



Avaya Solution & Interoperability Test Lab

Application Notes for Mutare Voice with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Mutare Voice v2.0.1.0 with Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, and Avaya Session Border Controller for Enterprise 8.1. Mutare Voice is a voicemail replacement solution that includes Call Completion (formerly Smart Assist by Mutare) and Spam Filter. Voice Call Completion answers missed calls, records voice messages, converts voice messages to text, and delivers a notification with voice message, text message, and caller information as an email and/or SMS text message to the call recipient. Voice Spam Filter allows the caller ID of an incoming call to be checked against enterprise-generated allowlists and blocklists, as well as, third-party robocall lists. Mutare Voice integrates with Avaya Session Border Controller for Enterprise and Avaya Aura® Session Manager via SIP trunks.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 configuration steps required to integrate Mutare Voice with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise (SBCE). Mutare Voice is a voicemail replacement solution that includes Call Completion (formerly Smart Assist by Mutare) and Spam Filter. Mutare Voice integrates with Avaya Session Border Controller for Enterprise and Avaya Aura® Session Manager via SIP trunks.

Voice Call Completion answers missed calls, records voice messages, converts voice messages to text, and delivers a notification with voice message, text message, and caller information as an email and/or SMS text message to the call recipient. As an option, customers may add Mutare's giSTT speech-to-text transcription service to Mutare Voice to convert the content of a recorded voice message to text and delivers the transcription in the body of the email or text message.

Voice Spam Filter identifies unwanted spam calls and applies the appropriate call treatment. Incoming calls to the Avaya SIP-enabled network are delivered by SBCE to Voice Spam Filter via a SIP trunk. Voice Spam Filter examines the SIP call signaling information to identify the caller ID and checks the caller ID against an enterprise-generated whitelist and blacklist, as well as third-party dynamic robocall lists hosted in the cloud. Non-spam calls are released by Voice Spam Filter to Session Manager and allow the call to complete, which may result in the call covering to Voice Call Completion if the called party doesn't answer. Spam calls are configured to be dropped or redirected to an announcement or alternate destination on Communication Manager. In addition, a CAPTCHA feature could be applied to the spam service, which would require the caller to enter a code to verify that the call is indeed a human and not a robocall.

Voice Spam Filter consists of an Application Server, Screening Proxy Server, and a CAPTCHA Server. Voice Call Completion only requires the Application Server. The Screening Proxy interfaces to both SBCE and Session Manager via two separate SIP trunks. The third-party robocall list was hosted in the cloud and accessed via the Internet. The Application Server also interfaced to Session Manager via a SIP trunk. Mutare giSTT, used to transcribe voice messages to text messages, was hosted in the cloud.

2. General Test Approach and Test Results

The feature test cases were performed manually. To verify Voice Spam Filter, inbound calls were made from different PSTN calling numbers that were matched against the enterprise whitelist, enterprise blacklist, and dynamic robocall list in an external database, and the appropriate spam call handling treatment was verified.

To verify Voice Call Completion, 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.

The serviceability test cases were performed manually, such as disconnecting/reconnecting the Ethernet cables to the Mutare Voice servers and restarting the Mutare Voice servers.

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 Mutare Voice did not include use of any specific encryption features as requested by Mutare.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk from Session Manager to Voice Application Server and Voice Screening Proxy using TCP transport and verifying the exchange of SIP OPTIONS messages.
- Filtering incoming calls through Voice Spam Filter. Verified that potential spam calls were treated appropriate according the configured action, such as Allow, Drop, Route, CAPTCHA Drop and CAPTCHA Route.
- Routing calls directly from SBCE to Session Manager when Voice Screening Proxy is not available.
- Call coverage to Voice Call Completion for missed calls with Direct IP Media (Shuffling) enabled and disabled.
- 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.
- 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.
- Managing messages using the Voice TUI.
- Handling incoming calls by the Voice Auto Attendant.
- Verifying Dial By Name and Delegation features.
- G.711 mu-law codec support.

- Verifying the system recovery after a reboot of the Mutare Voice servers and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observation(s):

- Currently, Voice Call Completion doesn't support Message Waiting Indicator (MWI), which provides a notification on a telephone when there are new voicemail messages.
- When a call covers to Voice Call Completion, the SDP in the SIP Invite message should only specify RTP, not both RTP and SRTP, to prevent DMTF issues.

2.3. Support

Technical support on Mutare Voice Spam Filter can be obtained through the following:

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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The two main components of Mutare Voice are Spam Filter and Call Completion. Voice Spam Filter consists of an Application Server, Screening Proxy, and a CAPTCHA Server. Voice Call Completion resides entirely in the Voice Application Server. Incoming PSTN calls arrive at the SBCE and are delivered to Voice Screening Proxy for spam filtering via a SIP trunk. If the call was flagged as a potential spam call, Voice CAPTCHA will prompt the caller for a pin or code, if enabled, to ensure the caller is a human and not a robocall. If the incoming call is not a spam call, Voice Screening Proxy releases the call to Session Manager to allow the call to proceed using a direct SIP trunk. The Voice Application Server allows configuration of Voice Spam Filter and Voice Call Completion features and provides access to spam filter logs and user accounts. As mentioned, the Voice Screening Proxy interfaces to both SBCE and Session Manager via two separate SIP trunks. The Voice Application Server also interfaces to Session Manager via a SIP trunk. Mutare giSTT, used to transcribe voice messages to text messages, was hosted in the cloud, along with the third-party robocall list were hosted in the cloud.

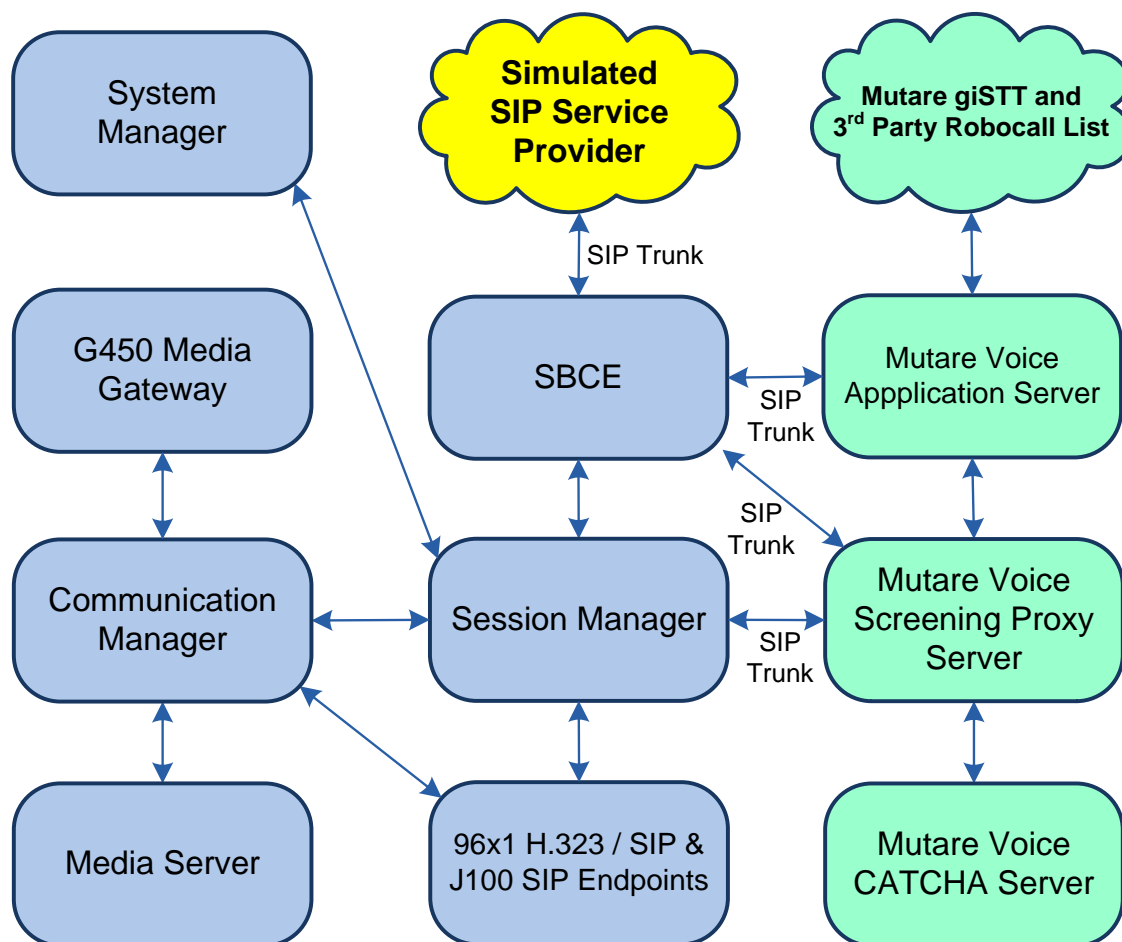


Figure 1: Avaya SIP-based Network with Mutare Voice

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.2.0.0-FP2
Avaya G450 Media Gateway	FW 41.24.0
Avaya Aura® Media Server	v.8.0.2.93
Avaya Aura® System Manager	8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No.: 8.1.2.0.0611167 Feature Pack 2
Avaya Aura® Session Manager	8.1.2.0.812039
Avaya Session Border Controller for Enterprise	8.1.0.0-14-18490
Avaya 96x1 Series IP Deskphones	6.8304 (H.323) 7.1.9.0.8 (SIP)
Avaya J100 Series IP Deskphones	4.0.5.0.10 (SIP)
Mutare Voice Application Server on Windows Server 2016	v2.0.1.0
Mutare Voice Screening Proxy on CentOS 7.8 <ul style="list-style-type: none">• opensips.cfg	2.4.8 (OpenSIPS) 4/16/2020
Mutare Voice CAPTCHA on Debian 4.9	1.10.2-release-13 (FreeSwitch)

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 enable call coverage to Voice Call Completion. In addition, phantom stations are configured to support calls to the Mutare Voice Telephone User Interface (TUI) and Auto Attendant. 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 Phantom Stations
- Administer AAR Call Routing

5.1. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
default	0.0.0.0	
devcon-aes	10.64.102.119	
devcon-ams	10.64.102.118	
devcon-sm	10.64.102.117	
procr	10.64.102.115	
procr6	::	
(6 of 6 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 Voice Call Completion. 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.

Note: Voice Call Completion requires that only RTP be offered in the SIP SDP messaging. That is, both RTP and SRTP shouldn't be offered to Voice Call Completion to prevent DTMF issues. Note that no media encryption is configured in the IP Codec Set. To support SRTP for Avaya IP deskphones a different IP Codec Set should be used with encryption enabled.

change ip-codec-set 1				Page 1 of 2	
IP MEDIA PARAMETERS					
Codec Set: 1					
	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1:	G.711MU	n	2	20	
2:					
3:					
4:					
5:					
6:					
7:					
	Media Encryption		Encrypted SRTCP: best-effort		
1:	none				
2:					
3:					
4:					
5:					

5.3. Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for calls covering to Voice Call Completion 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 enabled. The **Authoritative Domain** for this configuration is *avaya.com*.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	Authoritative Domain: avaya.com	
Name:	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? n
UDP Port Max: 50999		
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		

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 (*devcon-sm*) 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.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- **Direct IP-IP Audio Connections** is enable to allow shuffling for calls routed over the trunk group associated with this signaling group.

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

add signaling-group 10		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? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
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: avaya.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Voice Call Completion. 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 10		Page 1 of 22	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: To devcon-sm	COR: 1	TN: 1	TAC: 1010
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: 10		
	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 10		Page 3 of 5	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private		
	UUI Treatment: shared		
	Maximum Size of UUI Contents: 128		
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Hold/Unhold Notifications? y		
	Modify Tandem Calling Number: tandem-cpn-form		
Send UCID? y			
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. Note that Voice Call Completion is configured to examine the number in the Diversion header in **Section 9.1** to determine if the call should be directed to a subscriber's voicemail, the TUI, or auto attendant.

add trunk-group 10	Page 5 of 5
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:	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

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 ‘7’ 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	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	7			5	Total Administered: 1
					Maximum Entries: 540

5.6. Administer Hunt Group

Configure a hunt group as shown below. Specify the number in the **Group Number** field that will be used to route calls to Voice Call Completion. In this example, missed calls will be forwarded to the Voice Call Completion extension number 78550 for users configured with call coverage to Voice Call Completion.

add hunt-group 30		Page	1 of 60
HUNT GROUP			
Group Number: 30		ACD? n	
Group Name: Mutare Voice CC		Queue? n	
Group Extension: 78550		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 Voice Call Completion is accessed via SIP. Set the **Voice Mail Number** and the **Voice Mail Handle** fields to the digits used to route calls to Voice Call Completion 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 Voice Call Completion.

add hunt-group 30		Page	2 of 60
HUNT GROUP			
Message Center: sip-adjunct			
Voice Mail Number	Voice Mail Handle	Routing Digits	
		(e.g., AAR/ARS Access Code)	
78550	78550	8	

5.7. Administer Coverage Path

Configure the coverage path for the hunt group, which is group *h30* 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 Voice Call Completion (not shown in these Application Notes).

add coverage path 30		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 30			
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: h30	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

5.8. Administer Phantom Stations

This section covers the configuration of phantom stations for the Mutare Voice TUI and Auto Attendant. The TUI allows subscribers to call into Voice Call Completion and manage their messages. A customized menu for the Auto Attendant can be configured to provide the caller with various options, such as call transfer.

Voice Call Completion is configured to examine the number in the SIP Diversion header (see **Section 9.1**) to determine if the call should be directed to the TUI or auto attendant. The Diversion header is sent when a call covers to Voice Call Completion. That is, when a call is placed to either the TUI or Auto Attendant phantom station, the call automatically covers to Voice Call Completion, as specified in the call coverage path, with the TUI or Auto Attendant number in the Diversion header. Voice Call Completion then delivers the call to the TUI or Auto Attendant depending on the number in the Diversion header.

5.8.1. Phantom Station for Mutare Voice TUI

Add a phantom station using the **add station <extension>** command, where *<extension>* is the TUI number configured in **Section 9.3**. Set **Port** to *X* to designate it as a phantom station and set **Coverage Path 1** to the Voice Call Completion coverage path (e.g., *30*) configured in **Section 5.7**. Provide a descriptive name (e.g., *Mutare TUI*).

add station 77333		Page 1 of 5
STATION		
Extension: 77333	Lock Messages? n	BCC: 0
Type: 6408D+	Security Code:	TN: 1
Port: X	Coverage Path 1: 30	COR: 1
Name: Mutare TUI	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Module? n	Message Lamp Ext: 77333	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	Remote Office Phone? n	
	IP Video? n	

5.8.2. Phantom Station for Mutare Voice Auto Attendant

Add a phantom station using the **add station** <extension> command, where <extension> is the Auto Attendant number configured in **Section 9.4**. Set **Port** to *X* to designate it as a phantom station and set **Coverage Path 1** to the Voice Call Completion coverage path (e.g., 30) configured in **Section 5.7**. Provide a descriptive name (e.g., *Mutare AA*).

add station 77334		Page	1 of	5
STATION				
Extension: 77334	Lock Messages? n	BCC: 0		
Type: 6408D+	Security Code:	TN: 1		
Port: X	Coverage Path 1: 30	COR: 1		
Name: Mutare AA	Coverage Path 2:	COS: 1		
Unicode Name? n	Hunt-to Station:			
STATION OPTIONS				
		Time of Day Lock Table:		
Loss Group: 2	Personalized Ringing Pattern: 1			
Data Module? n	Message Lamp Ext: 77334			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	Remote Office Phone? n			
	IP Video? n			

5.9. 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 beginning with “78” to route pattern 10 as shown below. Calls to 78550 are routed to Voice Call Completion on Session Manager.

change aar analysis 7						Page	1 of	2
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 2		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
7		7	7	254	aar		n	
78		5	5	10	lev0		n	
8		7	7	254	aar		n	
9		7	7	254	aar		n	

Configure a preference in **Route Pattern 10** to route calls over SIP trunk group 10 as shown below.

change route-pattern 10										Page 1 of 3	
Pattern Number: 10										Pattern Name: To devcon-sm	
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: 10		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						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	

6. Configure Avaya Aura® Session Manager

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

- Adaptation
- SIP Entities for Communication Manager, Voice Spam Filter, and Voice Call Completion
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and Voice Call Completion
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

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

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 Voice Call Completion.*

6.1. Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made; for example, replacing a domain name with an IP address as shown in this section. To create an **Adaptation** that will be applied to the Voice Call Completion SIP entity in **Section 6.2.3**, navigate to **Elements → Routing → Adaptations** and click on the **New** button (not shown). In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., *Mutare Voice CC Adaptation*).
- **Module Name:** Select **DigitConversionAdapter**.
- **Module Parameter Type:** Select **Single Parameter**.
- **Module Parameter:** Enter the Voice Application Server IP address.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and contains a 'General' section with the following fields:

- * Adaptation Name:** Mutare Voice CC Adaptation
- Notes:** (empty text area)
- * Module Name:** DigitConversionAdapter (dropdown menu)
- Type:** digit (text field)
- State:** enabled (dropdown menu)
- Module Parameter Type:** Single Parameter (dropdown menu)
- Module Parameter :** 10.64.102.112 (text field)
- Egress URI Parameters:** (empty text area)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form, along with a 'Help ?' link.

6.2. Add SIP Entities

In the sample configuration, three SIP Entities were added for Communication Manager, Voice Spam Filter, and Voice Call Completion. This section also covers the configuration of the Entity Links.

6.2.1. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Voice Spam Filter.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **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 the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main area displays the 'SIP Entity Details' form with the following fields:

- Name:** devcon-cm
- FQDN or IP Address:** 10.64.102.115
- Type:** CM
- Notes:**
- Adaptation:** CM Adaptation
- Location:** Thornton
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:**
- Securable:** ☐
- Call Detail Recording:** none

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to *5061*.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to *5061*.
- **Connection Policy:** Set to *trusted*.

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	Dem New Service
<input type="checkbox"/>	* devcon-cm Link	devcon-sm	TLS	* 5061	devcon-cm	* 5061	trusted	<input type="checkbox"/>

Select : All, None

6.2.2. SIP Entity for Voice Spam Filter

A SIP Entity must be added for Voice Spam Filter. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Voice Spam Filter.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Voice Screening Proxy Server.
- **Type:** Select *SIP Trunk*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main area displays the 'SIP Entity Details' form with the following fields:

- Name:** Mutare Voice Screening Proxy
- FQDN or IP Address:** 10.64.102.104
- Type:** SIP Trunk
- Notes:** Mutare Voice Screening Proxy
- Adaptation:** (empty dropdown)
- Location:** Thornton
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TCP*.
- **Port:** Set to *5060*.
- **SIP Entity 2:** The Voice Spam Filter entity name from this section.
- **Port:** Set to *5060*.
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove		Filter: Enable						
1 Item								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* Mutare SCP Link	devcon-sm	TCP	* 5060	Mutare Voice Screening Pro	* 5060	trusted	<input type="checkbox"/>

Select : All, None

6.2.3. SIP Entity for Voice Call Completion

A SIP Entity must be added for Voice Call Completion. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Voice Call Completion.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of Voice Call Completion (i.e., Voice Application Server).
- **Type:** Select *SIP Trunk*.
- **Adaptation :** Select the Adaptation configured in **Section 6.1**.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, Shortcuts, a search bar, a notification bell, and a user profile labeled 'admin'. Below this is a secondary navigation bar with 'Home' and 'Routing' tabs. The left sidebar is a dark-themed navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations, Adaptations, Regular Expressi..., Device Mappings, SIP Entities (highlighted in blue), Entity Links, and Time Ranges. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form contains the following fields and values: 'Name' (required) is 'Mutare Voice Application Server'; 'FQDN or IP Address' (required) is '10.64.102.112'; 'Type' is 'SIP Trunk'; 'Notes' is 'Call Completion (formerly SAM)'; 'Adaptation' is 'Mutare Voice CC Adaptation'; 'Location' is 'Thornton'; 'Time Zone' is 'America/New_York'; 'SIP Timer B/F (in seconds)' (required) is '4'; 'Minimum TLS Version' is 'Use Global Setting'; 'Credential name' is an empty text field; 'Securable' is an unchecked checkbox; and 'Call Detail Recording' is 'egress'. 'Commit' and 'Cancel' buttons are located at the top right of the form area. A 'Help ?' link is also visible in the top right corner of the main content area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TCP*.
- **Port:** Set to *5060*.
- **SIP Entity 2:** The Voice Call Completion entity name from this section.
- **Port:** Set to *5060*.
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove		Filter: Enable						
1 Item								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* Mutare App Svr Link	devcon-sm	TCP	* 5060	Mutare Voice Application S	* 5060	trusted	<input type="checkbox"/>

Select : All, None

6.3. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.2**. A routing policy was added for Voice Call Completion. 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:

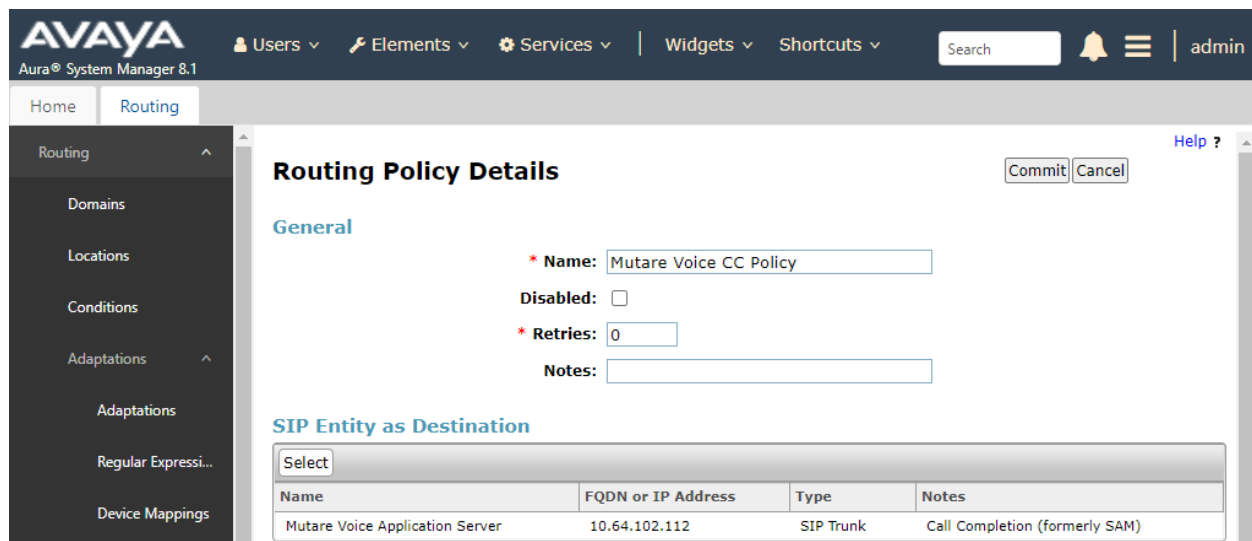
Under *General*:

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 following screen shows the Voice Call Completion Routing Policy.



AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

Adaptations

Regular Expressi...

Device Mappings

Routing Policy Details Commit Cancel Help ?

General

* Name: Mutare Voice CC Policy

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Mutare Voice Application Server	10.64.102.112	SIP Trunk	Call Completion (formerly SAM)

6.4. Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, 78550 will be routed to Voice Call Completion.

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 Voice Call Completion.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a tree view with 'Routing' selected, and 'Dial Patterns' highlighted. The main content area is titled 'Dial Pattern Details' and contains a 'General' section with the following fields:

- Pattern:** 78550
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- SIP Domain:** -ALL-
- Notes:** Mutare Voice CC

Below the 'General' section is a section titled 'Originating Locations and Routing Policies'. It includes an 'Add' button and a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Thornton		Mutare SAM Policy	0	<input type="checkbox"/>	Mutare Voice Application Server	

At the bottom of the table, there is a 'Select' dropdown menu with options 'All', 'None', and 'Filter: Enable'.

6.5. Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top header includes the Avaya logo, navigation links for Users, Elements, Services, Widgets, and Shortcuts, a search bar, and a user profile for 'admin'. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing 'Dashboard' and 'Session Manager Administration' (selected). The main content area is titled 'Edit Session Manager' and includes 'Commit' and 'Cancel' buttons. Below the title is a breadcrumb trail: 'General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Logging |'. The 'General' section contains the following fields: 'SIP Entity Name' (devcon-sm), 'Description' (empty), '*Management Access Point Host Name/IP' (10.64.102.116), '*Direct Routing to Endpoints' (Enable), 'Data Center' (None), 'Avaya Aura Device Services Server Pairing' (None), and 'Maintenance Mode' (unchecked). The 'Security Module' section contains the following fields: 'SIP Entity IP Address' (10.64.102.117), '*Network Mask' (255.255.255.0), '*Default Gateway' (10.64.102.1), '*Call Control PHB' (46), and '*SIP Firewall Configuration' (SM 6.3.8.0).

The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to SIP entities, including Voice Spam Filter and Voice Call Completion. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 600 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.

Monitoring ▼

Enable SIP Monitoring ☒

*Proactive cycle time (secs)

600

*Reactive cycle time (secs)

120

*Number of Tries

1

*Number of Successes

1

Enable CRLF Keep Alive Monitoring ☐

*CRLF Ping Interval (secs)

0

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of SBCE required to establish a SIP trunk and allow routing to the Voice Screening Proxy Server. Incoming PSTN calls are received by SBCE and routed to the Voice Screening Proxy, if it's in-service and running. Otherwise, the calls are routed to the backup Session Manager SIP trunk. If the incoming call is not flagged as a potential spam call per the Voice Screening Proxy, the call is released and routed from the Voice Screening Proxy directly to Session Manager bypassing SBCE.

This section covers the following SBCE configuration:

- Launch SBCE Web Interface
- Administer SIP Server Profile
- Administer Routing Profile
- Administer Interworking Profile

7.1. Launch SBCE Web Interface

Access the SBCE web interface by using the URL “https://<ip-address>/sbc” in an Internet browser window, where <ip-address> is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



Session Border Controller for Enterprise

Log In

Username:

Continue

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

7.2. Administer SIP Server Profile

In the subsequent screen, select **Device** → **SBCE** from the left top menu, followed by **Backup/Restore** → **Services** → **SIP Servers** from the left pane to display the existing SIP server profiles.

Select the SIP server profile associated with Session Manager, in this case *Session Manager* as shown below. Click **Edit**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar contains a tree view with 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services' (expanded), 'SIP Servers' (selected), 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The main content area is titled 'SIP Servers: Session Manager' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below these are tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing a form with 'Server Type' (Call Server), 'TLS Client Profile' (sbceInternal), and 'DNS Query Type' (NONE/A). Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport', containing one entry: '10.64.102.117', '5061', and 'TLS'. An 'Edit' button is located below the table.

IP Address / FQDN	Port	Transport
10.64.102.117	5061	TLS

The **Edit SIP Server Profile – General** pop-up screen is displayed. Click **Add** to add an entry.

The screenshot shows the 'Edit SIP Server Profile - General' pop-up screen. It has a title bar with 'Edit SIP Server Profile - General' and a close button (X). A blue banner at the top states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this are four rows of configuration fields: 'Server Type' (Call Server), 'SIP Domain' (empty), 'DNS Query Type' (NONE/A), and 'TLS Client Profile' (sbceInternal). An 'Add' button is located to the right of these fields. Below the fields is a table with columns 'IP Address / FQDN', 'Port', and 'Transport', containing one entry: '10.64.102.117', '5061', and 'TLS'. A 'Delete' button is to the right of the table. At the bottom is a 'Finish' button.

IP Address / FQDN	Port	Transport
10.64.102.117	5061	TLS

In the new entry, enter the IP address of the Voice Screening Proxy server for **IP Address / FQDN**. For **Port** and **Transport**, enter and select the values correspond to the Voice Spam Filter SIP entity link in **Section 6.2.2**.

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type

Call Server

SIP Domain

DNS Query Type

NONE/A

TLS Client Profile

sbcelInternal

Add

IP Address / FQDN	Port	Transport	
10.64.102.117	5061	TLS	Delete
10.64.102.104	5060	TCP	Delete

Finish

7.3. Administer Routing Profile

Select **Backup/Restore** → **Configuration Profiles** → **Routing** from the left pane to display the existing routing profiles.

Select the routing profile associated with Session Manager, in this case *Route-to-SM*, as shown below. Click **Edit**.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists navigation options: 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles' (selected), 'Domain DoS', 'Server Interworking', 'Media Forking', 'Routing' (highlighted in red), 'Topology Hiding', 'Signaling Manipulation', and 'URI Groups'. The main content area is titled 'Routing Profiles: Route-to-SM' and includes buttons for 'Add', 'Rename', 'Clone', and 'Delete'. A description box says 'Click here to add a description.' Below this is a 'Routing Profile' section with an 'Update Priority' button and an 'Add' button. A table lists routing rules with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The first rule has Priority 1, URI Group *, Time of Day default, Load Balancing Priority, Next Hop Address 10.64.102.117:5061, and Transport TLS. The 'Edit' button for this rule is highlighted with a red box.

The **Profile : Route-to-SM – Edit Rule** pop-up screen is displayed. Click **Add** to add an entry.

The screenshot shows the 'Profile : Route-to-SM – Edit Rule' pop-up screen. It contains various configuration options: URI Group (dropdown with *), Time of Day (dropdown with default), Load Balancing (dropdown with Priority), NAPTR (checkbox), Transport (dropdown with None), LDAP Routing (checkbox), LDAP Server Profile (dropdown with None), LDAP Base DN (Search) (dropdown with None), Matched Attribute Priority (checkbox), Alternate Routing (checkbox), Next Hop Priority (checkbox with checkmark), Next Hop In-Dialog (checkbox), Ignore Route Header (checkbox), ENUM (checkbox), and ENUM Suffix (text field). An 'Add' button is highlighted with a red box. Below the configuration options is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row has Priority 1, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile Session, Next Hop Address 10.64.102.117, and Transport None. A 'Delete' button is next to the last row. At the bottom is a 'Finish' button.

In the existing entry, update the **Priority / Weight** to a lesser priority, such as 2 as shown below.

In the new entry, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Priority / Weight:** The highest priority of *1*.
- **SIP Server Profile:** The SIP server profile for Session Manager, in this case *Session Manager*.
- **Next Hop Address:** Select the address entry associated with Voice Screening Proxy.

With this routing configuration, inbound calls to be routed from SBCE to Session Manager will now route to Voice Screening Proxy as primary and will only route to Session Manager as alternate when the Voice Screening Proxy is not available.

Profile : Route-to-SM - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session	10.64.102.104	None	Delete
2				Session	10.64.102.117:5061 (TLS)		Delete
					10.64.102.104:5060 (TCP)		

Finish

7.4. Administer Interworking Profile

Select **Backup/Restore** → **Configuration Profiles** → **Server Interworking** from the left pane to display the existing interworking profiles. Select the interworking profile associated with Session Manager, in this case *Avaya-SM*, as shown below. Select the **Timers** tab in the right pane and click **Edit**.

Device: SBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy

Interworking Profiles: Avaya-SM

Add Rename Clone Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	---
Invite Expire	---
Retry After	---

Edit

The **Editing Profile: Avaya-SM** pop-up screen is displayed. For **Trans Expire**, enter an appropriate short duration. In the compliance testing, two seconds was used as the allotted time for SBCE to wait for a route response from Voice Screening Proxy as primary before routing to Session Manager as alternate.

Editing Profile: Avaya-SM X

All fields are optional.

SIP Timers	
Min-SE	seconds, [90 - 86400]
Init Timer	milliseconds, [50 - 1000]
Max Timer	milliseconds, [200 - 8000]
Trans Expire	2 seconds, [1 - 64]
Invite Expire	seconds, [180 - 300]
Retry After	seconds, [2 - 32]

Finish

8. Configure Mutare Voice Spam Filter

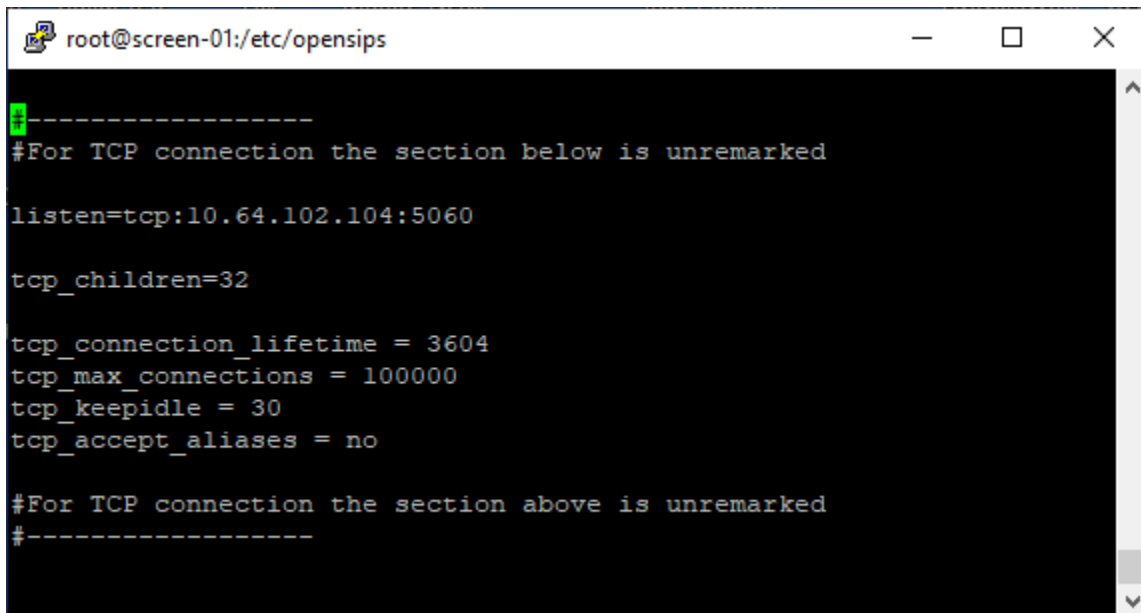
This section provides the procedure for configuring Voice Spam Filter. The procedure includes the following areas:

- Administer opensips.cfg
- Administer SQL
- Administer Control Panel
- Administer Rules Manager

The configuration of Voice Spam Filter is typically performed by a Mutare operations technician. The procedural steps are presented in these Application Notes for informational purposes. This section assumes that values for API URL, Connect URL, appliance ID, account ID, and token have all been obtained from Voice Application Server and configured on Voice Screening Proxy.

8.1. Administer opensips.cfg

Log into the Voice Screening Proxy Server with super user credentials. Navigate to the `/etc/opensips` directory and edit the `opensips.cfg` file. Scroll down to the **Global Parameters** sub-section and uncomment out six TCP related parameters shown below. For the **listen** parameter, replace the default IP address with the Voice Screening Proxy Server IP address.



```
root@screen-01:/etc/opensips
#-----
#For TCP connection the section below is unremarked

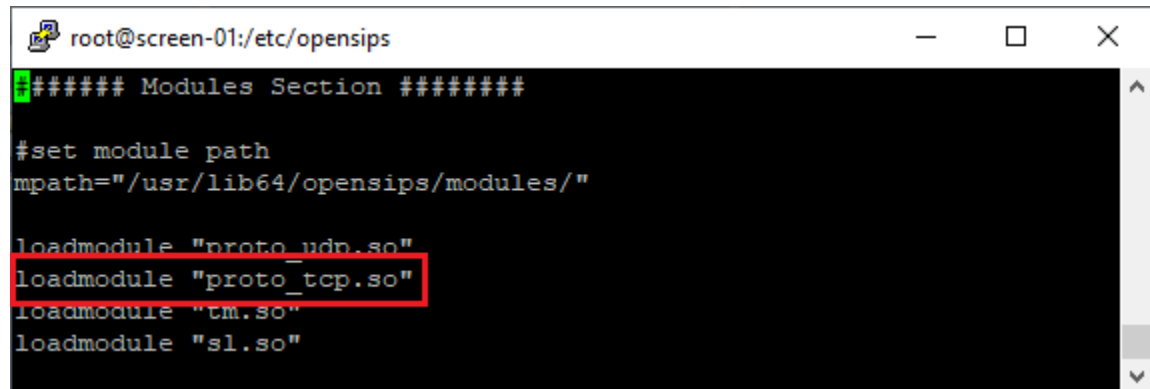
listen=tcp:10.64.102.104:5060

tcp_children=32

tcp_connection_lifetime = 3604
tcp_max_connections = 100000
tcp_keepidle = 30
tcp_accept_aliases = no

#For TCP connection the section above is unremarked
#-----
```

Scroll down to the **Modules Section** and uncomment out the TCP related module shown below.

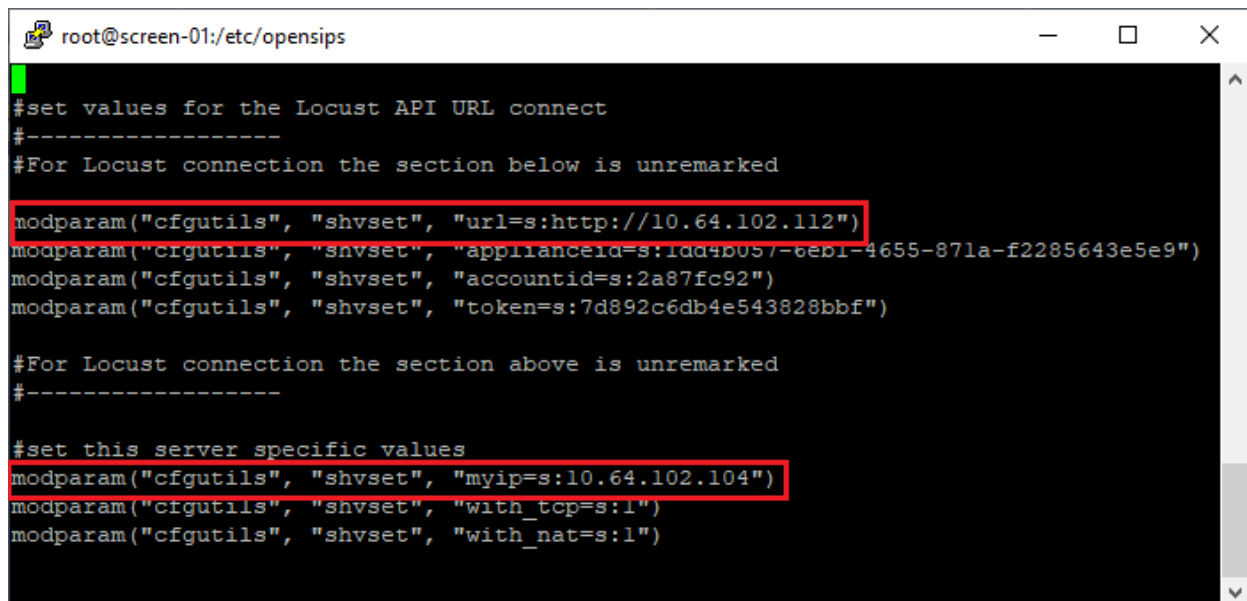


```
root@screen-01:/etc/opensips
##### Modules Section #####

#set module path
mpath="/usr/lib64/opensips/modules/"

loadmodule "proto_udp.so"
loadmodule "proto_tcp.so"
loadmodule "tm.so"
loadmodule "sl.so"
```

Scroll further down in the Modules Section and point the **url** to the Voice Application Server IP address (e.g., *10.64.102.112*) and **myip** to the Voice Screening Proxy IP address (e.g., *10.64.102.104*) as shown below.



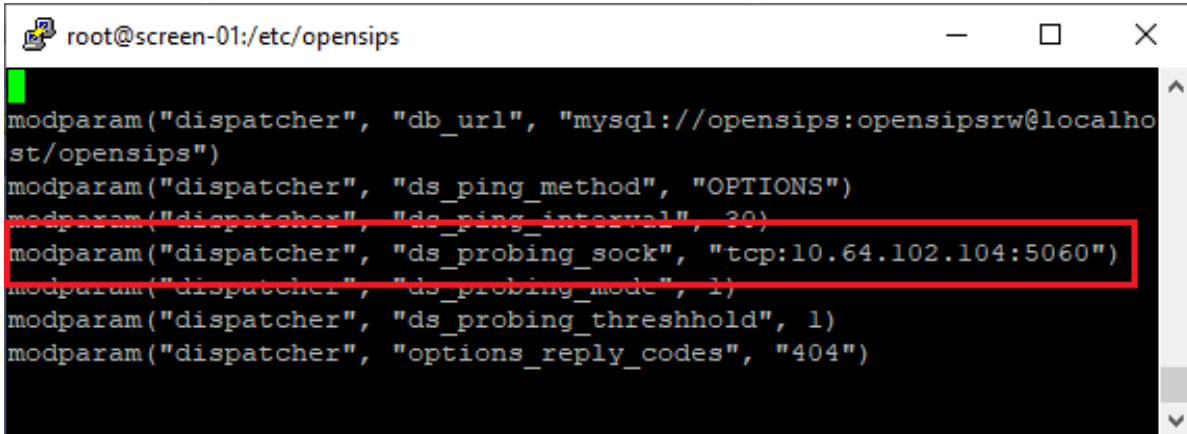
```
root@screen-01:/etc/opensips

#set values for the Locust API URL connect
#-----
#For Locust connection the section below is unremarked
modparam("cfgutils", "shvset", "url=s:http://10.64.102.112")
modparam("cfgutils", "shvset", "applianceid=s:1dd4b05/-6eb1-4655-871a-f2285643e5e9")
modparam("cfgutils", "shvset", "accountid=s:2a87fc92")
modparam("cfgutils", "shvset", "token=s:7d892c6db4e543828bbf")

#For Locust connection the section above is unremarked
#-----

#set this server specific values
modparam("cfgutils", "shvset", "myip=s:10.64.102.104")
modparam("cfgutils", "shvset", "with_tcp=s:1")
modparam("cfgutils", "shvset", "with_nat=s:1")
```

Scroll down to the section shown below, uncomment out the TCP related line and replace the default IP address with the IP address of Voice Screening Proxy as shown below.



```
root@screen-01:/etc/opensips
modparam("dispatcher", "db_url", "mysql://opensips:opensipsrw@localhost/opensips")
modparam("dispatcher", "ds_ping_method", "OPTIONS")
modparam("dispatcher", "ds_ping_interval", 30)
modparam("dispatcher", "ds_probing_sock", "tcp:10.64.102.104:5060")
modparam("dispatcher", "ds_probing_mode", 1)
modparam("dispatcher", "ds_probing_threshold", 1)
modparam("dispatcher", "options_reply_codes", "404")
```

8.2. Administer SQL

From the command line, enter the two SQL commands shown below to update the next hop destination to the IP address of the Session Manager signaling interface.

- `mysql -uopensips -popensipsrw`
- `UPDATE opensips.dispatcher set destination='sip:10.64.102.117:5060' where id=1;`

Next, enter the following SQL command to set the TCP socket.

- `UPDATE opensips.dispatcher set socket='tcp:10.64.102.104:5060' where id=1;`

Enter the second SQL command below to ensure the TCP socket was set correctly.

```
mutareadmin@screen-01:~$
[mutareadmin@screen-01 ~]$ mysql -uopensips -popensipsrw
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 120
Server version: 5.6.49 MySQL Community Server (GPL)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

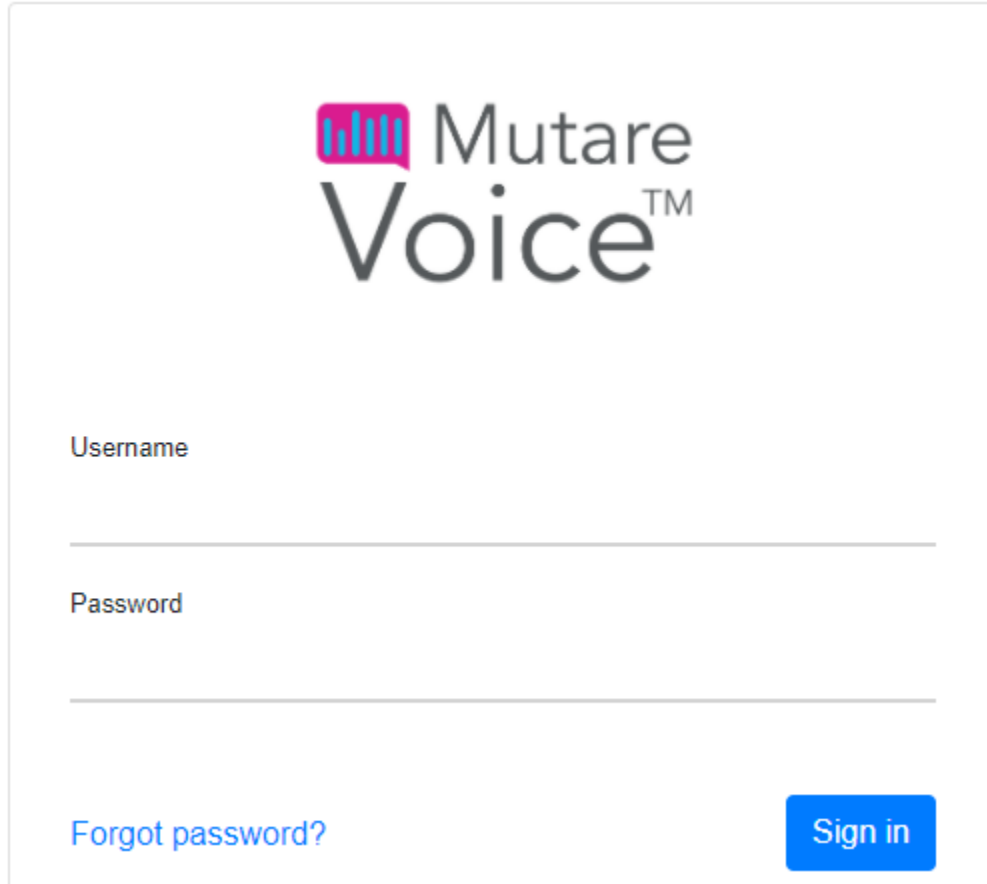
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from opensips.dispatcher;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | setid | destination          | socket          | state | weight | priority | attrs | description |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | 1     | sip:10.64.102.117:5060 | tcp:10.64.102.104:5060 | 0    | 1      | 0        |      | SM          |
| 2  | 2     | sip:10.64.102.109:5060 | NULL            | 0    | 1      | 0        |      | CAPTCHA-1   |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

8.3. Administer Control Panel

Access the Voice web interface by using the URL “http://<ip-address>” in an Internet browser window, where <ip-address> is the IP address of the Voice Application Server. The screen below is displayed. Log in with admin credentials.



The image shows the login interface for Mutare Voice. At the top center is the Mutare Voice logo, which consists of a pink speech bubble icon with four vertical bars of increasing height inside it, followed by the text "Mutare Voice™" in a dark grey sans-serif font. Below the logo are two input fields. The first field is labeled "Username" in a light grey font and has a horizontal line below it for text entry. The second field is labeled "Password" in a light grey font and also has a horizontal line below it. At the bottom left of the form is a blue hyperlink that says "Forgot password?". At the bottom right is a blue rectangular button with the white text "Sign in".

In the subsequent screen (not shown), select **Spam Filter → Control Panel** from the top menu to display the screen below. To allow incoming calls to be analyzed by the spam filter, select **Active Analyze (Analyze to Drop, Route, or Allow)** as shown below. To allow Voice Spam Filter to apply the robocall external database, set the **Check External Spam Service for** field to *All Calls*. To disable the robocall external database, set the field to *No Calls*. If the robocall external database is enabled, set the appropriate action to take for spam calls. In the example below, spam calls are routed to extension 78002. Additional actions include dropping spam calls and prompting the caller for a set of numbers as determined by the CAPTCHA system.

How to handle your Spam?

Passive Log Only (Allow Call)
Log, do not analyze, and release call.

Passive Analyze (Allow Call and Analyze)
Log, analyze, and release call.

Active Analyze (Analyze to Drop, Route, or Allow) **Active**
Log, analyze, and take action.

Default Route Address for Rules Manager
1234567890@IPAddressOrDomain
Default Route Address is applied to rules on Rules Manager when Route is selected.

All Check External Spam Service for
All calls
Log External Spam Service analysis for all calls.

Choose the action to take for calls not matched by Rules
Route External Spammers 78002@10.64.102.117
Drop External Spammers
Route External Spammers
CAPTCHA External Spammers

CAPTCHA Settings

☒ CAPTCHA is Enabled

Scroll down to the CAPTCHA Settings section to enable CAPTCHA as shown below. This section also specifies other settings such as the number of digits and how many retries.

CAPTCHA Settings

☒ CAPTCHA is Enabled

How many digits? 2 How many seconds? 3 How many tries? 2

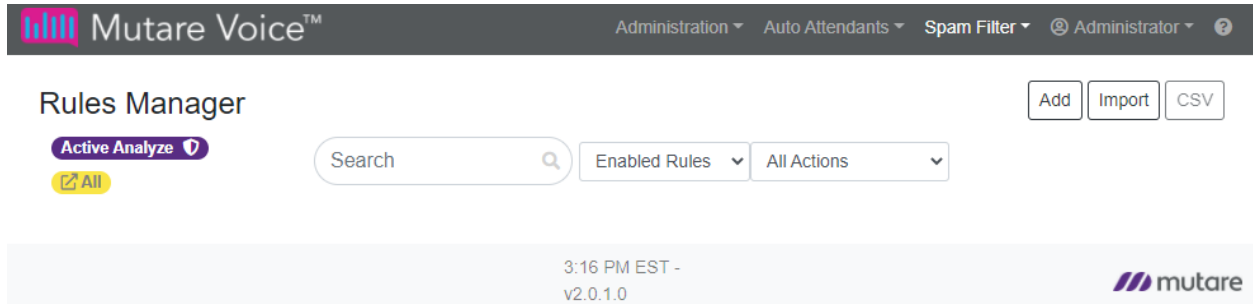
Failed Action: Drop

11:08 AM EST -
v2.0.1.0

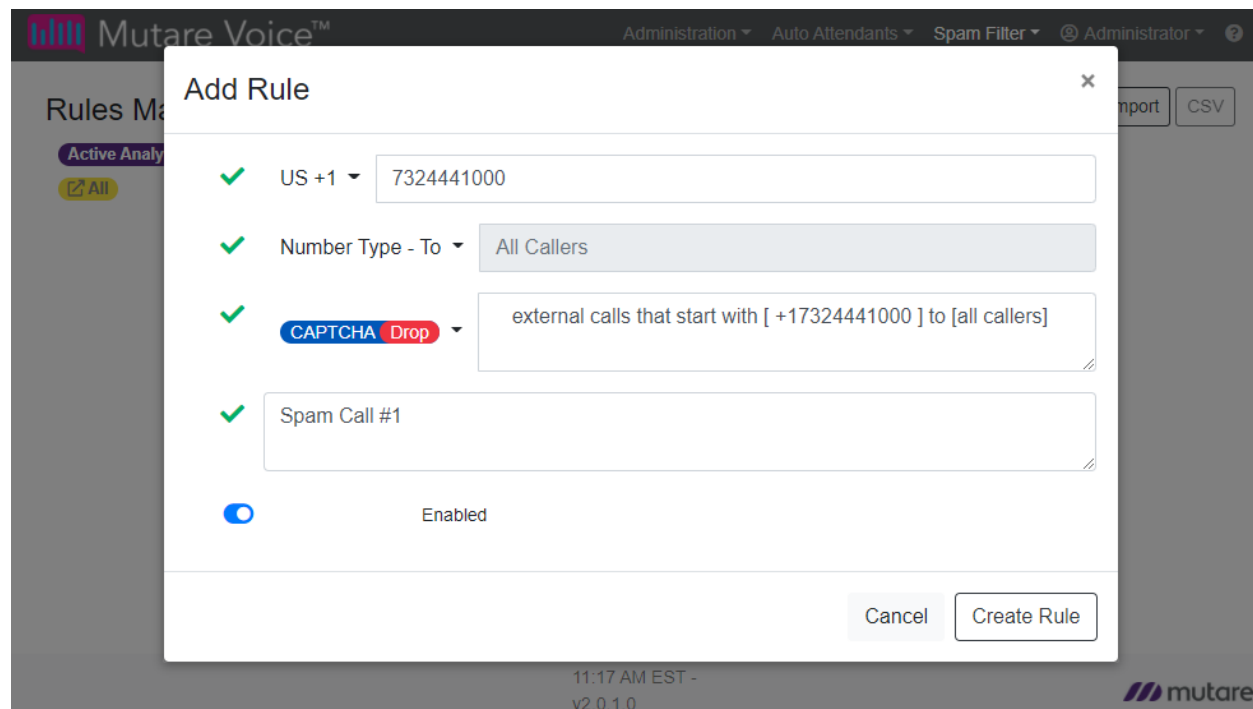
mutare

8.4. Administer Rules Manager


Select **Spam Filter** → **Rules Manager** from the top menu to display the **Rules Manager** screen below. Click **Import** to import a CSV file with existing numbers or **Add** to add individual numbers. In the compliance testing, **Add** was used.



The **Add Rule** pop-up box is displayed next. Set the number type to *US +1* followed by a 10-digit number. If the caller ID matches the specified 10-digit number, then this rule applied. Next, specify the action to take if the caller ID matches the rule. The options are *Allow*, *Drop*, *Route*, *CAPTCHA Drop*, and *CAPTCHA Route*. In the following example, *CAPTCHA Drop* was selected, which means that the caller will be prompted for a CAPTCHA code. If the code is entered corrected, the incoming call is allowed to complete; otherwise, the incoming call is dropped. Lastly, enter a description and then click *Create Rule*. Note that the Allow action is for the whitelist. These rules are applied before the robocall external database, if enabled. That is, if a caller ID in on the whitelist and also in the robocall list, the call is allowed to complete.




Repeat the procedure in this section to configure all calling numbers for the enterprise whitelist and blacklist. In the compliance test, the following entry was used and all available actions were verified.

 **Mutare Voice™**

Administration ▾ Auto Attendants ▾ Spam Filter ▾ Administrator ▾ ?



Rules Manager

Active Analyze ⓘ


Search 

Enabled Rules ▾ All Actions ▾

🔗 All

Enabled	Action	From Number ↕	To Number ↕	Description ↕	Updated ▾	
<input checked="" type="checkbox"/>	CAPTCHA Drop	+17324441000	All	Spam Call #1	added just now	 

11:17 AM EST -
v2.0.1.0

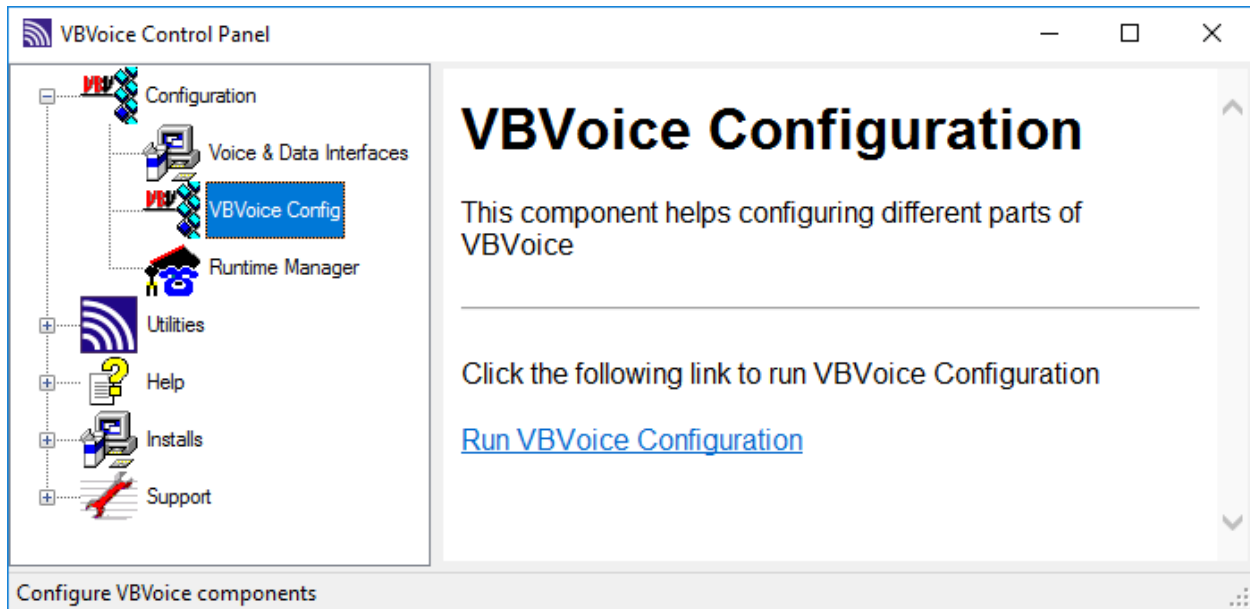


9. Configure Mutare Voice Call Completion

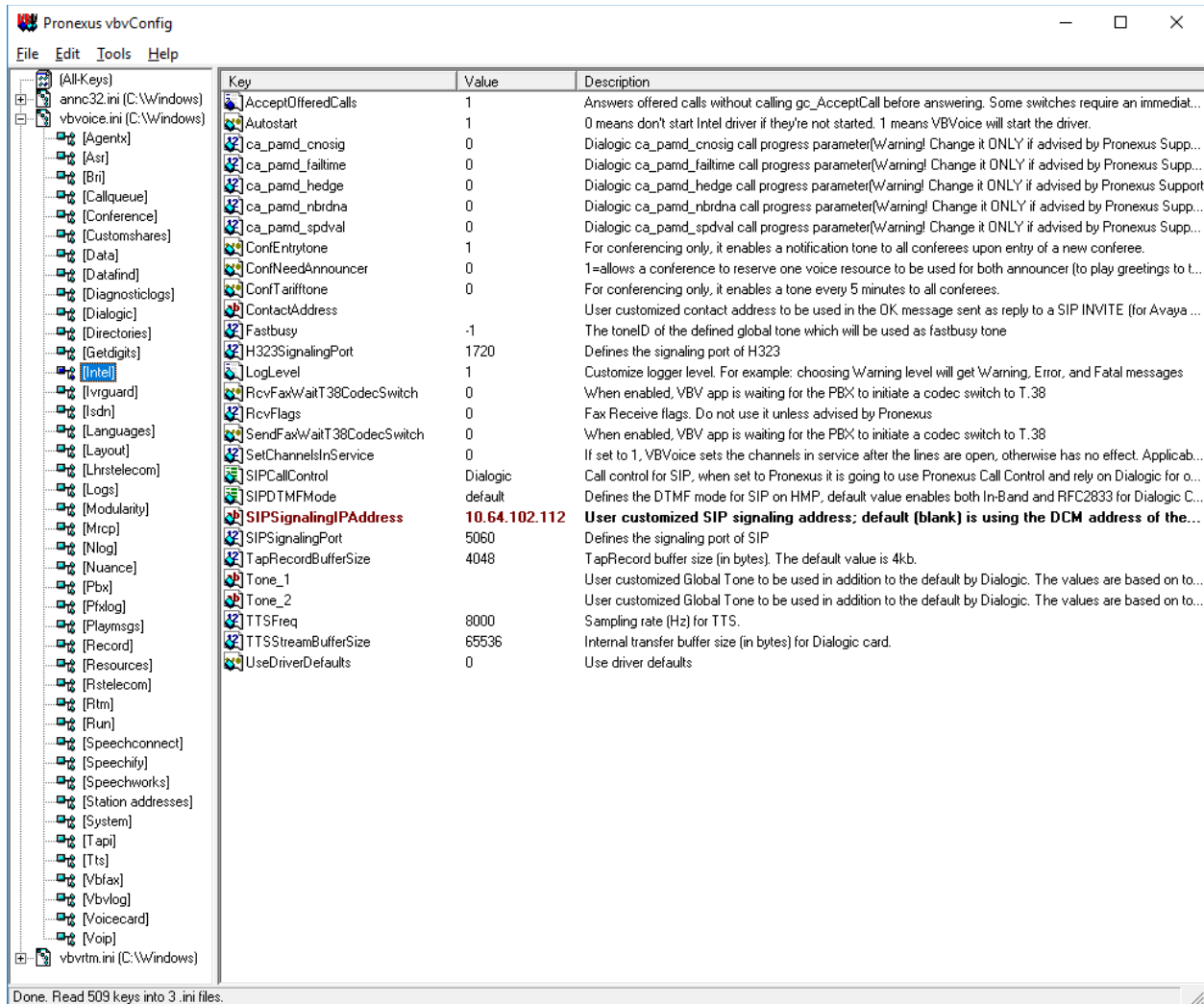
This section covers the configuration of Voice Call Completion, including SIP parameters via **VBVoice Configuration**, a user and tenant via the Voice web interface, and a personal recording (optional). Refer to [6] for additional information on configuring Voice Call Completion.

9.1. VBVoice Configuration

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



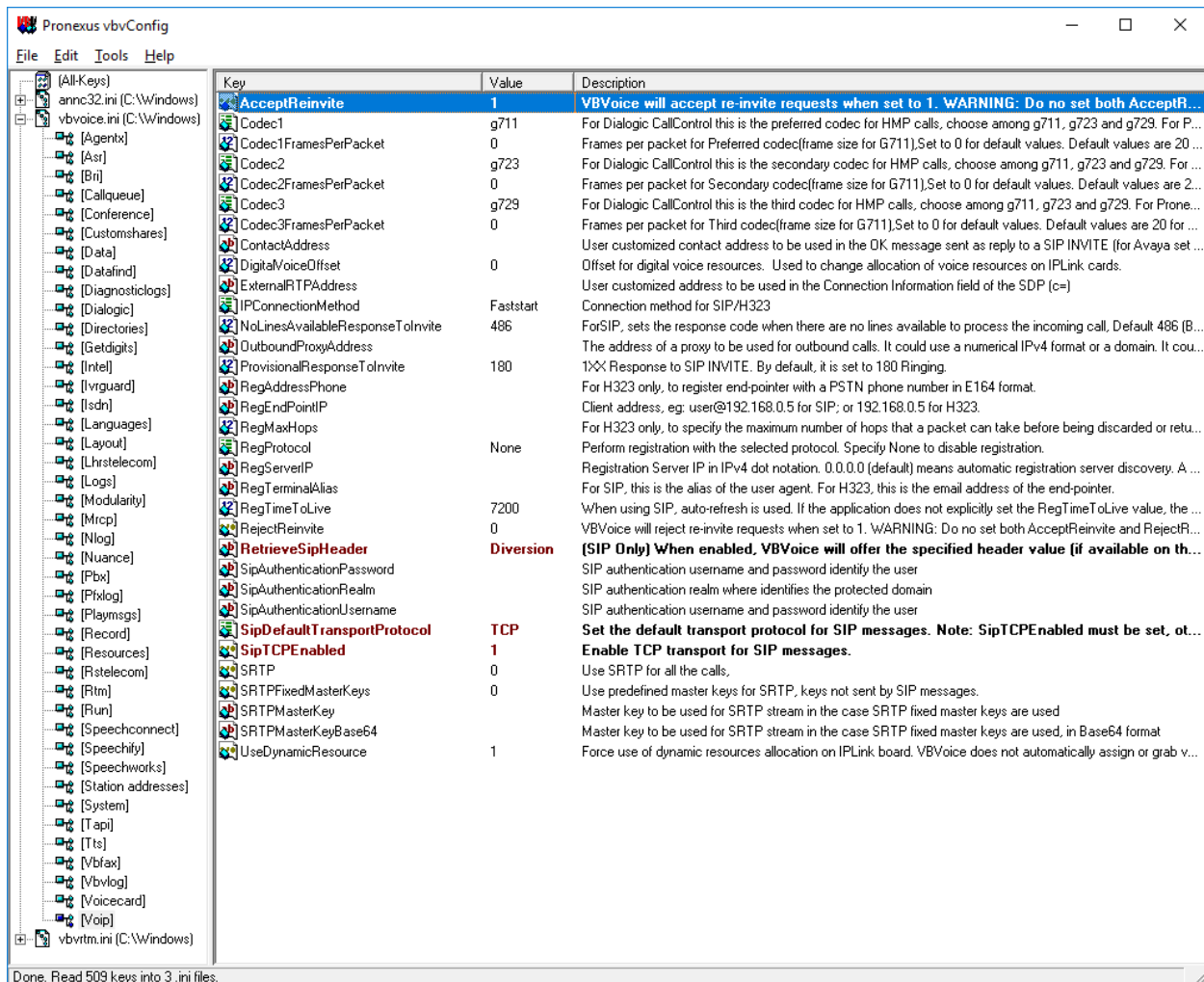
In the **Pronexus vbvConfig** windows displayed below, navigate to **vbvoice.ini** → **Intel**. Set the **SIPSignalingIPAddress** to the IP address of the Voice Application Server and verify that **SIPSignalingPort** is set to **5060**, the default value. Use the default values for the other parameters.



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.




9.2. Configure Voice Call Completion User

Log into the Voice web interface with admin credentials and navigate to **Administration** → **Users** to display the **Users** webpage below. Click **Add** to create a user.

 Mutare Voice™











Administration ▾ Auto Attendants ▾ Spam Filter ▾ @ Administrator ▾ ?

Users

Search 

Active ▾

Add


Display Name ▲	Phone Number	User Name	Role	Notes	Active
Admin, Mutare		mutare	Admin		 
Administrator		Admin	Admin		 
TUI, Mutare		tui	User		 
User, Test	77301	testuser	User		 
User2, Test	78002	testuser2	User		 

5 Users

Page 1 of 1

« < > »

12:04 PM EST -
v2.0.1.0



In the **Create User** screen, fill in the user's name, username, and password. The username and password will allow the user to access their account via the Voice web interface.

Create User

First Name

Sam

Last Name

Elliot

Username

elliott

Password

.....

Confirm Password

.....

Cancel

Create

The following screen is displayed with the user's info previously entered automatically populated. In the **Your Phone Numbers** section, click on **Add a Number**.

Mutare Voice™ Administration ▾ Auto Attendants ▾ Spam Filter ▾ @ Administrator ▾ ?

This is not your profile!

←

Elliot, Sam
elliot
Active **User**

[+ Add a Number](#)
[Add a Notification Method](#)
Call 77333 to listen to Mutare Voice Messages

0 0

General Admin

First Name ⓘ Last Name User Name ⓘ Email Address ⓘ

Sam Elliot elliot Email Address

Full Name ⓘ Password Confirm Password

Elliot, Sam

Type Your Name So a Computer Can Pronounce It ⓘ Time Zone ⓘ

Type Your Name So a Computer Can Pronou Central ▾

Your Phone Numbers

[Add a Number](#)

You currently have no numbers setup for Mutare Voice.


Dial By Name Number ⓘ

Do not include me in the Dial By Name ▾


Manage Blocked Callers

12:10 PM EST - v2.0.1.0

In the subsequent screen shown below, enter the user's number (e.g., 78001) and enable the features shown below. **Allow caller to press zero to transfer to another number** was enabled to allow the caller to press '0' and be routed to another specified number (e.g., 7324441001). In this example, extension 78001 will receive an **Announcement** that contains *Notify w/Msg / Personalized / Transcription* for any missed call. Return to the previous user profile screen.

 Mutare Voice™

Administration ▾ Auto Attendants ▾ Spam Filter ▾ Administrator ▾ ?



Add Number for User: Elliot, Sam

Enter Phone Number ⓘ

78001

What should Mutare Voice do after playing the announcement to the caller?

☒ Allow caller to leave message

☐ Allow caller to review message ⓘ


☒ Allow caller to press zero to transfer to another number

Where should Mutare Voice transfer the caller if they press zero? ⓘ

United States +1 ▾ 7324441001

What announcement should Mutare Voice play to the caller?


Notify w/Msg | Personalized | Transcription ▾

 Hi, this is... [Full name] I will be notified you called. If you would like to add a voice message, please do so and it will be transcribed for a quicker response.

What language should Mutare Voice use for message transcription? ⓘ


en-US ▾

☒ Send me notifications when caller hangs up without leaving message ⓘ

 Out of Office Settings

Configure

12:12 PM EST -
v2.0.1.0



The user's number configured above is displayed as shown below. The **Dial By Name** feature was enabled for this user by specifying the user's number in the **Dial By Name Number** field. Dial By Name allows callers to dial the first few letters of a known party when using the Auto Attendant feature and have Mutare Voice transfer the call to that person's extension.

Administration ▾ Auto Attendants ▾ Spam Filter ▾ Administrator ▾

This is not your profile!

Elliot, Sam
elliot
Active User

Record your Personal Announcement
Configure Out of Office ▾
Add a Number
Add a Notification Method
Call 77333 to listen to Mutare Voice Messages

0 Delegates
0 Delegated

General Admin

First Name ⓘ Last Name User Name ⓘ Email Address ⓘ

Sam Elliot elliot Email Address

Full Name ⓘ Password Confirm Password

Elliot, Sam

Type Your Name So a Computer Can Pronounce It ⓘ Time Zone ⓘ

Type Your Name So a Computer Can Pronounce It Central ▾

Your Phone Numbers

Add a Number

Number	Announcement ⓘ	Out Of Office ⓘ	Zero Out ⓘ
78001	Notify w/Msg Personalized Transcription Hi, this is... [Full name] I will be notified you called. If you would like to add a voice message, please do so and it will be transcribed for a quicker response.	Off	(732) 444-1001

Dial By Name Number ⓘ

78001 ▾

Manage Blocked Callers

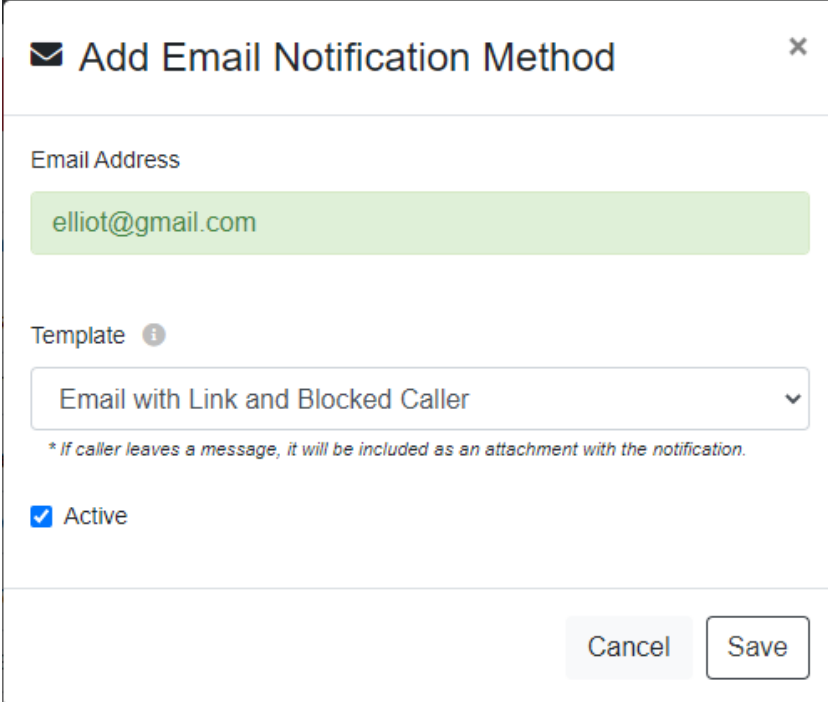
In the **Your Notification Methods** section, click on **Add a Notification Method**.

The screenshot shows the Mutare Voice user interface. At the top, a dark header bar contains the Mutare Voice logo and navigation links: Administration, Auto Attendants, Spam Filter, and Administrator. Below this is a red banner that reads "This is not your profile!". The main content area is divided into a left sidebar and a right main panel. The sidebar shows the user's profile: a circular avatar placeholder, the name "Elliot, Sam", the username "elliott", and status indicators "Active" and "User". Below the profile are links for "Record your Personal Announcement", "Configure Out of Office", "Add a Number", and "Add a Notification Method". At the bottom of the sidebar are icons for messages and calls, both showing a count of 0. The main panel has two tabs: "General" (selected) and "Admin". Under the "General" tab, there are fields for "First Name" (Sam), "Last Name" (Elliot), "User Name" (elliott), "Email Address" (Email Address), "Full Name" (Elliot, Sam), "Password" (masked with dots), "Confirm Password" (masked with dots), "Type Your Name So a Computer Can Pronounce It" (Type Your Name So a Computer Can Pronounce It), and "Time Zone" (Central). Below these fields are three sections: "Your Phone Numbers", "Your Notification Methods", and "Your Saved Personal Announcements". The "Your Notification Methods" section contains a link "Add a Notification Method" and a checkbox "Use 24-hr format?". A red message box states "You are currently not receiving notifications for missed calls." The footer of the page shows the time "12:16 PM EST - v2.0.1.0" and the Mutare logo.

The following dialog box will be used to add Email and SMS notification methods. First, select **Email**.

The dialog box is titled "How would you like to be notified?" and has a close button (X) in the top right corner. It contains three radio button options: "Email" (selected), "Mutare Text Alert Message", and "SMS". At the bottom right, there is a "Cancel" button.

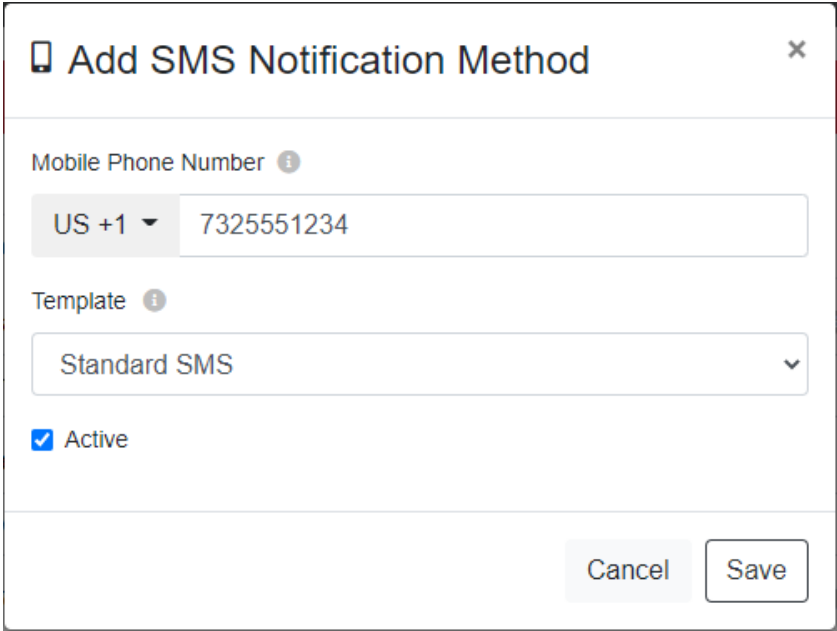
In the **Add Email Notification Method** pop-up screen, enter the user's email address and mark as active.



The screenshot shows a pop-up window titled "Add Email Notification Method" with a close button (X) in the top right corner. The form contains the following fields and controls:

- Email Address:** A text input field containing "elliott@gmail.com".
- Template:** A dropdown menu with "Email with Link and Blocked Caller" selected. Below the dropdown is a small italicized note: "* If caller leaves a message, it will be included as an attachment with the notification."
- Active:** A checkbox that is checked, labeled "Active".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Next, add SMS as a second notification method. Enter the user's **Mobile Phone Number**, select *Standard SMS* as the **Template**, and mark as active.



The screenshot shows a pop-up window titled "Add SMS Notification Method" with a close button (X) in the top right corner. The form contains the following fields and controls:

- Mobile Phone Number:** A text input field with a country code dropdown set to "US +1" and the number "7325551234".
- Template:** A dropdown menu with "Standard SMS" selected.
- Active:** A checkbox that is checked, labeled "Active".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Return to the user profile and verify that the two notification methods are now listed as shown below. This user will receive a SMS notification at (732) 555 – 1234 and an email notification at elliott@gmail.com.

Mutare Voice™
 Administration ▾ Auto Attendants ▾ Spam Filter ▾ @ Administrator ▾ ?

This is not your profile!

Elliot, Sam
elliott

Active User

Record your Personal Announcement

Configure Out of Office ▾

Add a Number

Add a Notification Method

Call 77333 to listen to Mutare Voice Messages

✉ 0 📧 0

General Admin

First Name ⓘ

Last Name

User Name ⓘ

Email Address ⓘ

Sam

Elliot

elliott

Email Address

Full Name ⓘ

Password

Confirm Password

Elliot, Sam

.....

.....

Type Your Name So a Computer Can Pronounce It ⓘ

Time Zone ⓘ

Type Your Name So a Computer Can Pronounce It

Central ▾

Your Phone Numbers

Your Notification Methods

[Add a Notification Method](#)

☐ Use 24-hr format?

Send Notifications to...	Template ⓘ	Active		
📱 (732) 555-1234	Standard SMS	✓		
✉ elliott@gmail.com	Email with Link and Blocked Caller	✓		

12:16 PM EST -
v2.0.1.0

To allow the user to call the TUI from an authorized phone, add the authorized number as shown below. In the example below, the authorized number is *78001*.

Mutare Voice™ Administration Auto Attendants Spam Filter Administrator ?

This is not your profile!

Elliot, Sam
elliott
Active User

[Record your Personal Announcement](#)
[Configure Out of Office](#)
[Add a Number](#)
[Add a Notification Method](#)
Call 77333 to listen to Mutare Voice Messages

0 0

0 Delegates
[0 Delegated](#)

+ Delegates
Users that can edit your profile

Elliot, Sam

Type Your Name So a Computer Can Pronounce It [?](#) Time Zone [?](#)
Type Your Name So a Computer Can Pronounce Central

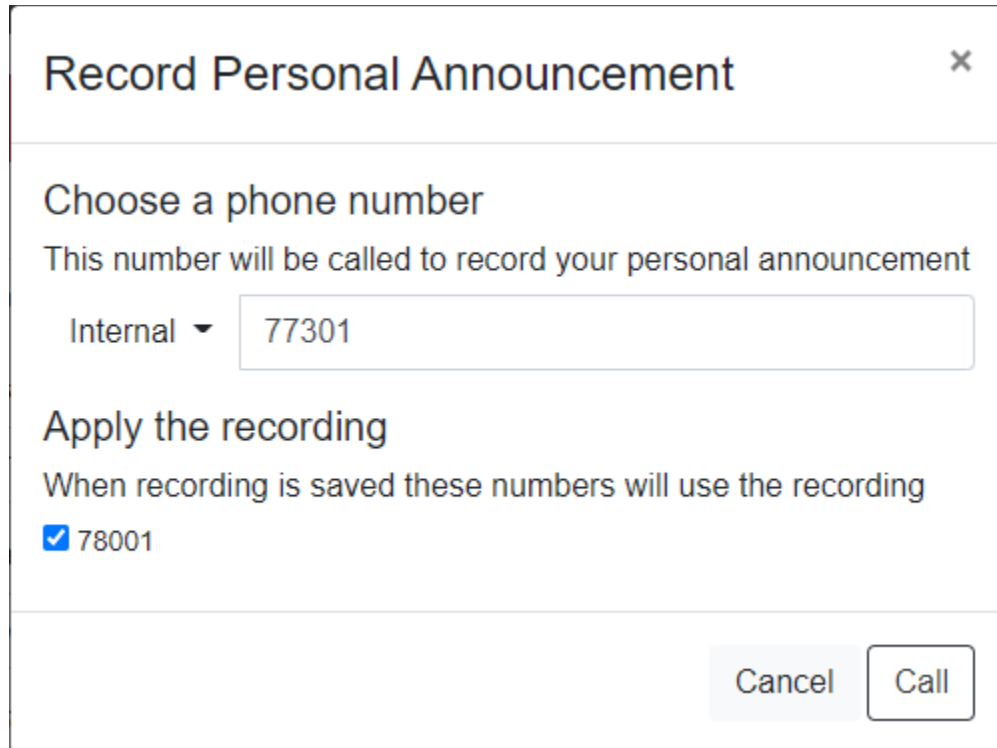
[Your Phone Numbers](#)
[Your Notification Methods](#)
[Your Saved Personal Announcements](#)
[Phone Message Retrieval](#)

Message Playback Order
☐ Play unread messages first [?](#)
☒ Play messages from newest to oldest [?](#)
☐ Notification will mark messages read [?](#)
[Add Authorized Number](#)

78001 [✕](#)
Extension

Optionally, the user may record a personal announcement for missed calls. A personal greeting is recorded by Voice Call Completion by placing an outbound call to a phone number. Once the call is answered, the user will be prompted to record a personal announcement. To record a personal announcement, click on the option in the left pane of the user profile.

The **Record 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. The following example shows an outbound call to be placed to an internal number, but the call could also be placed to a PSTN number.



The image shows a dialog box titled "Record Personal Announcement" with a close button (X) in the top right corner. The dialog is divided into two main sections. The first section, "Choose a phone number", includes a sub-header "This number will be called to record your personal announcement". Below this, there is a dropdown menu currently set to "Internal" and a text input field containing the number "77301". The second section, "Apply the recording", includes a sub-header "When recording is saved these numbers will use the recording". Below this, there is a list of numbers with checkboxes; the number "78001" is checked. At the bottom right of the dialog, there are two buttons: "Cancel" and "Call".

Record Personal Announcement [X]

Choose a phone number

This number will be called to record your personal announcement

Internal ▼ 77301

Apply the recording

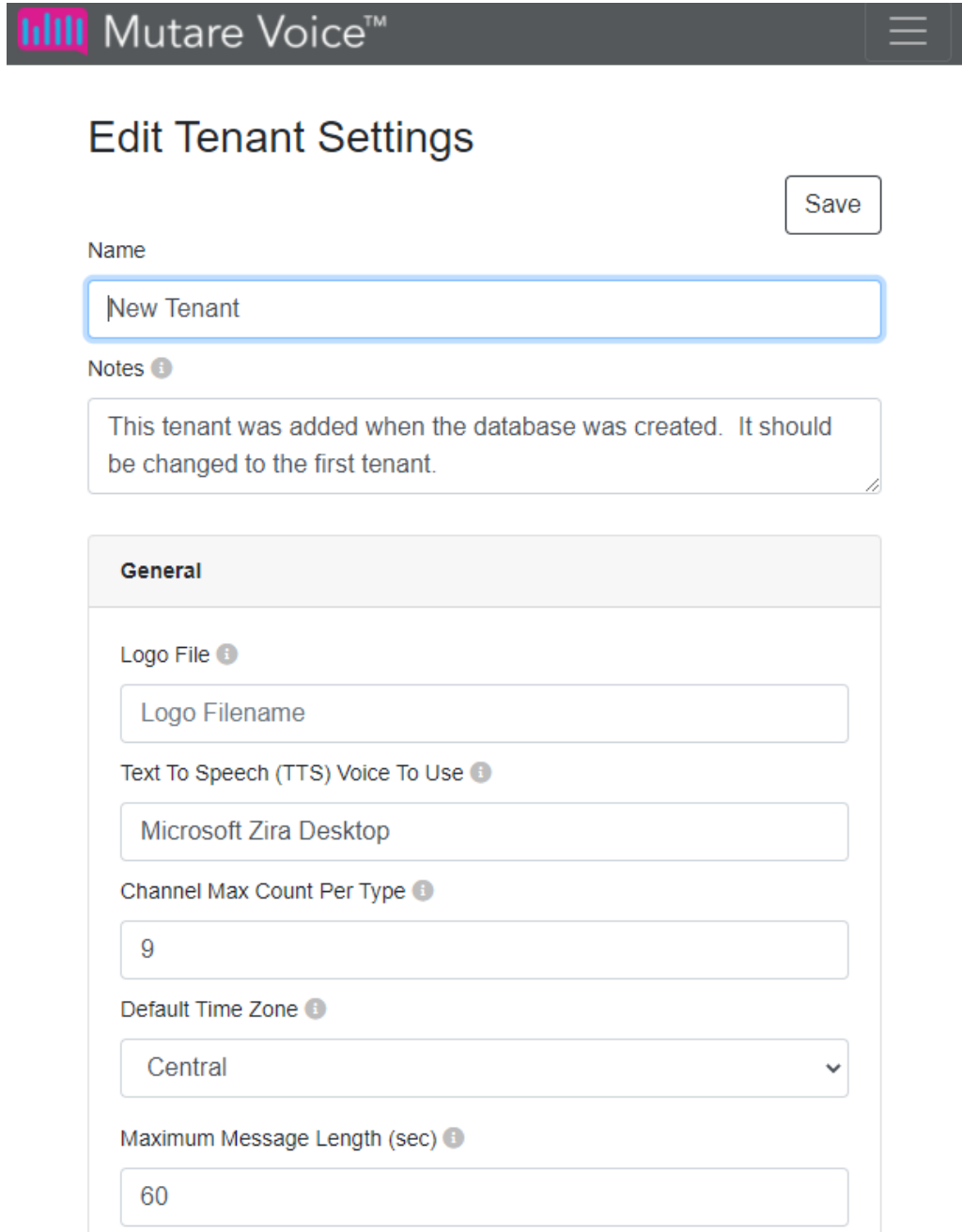
When recording is saved these numbers will use the recording

☒ 78001

Cancel Call

9.3. Configure Tenant Settings

From the Voice web interface, select **Administration** → **Tenant Settings**. The Tenant Settings webpage is displayed as shown below. Provide a descriptive name in the **Name** field.



The screenshot shows the Mutare Voice web interface. At the top is a dark header with the Mutare Voice logo and a hamburger menu icon. Below the header is the title "Edit Tenant Settings" and a "Save" button. The "Name" field contains "New Tenant". The "Notes" section contains a message: "This tenant was added when the database was created. It should be changed to the first tenant." Below this is a "General" tab with several settings: "Logo File" (with a sub-field "Logo Filename"), "Text To Speech (TTS) Voice To Use" (set to "Microsoft Zira Desktop"), "Channel Max Count Per Type" (set to "9"), "Default Time Zone" (set to "Central"), and "Maximum Message Length (sec)" (set to "60").

Mutare Voice™

Edit Tenant Settings

Save

Name

New Tenant

Notes ⓘ

This tenant was added when the database was created. It should be changed to the first tenant.

General

Logo File ⓘ

Logo Filename

Text To Speech (TTS) Voice To Use ⓘ

Microsoft Zira Desktop

Channel Max Count Per Type ⓘ

9



Default Time Zone ⓘ

Central ▼

Maximum Message Length (sec) ⓘ

60

Scroll down and configure the **Outbound ANI Name** and **Outbound ANI Number** fields.


 Mutare Voice™

Outbound ANI Name


Avaya

Outbound ANI Number


8005551212@10.64.102.112

Days to Keep Recordings 


30

Days to Keep Transcriptions 

30



Number Help Text 


Enter your extension number. Contact your administrator for as


Email Addresses for Notifications of Locked Out Users 


Email Addresses for Notifications of Locked Out Users


Scroll down and enable the desired features in the following section.


 Mutare Voice™


☒ Enable Dial By Name 


☒ Allow Users to call their phone to play message on handset 


☒ Allow Users to call external numbers to play message on handset 


☒ Allow Users to call external number to record personal announcements 



☒ Enable Message Review 

☒ Users may add, edit, delete Phone Numbers 

☒ Enable User Delegation 

☐ User can Add Delegates 

☒ Enable Forgot Password link on Login page? 



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

SMTP

Domain Name Whitelist ⓘ

Server ⓘ

Port ⓘ

Account ⓘ

Password ⓘ

From Address ⓘ

☒ Use SSL ⓘ

Scroll down to the **Zero Out** section to enable the feature. The option to allow users to be transferred to external numbers is also provided.

Zero Out

☒ Enabled? ⓘ

☒ Allow Users to transfer to external numbers ⓘ

Caller Pressed Zero Tag Text ⓘ

The caller pressed zero to transfer to {Zero Out Number}.

Caller Pressed Zero Tag HTML ⓘ

```
<p><font face="Arial, Helvetica, sans-serif" size="3"
color="#41444a" style="font-size:16px;line-
height:19px;">The caller pressed zero to transfer to {Zero
Out Number}.</font></p>
```

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.

Primary SMS Provider

Account

AC39e88036687f29fd79fac0436f8efd5c

Token

.....

From Phone

+18472216279

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

Speech To Text (STT)

Callback Timeout ⓘ

60

Default Language

en-US ▼

AccountId

G66667566

Token

.....

Rest Url

https://gistt.mutare.com/api

Audio Quality Threshold ⓘ

0

Poor Quality Audio Message ⓘ

The caller's message was unable to be transcribed due to poor

☐ Callbacks ⓘ

☒ Default Is Enabled ⓘ

Scroll down to the Phone Message Retrieval section to enable TUI and specify the TUI pilot number (e.g., 77333). Note that this pilot number matches the extension of the phantom station in **Section 5.8.1**.

Phone Message Retrieval

☒ Enabled for Users? ⓘ

Mark All Messages "Read"... ⓘ

Pilot Number ⓘ >

77333

Pilot Number Display ⓘ >

77333

☒ Allow users to self-authorize phone numbers for message retrieval? ⓘ >

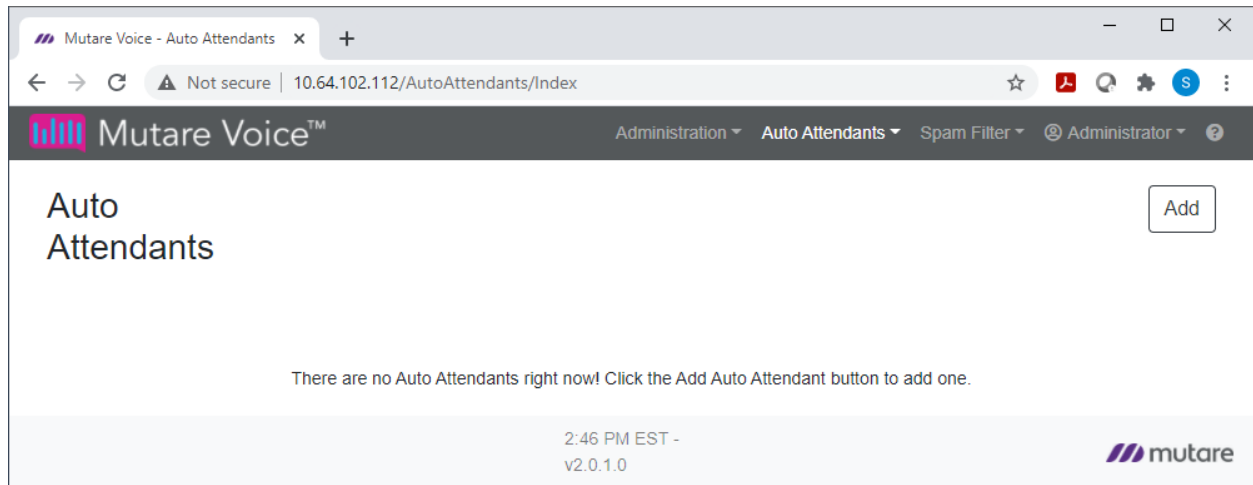
Authorized Number Message ⓘ >

Enter extension number for desk phone. Enter external numbers as +1XXXYYYZZZZ.


Messages older than 30 days are automatically deleted. This value can be changed in the "Days to Keep Recordings" setting.

9.4. Configure Auto Attendant

To add an Auto Attendant, navigate to **Auto Attendants** → **Auto Attendants** to display the webpage below. Click **Add**.



In the **Auto Attendant** webpage, specify a **Name** for the Auto Attendant and the **Extension** (e.g., 77334). The extension should match the phantom station extension configured in **Section 5.8.2**. Next, upload a **Menu Recording**. In the **In-Call Options** section, configure the desired menu options. In the following example, one menu option is provided that allows **Dial By Name**.

 Mutare Voice™
 Administration ▾ Auto Attendants ▾ Spam Filter ▾ Administrator ▾ ?


← Add Auto Attendant Unsaved changes Save



Name

Extension ⓘ

Description




Schedule
 ▾
**This schedule is always open so there is no Closed Hours Menu*
 Blocked Caller Action ⓘ
 ▾

 Open Hours Menu

Menu Recording ⓘ
 Recording uploaded.  

Notes / Script for Recording

In-Call Options

Option	Name	Action	Details
1	Dial By Name	 Dial By Name	 
2		None	Add ▾
3		None	Add ▾

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager, SBCE, Voice Spam Filter, and Voice Call Completion.

1. From the System Manager home page (not shown), select **Elements → Session Manager** from the top menu to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Voice Spam Filter entity name from **Section 6.2.2**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', 'Shortcuts', a search bar, and a user profile 'admin'. The left sidebar shows a menu with 'Session Manager' expanded, containing 'Dashboard', 'Session Manager Ad...', 'Global Settings', 'Communication Prof...', 'Network Configur...', 'Device and Locati...', 'Application Confi...', 'System Status', and 'SIP Entity Monit...'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a description: 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' Below this, there's a section 'Status Details for the selected Session Manager:' followed by 'All Entity Links to SIP Entity: Mutare Voice Screening Proxy'. A 'Summary View' button is present. A table shows '1 Item' with a filter set to 'Enable'. The table has columns: Session Manager Name, Session Manager IP Address, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The data row shows 'devcon-sm' with IP '10.64.102.104', Port '5060', Proto. 'TCP', Deny 'FALSE', Conn. Status 'UP', Reason Code '200 OK', and Link Status 'UP'. A 'Select : None' dropdown is at the bottom.

Session Manager Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	10.64.102.104	5060	TCP	FALSE	UP	200 OK	UP

2. Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Voice Call Completion entity name from **Section 6.2.3**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

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.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Mutare Voice Application Server

Summary View

1 Item Filter: Enable

	Session Manager Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	devcon-sm	IPv4	10.64.102.112	5060	TCP	FALSE	UP	200 OK	UP

Select : None

3. Configure a spam filter rule, such as CAPTCHA Drop, that matches the caller ID of the incoming call. Also, configure Voice Call Completion user as described in these Application Notes.
4. Place an incoming PSTN call to the subscriber. Verify that the incoming call is flagged as a potential spam call by Voice Spam Filter and the call is sent to the CAPTCHA system.
5. The user enters the numbers requested by the CAPTCHA system and the call is allowed to ring at the subscriber.
6. The subscriber doesn't answer and the missed call notification is sent to Email and SMS with a transcription.
7. Verify that the incoming call was logged in the Call History Report. A sample Call History Report is shown below.



Call History Report

Search for Caller ID, Called Number

More Filters

CSV

Calls from Today

Call ID	Call Time	Caller ID	CNAM	Called Number	Action	Reason	External Spam Service	Filter Mode	CAPTCHA Result	SIP
ebb920d6...	1/6/2021 12:01:44 PM	7324441000	Extn41000	97327777301	CAPTCHA	Rule	Passed	Active	Success	
3fc21339...	1/6/2021 11:13:38 AM	3612002438	Extn41001	97327777301	Route-78002@10.64.102.117	Robocall +	Robocall	Active		
9ab5178b...	1/6/2021 11:12:23 AM	3612002438	Extn41001	97327777301	CAPTCHA	Robocall +	Robocall	Active	Success	
db94da49...	1/6/2021 11:12:00 AM	3612002438	Extn41001	97327777301	Drop	Robocall +	Robocall	Active		
37754e41...	1/6/2021 11:11:43 AM	7324441000	Extn41000	97327777301	CAPTCHA	Rule	Passed	Active	Success	
ebf0795c...	1/6/2021 11:11:26 AM	3612002438	Extn41001	97327777301	Drop	Robocall +	Robocall	Active		
077f4979...	1/6/2021 11:10:22 AM	3612002438	Extn41001	917327777301	Allow	Timeout +	Not Checked	Active		

12:59 PM EST -
v2.0.1.0

11. Conclusion

These Application Notes have described the administration steps required to Mutare Voice with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Mutare Voice was able to filter spam calls and take the appropriate action and 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**.

12. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, October 2020, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020, available at <http://support.avaya.com>.
- [5] *Mutare Voice User Guide*, Version 2.0.0, September 20, 2020, available at <https://mutare.com/knowledge/tech-docs>.
- [6] *Mutare Voice Admin Guide*, Version 2.0.0, October 13, 2020, available at <https://mutare.com/knowledge/tech-docs>.

©2021 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.