



Nexmo SIP Trunking Configuration Guide

**Avaya Aura 6.3.18.0.631804
With
Avaya SBCe 6.3.7-01-12611**

June 2017

Contents

1 Introduction.....	4
2 SIP Trunking Network Components.....	4
2.1 Network Components.....	4
3 Features.....	5
3.1.1 Features Supported.....	5
3.1.2 Features Not Supported by PBX.....	5
3.1.3 Caveats and Limitations.....	5
4 Configuration.....	6
4.1 IP Address Worksheet.....	6
4.2 Configuring Avaya Aura Communication Manager.....	7
4.2.1 Licenses.....	7
4.2.2 System Features.....	8
4.2.3 IP Node Names.....	8
4.2.4 IP Codecs.....	9
4.2.5 IP Network Region.....	9
4.2.6 Signaling Group.....	10
4.2.7 Trunk Group.....	10
4.2.8 Route Pattern.....	12
4.2.9 Dialing Pattern and Feature Code.....	12
4.2.10 Call Routing.....	13
4.2.11 Caller ID.....	13
4.2.12 Avaya Aura Extensions.....	14
4.3 Configuring Avaya Aura Session Manager.....	16
4.3.1 Add Adaptations.....	17
4.3.2 SIP Entities.....	18
4.3.3 Routing Policies.....	21
4.3.4 Dial Patterns.....	22
4.3.5 SIP Extension.....	24
4.4 Configuring Avaya Session Border Controller for Enterprise.....	26
4.4.1 Global Profile.....	26
4.4.2 Domain Policies.....	34
4.4.3 Device Specific Settings.....	37

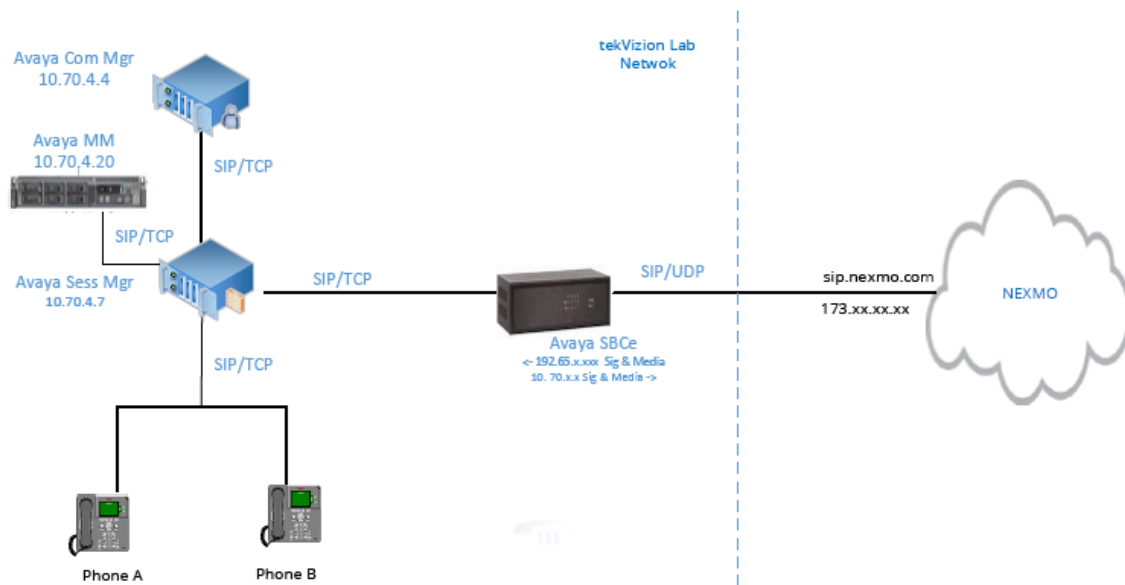
4.5 Avaya Modular Messaging.....	39
4.6 Nexmo Configuration.....	41
4.6.1 Configure Numbers in Nexmo Account.....	41

1 Introduction

This document is intended for the SIP trunk customer's technical staff and Value Added Retailer (VAR) having installation and operational responsibilities. This configuration guide provides steps for configuring Avaya Aura 6.3.18.0.631804 and Avaya SBCe 6.3.7-01-12611 to Nexmo SIP Trunking services.

2 SIP Trunking Network Components

The network for the SIP trunk reference configuration is illustrated below and is representative of an Avaya Aura and Avaya SBCe configuration to Nexmo SIP trunking.



2.1 Network Components

Component	Version	Comments
Avaya Aura	6.3.18.0.631804	
Avaya SBCe	6.3.7-01-12611	
Avaya MM	5.2-11.0	Avaya Voicemail

Avaya 9630G	Version: SIP96xx_2_6_14.5.bin	Avaya Phone
Cisco IP Phone	Model: CP-7965	This Cisco IP Phone is the PSTN test device
	App Load ID: jar45sccp.9-4-2TH1-1.sbn	
	Boot Load ID: tnp65.9-3-1-CR17.bin	

3 Features

3.1.1 Features Supported

- Incoming and outgoing off-net calls using G711ULAW & G711ALAW voice codecs
- Calling Line (number) Identification Presentation
- Calling Line (number) Identification Restriction
- Call hold and resume
- Call transfer (unattended and attended)
- Call Conference
- Call forward (all, no answer)
- DTMF relay both directions (RFC2833)
- Media flow-through on Avaya SBCe

3.1.2 Features Not Supported by PBX

- None

3.1.3 Caveats and Limitations

- Session refresh is always done by Avaya Aura. The issue does not impact the calls.

4 Configuration

4.1 IP Address Worksheet

The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document, and are for **illustrative purposes only**. The customer must obtain and use the values for your deployment.

Table 1 – IP Addresses

Component	Lab Value	Customer Value
Avaya SBCe		
LAN IP Address	10.70.4.13	
LAN Subnet Mask	255.255.255.0	
WAN IP Address	192.xx.xx.XXX	
WAN Subnet Mask	255.255.255.128	
Avaya Aura		
System IP Address	10.70.4.3	

4.2 Configuring Avaya Aura Communication Manager

This section describes the Avaya Aura Communication Manager configuration necessary to support connectivity to Avaya SBCe. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Nexmo via Avaya SBCe. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and Session Manager has been previously completed.

The Avaya Aura Communication Manager configuration was performed using System Access Terminal (SAT) via Putty.

```
This system is restricted to authorized users for legitimate business purposes.
Unauthorized access is a criminal violation of the law.
Copyright 1992 - 2013 Avaya Inc. All Rights Reserved.
Except where expressly stated otherwise, this Product is protected by copyright
and other laws respecting proprietary rights. Certain software programs or
portions thereof included in this Product may contain software distributed
under third party agreements, which may contain terms that expand or limit
rights to use certain portions of the Product. Information identifying third
party components and terms that apply to them are available on Avaya's web
site at: http://support.avaya.com/ThirdPartyLicense/.
```

4.2.1 Licenses

In order to connect to Nexmo, Avaya Aura Communication Manager needs to have enough SIP trunk licenses. Use the display system-parameters customer-options command to verify the available SIP Trunk licenses

```
display system-parameters customer-options Page 2 of 12
OPTIONAL FEATURES

IP PORT CAPACITIES USED
Maximum Administered H.323 Trunks: 4000 0
Maximum Concurrently Registered IP Stations: 2400 1
Maximum Administered Remote Office Trunks: 4000 0
Maximum Concurrently Registered Remote Office Stations: 2400 0
Maximum Concurrently Registered IP eCons: 28 0
Max Concur Registered Unauthenticated H.323 Stations: 100 0
Maximum Video Capable Stations: 2400 0
Maximum Video Capable IP Softphones: 20 0
Maximum Administered SIP Trunks: 4000 35
Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
Maximum Number of DS1 Boards with Echo Cancellation: 80 0
```

Figure 1: Cisco UCM Version

4.2.2 System Features

Use the change system-parameters features command and ensure Trunk to Trunk Transfer is set to all

```
change system-parameters features Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? n
  Trunk-to-Trunk Transfer: all
  Automatic Callback with Called Party Queuing? n
  Automatic Callback - No Answer Timeout Interval (rings): 3
  Call Park Timeout Interval (minutes): 10
  Off-Premises Tone Detect Timeout Interval (seconds): 20
  AAR/ARS Dial Tone Required? n

  Music (or Silence) on Transferred Trunk Calls? no
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
  Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
  Automatic Circuit Assurance (ACA) Enabled? n

  Abbreviated Dial Programming by Assigned Lists? n
  Auto Abbreviated/Delayed Transition Interval (rings): 2
  Protocol for Caller ID Analog Terminals: Bellcore
  Display Calling Number for Room to Room Caller ID Calls? n
```

4.2.3 IP Node Names

Use the display node-names ip command to verify that node names have been properly defined for Communication Manager (procr) and Session Manager (AASM in this test). These node names will be needed for configuring the Signaling Group later.

```
display node-names ip
IP NODE NAMES
  Name          IP Address
  AASM          10.70.4.7
  AASMHA        10.70.4.24
  default       0.0.0.0
  procr         10.70.4.4
  procr6       ::
```


4.2.4 IP Codecs

The change ip-codec-set command is used for assigning the proper codecs. For this setup, ip-codec-set 1 is used.

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

IP CODEC SET

Codec Set: 1

Audio          Silence      Frames      Packet
Codec          Suppression  Per Pkt     Size (ms)
1: G.711MU      n           2           20
2: G.711A      n           2           20
3: G.729        n           2           20
4: G.722-64K   2           2           20
5:
6:
7:

Media Encryption
1: none
2:
3:
```

4.2.5 IP Network Region

For this test, IP Network region 3 was created using the change ip-network-region 1 command

```
display ip-network-region 1                               Page 1 of 20

IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: lab.tekvizion.com
Name: SIP
MEDIA PARAMETERS
Codec Set: 1      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
```

4.2.6 Signaling Group

Use the add signaling-group x command to create a signaling group 2 between Communication Manager and Session Manager for SIP trunk calls.

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

SIGNALING GROUP

Group Number: 2          Group Type: sip
IMS Enabled? n          Transport Method: tcp
Q-SIP? n
IP Video? y             Priority Video? n          Enforce SIPS URI for SRTP? n
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
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr          Far-end Node Name: AASM
Near-end Listen Port: 5060         Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: lab.tekvizion.com

Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate          RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                     Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3            IP Audio Hairpinning? n
Enable Layer 3 Test? y                        Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n        Alternate Route Timer(sec): 6
```

4.2.7 Trunk Group

Use the add trunk-group x command to create trunk groups for the associated signaling group, trunk group 2 is associated with Signaling group 2 for SIP trunk between CM and SM.

```
change trunk-group 2                                         Page 1 of 21

TRUNK GROUP

Group Number: 2          Group Type: sip          CDR Reports: y
Group Name: Trunk to PSTN          COR: 1          TN: 1          TAC: #002
Direction: two-way          Outgoing Display? n
Dial Access? n          Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
Member Assignment Method: auto
Signaling Group: 2
Number of Members: 6
```

```

change trunk-group 2                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: Auto

                                         Redirect On OPTIM Failure: 5000

  SCCAN? n                               Digital Loss Group: 18
                                         Preferred Minimum Session Refresh Interval(sec): 900

  Disconnect Supervision - In? y Out? y

  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n

  Caller ID for Service Link Call to H.323 1xC: station-extension

```

```

change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES

  ACA Assignment? n                               Measured: none
                                                    Maintenance Tests? y

  Suppress # Outpulsing? n   Numbering Format: public
                                                    UII Treatment: service-provider

                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n

  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y

```

- The Numbering Format is set to Public. Outbound calls to Nexmo uses this trunk and uses the Public Numbering table to send the calling party number.

```

change trunk-group 2                                     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: From
  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

```

- Send Diversion Header is enabled to send the diversion information for voice mail.

4.2.8 Route Pattern

Use the change route-pattern 2 command to add routing preference for SIP trunk to Session Manager.

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

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

- This route is associated with trunk group 2

4.2.9 Dialing Pattern and Feature Code

Use the change dialplan analysis and change feature-access-codes commands

```
change dialplan analysis
```

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

- ARS access code is set to 9

```
change feature-access-codes
```

FEATURE ACCESS CODE (FAC)										Page 1 of 10	
Abbreviated Dialing List1 Access Code:											
Abbreviated Dialing List2 Access Code:											
Abbreviated Dialing List3 Access Code:											
Abbreviated Dial - Prgm Group List Access Code:											
Announcement Access Code:											
Answer Back Access Code: *72											
Auto Alternate Routing (AAR) Access Code: 8											
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: *70											
Call Pickup Access Code: *71											
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:											

4.2.12 Avaya Aura Extensions

Create a SIP extension as shown below.

```
change off-pbx-telephone station-mapping 2140
```

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2140	OPS		-	2140	aar	1	
			-				
			-				
			-				
			-				
			-				
			-				

- Enter station extension.
- Application: Type OPS
- Trunk Selection: Type aar

```
change station 2140
```

STATION		
Extension: 2140	Lock Messages? <u>n</u>	BCC: 0
Type: <u>630SIP</u>	Security Code: <u>*</u>	TN: <u>1</u>
Port: <u>S00008</u>	Coverage Path 1: <u>1</u>	COR: <u>1</u>
Name: <u>Nexmo, U1</u>	Coverage Path 2: <u></u>	COS: <u>1</u>
	Hunt-to Station: <u></u>	
STATION OPTIONS		
Loss Group: <u>19</u>	Time of Day Lock Table: <u></u>	
	Message Lamp Ext: <u>2140</u>	
Display Language: <u>english</u>	Button Modules: <u>0</u>	
Survivable COR: <u>internal</u>		
Survivable Trunk Dest? <u>y</u>	IP SoftPhone? <u>n</u>	
	IP Video? <u>n</u>	

change station 2140Page 2 of 6

STATION

FEATURE OPTIONS

LWC Reception: spe

LWC Activation? y

CDR Privacy? n

Per Button Ring Control? n

Bridged Call Alerting? n

Active Station Ringing: single

Coverage Msg Retrieval? y

Auto Answer: none

Data Restriction? n

Idle Appearance Preference? n

Bridged Idle Line Preference? n

Restrict Last Appearance? y

H.320 Conversion? n

Per Station CPN - Send Calling Number?

EC500 State: enabled

MWI Served User Type:

AUDIX Name:

Coverage After Forwarding? s

Emergency Location Ext: 2140

Direct IP-IP Audio Connections? y

Always Use? n IP Audio Hairpinning? n

change station 2140Page 3 of 6

STATION

Bridged Appearance Origination Restriction? n

IP Phone Group ID:

ENHANCED CALL FORWARDING

	Forwarded Destination	Active
Unconditional For Internal Calls To:	<u>2301</u>	<u>y</u>
External Calls To:	<u>2301</u>	<u>y</u>
Busy For Internal Calls To:	<u> </u>	<u>n</u>
External Calls To:	<u> </u>	<u>n</u>
No Reply For Internal Calls To:	<u> </u>	<u>n</u>
External Calls To:	<u>187</u> <u> </u>	<u>y</u>

change station 2140Page 6 of 6

STATION

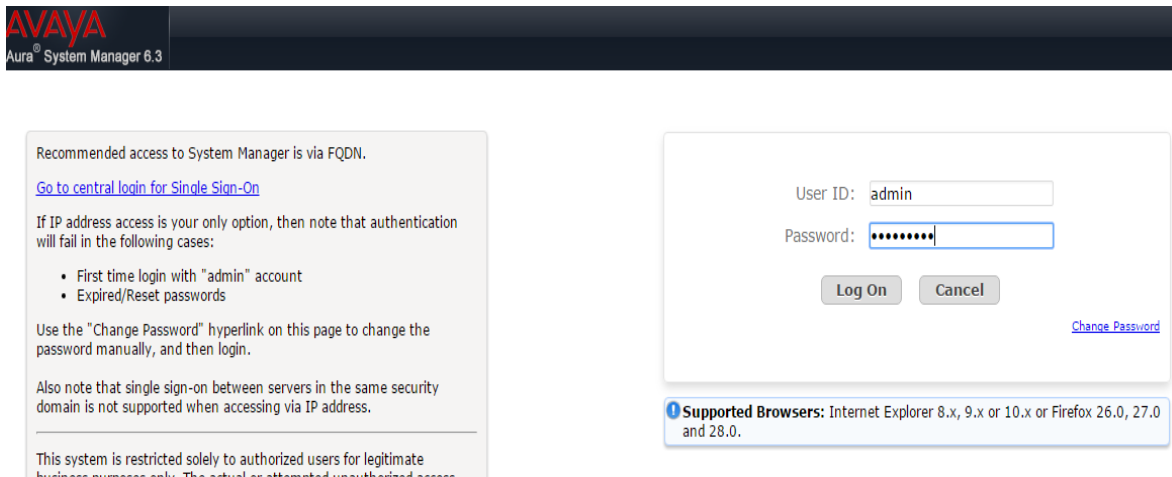
SIP FEATURE OPTIONS

Type of 3PCC Enabled: None

SIP Trunk: aar

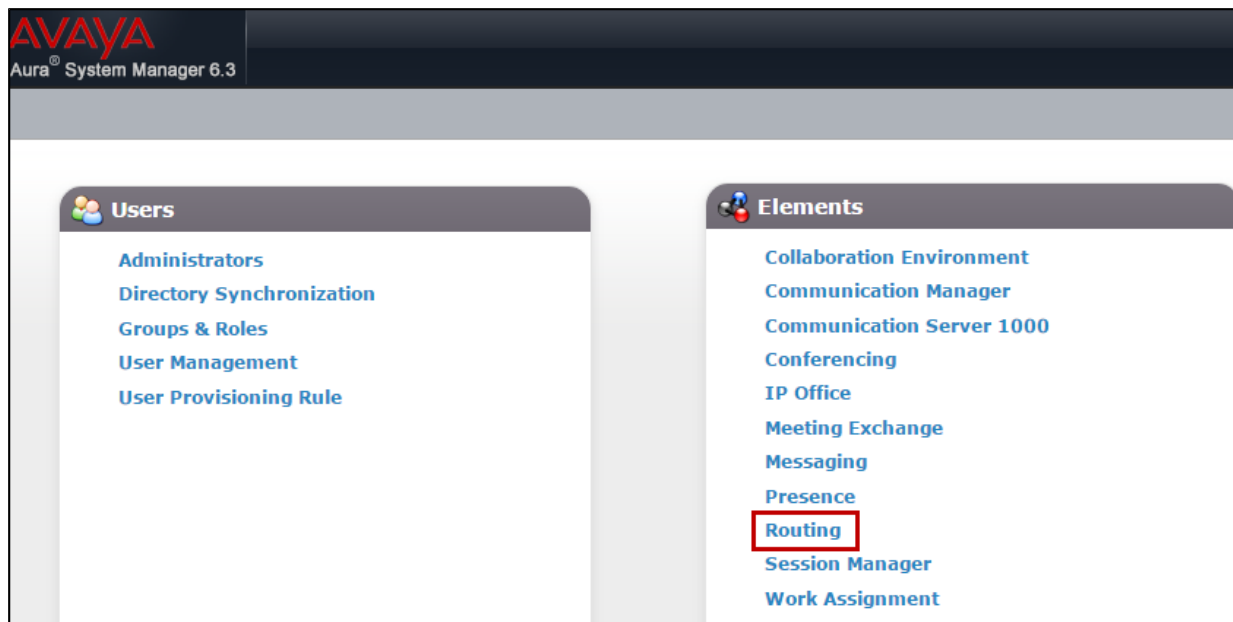
4.3 Configuring Avaya Aura Session Manager

The Avaya Aura Session Manager configuration utilizes Avaya Aura System Manager. The Avaya Aura System Manager Web login screen is accessed via <https://<IP Address/FQDN>>. Use admin as User ID and input associated password, and then click Log on. It is assumed that the Domain, Location and Endpoint for Session Manager have been previously configured.



The image shows the Avaya Aura System Manager 6.3 login interface. It features a dark header with the Avaya logo and 'Aura System Manager 6.3'. Below the header, there is a login form with fields for 'User ID' (containing 'admin') and 'Password' (masked with dots). There are 'Log On' and 'Cancel' buttons, and a 'Change Password' link. To the left of the form, there is a text box with instructions: 'Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: First time login with "admin" account, Expired/Reset passwords. Use the "Change Password" hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address. This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access is prohibited.' Below the form, there is a note: 'Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 and 28.0.'

Navigate to **Home > Elements > Routing**



4.3.1 Add Adaptations

Modifications to the SIP messaging within the Session Manager can be made in the Adaptions module. The idea here is to create an adaptation entity, identified by its Name, and then assign it to a SIP Entity.

Navigate to **Routing > Adaptations > New**

4.3.1.1 *Adaptation for Avaya SBCe*

The following adaption rules are provisioned in the “Module parameter” field:

fromto =true: If set to true, then adaptation modifies From and To headers of the message.

Routing / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: AASBCE

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

Name	Value
fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*011	*10	*20		*3	+	destination		
*1	*11	*11		*0	+	destination		

Select : All, None

Commit Cancel

- An adaptation is created under the Digit Conversion for Outgoing Calls from SM to cause SM to insert the + sign in the From and To headers on SM-originated calls routed to Avaya SBCe.

4.3.2 SIP Entities

4.3.2.1 SIP Entity for Avaya SBCe

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: AASBCE

* FQDN or IP Address: 10.70.4.13

Type: SIP Trunk

Notes:

Adaptation: AASBCE

Location: Plano

Time Zone: America/Chicago

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item								Filter: Enable
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* AASM6_AASBCE_5060_1	AASM6	TCP	* 5060	AASBCE	* 5060	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items			Filter: Enable
<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

- Add the AvayaSBC Adaption created earlier, to the SIP Entity
- The link between the SM and the Avaya sBCe was configured as trusted using TCP protocol and port 5060

4.3.2.2 SIP Entity for Avaya CM

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: AACM6

* FQDN or IP Address: 10.70.4.4

Type: CM

Notes: CM 6.3

Adaptation:

Location: Plano

Time Zone: America/Chicago

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item								Filter: Enable
	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* AASM6_AACM6_5060_TC	AASM6	TCP	* 5060	AACM6	* 5060	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items			Filter: Enable
	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

- The link between the Avaya SM and the CM was configured as trusted using TCP protocol and port 5060.

4.3.2.3 SIP Entity for Avaya MM

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

Cancel

General

* Name:

AAMM

* FQDN or IP Address:

10.70.4.20

Type:

Modular Messaging

Notes:

Modular Messaging

Adaptation:

Location:

Plano

Time Zone:

America/Chicago

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

Loop Detection

Loop Detection Mode:

Off

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV:

Add

Remove

1 Item

Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* AASM_AAMM	AASM6	TCP	* 5060	AAMM	* 5060	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add

Remove

0 Items

Filter: Enable

	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--	-------------------------------	---------------------	-------

Commit

Cancel

- The link between the Avaya SM and the Avaya MM was configured as trusted using TCP protocol and port 5060

4.3.3 Routing Policies

Navigate to **Routing > Routing Policies > New**

4.3.3.1 Routing Policy to Avaya SBCe

Create a routing policy to Avaya SBCe as shown below.

The screenshot shows the 'Routing Policy Details' form in a web application. The left sidebar contains a menu with 'Routing Policies' selected. The main area has a breadcrumb 'Home / Elements / Routing / Routing Policies' and buttons for 'Commit' and 'Cancel'. The 'General' tab is active, showing fields for 'Name' (to_AASBCE), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section with a 'Select' button and a table.

Name	FQDN or IP Address	Type
AASBCE	10.70.4.13	SIP Trunk

4.3.3.2 Routing Policy to Avaya CM

Create a routing policy to Avaya CM as shown below

The screenshot shows the 'Routing Policy Details' form for a policy named 'to_AACM'. The 'General' tab is active, showing fields for 'Name' (to_AACM), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section with a 'Select' button and a table.

Name	FQDN or IP Address	Type	Notes
AACM6	10.70.4.4	CM	CM 6.3

4.3.3.3 Routing Policy to Avaya MM

Create a routing policy to Avaya MM as shown below

The screenshot shows the 'Routing Policy Details' form for a policy named 'to AAMM'. The 'General' tab is active, showing fields for 'Name' (to AAMM), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section with a 'Select' button and a table.

Name	FQDN or IP Address	Type	Notes
AAMM	10.70.4.20	Modular Messaging	Modular Messaging

4.3.4 Dial Patterns

4.3.4.1 Routing Policy to Avaya SBCe

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

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

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Plano	Plano	to_AASBCE	0	<input type="checkbox"/>	AASBCE	

Select : All, None

- Create a dial pattern to route the call to PSTN via Avaya SBCe and link the Routing Policy to Avaya SBCe as shown above.

4.3.4.2 Routing Policy to Avaya CM

Home / User Management x Routing x

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

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

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Plano	Plano	to_AACM	0	<input type="checkbox"/>	AACM6	

- Create a dial pattern to route the call to Avaya Aura and link the Routing Policy to Avaya CM as shown above

4.3.4.3 Routing Policy to Avaya MM

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

CommitCancel

General

* Pattern:2301

* Min:4

* Max:4

Emergency Call:☐

Emergency Priority:1

Emergency Type:

SIP Domain:lab.tekvizion.com ▼

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Plano	Plano	to AAMM	0	<input type="checkbox"/>	AAMM	

- Create a dial pattern to route the call to Avaya MM and link the Routing Policy to Avaya MM as shown above

4.3.5 SIP Extension

Create a SIP user profile as shown below.



Navigate to **User Management > Endpoints > Manage Users**

The screenshot displays the 'User Profile Edit' page for the user 2140@lab.tekvizion.com. The left sidebar shows the 'User Management' menu with 'Manage Users' selected. The main content area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' field and a 'Name' dropdown set to 'Primary'. Below this is a 'Communication Address' section with a table listing the user's SIP address.

Type	Handle	Domain
Avaya SIP	2140	lab.tekvizion.com

☒ **Session Manager Profile**

SIP Registration

* Primary Session Manager

Primary	Secondary	Maximum
6	0	6

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence

Termination Sequence

Call Routing Settings

* Home Location

Conference Factory Set

Call History Settings

Enable Centralized Call History? ☐

☐ **Collaboration Environment Profile**

☒ **CM Endpoint Profile**

* System

* Profile Type

Use Existing Endpoints ☐

* Extension

Template

Set Type

Security Code

Port

Voice Mail Number

Preferred Handle

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

Override Endpoint Name and Localized Name ☒

☐ **CS 1000 Endpoint Profile**

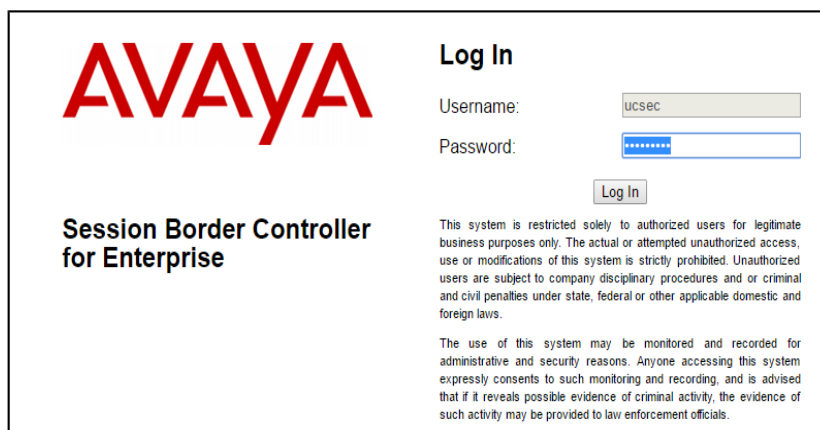
☐ **Messaging Profile**

☐ **CallPilot Messaging Profile**

☐ **IP Office Endpoint Profile**

4.4 Configuring Avaya Session Border Controller for Enterprise

- Log into Avaya Session Border Controller for Enterprise (SBCE) web interface by typing “https://X.X.X.X/sbc”.
- Enter the assigned Username and Password
- Click Log In



The image shows the login page of the Avaya Session Border Controller for Enterprise (SBCE) web interface. On the left, there is the Avaya logo in red and the text "Session Border Controller for Enterprise". On the right, there is a "Log In" section with a "Username:" field containing "UCSEC" and a "Password:" field with masked characters. Below the password field is a "Log In" button. To the right of the button, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Below this, another disclaimer states: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials."

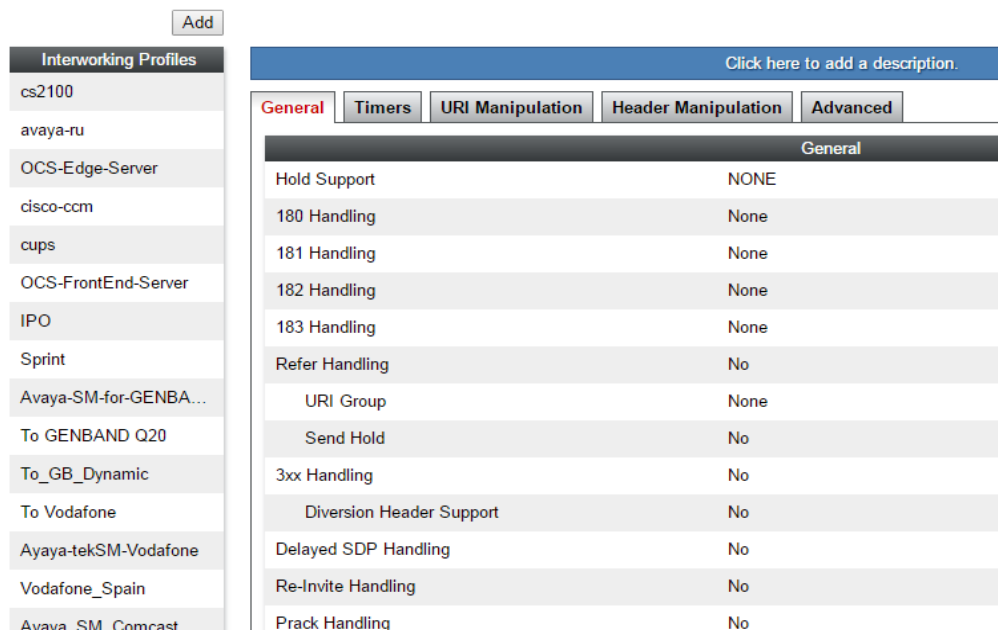
4.4.1 Global Profile

4.4.1.1 Server Interworking

Navigate to System Management > Global Profiles > Server Interworking. Create a clone named AASM of predefined Interworking Profile avaya-ru as shown below.

Create a Serving Interworking profile for Avaya SM as shown below.

Interworking Profiles: Avaya SM



The image shows the "Interworking Profiles: Avaya SM" configuration page. On the left, there is a list of "Interworking Profiles" with an "Add" button above it. The list includes: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, OCS-FrontEnd-Server, IPO, Sprint, Avaya-SM-for-GENBA..., To GENBAND Q20, To_GB_Dynamic, To Vodafone, Ayaya-tekSM-Vodafone, Vodafone_Spain, and Avaya SM Comcast. The "Avaya SM Comcast" profile is selected. On the right, there is a configuration table for the selected profile. The table has tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of settings.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No

Interworking Profiles: Avaya SM

Add

RenameClone

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

disco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

To Vodafone

Avaya-tekSM-Vodafone

Vodafone_Spain

Avaya_SM_Comcast

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

Allow 18X SDP

No

T.38 Support

Yes

URI Scheme

SIP

Via Header Format

RFC3261

Privacy

Privacy Enabled

No

User Name

P-Asserted-Identity

No

P-Preferred-Identity

No

Privacy Header

DTMF

DTMF Support

None

Edit

Interworking Profiles: Avaya SM

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

disco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

SIP Timers

Min-SE

Init Timer

Max Timer

Trans Expire

Invite Expire

Transport Timers

TCP Connection Inactive Timer

Edit

27

Interworking Profiles: Avaya SM

Click here to add a description.	
General	Timers
Record Routes	Both Sides
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

To Vodafone

Ayaya-tekSM-Vodafone

Vodafone_Spain

Click here to add a description.	
General	Timers
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No
Lync Extensions	No

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

To Vodafone

Ayaya-tekSM-Vodafone

Vodafone_Spain

Avaya SM Comcast

Create a Serving Interworking profile for Nexmo as shown below.

Interworking Profiles: Nexmo

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

To Vodafone

Ayaya-tekSM-Vodafone

Vodafone_Spain

Avaya_SM_Comcast

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

General

Hold Support

NONE

180 Handling

None

181 Handling

None

182 Handling

None

183 Handling

None

Refer Handling

No

URI Group

None

Send Hold

No

3xx Handling

No

Diversion Header Support

No

Delayed SDP Handling

No

Re-Invite Handling

No

Prack Handling

No

Interworking Profiles: Nexmo

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

IPO

Sprint

Avaya-SM-for-GENBA...

To GENBAND Q20

To_GB_Dynamic

To Vodafone

Ayaya-tekSM-Vodafone

Vodafone_Spain

Avaya SM Comcast

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

Allow 18X SDP

No

T.38 Support

Yes

URI Scheme

SIP

Via Header Format

RFC3261

Privacy

Privacy Enabled

No

User Name

P-Asserted-Identity

No

P-Preferred-Identity

No

Privacy Header

DTMF

DTMF Support

None

Edit

Interworking Profiles: Nexmo

Add

Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
disco-ccm
cups
OCS-FrontEnd-Server
IPO
Sprint
Avaya-SM-for-GENBA...
To GENBAND Q20
To GB Dvnmic

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

SIP Timers

Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	---
Invite Expire	---

Transport Timers

TCP Connection Inactive Timer	---
-------------------------------	-----

Edit

Interworking Profiles: Nexmo

Add

Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
OCS-FrontEnd-Server
IPO
Sprint
Avaya-SM-for-GENBA...
To GENBAND Q20
To_GB_Dynamic
To Vodafone
Ayaya-tekSM-Vodafone
Vodafone_Spain

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

Record Routes	Both Sides
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes

Interworking Profiles: Nexmo

Add

Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
OCS-FrontEnd-Server
IPO
Sprint
Avaya-SM-for-GENBA...
To GENBAND Q20
To_GB_Dynamic
To Vodafone
Ayaya-tekSM-Vodafone
Vodafone_Spain

Click here to add a description.

General

Timers

URI Manipulation

Header Manipulation

Advanced

Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No
Lync Extensions	No

4.4.1.2 Routing

Navigate to **System Management > Global Profiles > Routing**

Creating a Routing profile for Avaya Session Manager as shown below.

Routing Profiles: Avaya SM

Buttons: Add, Rename

Routing Profiles

- default
- Route_to_Sprint
- Route_to_SM
- Route_to_GENBAND_S...
- Route_to_GB_Dynamic
- Avaya SM**
- Nexmo

Profile : Avaya SM - Edit Rule

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR ☐

Transport: None Next Hop Priority ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Avaya SM	10.70.4.7:5060 (TCP)	None	Delete

Creating a Routing profile for Nexmo as shown below.

Routing Profiles: Nexmo

Buttons: Add, Rename

Routing Profiles

- default
- Route_to_Sprint
- Route_to_SM
- Route_to_GENBAND_S...
- Route_to_GB_Dynamic
- Avaya SM
- Nexmo**

Profile : Nexmo - Edit Rule

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR ☐

Transport: None Next Hop Priority ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Nexmo	sip.nexmo.com:5060 (UDP)	None	Delete

4.4.1.3 Server Configuration

Navigate to **System Management > Global Profiles > Server Configuration**

Create a Server configuration profile for Avaya Session Manager as shown below.

Server Configuration: Avaya SM

Edit Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

IP Address / FQDN	Port	Transport
10.70.4.7	5060	TCP

Buttons: Add, Delete, Finish

Server Configuration: Avaya SM

Server Profiles

- Sprint
- Sprint_Backup
- Avaya_SM
- GENBAND_SBC
- GB_SBC_Dynamic
- Vodafone_WAN
- Avaya SM**

Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya SM
Signaling Manipulation Script	None
Connection Type	SUBID

Buttons: Add, Edit

Create a Server configuration profile for Nexmo as shown below.

Server Configuration: Nexmo

Add

Edit Server Configuration Profile - General X

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type **Add**

IP Address / FQDN	Port	Transport	
<input type="text" value="sip.nexmo.com"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	Delete

Finish

Server Configuration: Nexmo

Add

Server Profiles

- Sprint
- Sprint_Backup
- Avaya_SM
- GENBAND_SBC
- GB_SBC_Dynamic

General **Authentication** **Heartbeat** **Advanced**

Enable Authentication ☒

User Name

Realm

Edit

Server Configuration: Nexmo

Add

Server Profiles

- Sprint
- Sprint_Backup
- Avaya_SM
- GENBAND_SBC
- GB_SBC_Dynamic
- Vodafone_WAN
- Avaya SM

General **Authentication** **Heartbeat** **Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile

Signaling Manipulation Script

Connection Type

Edit

4.4.1.4 Topology Hiding

Navigate to **System Management > Global Profiles > Topology Hiding**

Creating a Topology hiding profile for Avaya Session Manager as shown below

Topology Hiding Profiles: Avaya SM

Add

RenameClone

Topology Hiding Profiles

default

cisco_th_profile

vodafone

CTLProfile

Service_Provider

Avaya SM

Vodafone_Spain

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	lab.tekvizion.com
To	IP/Domain	Overwrite	lab.tekvizion.com
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	lab.tekvizion.com
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

Edit

4.4.2 Domain Policies

4.4.2.1 Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message.

Headers such as P-Location, P-Charging-Vector and others are sent in SIP messages from Session Manager to the Avaya SBCe for egress to the Nexmo.

A Signaling Rule was created, to later be applied in the direction of the enterprise to block unwanted headers coming from Session Manager from being propagated to Nexmo.

Signaling Rules: Nexmo

Add

Filter By Device...

Signaling Rules

default

No-Content-Type-Checks

remap_error

Avaya-CTL

Sess_Mgr_CM_SigRule

SP-EN-SR

Nexmo

Click here to add a description.

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoSUCID

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

Signaling Rules: Nexmo

[Add](#) [Filter By Device...](#)

Signaling Rules
default
No-Content-Type-Checks
remap_error
Avaya-CTL
Sess_Mgr_CM_SigRule
SP-EN-SR
Nexmo

[Click here to add a description.](#)
General Requests Responses Request Headers Response Headers Signaling QoS UCID
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 ☒
Action Allow Multipart Action Allow
Exception List Exception List
[Edit](#)

Signaling Rules: Nexmo [Add](#) [Filter By Device...](#) [Rename](#) [Clone](#) [Delete](#)

Signaling Rules
default
No-Content-Type-Checks
remap_error
Avaya-CTL
Sess_Mgr_CM_SigRule
SP-EN-SR
Nexmo

[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	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
3	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
4	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete

Signaling Rules: Nexmo

[Add](#) [Filter By Device...](#)

Signaling Rules
default
No-Content-Type-Checks
remap_error
Avaya-CTL
Sess_Mgr_CM_SigRule
SP-EN-SR
Nexmo

[Click here to add a description.](#)
General Requests Responses Request Headers Response Headers **Signaling QoS** UCID
Signaling QoS ☒
QoS Type DSCP
DSCP EF
[Edit](#)

4.4.2.2 End Point Policy Groups

End Point Policy group “Avaya SM” is created as shown below

Policy Groups: Avaya SM

Add

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-subscriber
- avaya-def-high-server
- Avaya SM**
- Nexmo

Edit Policy Set X

Application Rule	default ▼
Border Rule	default ▼
Media Rule	default-low-med ▼
Security Rule	default-low ▼
Signaling Rule	Nexmo ▼

Finish

Policy Groups: Nexmo

Add Filter By Device... ▼

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-subscriber
- avaya-def-high-server
- Avaya SM
- Nexmo**

Edit Policy Set X

Application Rule	default ▼
Border Rule	default ▼
Media Rule	default-low-med ▼
Security Rule	default-low ▼
Signaling Rule	default ▼

Finish

4.4.3 Device Specific Settings

4.4.3.1 Media Interface

Navigate to **System Management > Device Specific Settings > Media Interface**. Create Internal and External Media Interface as shown below.

Media Interface: tekasbce

Devices

tekasbce

Media Interface

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

Add

Name	Media IP Network	Port Range		
Ext_Med_Interface	192.6 SBC WAN (B1, VLAN 0)	35000 - 40000	Edit	Delete
Int_Med_Interface	10.70.4.13 SBC LAN (A1, VLAN 0)	35000 - 40000	Edit	Delete

4.4.3.2 Signaling Interface

Navigate to **System Management > Device Specific Settings > Signaling Interface**. Create Internal and External Signaling Interface as shown below.

Signaling Interface: tekasbce

Devices

tekasbce

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
External_Sig_Interface	192.6 SBC WAN (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
Internal_Sig_Interface	10.70.4.13 SBC LAN (A1, VLAN 0)	5060	---	---	None	Edit	Delete

4.4.3.3 End Point Flows

Navigate to **System Management > Device Specific Settings > End Point Flows**. Select the Server Flows tab and click Add. Create a Server flow for Avaya Session Manager as shown below.

Edit Flow: Avaya SM	
Flow Name	Avaya SM
Server Configuration	Avaya SM
URI Group	*
Transport	TCP
Remote Subnet	*
Received Interface	External_Sig_Interface
Signaling Interface	Internal_Sig_Interface
Media Interface	Int_Med_Interface
End Point Policy Group	Avaya SM
Routing Profile	Nexmo
Topology Hiding Profile	Avaya SM
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Select the Server Flows tab and click Add. Create a Server flow for Nexmo as shown below.

Edit Flow: Vodafone_Spain	
Flow Name	Nexmo
Server Configuration	Nexmo
URI Group	*
Transport	UDP
Remote Subnet	*
Received Interface	Internal_Sig_Interface
Signaling Interface	External_Sig_Interface
Media Interface	Ext_Med_Interface
End Point Policy Group	Nexmo
Routing Profile	Avaya SM
Topology Hiding Profile	default
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

4.5 Avaya Modular Messaging

This section describes the steps for configuring the Avaya Modular Messaging to interoperate with Avaya Aura Session Manager via SIP trunking.

4.5.1.1 Messaging Server

Navigate to *Messaging Administration > Networked Machines* to configure Modular Messaging Server parameters as shown below.

Edit Networked Machine			
Machine Name	tekammss	Password	
		Confirm Password	
IP Address	10.70.4.21	Machine Type	tcpip ▼
Mailbox Number Length	4 ▼	Default Community	1 ▼
Updates In	yes ▼	Updates Out	yes ▼
LDAP Port	56389	Log Updates In	no ▼
MAILBOX NUMBER RANGES			
Prefix	Starting Mailbox Number	Ending Mailbox Number	
	20000	29999	

4.5.1.2 Subscriber

Navigate to **Messaging Administration > Subscriber Management**. Configure a subscriber for the Messaging server as shown below.

Edit Local Subscriber

BASIC INFORMATION * (Required Fields)			
*Last Name	user	First Name	2140
*Password		*Mailbox Number	2140
*Numeric Address	2140	PBX Extension	2140
*Class Of Service	0 - test ▼	*Community ID	1 ▼

SUBSCRIBER DIRECTORY			
Email Handle	local.avaya @tekammss.tekvizion.com	Telephone Number	
Common Name	avaya local	ASCII Version of Name	avaya, local

SUBSCRIBER SECURITY			
Immediately Expire Password?	no ▼	Is Mailbox Locked?	no ▼

MAILBOX FEATURES			
Personal Operator Mailbox	<input type="text"/>	Personal Operator Schedule	Always Active ▼
VoiceMail Enabled	yes ▼	Intercom Paging	paging is off ▼

TUI MESSAGE ORDER			
TUI New Message Order	urgent first then newest ▼	TUI Saved Message Order	urgent first then newest ▼
TUI Deleted Message Order	urgent first then newest ▼	TUI Admin Message Order	urgent first then newest ▼

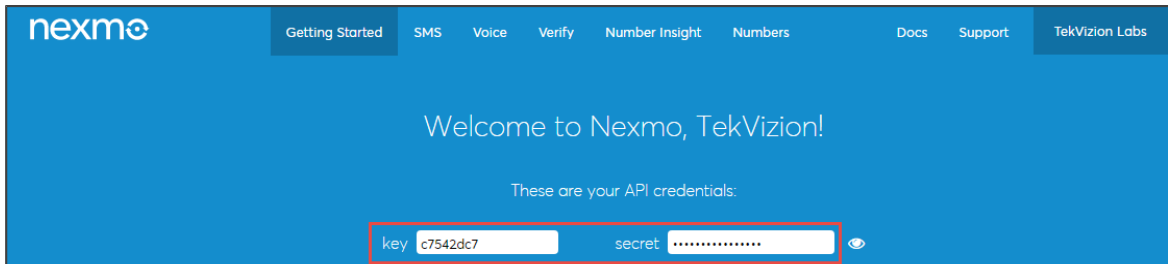
SECONDARY EXTENSIONS			
<div>No Secondary Extensions ▲</div> <div></div>		<input data-bbox="695 619 760 640" type="button" value=" <--Add-- "/>	Secondary Extension <input type="text"/>
		<input data-bbox="703 661 751 682" type="button" value="Delete"/>	Caller Application (none) ▼

MISCELLANEOUS			
Miscellaneous1	<input type="text"/>	Miscellaneous2	<input type="text"/>
Miscellaneous3	<input type="text"/>	Miscellaneous4	<input type="text"/>

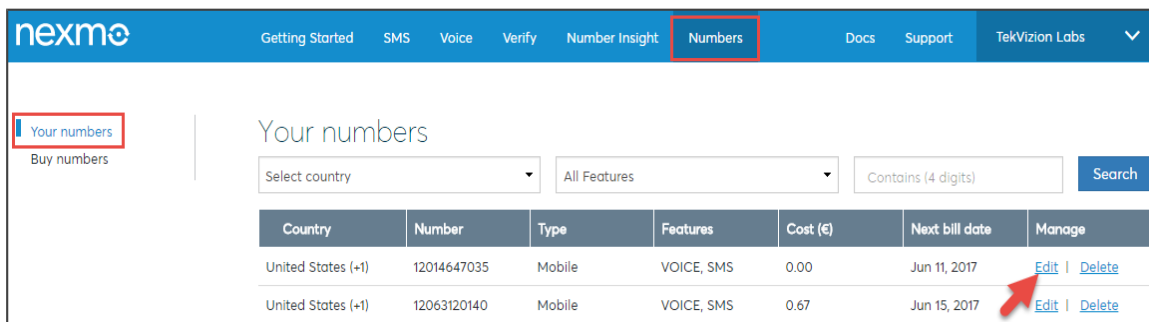
4.6 Nexmo Configuration

4.6.1 Configure Numbers in Nexmo Account

1. Login to the Nexmo account using the credentials provided at the time of registration. A **Key** and **Secret** will be displayed on the dashboard and this can be used as the username and password for Registration SIP Trunks.



2. In order to provide the URL to which the call has to be routed from Nexmo, navigate to the **Numbers** tab
3. Click **Edit** against each number as shown below



1. A pop-up will be displayed
2. Select the "**Forward to**" and provide the URL to which the calls route
3. Click **Update** to save the changes

Settings for 12014647035

SMS

Webhook URL

Voice

Forward to URL

Forward to SIP 12014647035@nexmo.tekvizionlabs.x

Status webhook URL

Cancel Update