



Avaya Solution & Interoperability Test Lab

Application Notes for Smart Assist by Mutare with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the steps required to integrate Smart Assist by Mutare with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Smart Assist by Mutare is a voicemail replacement solution that completes a missed call, records a voice memo, transcribes the voice memo to text, and delivers the text message as an email and/or SMS text message to the intended call recipient. If the caller chooses not to record a voice memo, Smart Assist delivers the caller ID of the missed call. As an option, customers may opt to add Mutare's giSTT speech-to-text transcription service to Smart Assist by Mutare. Mutare giSTT converts the content of a recorded voice message to text and delivers the transcription in the body of the email or text message.

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.

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.

1 Introduction

These Application Notes describe the steps required to integrate Smart Assist by Mutare with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager). Smart Assist by Mutare (SAM) is a voicemail replacement solution that completes a missed call, records a voice memo, transcribes the voice memo to text, and delivers the text message as an email and/or SMS text message to the intended call recipient. If the caller chooses not to record a voice memo, Smart Assist delivers the caller ID of the missed call. As an option, customers may opt to add Mutare's giSTT speech-to-text transcription service to SAM. Mutare giSTT converts the content of a recorded voice message to text and delivers the transcription in the body of the email or text message.

SAM intergrades with Avaya Aura® environment via SIP/RTP. During compliance testing, SAM was installed on cloud based environment. SIP/RTP (UDP) traffic between Avaya Aura® environment and SAM was routed via Avaya Session Border Controller for Enterprise (Avaya SBCE).

2 General Test Approach

To verify interoperability of SAM with Communication Manager and Session Manager, missed call notifications, including caller ID, voice message, and voice message transcription, were delivered to the call recipient via email and/or SMS text notice.

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 these DevConnect Application Notes 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 these Application Notes, the interface between Avaya systems and Smart Assist by Mutare did not include use of any specific encryption features as requested by Mutare.

This test was conducted in a lab cloud environment simulating a basic customer configuration. The testing focused on the standards-based interface between the Avaya solution and the third

party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between SAM and Session Manager (via Avaya SBCE) using UDP transport and verifying the exchange of SIP OPTIONS messages.
- Missed calls covering to SAM.
- Delivering missed call notifications with caller ID to the call recipient via email and an SMS text notice.
- Delivering voice message file to the call recipient via email.
- Delivering voice memo transcription to call recipient's email and as an SMS text notice.
- Delivering call to a PSTN number instead of leaving a voicemail.
- Using Mutare giSTT cloud service to transcribe voice messages.
- Recording personalized greetings in SAM, which requires an outbound call from SAM to a local or PSTN station.
- G.711 mu-law codec support.
- Proper system recovery after a reboot of the SAM server and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following observation:

- When SAM sends a SIP REFER to Session Manager, the Refer-to header contains a local IP Address. During compliance testing, Avaya SBCE, converted the local IP Address to a domain. Without the use of Avaya SBCE, this call would fail. This is only applicable when SAM delivers the call to a PSTN number instead of leaving a voicemail.

2.3 Support

For technical support on Smart Assist by Mutare, contact Mutare Support via phone or email.

- **Phone:** +1 (855) 782-3890
- **Email:** help@mutare.com
- **Website:** <http://www.mutare.com/support.asp>

3 Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya and Mutare products:

- Avaya Aura® Communication Manager running in a virtual environment with an Avaya G450 Media Gateway.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk that provides SIP connectivity for Smart Assist by Mutare.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya Aura® Media Server.
- Avaya Session Border Controller for Enterprise.
- Smart Assist by Mutare running in a virtual environment.
- Mutare giSTT in the cloud used for message transcription.

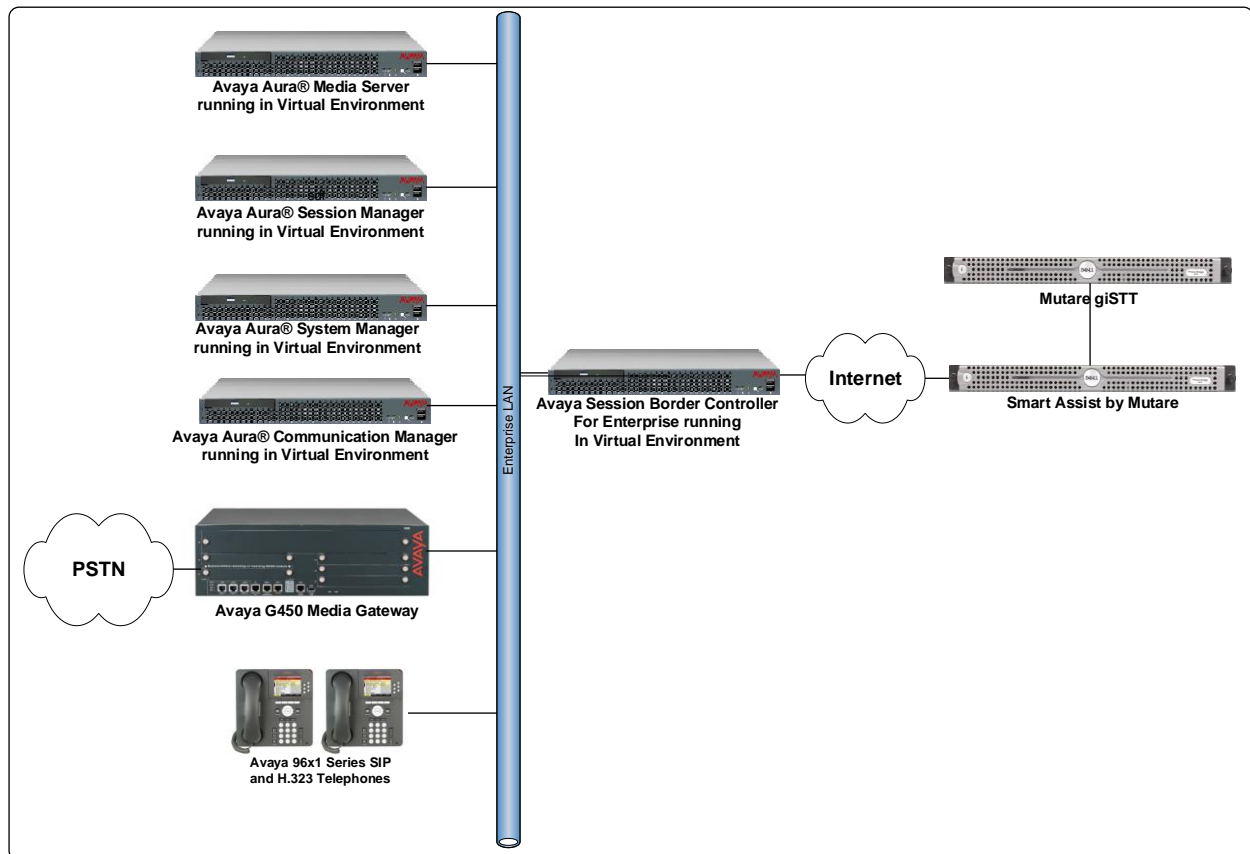


Figure 1: Avaya environment with Smart Assist by Mutare SAM

4 Equipment and Software Validated

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

Hardware Component	Version
Avaya Aura® Communication Manager running in a Virtual Environment	7.1.2.0.0-FP2 (R017x.00.0.532.0 with Patch 24184)
Avaya G450 Media Gateway	37.19.0
Avaya Session Border Controller for Enterprise	7.2.1.0-05-14222
Avaya Aura® Media Server running in a Virtual Environment	7.8.0.240
Avaya Aura® Session Manager running in a Virtual Environment	7.1.2.0.712004
Avaya Aura® System Manager running in a Virtual Environment	7.1.2.0.057353
Avaya 96x1 Series IP Telephones	6.6.6 (H.323) 7.1.0.1 (SIP)
Smart Assist by Mutare	1.6
Mutare giSTT	1.9.0

5 Configure Avaya Aura® Communication Manager

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager and call coverage to SAM. Communication Manager is configured through the System Access Terminal (SAT). The procedures include the following areas:

- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer Private Numbering
- Administer Hunt Group
- Administer Coverage Path
- Administer AAR Call Routing

5.1 Administer IP Node Names

In the **IP Node Names** form, note down the IP address for Communication Manager (*procr*) and add an entry for Session Manager (*asm*). The name configured for Session Manager will be used in other configuration screens of Communication Manager.

change node-names ip asm		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
asm	10.64.110.12	
cms	10.64.110.18	
default	0.0.0.0	
procr	10.64.110.10	
procr6	::	
(5 of 7 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

5.2 Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec to be used by SAM. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU was used.

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

5.3 Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for calls covering to SAM and specify whether **IP-IP Direct Audio** (Shuffling) is required for the test. Shuffling allows audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Aura® Media Server after call establishment. For this compliance test, shuffling was disabled, because it is not currently supported by SAM. However, if shuffling is enabled, the call to SAM would complete successfully, but the call would not be shuffled. The **Authoritative Domain** for this configuration is *avaya.com*.

change ip-network-region 1		Page 1 of 20	
IP NETWORK REGION			
Region: 1			
Location: 1		Authoritative Domain: avaya.com	
Name:		Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: no	
Codec Set: 1		Inter-region IP-IP Direct Audio: no	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3329			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 6			
Audio 802.1p Priority: 6			
Video 802.1p Priority: 5			
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y		RSVP Enabled? n	
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

5.4 Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify Communication Manager (*procr*) and the Session Manager (*asm*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 10	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		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: devcon-sm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
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	

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to SAM. Set the **Group Type** field to *sip*, set the **Service Type** field to *public-ntwrk*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: asm	COR: 1	TN: 1	TAC: 101
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: 1			
Number of Members: 10			

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

On **Page 5** of the trunk group form, enable **Send Transferring Party Information** and **Send Diversion Header** as shown below.

add trunk-group 1		Page 5 of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n			
Send Transferring Party Information? y			
Network Call Redirection? n			
Send Diversion Header? y			
Support Request History? y			
Telephone Event Payload Type: 100			

5.5 Administer Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with ‘5’ and ‘6’ whose calls are routed over any trunk group, including SIP trunk group 10, have the extension sent to the far-end for display purposes.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	5			5	Total Administered: 2
5	6			5	Maximum Entries: 540

5.6 Administer Hunt Group

Configure a hunt group as shown below. Specify the **Group Name** and **Group Extension**; Group Extension field that will be used to route calls to SAM. In this example, covered calls will be forwarded to the SAM extension number 62001 for users configured with call coverage to SAM.

add hunt-group 98		Page 1 of 60
HUNT GROUP		
Group Number: 98	ACD? n	
Group Name: Mutare SAM	Queue? n	
Group Extension: 62001	Vector? n	
Group Type: ucd-mia	Coverage Path:	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		

On **Page 2** of the hunt group, set the **Message Center** field to *sip-adjunct* since SAM is accessed via SIP. Set the **Voice Mail Number** and the **Voice Mail Handle** fields to the digits used to route calls to SAM and set the **Routing Digits** field to the AAR access code. In this example, the AAR feature access code was used to route calls. The voice mail number is used by Communication Manager to route calls to SAM.

add hunt-group 98		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits (e.g., AAR/ARS Access Code)
62001	62001	8

5.7 Administer Coverage Path

Configure the coverage path for the hunt group, which is group *h98* in this sample configuration. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the *Coverage Criteria*.

Note: This coverage path should be configured on stations that should cover calls to SAM (not shown in these Application Notes).

add coverage path 98		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 98			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 3
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h98	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

5.8 Administer AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits *62001* to route pattern *1* as shown below. Calls to *62001* are routed to SAM on Session Manager.

change aar analysis 62001							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
62001	5	5	1	aar		n	

Configure a preference in **Route Pattern 1** to route calls over SIP trunk group 1 as shown below. Configure **Numbering Format** to *lev0-pvt* as shown below.

change route-pattern 1													Page	1 of	3
Pattern Number: 1													Pattern Name:		
SCCAN? n				Secure SIP? n				Used for SIP stations? n							
Grp FRL NPA Pfx Hop Toll No. Inserted													DCS/ IXC		
No Mrk Lmt List Del Digits													QSIG		
Dgts													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 Sub Numbering LAR															
0 1 2 M 4 W Request													Dgts	Format	
1:	y	y	y	y	y	n	n	rest					lev0-pvt	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	

6 Configure Avaya Aura® Session Manager

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

- SIP Entities for Communication Manager and Avaya SBCE
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and Avaya SBCE
- Routing Policies and Dial Patterns

Note: Calls to SAM are routed via Avaya SBCE.

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of the adaptation, SIP entity, entity link, and call routing to SAM (via Avaya SBCE).

6.1 Add SIP Entities

In the sample configuration, two SIP Entities were added for Communication Manager and Avaya SBCE.

6.1.1 Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select one of the locations defined previously (not shown).
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.1', and a 'Last Logged on at April 10, 2018 2:07 PM' status. A search bar with 'GO...' and a 'Log off admin' link are also present. The left sidebar shows a tree view with 'Routing' expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form fields are: Name (acm71), FQDN or IP Address (10.64.110.10), Type (CM), Notes (empty), Adaptation (empty), Location (DevConnect), and Time Zone (America/Denver). 'Commit' and 'Cancel' buttons are at the top right of the form area.

6.1.2 Avaya Session Border Controller for Enterprise

A SIP Entity must be added for Avaya SBCE. Calls to SAM will be routed via Avaya SBCE. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the inside signaling interface of SBCE.
- **Type:** Select *SIP Trunk*.
- **Location:** Select the location defined previously (not shown).
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.1', and a 'Log off' button. The main content area is titled 'SIP Entity Details' and is divided into a left sidebar and a main form area. The sidebar contains a tree view with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main form area is titled 'SIP Entity Details' and has a 'General' tab selected. The form contains the following fields: 'Name' (text input, value: asbce), 'FQDN or IP Address' (text input, value: 10.64.91.48), 'Type' (dropdown menu, value: SIP Trunk), 'Notes' (text area), 'Adaptation' (dropdown menu), 'Location' (dropdown menu, value: DevConnect), and 'Time Zone' (dropdown menu, value: America/Fortaleza). There are 'Commit' and 'Cancel' buttons at the top right of the form area. The breadcrumb trail at the top of the form area reads 'Home / Elements / Routing / SIP Entities'.

6.2 Add Entity Links

This section covers the configuration of Entity Links for Communication Manager and Avaya SBCE.

6.2.1 Communication Manager Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol (e.g., *TLS*).
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If Trusted is not selected, calls from the associated SIP Entity specified in Section 6.1.1 will be denied.*

Click **Commit** to save the Entity Link definition.

AVAYA
Aura® System Manager 7.1

Home Routing

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	*asm_acm71_5061_TLS	*asm	TLS	*5061	*acm71	*5061

Select : All, None

Commit Cancel

6.2.2 Avaya Session Border Controller for Enterprise

The SIP trunk from Session Manager to Avaya SBCE is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol (e.g., *TCP*).
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the *asbce* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Selected *Trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in Section 6.1.2 will be denied.*

Click **Commit** to save the Entity Link definition.

AVAYA
Aura® System Manager 7.1

Home Routing

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	*asm_asbce_5060_TCP	*asm	TCP	*5060	*asbce	*5060

Select : All, None

Commit Cancel

6.3 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.1**. A routing policy was added for Communication Manager and SAM. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a "Last Logged on at April 10, 2018 2:07 PM" status. A search bar with "Go..." and a "Log off admin" button are also present. The left sidebar contains a tree view with "Routing" selected, showing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area displays the "Routing Policy Details" form. The breadcrumb trail is "Home / Elements / Routing / Routing Policies". The form has "Commit" and "Cancel" buttons. The "General" section includes fields for "Name" (cm71), "Disabled" (checkbox), "Retries" (0), and "Notes". The "SIP Entity as Destination" section features a "Select" button and a table with one entry: "acm71" with FQDN or IP Address "10.64.110.10" and Type "CM".

Name	FQDN or IP Address	Type	Notes
acm71	10.64.110.10	CM	

Similarly, add a Routing Policy for Avaya SBCE.

AVAYA
Aura® System Manager 7.1

Last Logged on at April 10, 2018 2:07 PM

Go... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: asbce

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
asbce	10.64.91.48	SIP Trunk	

6.4 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, calls to 5-digits extension starting 6 will be routed to Communication Manager and 62001 will be routed to SAM.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for routing calls to Communication Manager.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.1', and a 'Last Logged on at April 10, 2018 2:07 PM' status. The main navigation menu on the left lists 'Routing' (selected), 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns' (highlighted), 'Regular Expressions', and 'Defaults'. The breadcrumb trail is 'Home / Elements / Routing / Dial Patterns'. The 'Dial Pattern Details' form is displayed, with a 'Commit' button and a 'Cancel' button. The form has a 'General' tab. Fields include: '* Pattern: 6', '* Min: 5', '* Max: 5', 'Emergency Call: ☐', 'Emergency Priority: 1', 'Emergency Type: ', 'SIP Domain: -ALL- (dropdown)', and 'Notes: '. Below the form is a section titled 'Originating Locations and Routing Policies' with 'Add' and 'Remove' buttons. It shows '1 Item' with a refresh icon and a 'Filter: Enable' button. The table has columns: 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The table contains one row: 'DevConnect', 'cm71', '0', 'acm71'. At the bottom, there is a 'Select : All, None' dropdown.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
DevConnect		cm71	0	<input type="checkbox"/>	acm71	

Similarly, add a Dial Pattern *62001* for Avaya SBCE. Calls to 62001 are routed to SAM via Avaya SBCE.

AVAYA
Aura® System Manager 7.1

Last Logged on at April 10, 2018 2:07 PM

Go... [Log off](#) admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

[Commit](#) [Cancel](#) [Help ?](#)

General

* Pattern: 62001

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

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"/>	DevConnect		asbce	0	<input type="checkbox"/>	asbce	

Select : All, None

7 Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to SAM.

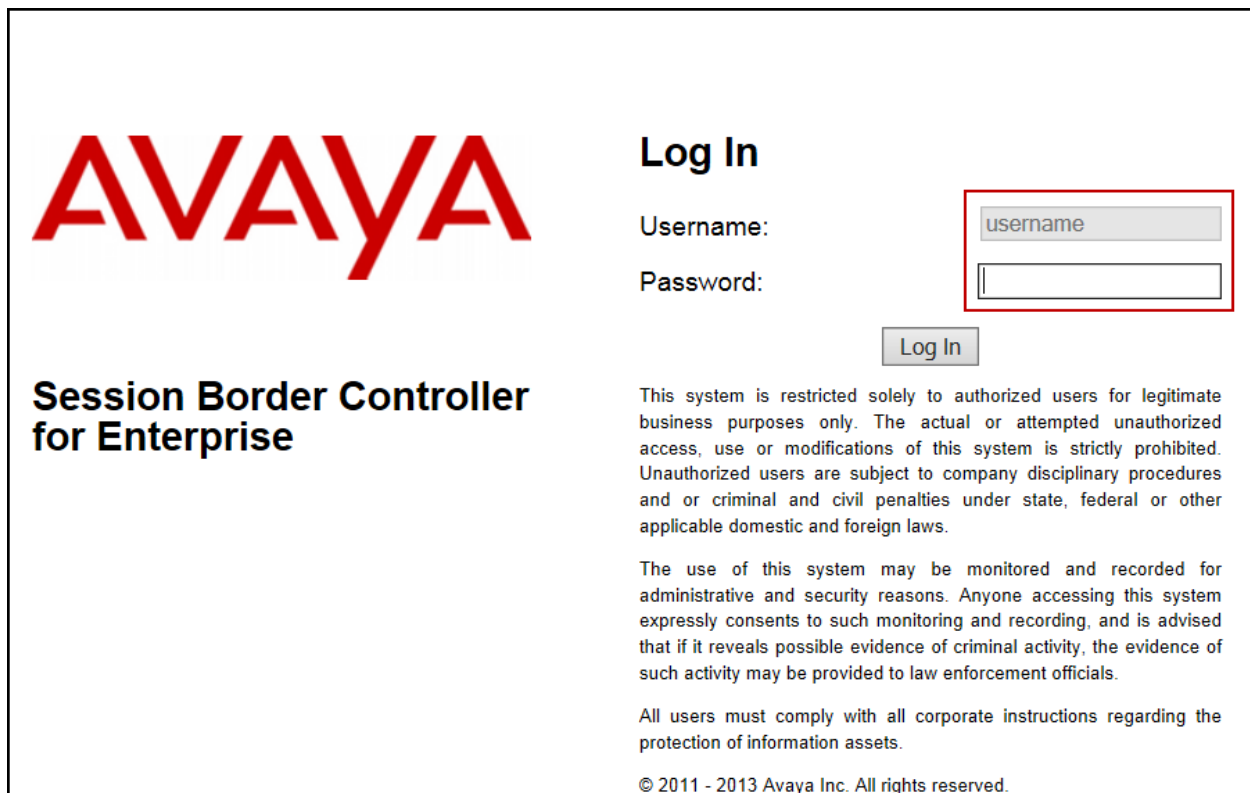
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

The screenshots that follow may have been cut out (not included) for brevity.

7.1 Log in Avaya SBCE

Use a web browser to access the Avaya SBCE Web interface. Enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a "Password:" label, and a "Log In" button. The username and password input fields are highlighted with a red border. Below the login fields, there is a disclaimer text block and a copyright notice at the bottom.

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

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.

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.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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

Alarms
Incidents
Status
Logs
Diagnostics
Users

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
TLS Management
Device Specific Settings

Dashboard

Information		
System Time	09:25:34 PM CST	Refresh
Version	6.3.000-19-4338	
Build Date	Fri Sep 26 09:14:23 EDT 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Alarms (past 24 hours)		
None found.		

Installed Devices		
EMS		
Avaya SBCE		

Incidents (past 24 hours)		
Avaya SBCE: No Server Flow Matched for Incoming Message		
Avaya SBCE: No Server Flow Matched for Incoming Message		
Avaya SBCE: No Server Flow Matched for Incoming Message		
Avaya SBCE: No Server Flow Matched for Incoming Message		
Avaya SBCE: No Server Flow Matched for Incoming Message		

Notes		
No notes found.		

On the left pane, navigate to **Device Specific Settings** → **Network Management** → **Networks**. This page displays the configured network interfaces and associated IP Addresses. For security reason, Public IP Addresses have been hidden in the screen capture below. During Compliance testing, internal interface **A1** and external interface **B1** were used.

Interfaces					
Networks					
Add					
Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Inside A1	10.64.91.1	255.255.255.0	A1	10.64.91.48, 10.64.91.49, 10.64.91.50	Edit Delete
Public B2		255.255.255.128	B2		Edit Delete
Verizon B1	1.1.1.1	255.255.255.0	B1	1.1.1.2	Edit Delete

KJA; Reviewed:
SPOC 5/31/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

24 of 57
MSAM-CMSM712

7.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows for the configuration of parameters across all devices.

7.2.1 Server Configuration

Server Profiles are created for Avaya SBCE's two peers, Session Manager and SAM.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** and enter the profile name: **Session Manager**.

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select **Call Server**.
- **IP Address / FQDN:** **10.64.110.12** (IP Address of Session Manager Security Module).
- **Port:** **5060** (This port must match the port number defined in **Section 6.2**).
- **Transports:** Select **TCP**.
- Click **Next**.

Server Type	Call Server	
SIP Domain	avaya.com	
TLS Client Profile	None	
Add		
IP Address / FQDN	Port	Transport
10.64.110.12	5060	TCP
		Delete
Finish		

- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select a preconfigured **Interworking Profile** from the drop-down menu.
- Click **Finish**.

Edit Server Configuration Profile - AdvancedX

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwork ▾
Signaling Manipulation Script	None ▾
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▾

Finish

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: **Service Provider** (not shown).

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** IP Address of SAM.
- **Port:** **5060** (This port must match the port number defined in **Section 6.6**).
- **Transports:** Select **UDP**.
- Click **Next**.

For security reason, the IP Address has been hidden.

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: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
	5060	UDP

Delete

Finish

- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

On the **Advanced** tab:

- Select a preconfigured **Interworking Profile** drop down menu.
- Click **Finish**.

Edit Server Configuration Profile - AdvancedX

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SIP Provider Interwk ▾
Signaling Manipulation Script	None ▾
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▾

Finish

7.2.2 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side (not shown):

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **route to SM71**.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select server configured for Session Manager in **Section 7.2.1**.
- Click **Finish**.

Profile : route to SM71 - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SM71	10.64.110.12:5060 (TCP)	None	Delete

Finish

Similarly, for SAM:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **route to Mutare**.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select server configured for SAM in **Section 7.2.1**.
- Click **Finish**.

Profile : route to Mutare - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

Next Hop Priority

☒

Next Hop In-Dialog

☐

Ignore Route Header

☐

ENUM

☐

ENUM Suffix

Add

Priority / Weight

Server Configuration

Next Hop Address

Transport

1

Mutare

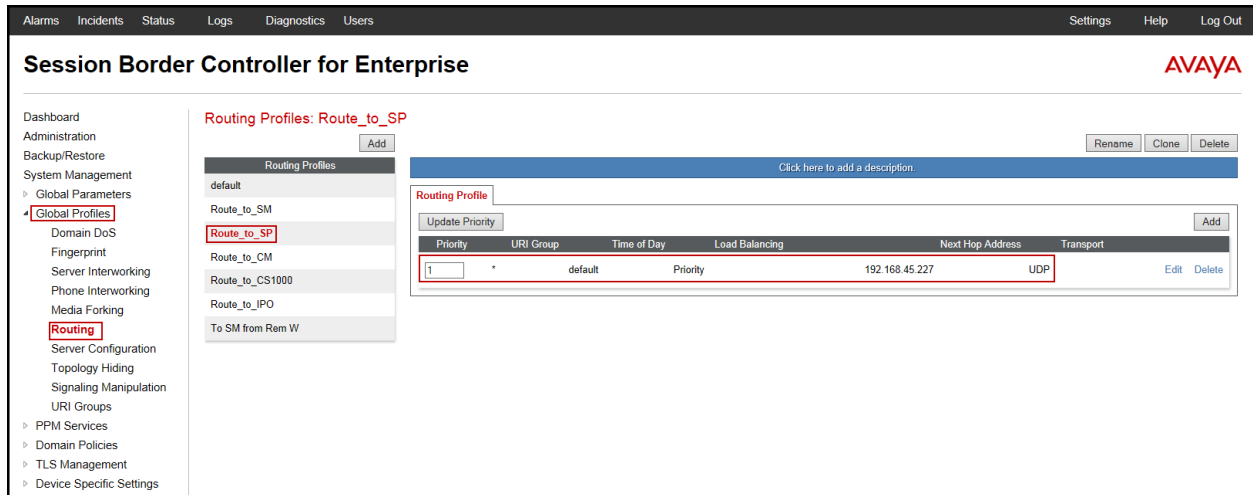
:5060 (UDP)

None

Delete

Finish

The following screen capture shows the newly created **Route_to_SP** Profile.



7.2.3 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

Note that this topology modifies, among others, the Refer-To header coming from SAM.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: SM71-Topology**.
- Click **Finish**.

The following screen capture shows the newly added **SM71-Topology** Profile. Edit the profile and configure as follows.

Edit Topology Hiding Profile
X

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

Similarly, to add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: Mutare-Topology**.
- Click **Finish**.

The following screen capture shows the newly added **Mutare-Topology** Profile. Note that for the SAM no values were overwritten (default).

Topology Hiding

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

Edit

7.3 Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Previously configured Domain Policy rules were used. Please refer to documentation in **Section 11** for further information.

7.4 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.4.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** menu on the left-hand side, select **Network Management**. Select the **Networks** Configuration tab.

For security reasons, public IP Addresses have been hidden. Inside A1 and Public B2 were used during compliance testing.

Network Management: SBC1

Devices
SBC1

Interfaces
Networks

Add

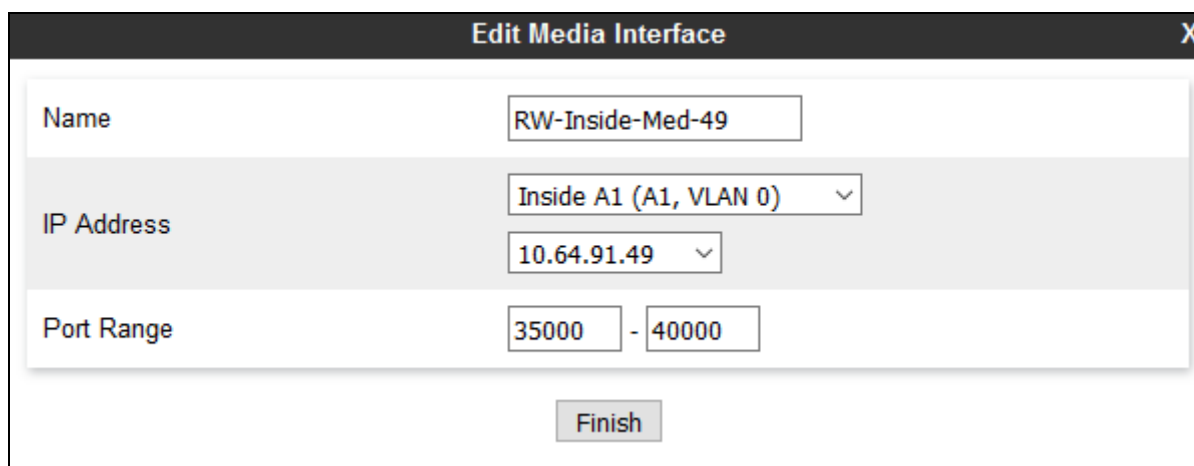
Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Inside A1	10.64.91.1	255.255.255.0	A1	10.64.91.48, 10.64.91.49, 10.64.91.50	Edit Delete
Public B2		255.255.255.128	B2		Edit Delete
Verizon B1	1.1.1.1	255.255.255.0	B1	1.1.1.2	Edit Delete

7.4.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area (not shown).
- **Name: RW-Inside-Med-49.**
- **IP Address: 10.64.91.49** (Inside or Private IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains three main configuration sections:

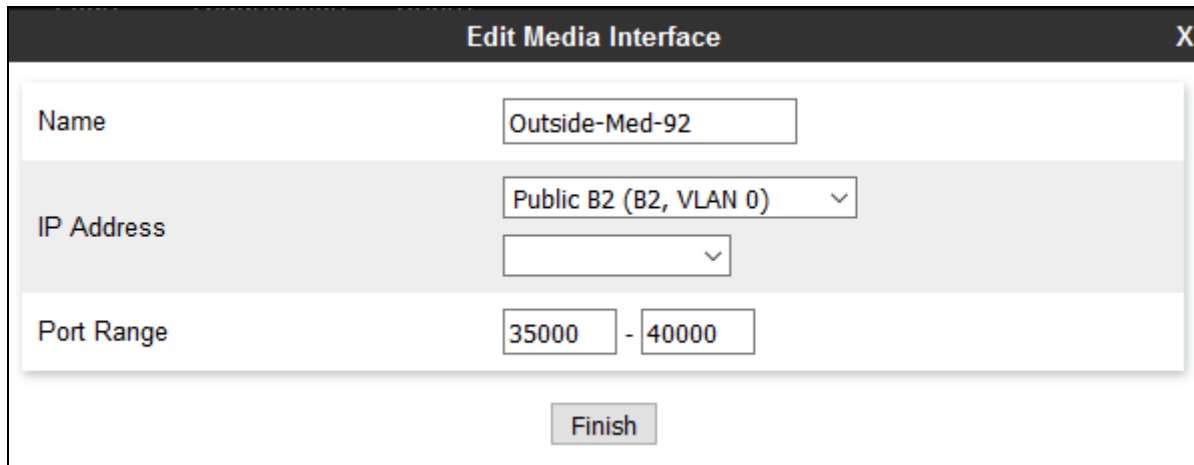
- Name:** A text input field containing "RW-Inside-Med-49".
- IP Address:** A section with two dropdown menus. The first dropdown is set to "Inside A1 (A1, VLAN 0)". The second dropdown is set to "10.64.91.49".
- Port Range:** Two input fields for the range, with "35000" in the first and "40000" in the second, separated by a hyphen.

At the bottom center of the window is a "Finish" button.

Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area (not shown).
- **Name: Outside-Med-92.**
- **IP Address:** Outside or Public IP Address of the Avaya SBCE, toward SAM.
- **Port Range: 35000-40000.**
- Click **Finish**.

For security reasons, public IP Address has been hidden.



The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains three main configuration sections:

- Name:** A text field containing "Outside-Med-92".
- IP Address:** A section with a dropdown menu showing "Public B2 (B2, VLAN 0)" and a smaller, empty dropdown menu below it.
- Port Range:** Two text fields containing "35000" and "40000" separated by a hyphen.

At the bottom center of the window is a "Finish" button.

7.4.3 Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left-hand side, select **Signaling Interface**.

Below is the configuration of the inside, private Signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Inside-sig-48.**
- Select **IP Address: 10.64.91.48** (Inside or Private IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port: 5060.**
- Click **Finish**.

Edit Signaling Interface X	
Name	Inside-sig-48
IP Address	Inside A1 (A1, VLAN 0) 10.64.91.48
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Inside-Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

Below is the configuration of the outside, public signaling Interface of the Avaya SBCE.

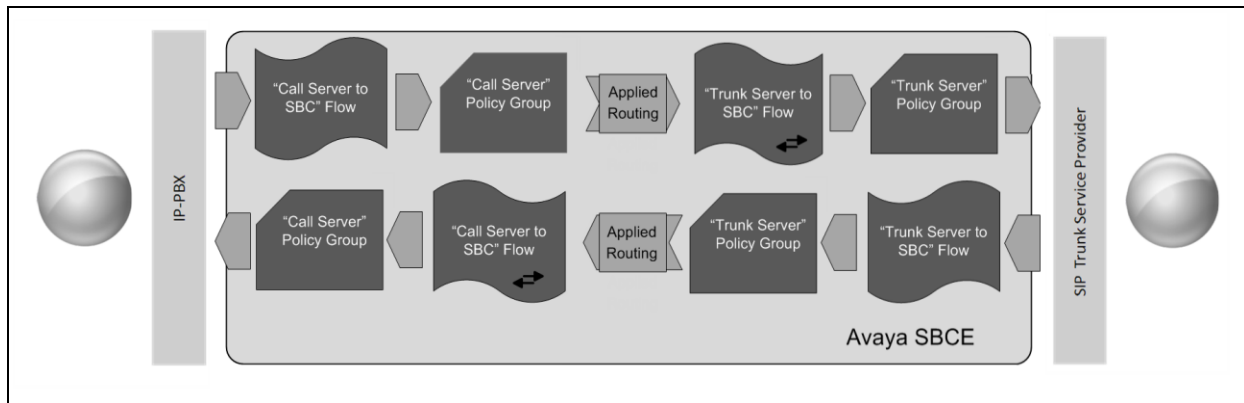
- Select **Add** in the **Signaling Interface** area.
- **Name: RW-Outside-sig-92.**
- **IP Address:** Outside or Public IP Address of the Avaya SBCE, toward SAM.
- **UDP Port: 5060.**
- Click **Finish**.

For security reason, public IP Address has been hidden.

Edit Signaling Interface X	
Name	RW-Outside-sig-92
IP Address	Public B2 (B2, VLAN 0) [dropdown] [hidden IP field]
TCP Port <small>Leave blank to disable</small>	[text box]
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	5056
TLS Profile	Outside-92 [dropdown]
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	[text box]
Finish	

7.4.4 End Point Flows

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through to SIP Trunk call.



The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add Flow** (not shown).

- **Name: Mutare Flow.**
- **Server Configuration: Mutare.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Inside-sig-48.**
- **Signaling Interface: RW-Outside-sig-92.**
- **Media Interface: Outside-Med-92.**
- **Routing Profile: route to SM71**
- **Topology Hiding Profile: Mutare-Topology.**
- **Click Finish.**

Edit Flow: Mutare flow		X
Flow Name	<input type="text" value="Mutare flow"/>	
Server Configuration	<input type="text" value="Mutare"/>	
URI Group	<input type="text" value="*/"/>	
Transport	<input type="text" value="UDP"/>	
Remote Subnet	<input type="text" value="*/"/>	
Received Interface	<input type="text" value="Inside-sig-48"/>	
Signaling Interface	<input type="text" value="RW-Outside-sig-92"/>	
Media Interface	<input type="text" value="Outside-Med-92"/>	
Secondary Media Interface	<input type="text" value="None"/>	
End Point Policy Group	<input type="text" value="default-low"/>	
Routing Profile	<input type="text" value="route to SM71"/>	
Topology Hiding Profile	<input type="text" value="Mutare-Topology"/>	
Signaling Manipulation Script	<input type="text" value="None"/>	
Remote Branch Office	<input type="text" value="Any"/>	
<input type="button" value="Finish"/>		

To create the call flow toward the Session Manager, click **Add Flow**.

- **Name:** SM71 Side.
- **Server Configuration:** SM71.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** RW-Outside-sig-92.
- **Signaling Interface:** Inside-sig-48.
- **Media Interface:** Inside-Med-48.
- **Routing Profile:** route to Mutare.

- **Topology Hiding Profile: SM71-Topology.**
- Click **Finish**.

Edit Flow: SM71 Side
X

Flow Name	SM71 Side
Server Configuration	SM71
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	RW-Outside-sig-92
Signaling Interface	Inside-sig-48
Media Interface	Inside-Med-48
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	route to Mutare
Topology Hiding Profile	SM71-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

8 Configure Smart Assist by Mutare

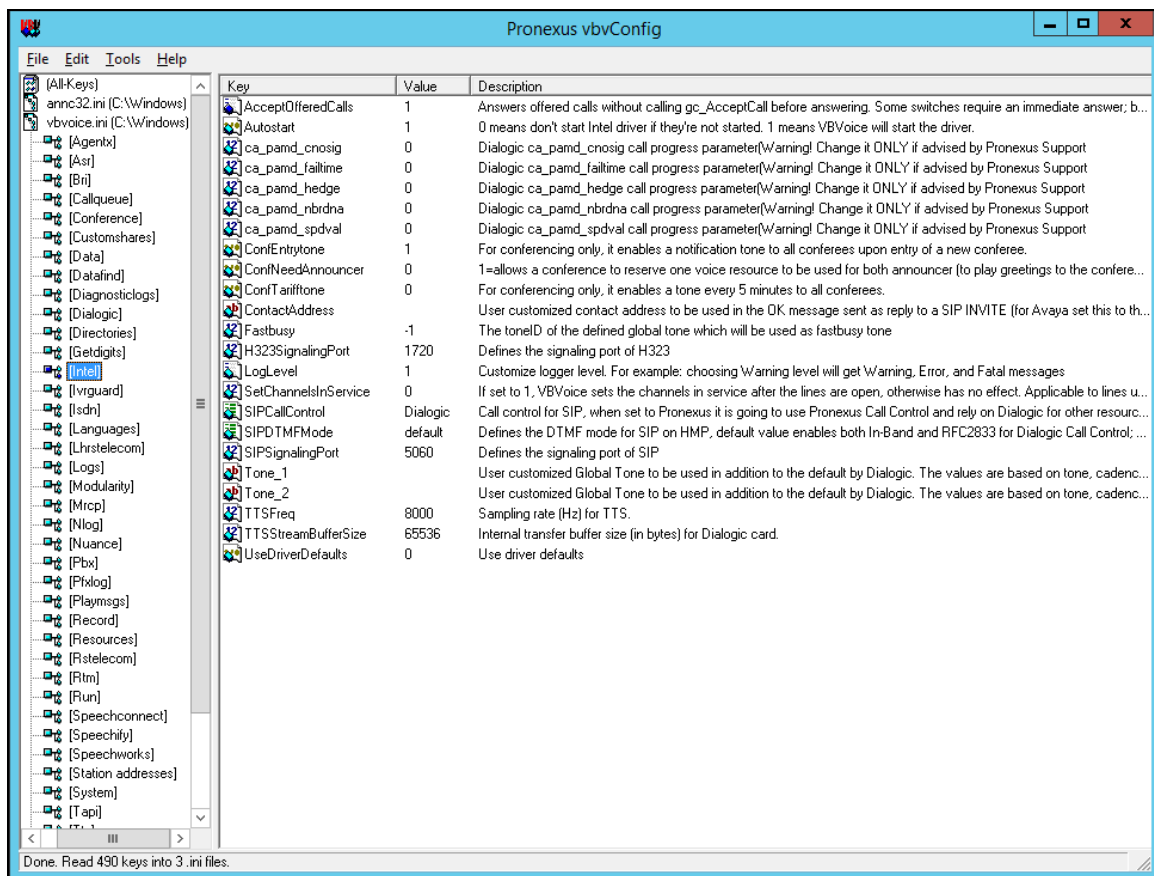
This section covers the configuration of SAM, including SIP parameters via **VBVoice Configuration**, a SAM user and tenant via the SAM web administration interface, and a personal recording (optional). Refer to [2] for additional information on configuring SAM.

8.1 VBVoice Configuration

Launch **VBVoice Configuration** and navigate to **Configuration → VBVoice Config** as shown below. Click on **Run VBVoice Configuration**.



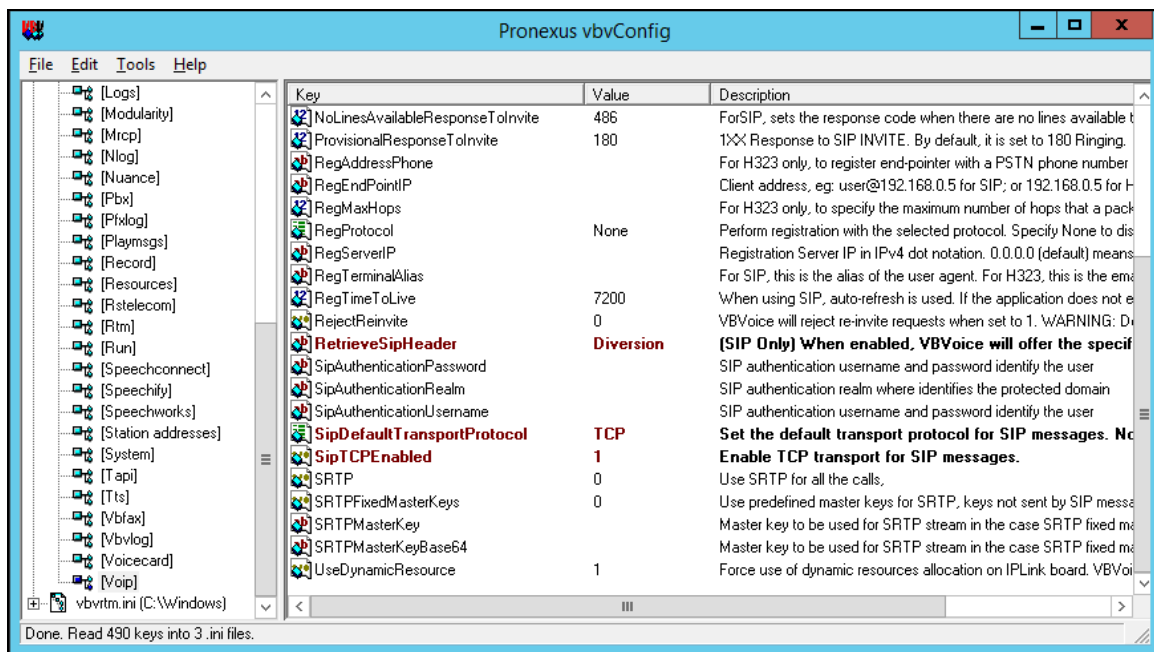
In the **Pronexus vbvConfig** windows displayed below, navigate to **vbvoice.ini** → **Intel**. Verify that **SIPSignalingPort** is set to **5060**, the default value. Continue to use the default values for the other parameters.



In the **Pronexus vbvConfig** window, navigate to **vbvoice.ini** → **Voip**. Modify the following parameters:

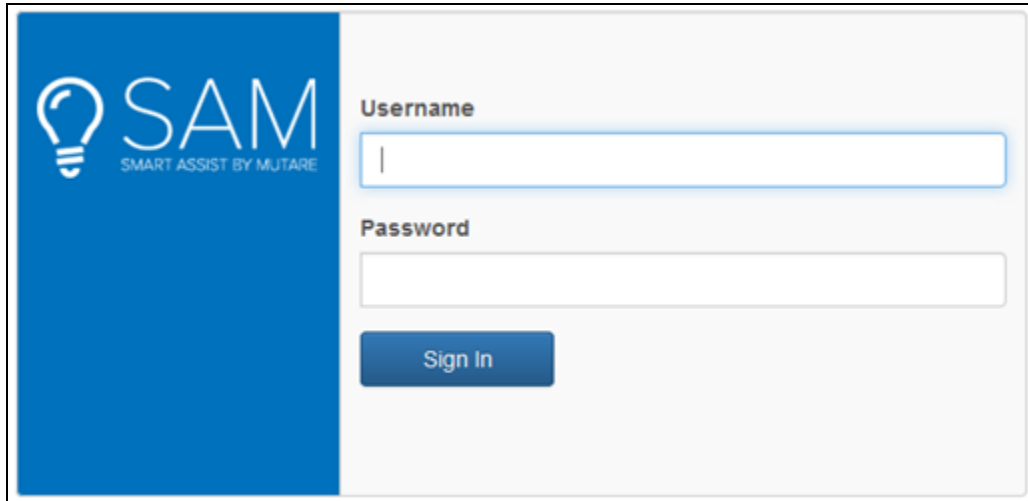
- **RetrieveSipHeader:** Set to *Diversion*.
- **SipDefaultTransportProtocol:** Set to *TCP*.
- **SipTCPEEnabled:** Set to '1'.

Use the default values for the remaining parameters.




8.2 Configure SAM User

Open an internet browser and enter the SAM IP address in the URL field to open the SAM Web administration interface. Enter the appropriate credentials and click the **Sign In** button.

The image shows the SAM Web administration interface login screen. On the left is a blue vertical banner with the SAM logo (a lightbulb icon) and the text "SAM SMART ASSIST BY MUTARE". To the right of the banner is a white login form. The form has two input fields: "Username" and "Password". Below the "Password" field is a blue "Sign In" button.

In the SAM Web administration interface, select **Users**, and then click the **Add User** button to add a user.

Administrator ▾

SAM
SMART ASSIST BY MUTARE

Users

Templates

Announcements

Recordings


Reports




Tenant

Settings

Active ▾


Search


 Add User

Display Name ▲	Phone Number	User Name	Role	Active	Edit
Administrator		Admin	Admin	✓	
User, IP	77301	IP User	Admin	✓	
User, SIP	78030	SIP User	Admin	✓	

3 Users

Page 1 of 1



Powered By:  Mutare

Current server time: 3:02 PM EST

The **New User** page should display. Configure the following fields:

- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.
- **User Name:** Enter the user name used to log into the SAM application.
- **Time Zone:** Enter the user's time zone.
- **Active:** Select this radio button to make the user entry active.
- **Password:** Enter password used to log into the SAM application.
- **Confirm Password:** Enter the same password as the previous field.

The screenshot shows the 'New User' page in the SAM application. The page has a blue header with the SAM logo and navigation tabs: Users, Templates, Announcements, Recordings, Reports, Tenant, and Settings. The 'Users' tab is selected. The page title is 'New User' with a back arrow. A 'Save' button is in the top right. The form fields are as follows:

- First Name:** Text input field with placeholder 'IP'.
- Last Name:** Text input field with placeholder 'User'.
- User Name:** Text input field with placeholder 'IP User'.
- Display Name:** Text input field with placeholder 'User, IP'.
- Override Text To Speech Name:** Text input field with placeholder 'Text To Speech Name'.
- Time Zone:** Dropdown menu with 'Eastern' selected.
- Active:** Radio button (selected) and **Inactive:** Radio button.
- Password:** Password input field with placeholder '*****'.
- Confirm Password:** Password input field with placeholder '*****'.

Scroll down the page and select the **Speech to Text Enabled** option to allow voice messages to be transcribed to text messages using Mutare giSTT.


Role


Administrator











☐ This account is temporarily locked out


☐ Force Password Change on Next Logon

☒ Speech To Text Enabled




Scroll down to the **Notification Preferences/User Channels** section. In this section, the user can set up the notification preferences for how they will receive a notification that a message has been left for them. Click on  to add a notification preference. For the first entry, specify a phone number (e.g., (932) 902-3202) to receive SMS notifications (set **Template** to *Standard SMS*) as shown in the first line of that section below. This entry should also be made *Active*.

Add another entry in this section by clicking . In the second entry, specify an email address (e.g., *mutaresam1@gmail.com*) to receive emails notification with a voice file. In this case, the **Template** field should be set to *Standard Email w/Voice File*. This entry should also be made *Active*.

Notification Preferences/ User Channels 						
Type	Value	Template	Active	Voice File	Edit	Delete
	(932) 902-3202	Standard SMS				
	mutaresam1@gmail.com	Standard Email w/Voice File				


Next, scroll down to the **Numbers** section. This section is where a user can configure what number they wish for the SAM application to call into when receiving a call. Click  to add an entry that associates the number of a SAM user to the type of announcement to be received. In this example, extension 77310 will receive an **Announcement** that contains *Notify w/Msg / Branded / Full Name / Transcription* for any missed call. As mentioned in the previous paragraph, this SAM user will receive a SMS notification at (932) 902 – 3202 and an email notification at mutaresam1@gmail.com. Click **Save**.

Numbers

Number	Announcement	Edit	Out Of Office (EST TZ)	Delete
77301	Notify w/Msg Branded Full Name Transcription			

Last Updated: 03/07/2017 11:23:17 AM | by: .

Save

Powered By:  Mutare

Current server time: 3:03 PM EST


8.3 Configure Personal Recording (Optional)

This section describes the procedure for recording a personal greeting for missed calls. A personal greeting is recorded by SAM by placing an outbound call to a phone number. Once the user answers the call, the user will be prompted to record a personal greeting.

To support the outbound calls required for personal recordings, changes have to be made to directly to the SAM SQL database. Mutare technical support can perform this step, but this is covered here for informational purposes. In the SQL database, configure the following tables:

- **Configurations Table:**
 - Enter a value for the **OutcallPrefix** setting for dialing a PSTN number. The default is '9'.
 - Enter a value for the **OutcallSuffix** setting, which will be added to the end of the phone number when making outbound calls. Typically, this will be @ followed by the IP address of Communication Manager (e.g., @10.64.102.115).
- **Tenants Table:**
 - Enter the caller ID for **OutcallingFromName** setting.
 - Enter a value for the **OutcallingFromNumber** setting. This is the caller ID for making outbound SIP calls in the format of <SAM Phone Number>@<SAM IP Address>.

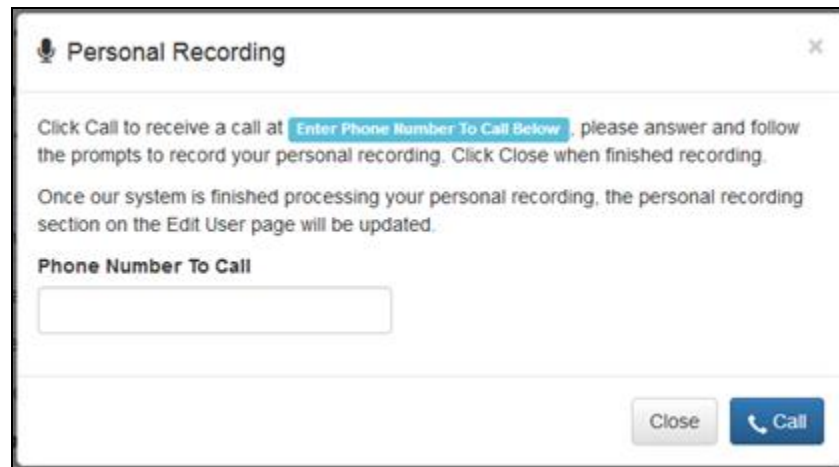
SAM may be configured to place outbound calls to local stations or PSTN numbers, but not both at the same time. For the compliance test, outbound calls were made to the PSTN.

Once the SQL database changes have been made as described above, open the configuration for the user added in **Section 8.2** and scroll down to the **Personal Recording** section shown below and click on .

Note: The **User Personal Greeting** check box under **Numbers** must be selected to use the personal greeting instead of the system greeting (not shown).

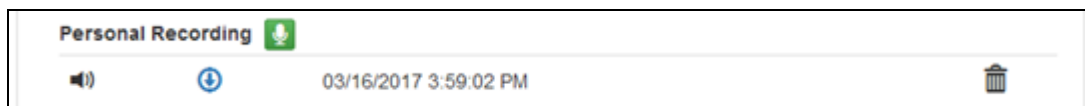


The **Personal Recording** dialog box is displayed as shown below. Enter the **Phone Number to Call** and then click the **Call** button to place the outbound call. For the compliance test, SAM was configured to place outbound calls to the PSTN when dialing 1 + <10-digit number> (e.g., 1 732 555 1212). SAM will automatically prefix the number '9' per SQL administration mentioned above.



The screenshot shows a dialog box titled "Personal Recording" with a close button (X) in the top right corner. The main text reads: "Click Call to receive a call at **Enter Phone Number To Call Below**, please answer and follow the prompts to record your personal recording. Click Close when finished recording." Below this, a smaller line of text states: "Once our system is finished processing your personal recording, the personal recording section on the Edit User page will be updated." There is a text input field labeled "Phone Number To Call". At the bottom right, there are two buttons: "Close" and "Call".

After the personal greeting has been recorded, the Personal Recording section for the SAM user will appear as follows. Once personal greeting can be maintained per user.



The screenshot shows a horizontal bar representing the "Personal Recording" section. It includes a speaker icon, a download icon, the timestamp "03/16/2017 3:59:02 PM", and a trash can icon for deletion.

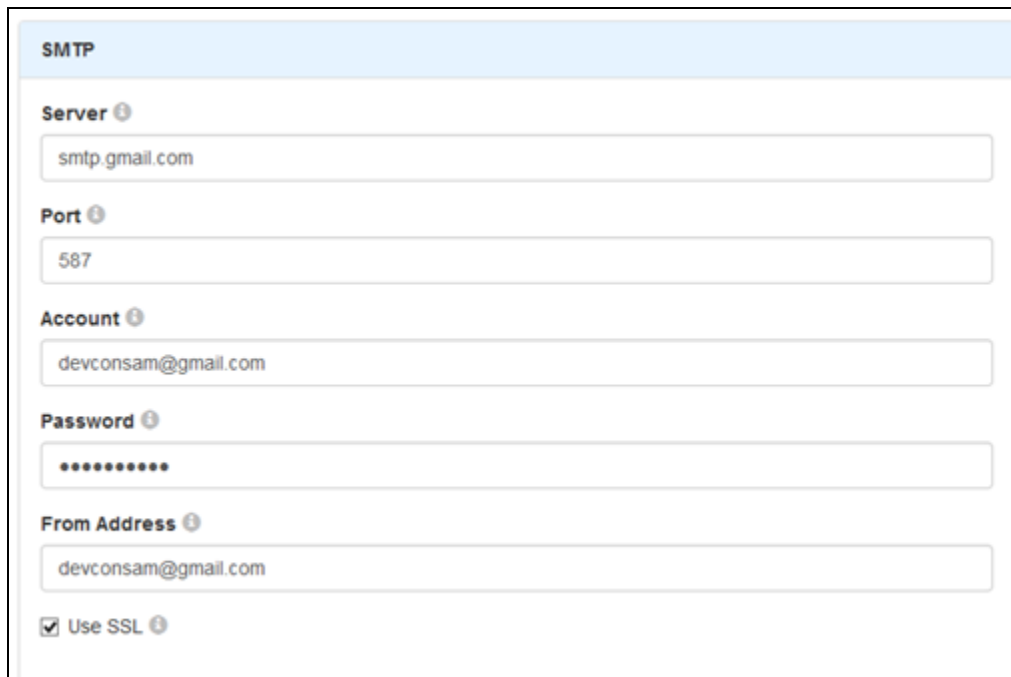
8.4 Configure SAM Tenant

From the SAM Web admin interface, select **Tenant** as shown below. Provide a descriptive name in the **Name** field. Use default values for other fields in this section as shown below.

The screenshot displays the SAM Web admin interface. At the top, a blue navigation bar contains the SAM logo and the text 'POWER. ADDED. BY AVAYA'. To the right of the logo are navigation tabs: 'Users', 'Templates', 'Announcements', 'Recordings', 'Reports', 'Tenant', and 'Settings'. The 'Tenant' tab is currently selected. In the top right corner of the navigation bar, the user role 'Administrator' is displayed with a dropdown arrow. Below the navigation bar, the main content area is titled 'Edit Tenant Settings'. On the right side of this section is a blue 'Save' button. The form contains several fields: a 'Name' field with a light green border containing the text 'New Tenant'; a 'Notes' field with a light gray border containing the text 'This tenant was added when the database was created. It should be changed to the first tenant.'; and a 'General' section with a light blue header. Under the 'General' header are five fields: 'Logo File' with a light gray border and the text 'Logo Filename'; 'Text To Speech (TTS) Voice To Use' with a light gray border and the text 'Microsoft Zira Desktop'; 'Channel Max Count Per Type' with a light gray border and the text '9'; 'Default Time Zone' with a light gray border and a dropdown menu showing 'Central'; and 'Maximum Message Length (sec)' with a light gray border and the text '60'.

Scroll down to the **SMTP** section and configure the following fields:

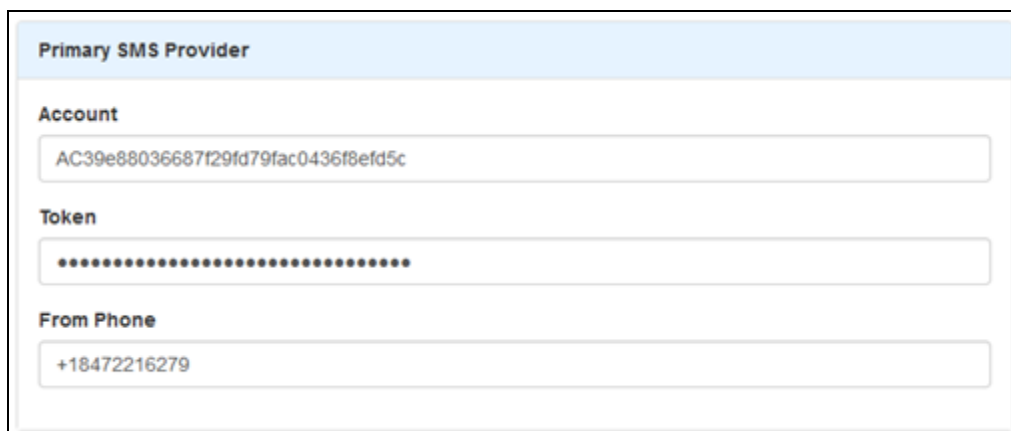
- **Server:** SMTP server to use for this tenant
- **Port:** SMTP port to use for this tenant
- **Account:** SMTP user account to authenticate with
- **Password:** SMTP user account password to authenticate this tenant
- **From Address:** SMTP from address. Should match the account SMS Provider
- **Use SSL:** Select checkbox



The screenshot shows the 'SMTP' configuration section of a web interface. It contains the following fields and values:

- Server:** smtp.gmail.com
- Port:** 587
- Account:** devconsam@gmail.com
- Password:** (masked with dots)
- From Address:** devconsam@gmail.com
- Use SSL:** ☒ Use SSL

Scroll down to the **Primary SMS Provider** section and configure the **Account**, **Token**, and **From Phone** fields. These field values are provided by the Mutare giSTT administrator. Mutare giSTT provides voice message to text message transcription, if desired.



The screenshot shows the 'Primary SMS Provider' configuration section of a web interface. It contains the following fields and values:

- Account:** AC39e88036687f29fd79fac0436f8efd5c
- Token:** (masked with dots)
- From Phone:** +18472216279

Scroll down to the **Speech to Text (STT)** section and configure the **Callback Timeout**, **Language**, **AccountId**, **Token**, and **Rest URL** fields as directed by the Mutare giSTT administrator. Click **Save**.

Speech To Text (STT)

Callback Timeout

900

Language

en-US

AccountId

G76289838

Token

.....

Rest Url


https://gistt.mutare.com/api

☒ Callbacks ⓘ

☐ Default Is Enabled ⓘ

Last Updated: 03/02/2017 03:09:17 PM | by: ,

Save

Powered By:  Mutare

Current server time: 3:05 PM EST

9 Verification Steps

This section provides the steps that can be performed to verify proper configuration of Smart Assist by Mutare with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

1. Verify that the SIP trunk between Session Manager and Avaya SBCE is up by navigating to **Home → Elements → Session Manager → System Status → SIP Entity Monitoring** on System Manager. Below is the status of the SIP trunk to Avaya SBCE indicating that the **Link Status** is *UP*.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: asbce

Summary View

Status Details for the selected Session Manager:

1 Items | Refresh

Filter: Enable

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> asm	IPv4	10.64.91.48	5060	TCP	FALSE	UP	200 OK	UP

2. SSH to the management IP Address of Avaya SBCE and run `tracesbc` command. Verify the `OPTIONS` message from Avaya SBCE to SAM are responded with `200 OK`.

For security reasons, public IP Address has been hidden.

SBC			
16:55:58.638	←OPTIONS→		SIP: sip :5060
16:55:58.638	→200 OK←		SIP: 200 OK (OPTIONS)

3. Place a call to a SAM user and let the call cover to SAM. Leave a voice message for the SAM user.
4. Verify that an email and SMS text notification were left for the SAM user.

10 Conclusion

These Application Notes have described the administration steps required to integrate Smart Assist by Mutare with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Smart Assist by Mutare was able to complete missed calls by recording voice memos, transcribing voice memos, sending the voice file to the call recipient via email and/or SMS text notice. All test cases passed with observations noted in **Section 2.2**.

11 References

This section references the Avaya and Mutare documentation relevant to these Application Notes. Avaya product documentation is available at <http://support.avaya.com>.

- [1] Avaya SBCE Administration and Maintenance Guide, *Version 7.2*
- [2] Mutare SAM Admin Guide, Last Updated: 1/31/2017, *Release 1.2.0*.

©2018 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