_public_5068_T	* Q.asm	TLS	* 5068	* Q.ACM_public	* 5068	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Figure 39: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.3**, **7.2.5** and **7.4.3**.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes 'Commit' and 'Cancel' buttons. Below the title, there is a table with the following data:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
*VNO-SBCE-Link	*Q.asm	TLS	5061	*Q.VNO-SBCE1	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

At the bottom of the table, there is a 'Select : All, None' option. The top right of the interface shows the user is logged in as 'admin' and the last login time is 'October 11, 2017 9:20 AM'.

Figure 40: Avaya SBCE Entity Link

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added; one for Communication Manager 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). In the new right pane that appears (shown on the next page), 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**. 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 screen shows the **Routing Policy Details** for the policy named **ACM_Public** associated with incoming PSTN calls from Vodafone DE to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **ACM_public**.

The screenshot displays the Avaya System Manager 7.1 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' tab is active, showing the 'Name' field set to 'ACM_Public', 'Disabled' as an unchecked checkbox, 'Retries' set to 0, and an empty 'Notes' field. Below this, the 'SIP Entity as Destination' section is visible, featuring a 'Select' button and a table listing available SIP entities. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. One entity is listed: 'ACM_public' with FQDN '192.168.67.202' and Type 'CM'.

Name	FQDN or IP Address	Type	Notes
ACM_public	192.168.67.202	CM	

Figure 41: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **VNJ-SBCE1-RP**, associated with outgoing calls from Communication Manager to the PSTN via Vodafone DE SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **VNJ-SBCE1**.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane is expanded to show 'Routing Policies'. The main content area is titled 'Routing Policy Details' for the policy 'VNJ-SBCE1-RP'. It includes fields for 'Name' (VNJ-SBCE1-RP), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which contains a table with the following data:

Select	Name	FQDN or IP Address	Type	Notes
<input checked="" type="checkbox"/>	VNJ-SBCE1	10.32.128.18	SIP Trunk	

Figure 42: Routing to Vodafone DE SIP Trunk

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to Vodafone DE SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination 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). In the new right pane that appears (shown on the next page), fill in the following:

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:** Enter the destination domain used in the match criteria
- **Notes:** Add a brief description (optional)

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

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

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound 13-digit dialed numbers that begin with **001** and have a destination **SIP Domain** of **customera.com** uses **Routing Policy Name** as **VNJ-SBCE1-RP** which is defined in **Section 6.7**.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button. The 'General' tab is active, showing the following fields:

- * Pattern: 001
- * Min: 13
- * Max: 13
- Emergency Call: ☐
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: customera.com
- Notes: Outbound Calls to US/Canada

Below these fields is a section titled 'Originating Locations and Routing Policies' with an 'Add' button. It contains a table with the following data:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		VNJ-SBCE1-RP	0	<input type="checkbox"/>	VNJ-SBCE1	

The table has a 'Filter: Enable' button and a 'Select: All, None' option at the bottom.

Figure 43: Dial Pattern_001

Note that with the above Dial Pattern, Vodafone DE did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 14 digit numbers that start with +4969 use **Routing Policy Name** as **ACM_Public** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Vodafone DE.

Dial Pattern Details

General

* Pattern: +4969
* Min: 14
* Max: 16

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: customera.com
Notes: Inbound Vodafone DE numbers

Originating Locations and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		ACM_Public	2	<input type="checkbox"/>	ACM_public	

Figure 44: Dial Pattern_+4969

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

Dial Patterns

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
001	13	13	<input type="checkbox"/>			customera.com	Outbound Calls to US
069138	6	14	<input type="checkbox"/>			customera.com	Outbound Vodafone Local Numbers
118	5	5	<input type="checkbox"/>			customera.com	Intl Directory Assistance
+4969	14	16	<input type="checkbox"/>			customera.com	Inbound Vodafone DE numbers

Figure 45: Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the Vodafone DE system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Vodafone DE system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in to Avaya Session Border Controller for Enterprise

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password** and click on **Log In** button.

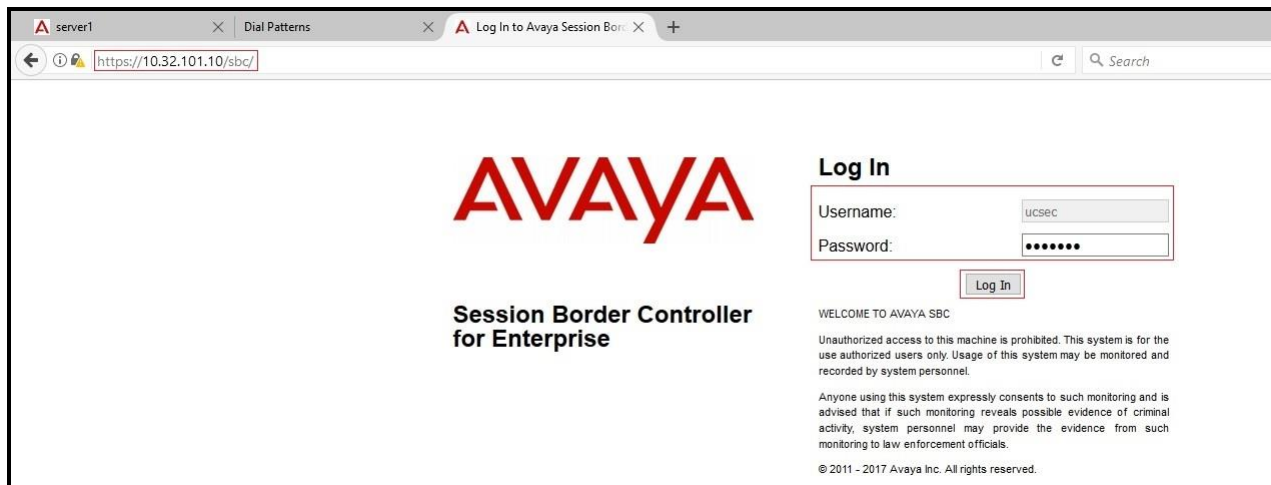


Figure 46: Avaya SBCE Login

The **Dashboard** main page will appear as shown below.

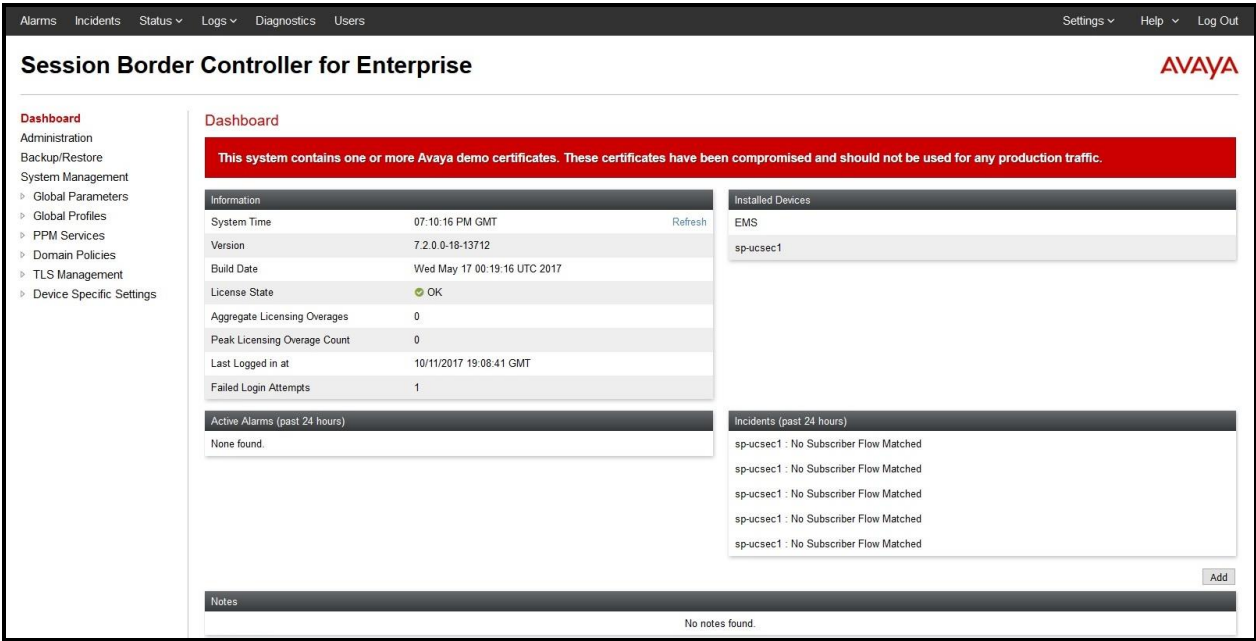


Figure 47: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single **Device Name sp-ucsec1** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

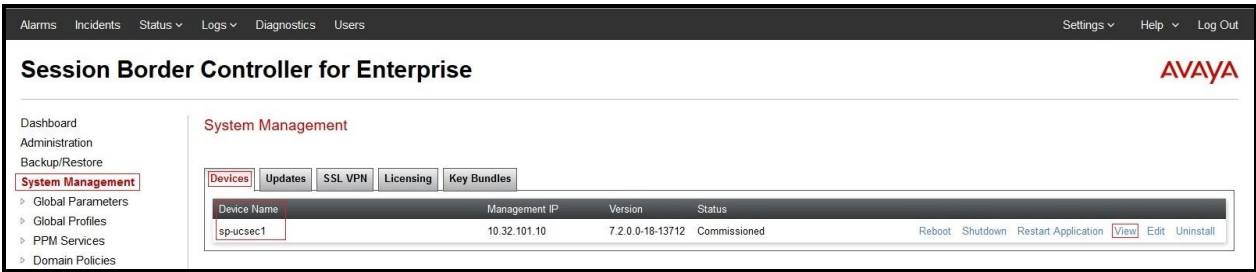


Figure 48: Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

System Information: sp-ucsec1
X

General Configuration

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions	0
Requested: 0	
Advanced Sessions	0
Requested: 0	
Scopia Video Sessions	0
Requested: 0	
CES Sessions	0
Requested: 0	
Transcoding Sessions	0
Requested: 0	
Encryption	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
10.32.128.19	10.32.128.19	255.255.255.0	10.32.128.254	A1
135.10.96.229	135.10.96.229	255.255.255.224	135.10.96.254	B1
135.10.96.230	135.10.96.230	255.255.255.224	135.10.96.254	B1
192.168.96.232	192.168.96.232	255.255.255.0	192.168.96.254	B1

DNS Configuration

Primary DNS	4.79.132.219
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.18

Management IP(s)

IP #1 (IPv4)	10.32.101.10
--------------	--------------

Figure 49: Avaya SBCE System Information

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name: Avaya-SM** and click **Finish** (not shown)

The following screen shows that Session Manager server interworking profile (named: **Avaya-SM**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. On the left, a sidebar menu lists various configuration areas, with "Server Interworking" highlighted under "Global Profiles". The main content area is titled "Interworking Profiles: Avaya-SM" and features a list of profiles on the left, including "cs2100", "OCS-Edge-Server", "cisco-ccm", "cups", "Sipera-Halo", "OCS-FrontEnd-Server", and "Avaya-SM". The "Avaya-SM" profile is selected, and its configuration is shown in a table with tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The "General" tab is active, displaying a table of parameters and their values.

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Figure 50: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – Vodafone DE SIP Trunk Site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** → **Add**

- Enter **Profile Name: SP-General** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)

The following screen shows that Vodafone DE server interworking profile (named: **SP-General**) was added.

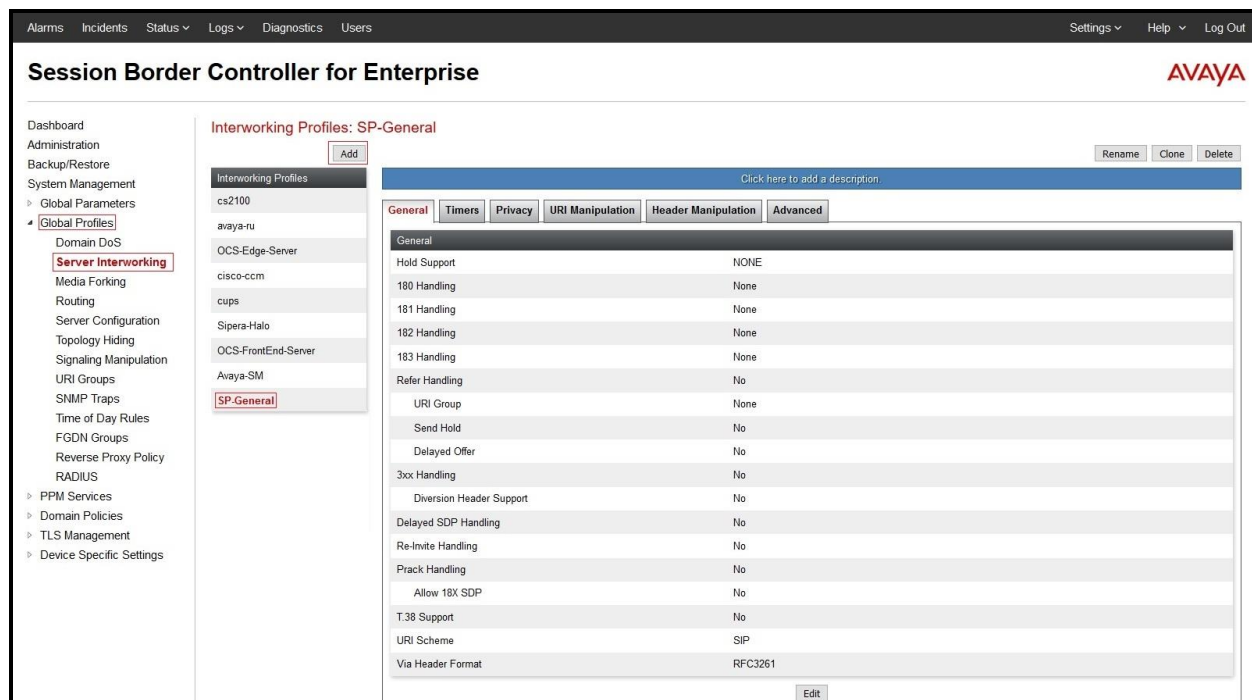


Figure 51: Server Interworking – Vodafone DE SIP Trunk site

7.2.3. Configure Server – Avaya Site

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name: Expway-SM**

On **General** tab, enter the following:

- **Server Type:** Select **Call Server**
- **TLS Client Profile:** Select **sbce1Client**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use. Session Manager 7.1 includes SMGR signed certs, not the Avaya demo certificates
- **IP Address/FQDN:** **192.168.67.47** (Session Manager IP Address) with **Port: 5060** and **Transport: TCP**
- **IP Address/FQDN:** **192.168.67.47** (Session Manager IP Address) with **Port: 5061** and **Transport: TLS**
- Click **Finish** (not shown)

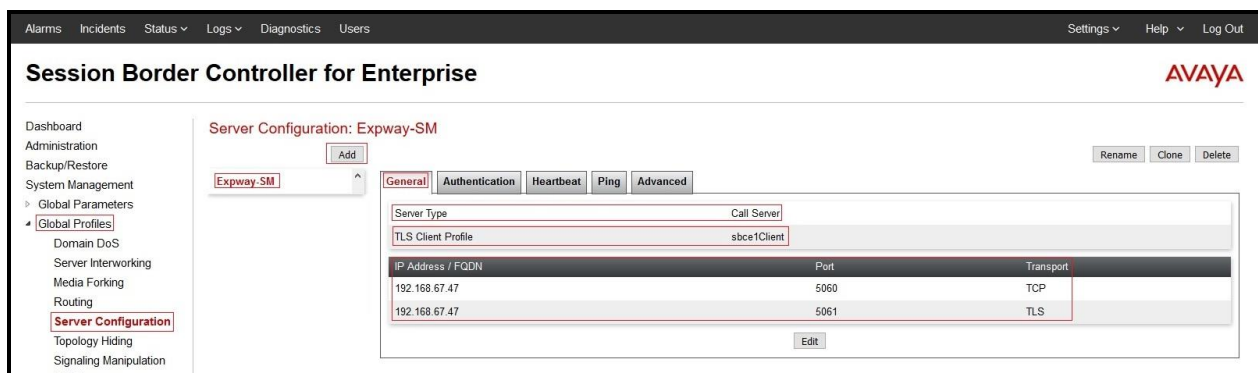


Figure 52: Server Configuration – General - Avaya site

On the **Advanced** tab

- **Enable Grooming** box is checked
- Select **Avaya-SM** for **Interworking Profile** (see Section 7.2.1)
- Click **Finish** (not shown)

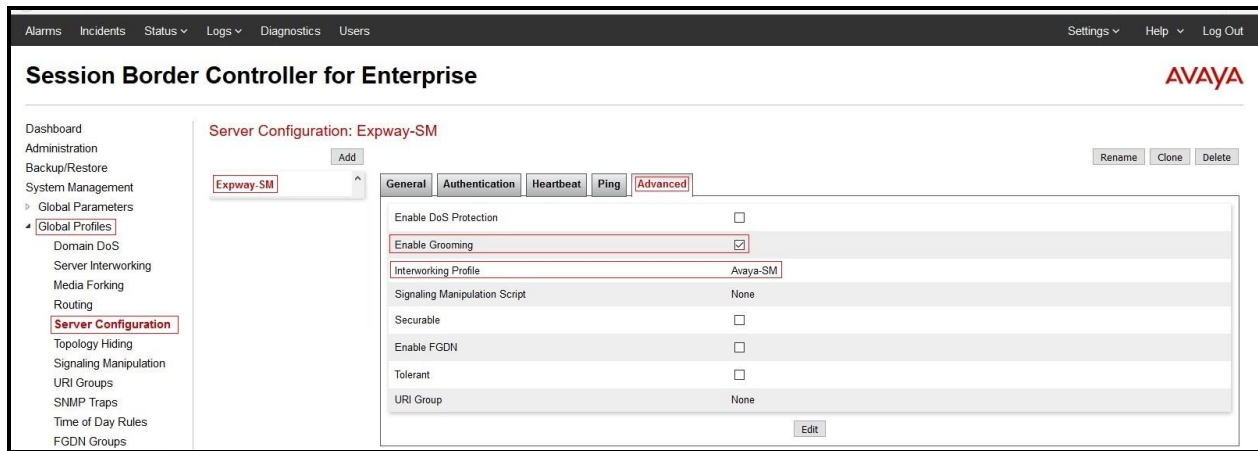


Figure 53: Server Configuration – Advanced - Avaya site

7.2.4. Configure Server – Vodafone DE SIP Trunk

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name: SP-VF-DE**

On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**
- **IP Address/FQDN:** **192.168.49.191** (Vodafone DE SIP Signaling Server IP Address)
- **Port:** **5060**
- **Transport:** **UDP**
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), and Topology Hiding. The main content area is titled 'Server Configuration: SP-VF-DE' and features an 'Add' button. Below this, there are tabs for General, Authentication, Heartbeat, Ping, and Advanced. The 'General' tab is active, showing a 'Server Type' dropdown set to 'Trunk Server'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with the values '192.168.49.191', '5060', and 'UDP'. An 'Edit' button is located at the bottom right of the table. The top of the interface includes a navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out.

IP Address / FQDN	Port	Transport
192.168.49.191	5060	UDP

Figure 54: Server Configuration – General - Vodafone DE

On the **Advanced** tab, enter the following:

- **Interworking Profile: SP-General** (see Section 7.2.2)
- Click **Finish** (not shown)

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main title is "Session Border Controller for Enterprise" with the Avaya logo. A left sidebar lists various configuration categories, with "Server Configuration" highlighted. The main content area is titled "Server Configuration: SP-VF-DE" and features tabs for General, Authentication, Heartbeat, Ping, and Advanced. The Advanced tab is active, showing a list of configuration options: Enable DoS Protection, Enable Grooming, Interworking Profile (set to SP-General), Signaling Manipulation Script (set to None), Securable, Enable FGDN, Tolerant, and URI Group (set to None). Each option has a checkbox or a text input field. An "Add" button is located above the configuration list, and an "Edit" button is at the bottom right of the list.

Figure 55: Server Configuration – Advanced - Vodafone DE

7.2.5. Configure Routing – Avaya Site

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.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name: To-ExpwaySM** and click **Next** button (Not Shown)

- Select **Load Balancing: Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**
- **Server Configuration: Expway-SM** (see Section 7.2.3)
- **Next Hop Address: 192.168.67.47:5061 (TLS)** (Session Manager IP Address)
- Click **Finish**

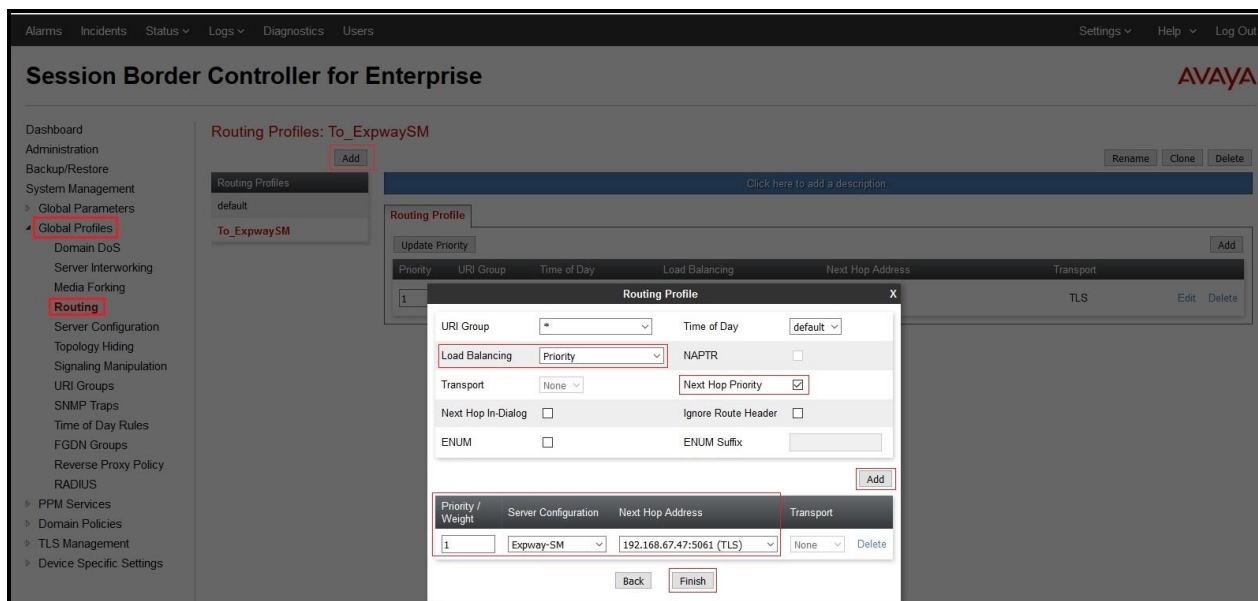


Figure 56: Routing to Session Manager

7.2.6. Configure Routing – Vodafone DE SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: To_Trunks** and click **Next** button (not shown)

- **Load Balancing: Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1, Server Configuration: SP-VF-DE** (see Section 7.2.4)
- **Next Hop Address: 192.168.49.191:5060 (UDP)** (Vodafone DE Signaling Server IP Address)
- Click **Finish**

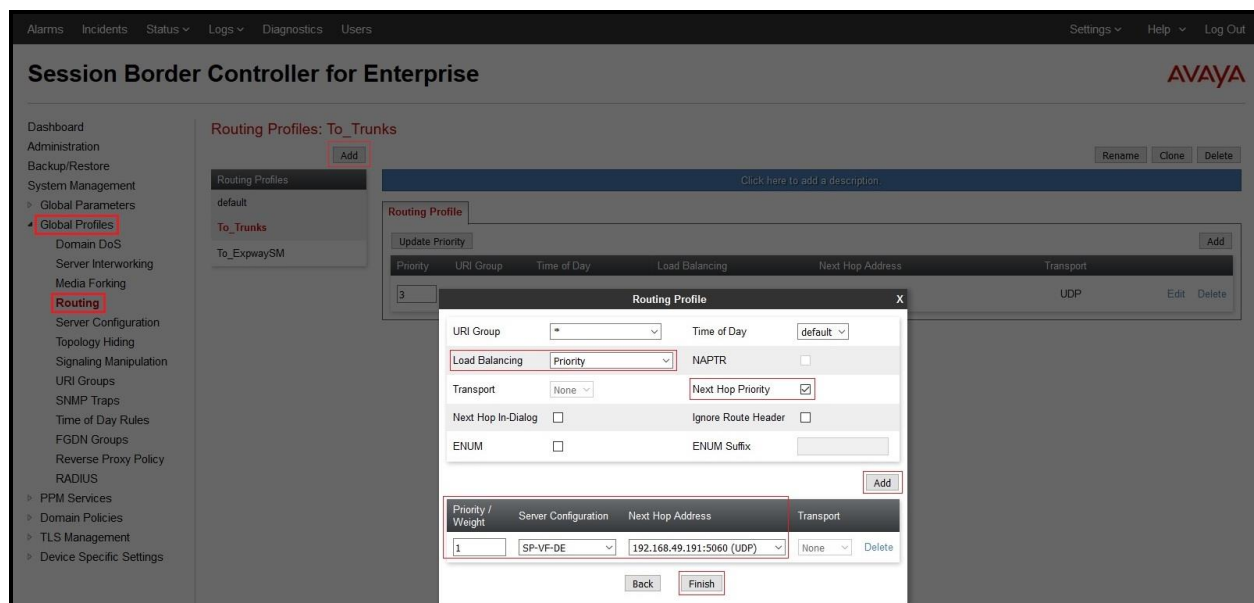


Figure 57: Routing to Vodafone DE SIP Trunk

7.2.7. Configure Topology Hiding – Avaya Site

The **Topology Hiding** screen allows an administrator to manage 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.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name: MT-Domain** and click **Finish** (not shown)

Select **MT-Domain** from **Topology Hiding Profiles** list and click **Edit** button

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **customera.com**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **customera.com**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **customera.com**

Click **Finish** (not shown)

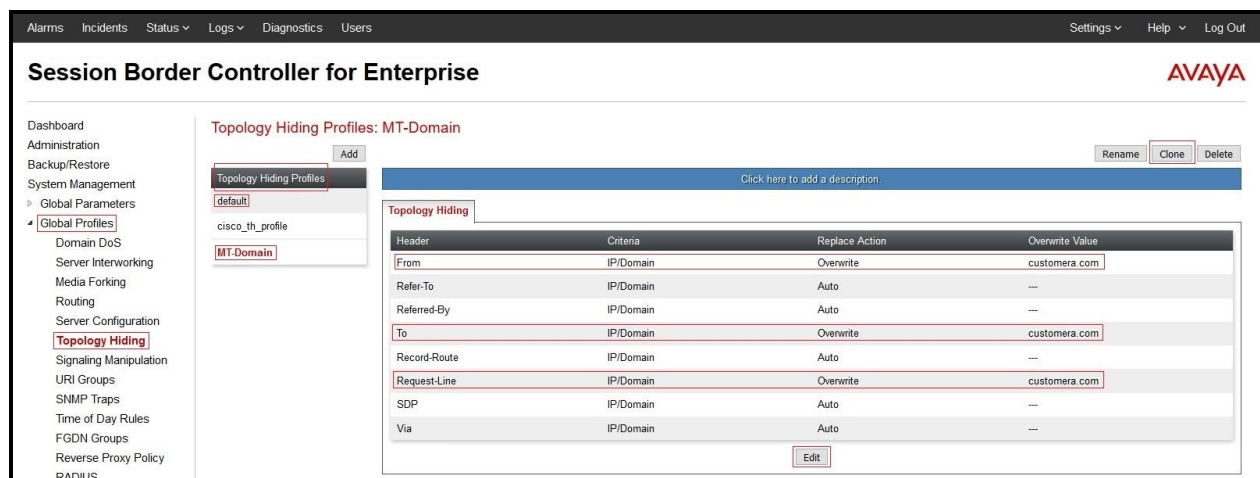


Figure 58: Topology Hiding To Session Manager

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name: VF-DE-TH** and click **Finish** (not shown)

Select **VF-DE-TH** from **Topology Hiding Profiles** list and click **Edit** button

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
In the **Overwrite Value** column: **avadeugm.arcor.de**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **avadeugm.arcor.de**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **avadeugm.arcor.de**

Click **Finish** (not shown)

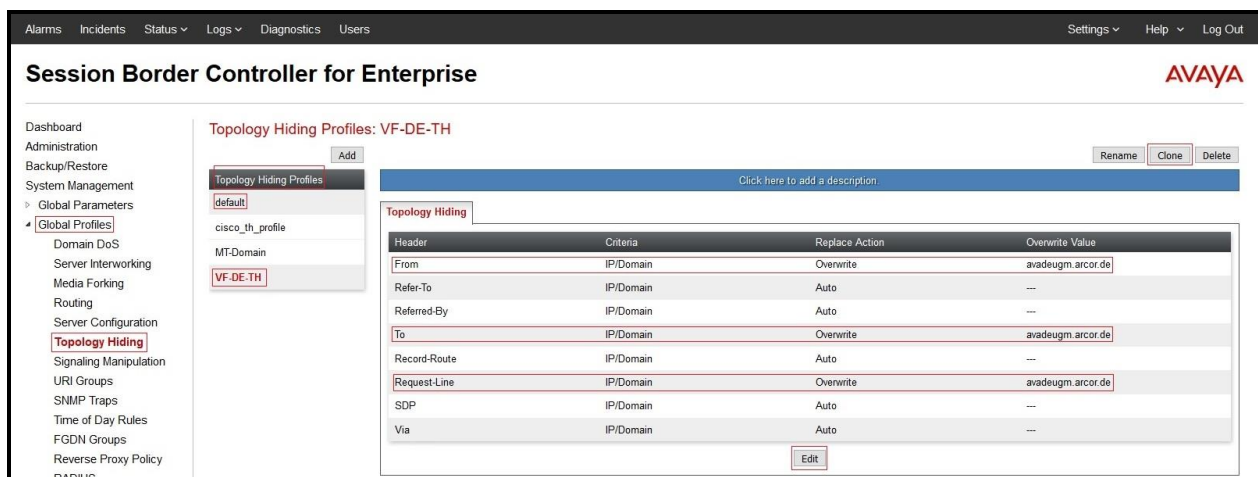


Figure 59: Topology Hiding To Vodafone DE

7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage 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 different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

7.3.1. Create Media Rules

Media Rules allow one to define 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 Avaya SBCE security product. For the compliance test, the predefined **default-low-med-enc** media rule (shown below) was used to clone and edit.

From the menu on the left-hand side, select **Domain Policies → Media Rules**

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name: ExpSM-SRTP-Pref**. Click **Finish** (not shown)
- Select **ExpSM-SRTP-Pref** under **Media Rules** to **Edit**

The **Encryption** tab indicates that **RTP** and **SRTP_AES_CM_128_HMAC_SHA1_80** encryption were used as **Preferred Formats** for Audio Encryption.

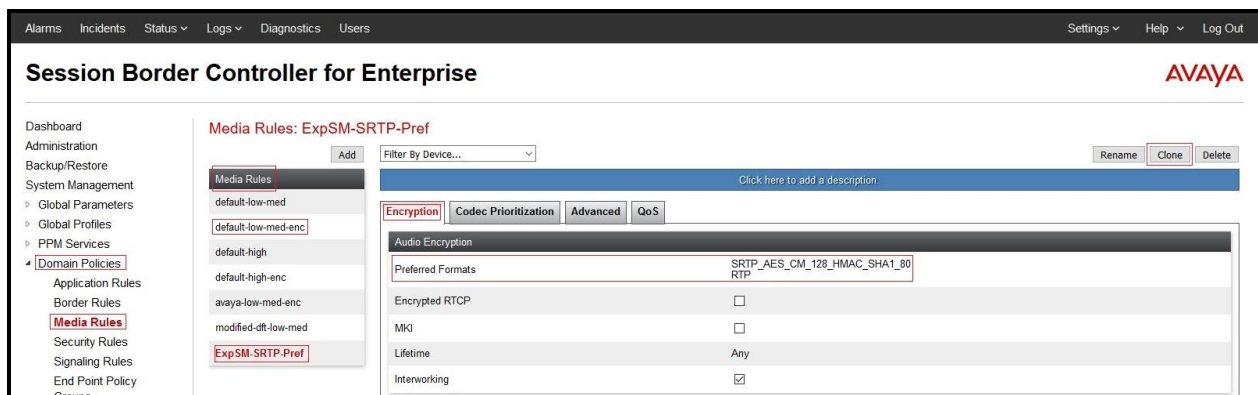


Figure 60: Media Rule - Encryption

The **Advanced** tab indicates that **Silencing Enabled** is checked and **Timeout** is **60 second(s)**.

Click here to add a description.

Encryption Codec Prioritization **Advanced** QoS

Silencing

Silencing Enabled	<input checked="" type="checkbox"/>
Timeout	60 second(s)

Binary Floor Control Protocol

BFCP Enabled	<input type="checkbox"/>
--------------	--------------------------

Far End Camera Control

FECC Enabled	<input type="checkbox"/>
--------------	--------------------------

ANAT

ANAT Enabled	<input type="checkbox"/>
--------------	--------------------------

Edit

Figure 61: Media Rule – Advanced

The **QoS** tab indicates that **Enabled** is checked for the **QoS Type** as **DSCP** and **Audio DSCP** is **EF**.

Click here to add a description.

Encryption Codec Prioritization Advanced **QoS**

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP EF

Video QoS

Video DSCP EF

Edit

Figure 62: Media Rule - QoS

7.3.2. Create Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.3.3**. Two specific signaling rules were created for Session Manager and the Vodafone DE.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by one or more pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

7.3.2.1 Signaling Rules – Session Manager

Signaling rule **SM-SRules-Aura7** was created for Session Manager. **SM-SRules-Aura7** was created using all default values except the Signaling QoS tab.

The **General** tab settings are shown below.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (highlighted), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), End Point Policy, Groups, Session Policies, TLS Management, and Device Specific Settings. The main content area is titled "Signaling Rules: SM-SRules-Aura7" and includes an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". Below this, it indicates "Showing page 1 of 2." and a "Click here to add a description" link. The "General" tab is selected, showing settings for Inbound and Outbound traffic. The Inbound section includes "Requests" (Allow), "Non-2XX Final Responses" (Allow), "Optional Request Headers" (Allow), and "Optional Response Headers" (Allow). The Outbound section includes "Requests" (Allow), "Non-2XX Final Responses" (Allow), "Optional Request Headers" (Allow), and "Optional Response Headers" (Allow). The "Content-Type Policy" section has "Enable Content-Type Checks" checked, "Action" set to "Allow", "Multipart Action" set to "Allow", and an "Exception List" field. An "Edit" button is at the bottom right of the settings area.

Figure 63: Signaling Rule – SM – General

The **Signaling QoS** tab settings are shown below.

Click here to add a description.

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

Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	DSCP
DSCP	EF

Edit

Figure 64: Signaling Rule – SM – Signaling QoS

7.3.2.2 Signaling Rules – Vodafone DE

Signaling rule **VF-DE-SR** was created for Vodafone DE. **VF-DE-SR** was created using all default values except the Request Headers tab.

The **General** tab settings are shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. A left-hand navigation menu lists various system management and policy configuration options, with 'Signaling Rules' highlighted under 'Domain Policies'. The main content area is titled 'Signaling Rules: VF-DE-SR' and includes an 'Add' button, a 'Filter By Device...' dropdown, and action buttons for 'Rename', 'Clone', and 'Delete'. Below this, a tabbed interface shows the 'General' tab selected, with other tabs for 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab contains sections for 'Inbound' and 'Outbound' rules, each with a table of settings. The 'Inbound' section includes 'Requests' (Allow), 'Non-2XX Final Responses' (Allow), 'Optional Request Headers' (Allow), and 'Optional Response Headers' (Allow). The 'Outbound' section has identical settings. Below these is the 'Content-Type Policy' section, which includes a checkbox for 'Enable Content-Type Checks' (checked), a table for 'Action' (Allow, Multipart Action, Allow), and an 'Exception List' field. An 'Edit' button is located at the bottom right of the configuration area.

Inbound			
Requests	Allow		
Non-2XX Final Responses	Allow		
Optional Request Headers	Allow		
Optional Response Headers	Allow		

Outbound			
Requests	Allow		
Non-2XX Final Responses	Allow		
Optional Request Headers	Allow		
Optional Response Headers	Allow		

Content-Type Policy			
Enable Content-Type Checks <input checked="" type="checkbox"/>			
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Figure 65: Signaling Rule – Vodafone – General

The **Request Headers** tab settings are shown below. The settings are used for a configuration change to fix audio issue (See item# 4 in **Section 2.2**).

Click here to add a description.

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

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Referred-By	ALL	Forbidden	Remove Header	No	OUT	Edit Delete

Figure 66: Signaling Rule – Vodafone – Request Header

7.3.3. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**.
- Enter **Group Name: SM**
 - **Application Rule: default-trunk**
 - **Border Rule: default**
 - **Media Rule: ExpSM-SRTP-Pref** (See in Section 7.3.1)
 - **Security Rule: default-low**
 - **Signaling Rule: SM-SRules-Aura7** (See in Section 7.3.2)
- Select **Finish** (not shown)

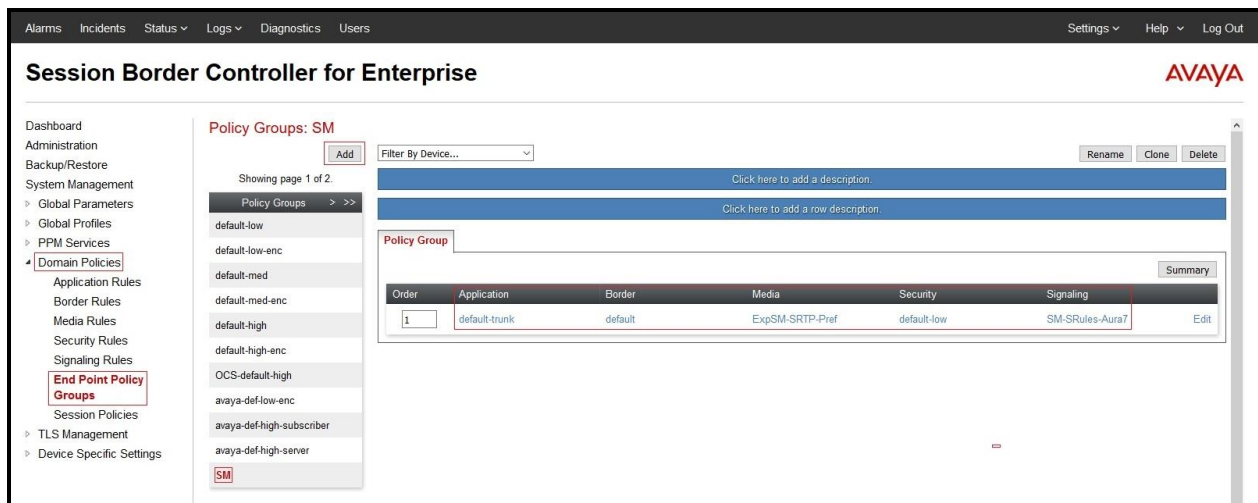


Figure 67: Endpoint Policy 1

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**.
- Enter **Group Name: VF-DE-EP-Policy**
 - **Application Rule: default-trunk**
 - **Border Rule: default**
 - **Media Rule: default-low-med**
 - **Security Rule: default-low**
 - **Signaling Rule: VF-DE-SR** (See in Section 7.3.2)
- Select **Finish** (not shown)

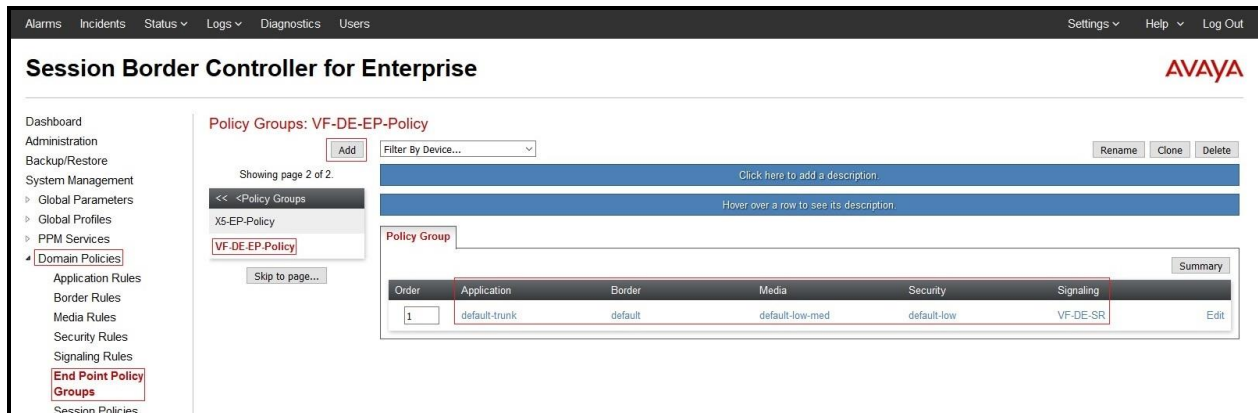


Figure 68: Endpoint Policy 2

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
 - **Name: Network_A1**
 - **Default Gateway: 10.32.128.254**
 - **Subnet Mask: 255.255.255.0**
 - **Interface: A1** (This is the Avaya SBCE inside interface)
 - Click the **Add** button to add the **IP Address** for inside interface: **10.32.128.18**
 - Click the **Finish** button to save the changes

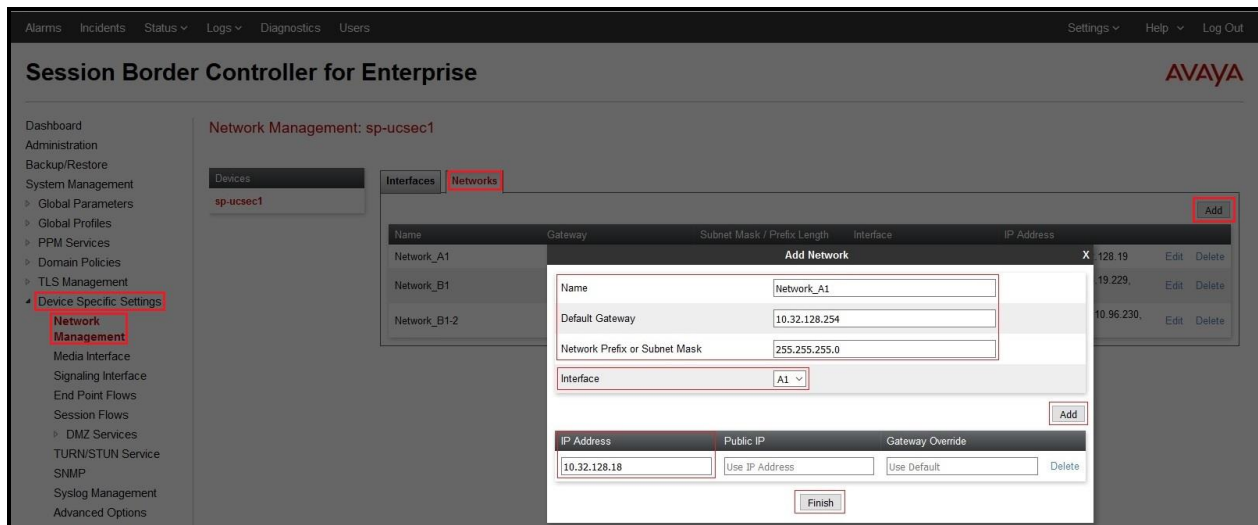


Figure 69: Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
 - **Name: Network_B1-2**
 - **Default Gateway: 192.168.96.254**
 - **Subnet Mask: 255.255.255.0**
 - **Interface: B1** (This is the Avaya SBCE outside interface)
 - Click the **Add** button to add the **IP Address** for outside interface: **192.168.96.232**
 - Click the **Finish** button to save the changes

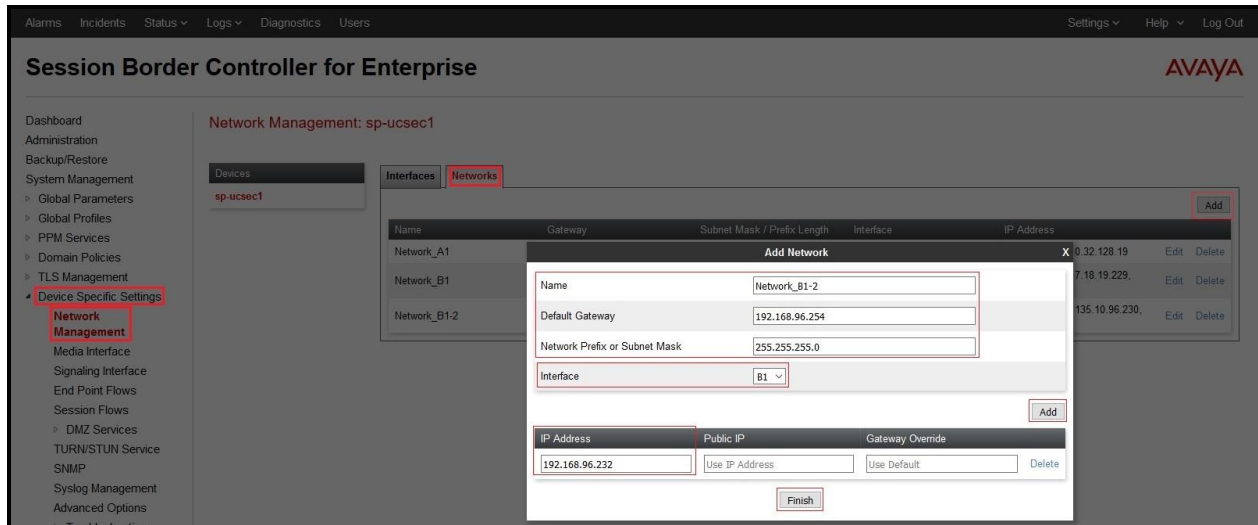


Figure 70: Network Management – Outside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state



Figure 71: Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the IP addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for inside port.

From the menu on the left-hand side, **Device Specific Settings** → **Media Interface**

- Select the **Add** button and enter the following:
 - **Name:** **Int_Media_Intf**
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.32.128.18** (Internal IP Address toward Session Manager)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
 - **Name:** **Ext_Media_Intf**
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **192.168.96.232** (External IP Address toward Vodafone DE)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)

Name	Media IP Network	Port Range	TLS Profile	Edit	Delete
Int_Media_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete
Ext_Media_Intf	192.168.96.232 Network_B1-2 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete
RW_Med_Outside_229	192.168.96.229 Network_B1-2 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete
RW_Med_Inside_19	10.32.128.19 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete

Figure 72: Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

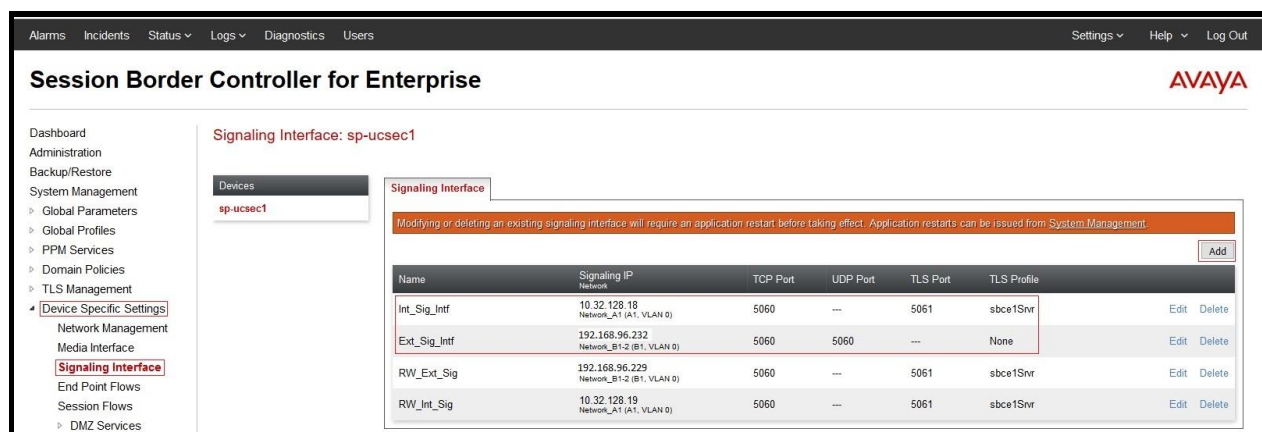
From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following:
 - **Name:** **Ext_Sig_Intf**
 - **IP Address:** Select **Network_B1-2 (B1,VLAN0)** and **192.168.96.232** (External IP Address toward Vodafone DE)
 - **UDP Port:** **5060**
 - Click **Finish** (not shown)

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following:
 - **Name:** **Int_Sig_Intf**
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.32.128.18** (Internal IP Address toward Session Manager)
 - **TLS Port:** **5061**
 - **TLS Profile:** **sbce1Srvr**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use. Session Manager 7.1 includes SMGR signed certs, not the Avaya demo certificates
 - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as Vodafone DE used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, System Management, and Device Specific Settings. The main content area is titled 'Signaling Interface: sp-ucsec1' and shows a table of configured signaling interfaces. A warning message at the top states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' The table has columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. There are four rows of data, each with Edit and Delete links.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	5060	---	5061	sbce1Srvr	Edit Delete
Ext_Sig_Intf	192.168.96.232 Network_B1-2 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
RW_Ext_Sig	192.168.96.229 Network_B1-2 (B1, VLAN 0)	5060	---	5061	sbce1Srvr	Edit Delete
RW_Int_Sig	10.32.128.19 Network_A1 (A1, VLAN 0)	5060	---	5061	sbce1Srvr	Edit Delete

Figure 73: Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows – SMVM Flow

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: Expway-SM**
 - **Server Configuration: Expway-SM** (see Section 7.2.3)
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: Ext_Sig_Intf** (see Section 7.4.3)
 - **Signaling Interface: Int_Sig_Intf** (see Section 7.4.3)
 - **Media Interface: Int_Media_Intf** (see Section 7.4.2)
 - **Secondary Media Interface: None**
 - **End Point Policy Group: SM** (see Section 7.3.3)
 - **Routing Profile: To_Trunks** (see Section 7.2.6)
 - **Topology Hiding Profile: MT-Domain** (see Section 7.2.7)
 - Leave other parameters as default
 - Click **Finish**

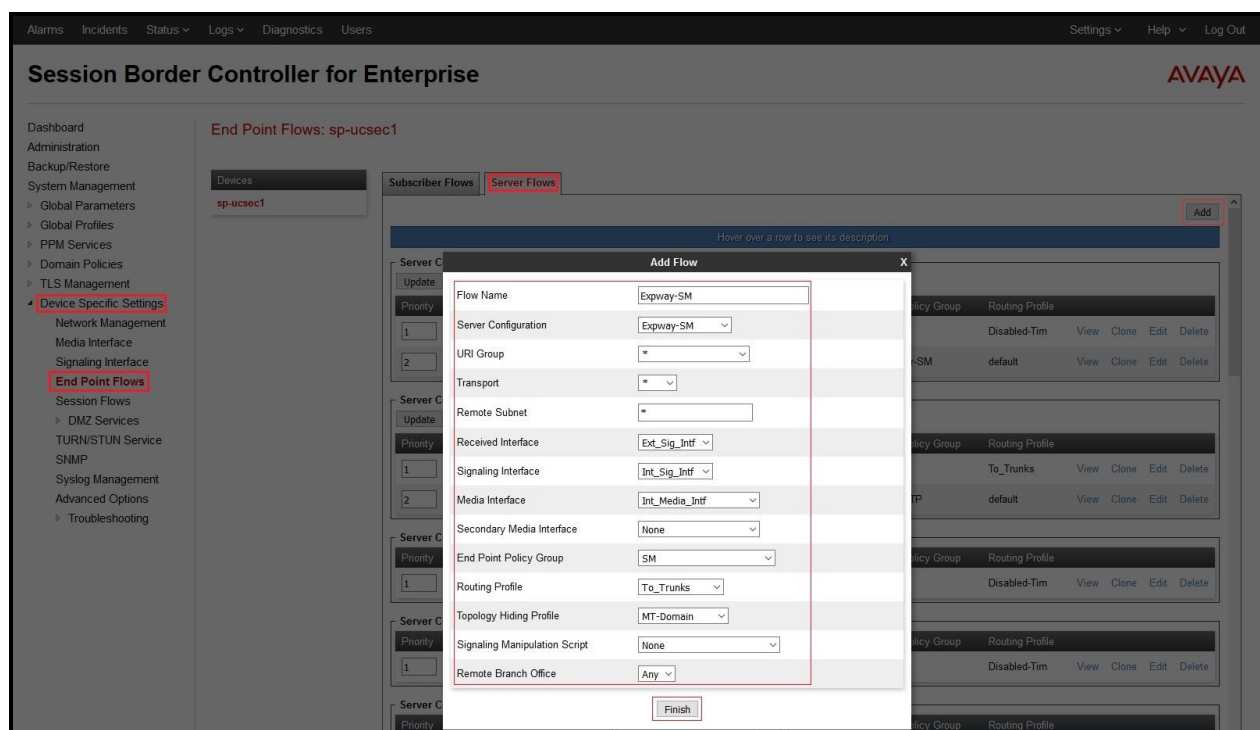


Figure 74: End Point Flow 1

7.4.4.2 Create End Point Flows – Vodafone DE SIP Trunk Flow

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: VF-DE-Flow**
 - **Server Configuration: SP-VF-DE** (see Section 7.2.4)
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: Int_Sig_Intf** (see Section 7.4.3)
 - **Signaling Interface: Ext_Sig_Intf** (see Section 7.4.3)
 - **Media Interface: Ext_Media_Intf** (see Section 7.4.2)
 - **Secondary Media Interface: None**
 - **End Point Policy Group: VF-DE-EP-Policy** (see Section 7.3.3)
 - **Routing Profile: To_ExpwaySM** (see Section 7.2.5)
 - **Topology Hiding Profile: VF-DE-TH** (see Section 7.2.7)
 - Leave other parameters as default
 - Click **Finish**

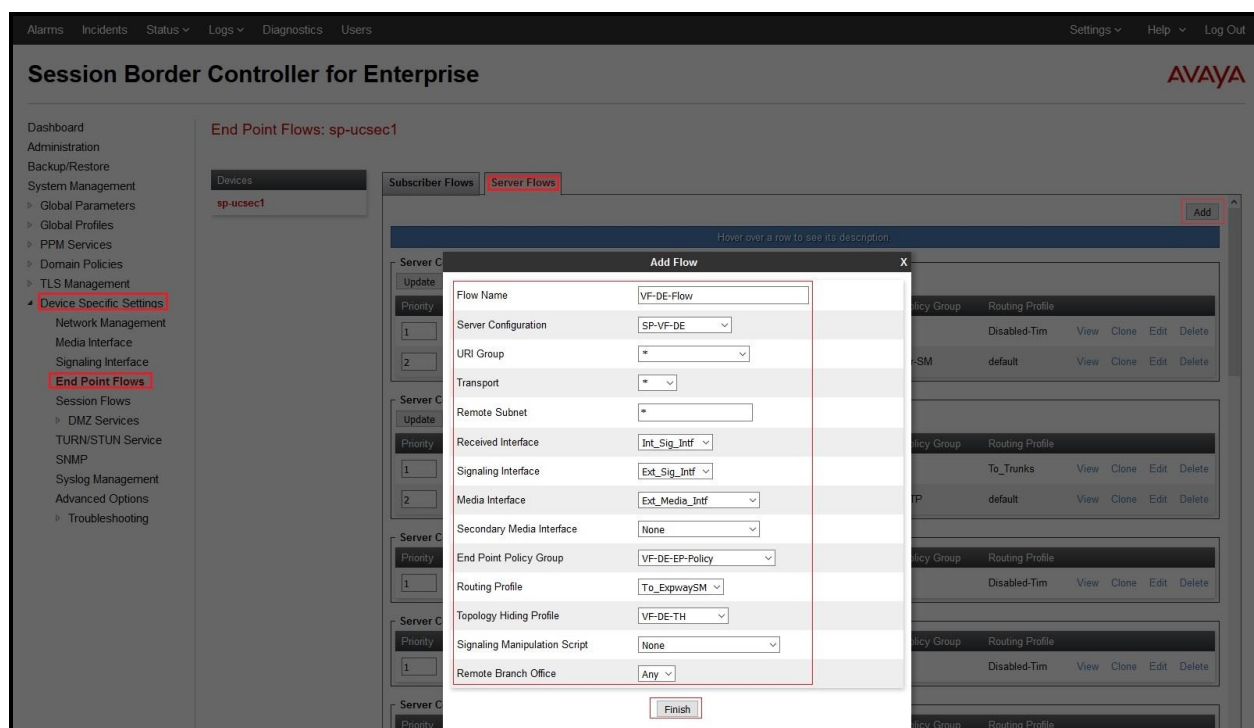


Figure 75: End Point Flow 2

8. Vodafone DE SIP Trunk Configuration

Vodafone DE is responsible for the network configuration of the Vodafone DE SIP Trunk service. Vodafone DE will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. Vodafone DE will provide the IP address of the Vodafone DE SIP Trunk SIP signaling/SBC IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. Vodafone DE also provides the Vodafone DE SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Vodafone DE SIP Trunk and the enterprise is a static IP address configuration.

9. Verification Steps

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.

Verification Steps:

1. 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.
2. 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.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

1. Communication Manager: Enter the following commands using the Communication Manager System Access Terminal (SAT) interface.
 - **list trace station** <extension number> - Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
 - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
 - **status trunk-group** <trunk-group number> - Displays trunk-group state information.
 - **status signaling-group** <signaling-group number> - Displays signaling-group state information.
2. Session Manager:
 - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
 - **traceSM** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
3. Avaya SBCE: Debug logging can be started in two different ways:
 - **GUI of the SBC: Device Specific Settings → Troubleshooting → Debugging.**
 - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
 - CALL PROCESSING: enable all subsystems under SSYNDI process.
 - PPM: enable all subsystems under CONFIG_PROXY process.The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
 - **Command Line Interface:** Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura[®] Communication Manager, Avaya Aura[®] Session Manager and Avaya Session Border Controller for Enterprise to Vodafone DE. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workaround.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at:

<http://support.avaya.com/>

Avaya Aura[®] Session Manager/System Manager

[1] *Administering Avaya Aura[®] Session Manager*, Release 7.1.1, Issue 2, August 2017

[2] *Administering Avaya Aura[®] System Manager*, Release 7.1.1, Issue 7, October 2017

Avaya Aura[®] Communication Manager

[3] *Administering Avaya Aura[®] Communication Manager*, Release 7.1.1, Issue 2, August 2017

Avaya Phones

[4] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition H.323*, Issue 1, April 2015

[5] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition SIP*, Issue 2, August 2015

[6] *Avaya one-X[®] Communicator Overview and Planning*, Release 6.2 FP6, April 2015

Avaya Session Border Controller for Enterprise

[7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2, Issue 3, September 2017

IETF (Internet Engineering Task Force) SIP Standard Specifications

[8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

Product documentation for Vodafone DE SIP Trunk SIP Trunk may be found at:

www.vodafone.de

©2017 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.