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 (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 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 and Avaya Aura® 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 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.

2 General Test Approach

To verify interoperability of Smart Assist by Mutare with Avaya Aura® Communication Manager and Avaya Aura® 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with 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.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between SAM and Session Manager using TCP 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.
- 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:

- SAM does not currently support Direct IP-IP Media (aka Shuffling).

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.
- Smart Assist by Mutare running in a virtual environment.
- Mutare giSTT in the cloud used for message transcription.

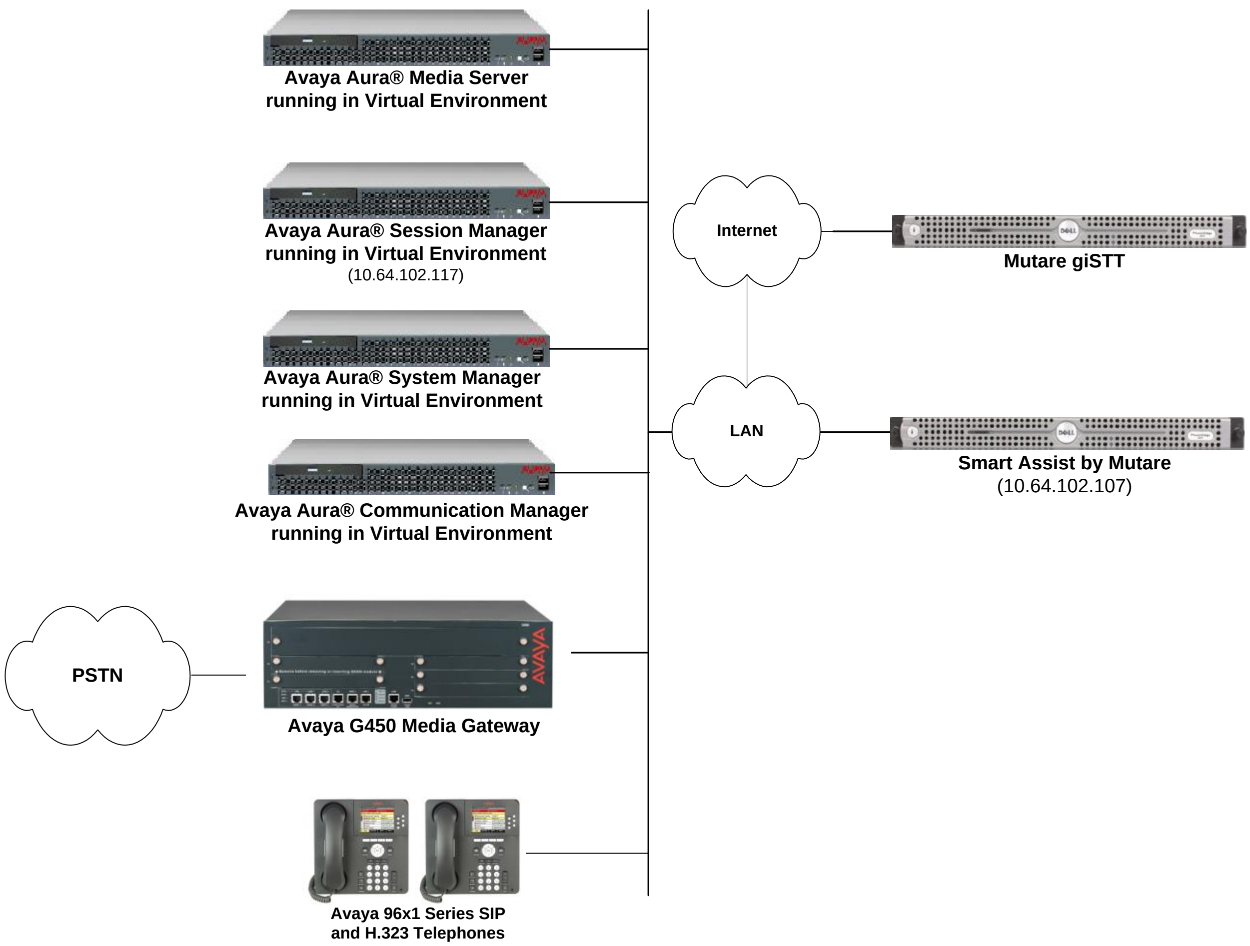


Figure 1: Avaya SIP Network with Smart Assist by Mutare and Mutare giSTT

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 with Avaya G450 Media Gateway	7.0.1.1 FP1 SP1 (R017x.00.0.441.0 with Patch 23384)
Avaya Aura® Media Server running in a Virtual Environment	7.7.0.375
Avaya Aura® Session Manager running in a Virtual Environment	7.0.1.1 (7.0.1.1.701114)
Avaya Aura® System Manager running in a Virtual Environment	7.0.1.1 (Build No. 7.0.0.016266 Software Update Revision No: 7.0.1.1.065378 Service Pack 1)
Avaya 96x1 Series IP Telephones	6.6401U (H.323) 7.0.1.2.9 (SIP)
Smart Assist by Mutare	1.2.0.0
Mutare giSTT (in the cloud)	1.7.5

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, 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-ams          10.64.102.118
devcon-sm           10.64.102.117
procr               10.64.102.115
procr6              ::

( 5  of 5    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      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*.

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

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 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 50                                          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 10                                          Page   5 of  22
                              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:
```

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 SAM. In this example, missed calls will be forwarded to the SAM extension number 78550 for users configured with call coverage to SAM.

```
add hunt-group 30                                              Page   1 of  60
                                  HUNT GROUP

            Group Number: 30                            ACD? n
              Group Name: Mutare SAM                  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 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 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 SAM (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 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 SAM 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 and SAM
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and SAM
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

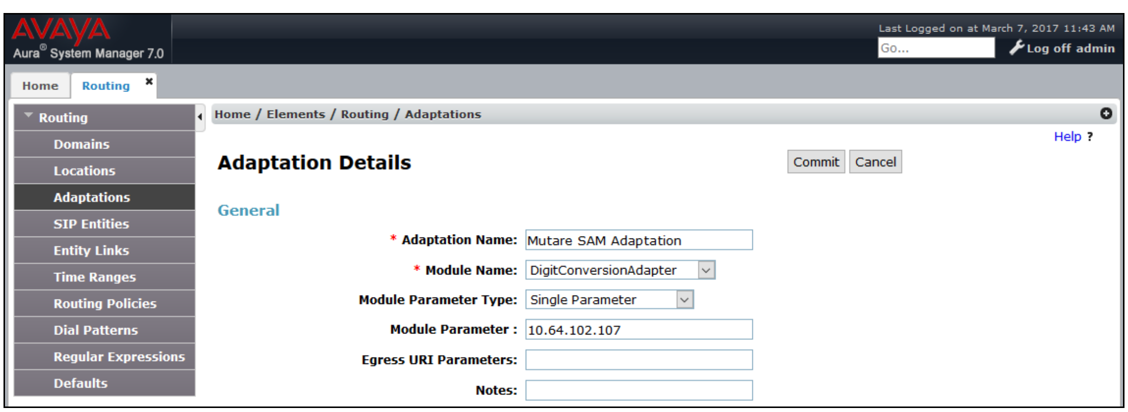
Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

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 for SAM.*

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 SAM SIP entity in **Section 6.2.2**, 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 SAM Adaptation*).
- **Module Name:** Select **DigitConversionAdapter**.
- **Module Parameter Type:** Select **Single Parameter**.
- **Module Parameter:** Enter the SAM IP address.



6.2 Add SIP Entities

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

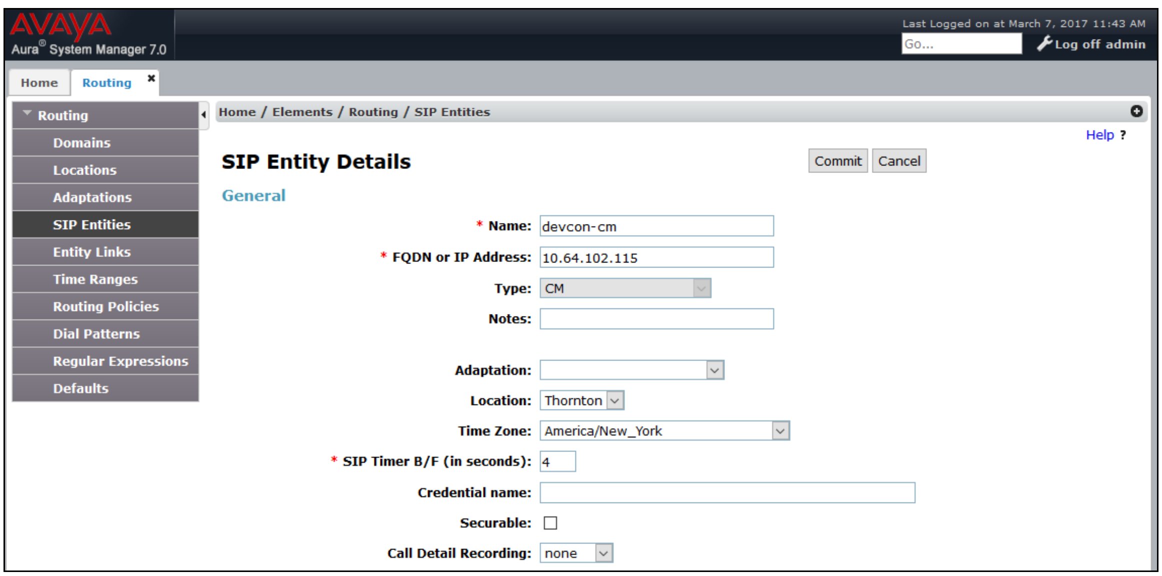
6.2.1 Avaya Aura® Communication Manager

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.

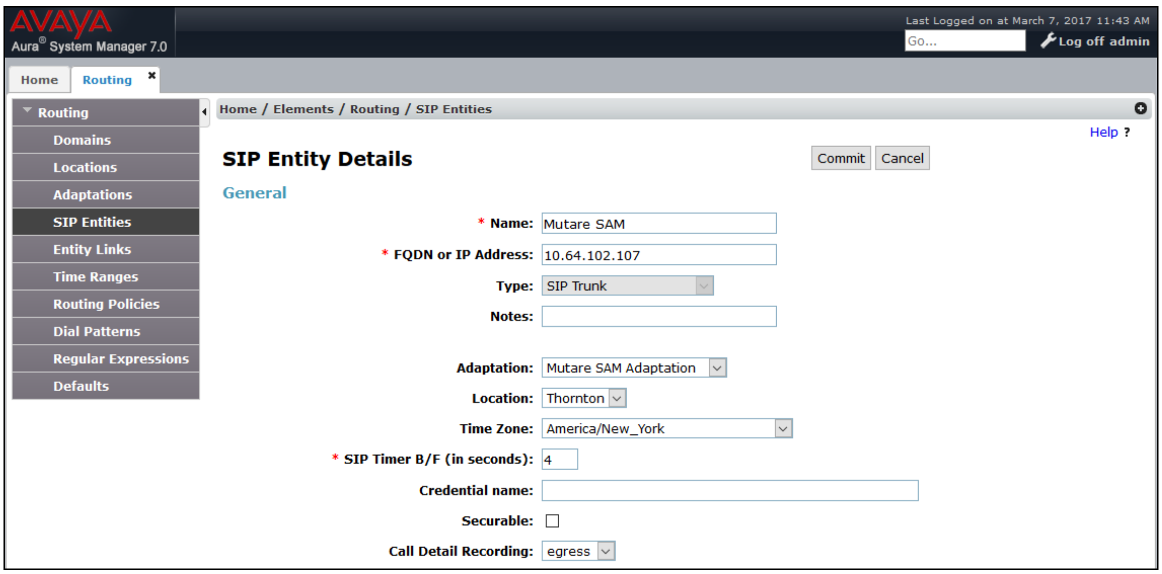


6.2.2 Smart Assist by Mutare

A SIP Entity must be added for SAM. 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 of SAM.
- **Type:** Select *SIP Trunk*.
- **Adaptation :** Select the Adaptation configured in **Section 6.1**.
- **Location:** Select the location defined previously (not shown).
- **Time Zone:** Time zone for this location.



6.3 Add Entity Links

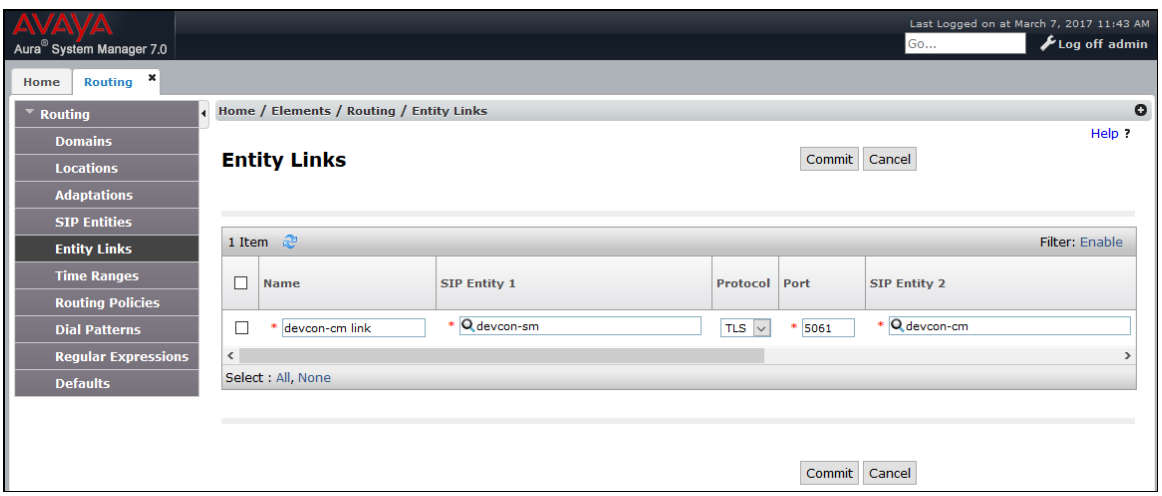
This section covers the configuration of Entity Links for Communication Manager and SAM.

6.3.1 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 (e.g., *devcon-cm Link*).
- **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 6.2.1*** *will be denied.*

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

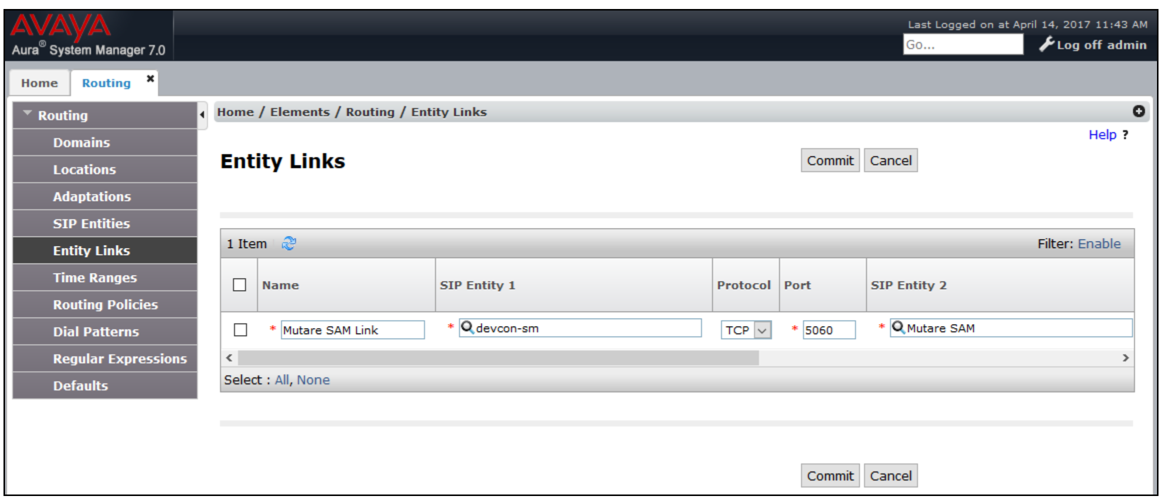


6.3.2 Smart Assist by Mutare Entity Link

The SIP trunk from Session Manager to SAM 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 (e.g., *Mutare SAM Link*).
- **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 *Mutare SAM* 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 6.2.2** will be denied.*

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



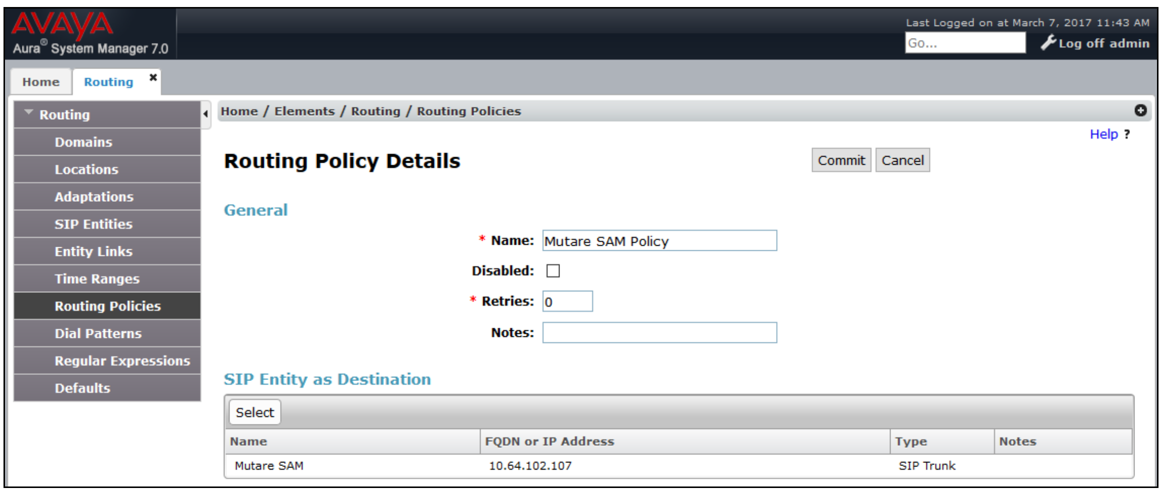
6.4 Add Routing Policies

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 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 following screen shows the SAM Routing Policy.



6.5 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 SAM.

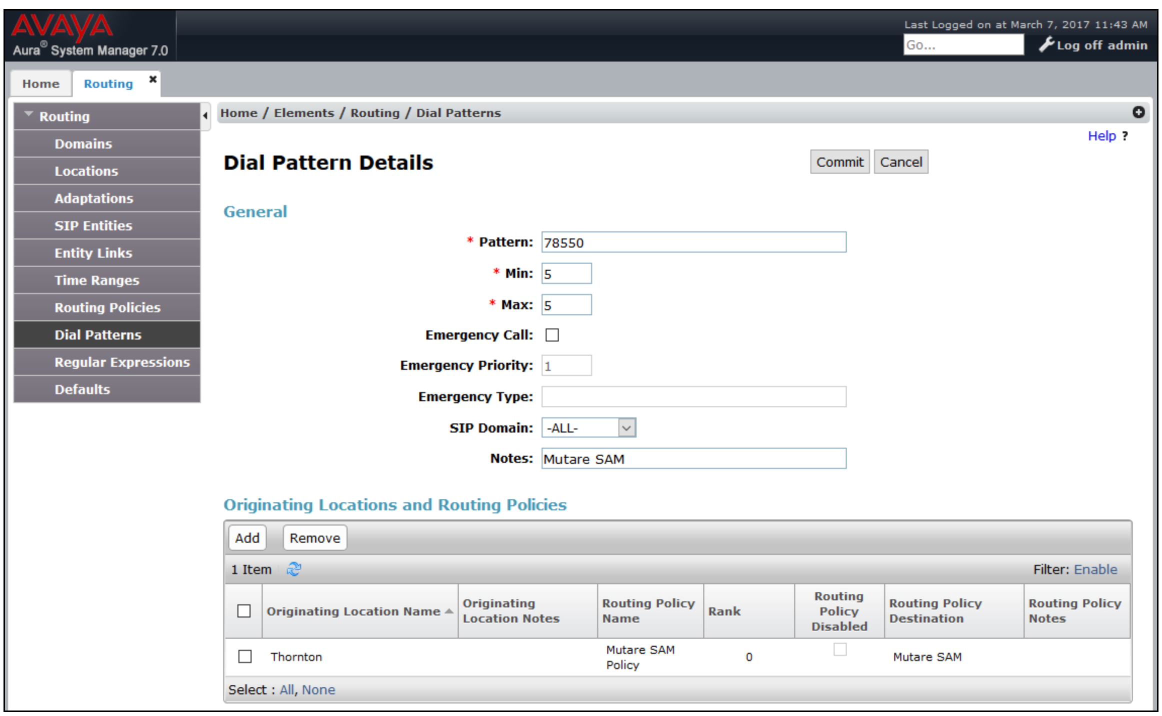
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

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 SAM.



6.6 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:

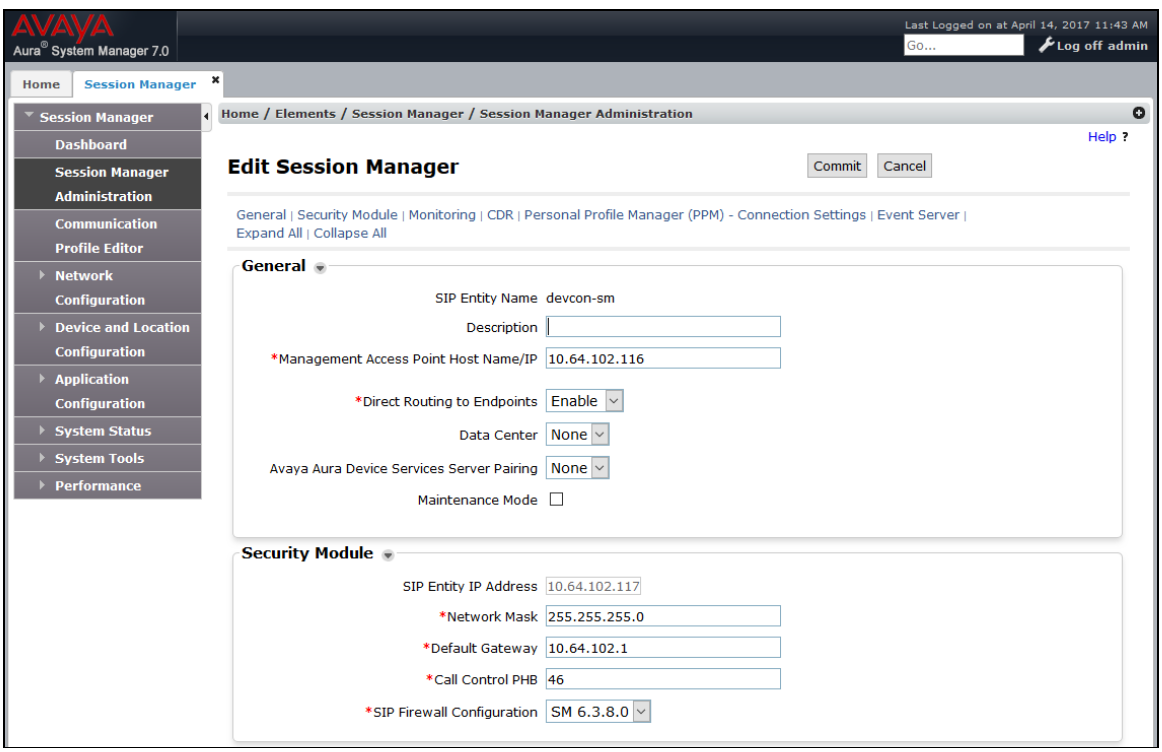
Under *General*:

- **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

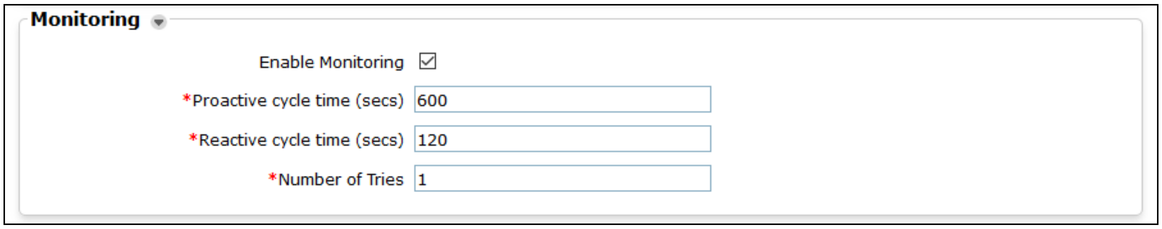
Under *Security Module*:

- **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 following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to SIP entities, including SAM. 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.



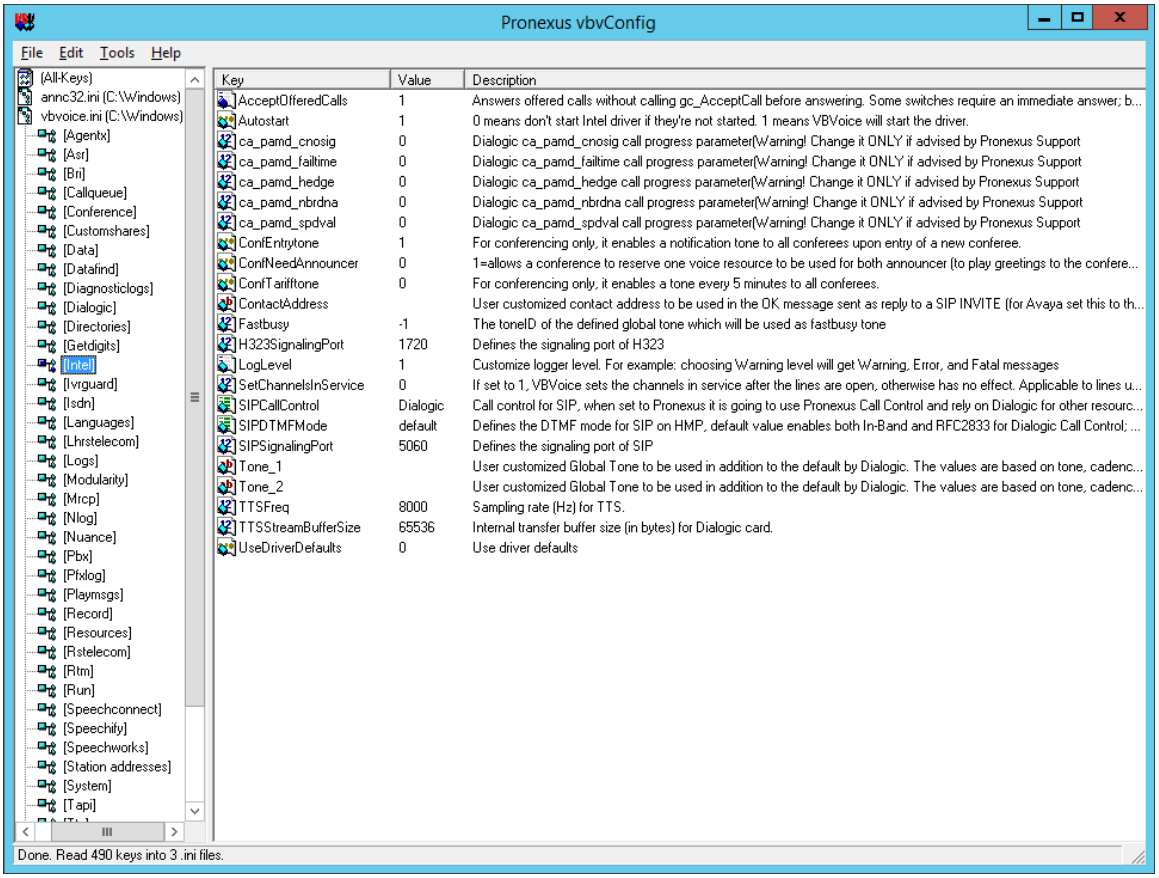
7 Configure Smart Assist by Mutare

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.

7.1 VBVoice Configuration

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

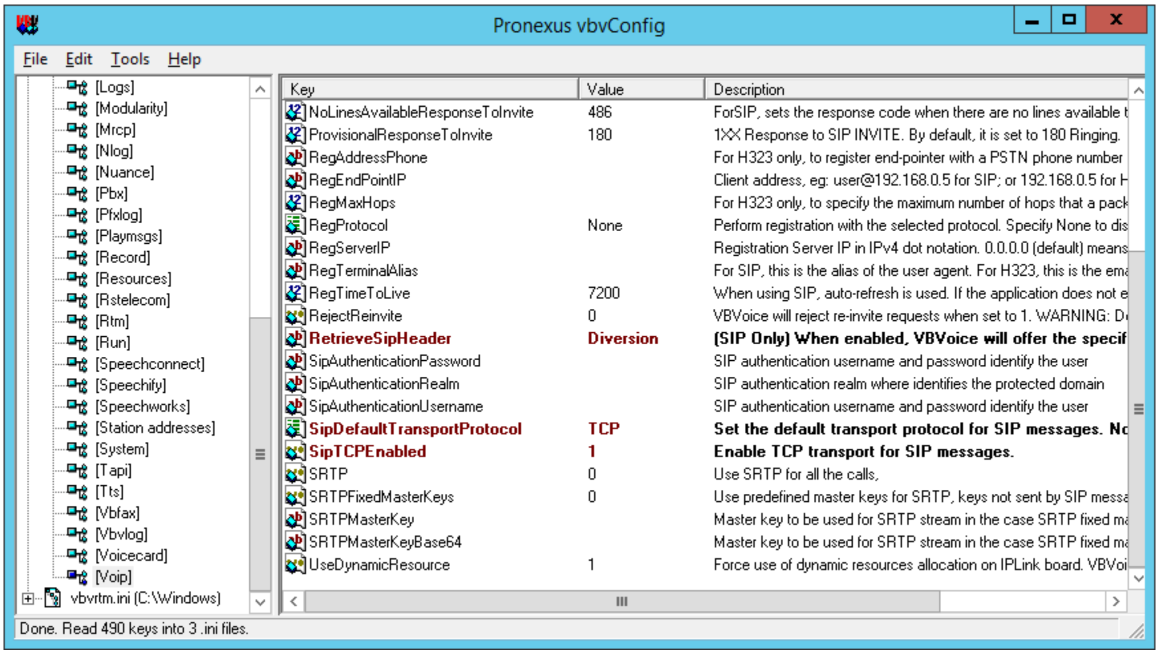
In the **Pronexus vbvConfig** windows displayed below, navigate to **vbvoice.ini → Intel**. Verify that **SIPSignalingPort** is set to *5060*, the default value. Continue to use the default values for the other parameters.



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

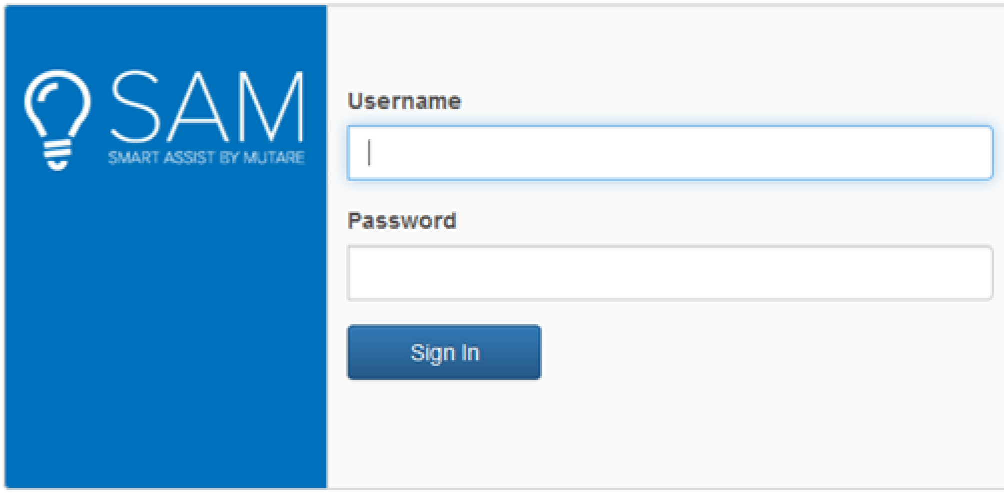
- **RetrieveSipHeader:** Set to *Diversion*.
- **SipDefaultTransportProtocol:** Set to *TCP*.
- **SipTCPEnabled:** Set to '1'.

Use the default values for the remaining parameters.

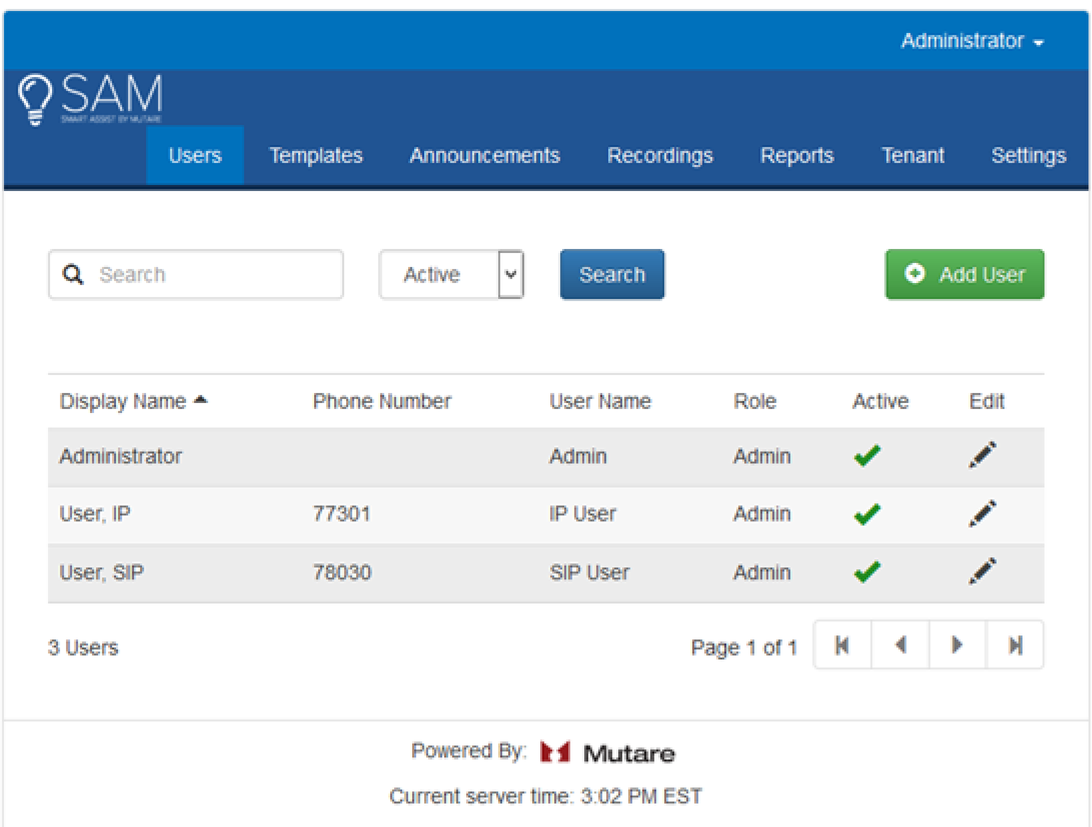


7.2 Configure SAM User

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.

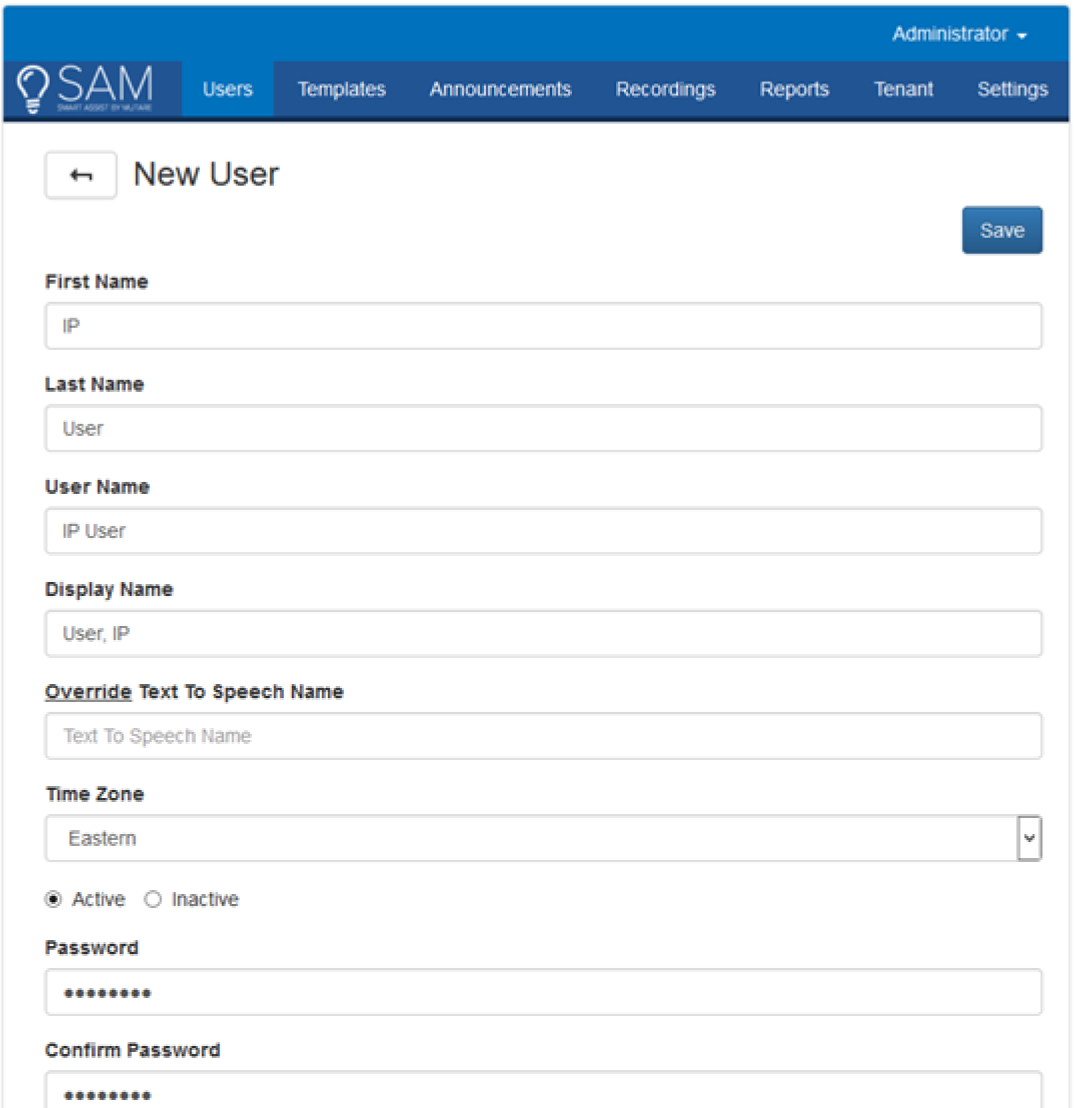


In the SAM Web administration interface, select **Users**, and then click the **Add User** button to add a user.

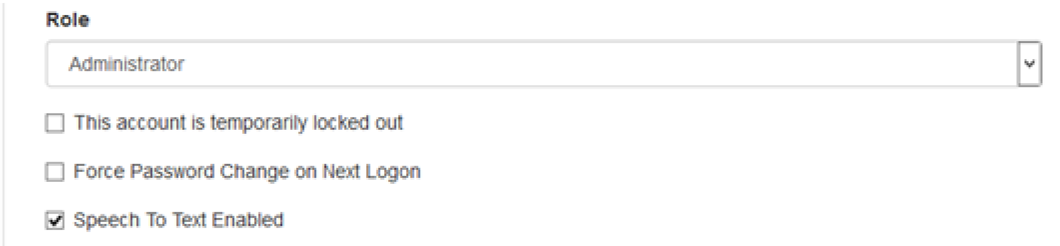


The **New User** page should display. Configure the following fields:

- **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.

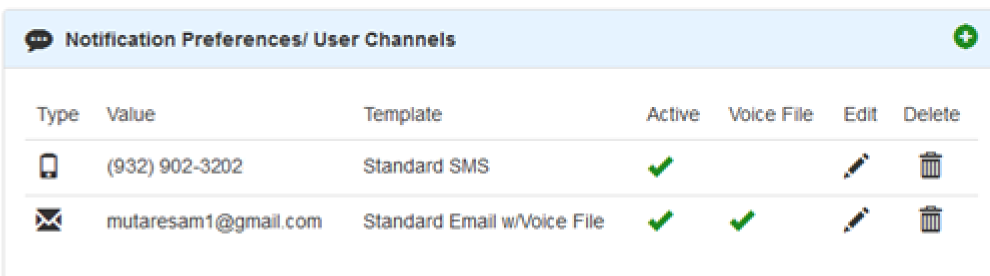


Scroll down the page and select the **Speech to Text Enabled** option to allow voice messages to be transcribed to text messages using Mutare giSTT.

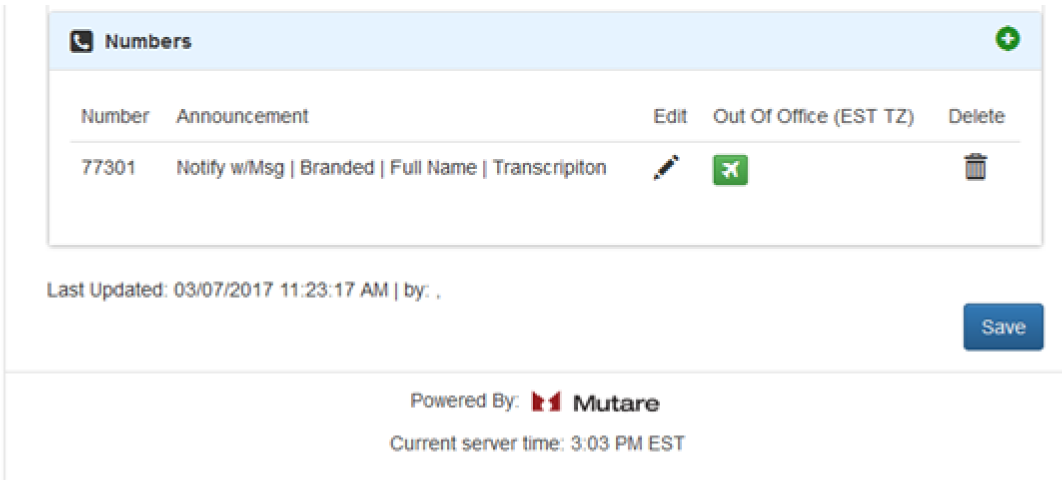


Scroll down to the **Notification Preferences/User Channels** section. In this section, the user can set up the notification preferences for how they will receive a notification that a message has been left for them. Click on to add a notification preference. For the first entry, specify a phone number (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*.



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**.



7.3 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:

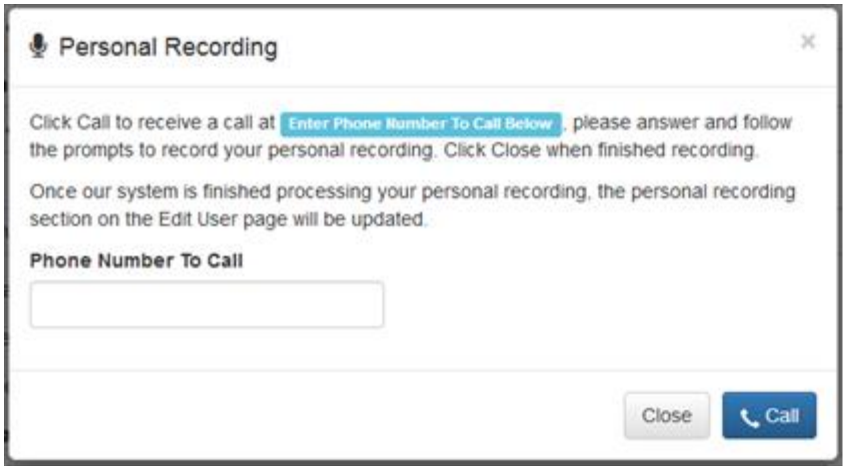
- **Configurations Table:**
  - Enter a value for the **OutcallPrefix** setting for dialing a PSTN number. The default is '9'.
  - Enter a value for the **OutcallSuffix** setting, which will be added to the end of the phone number when making outbound calls. Typically, this will be @ followed by the 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.

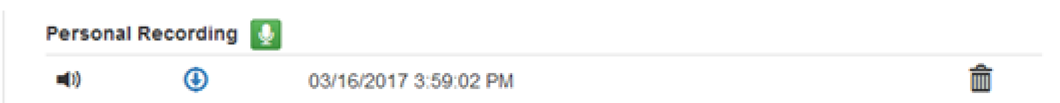
Once the SQL database changes have been made as described above, open the configuration for the user added in **Section 7.2** and scroll down to the **Personal Recording** section shown below and click on .

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.

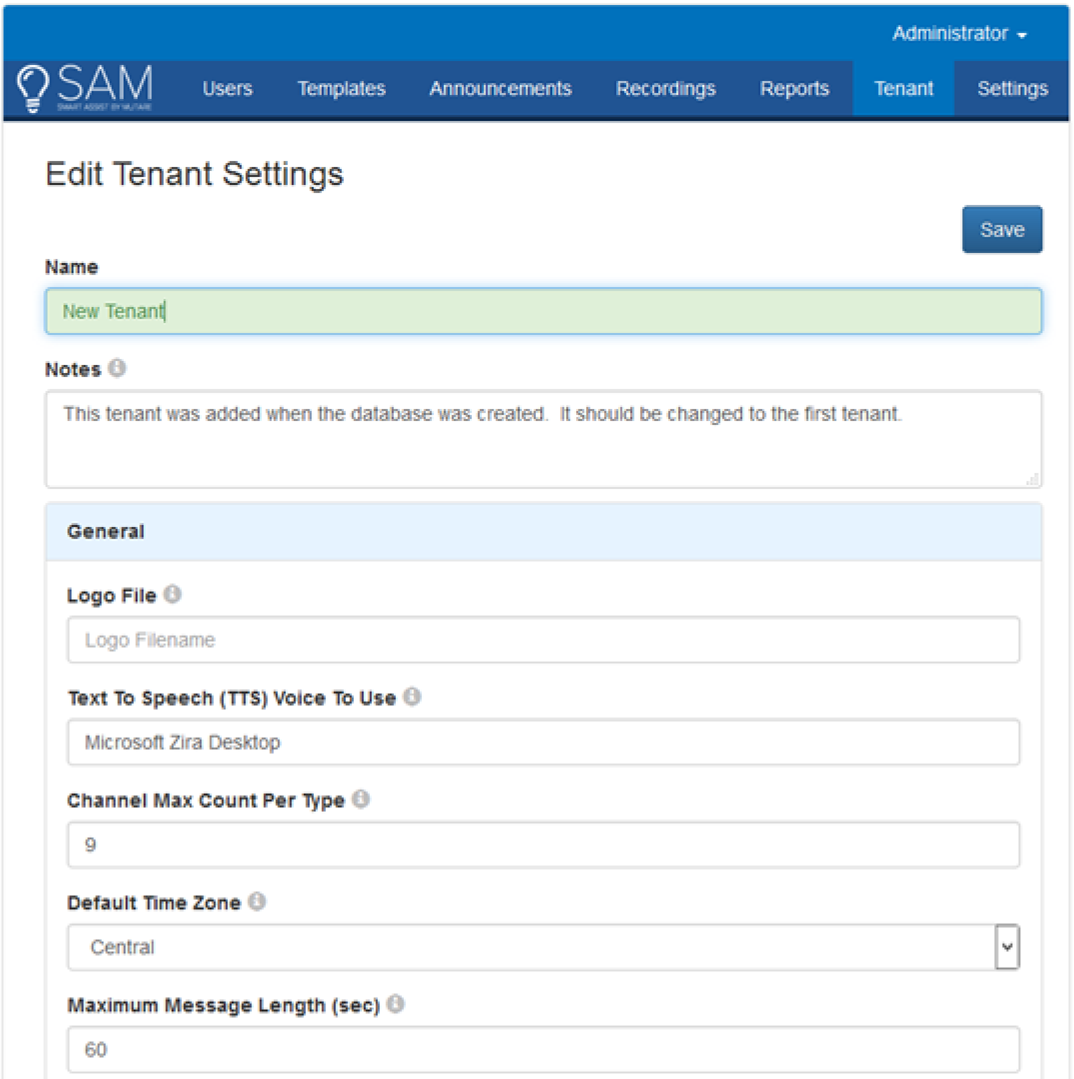


After the personal greeting has been recorded, the Personal Recording section for the SAM user will appear as follows. Once personal greeting can be maintained per user.



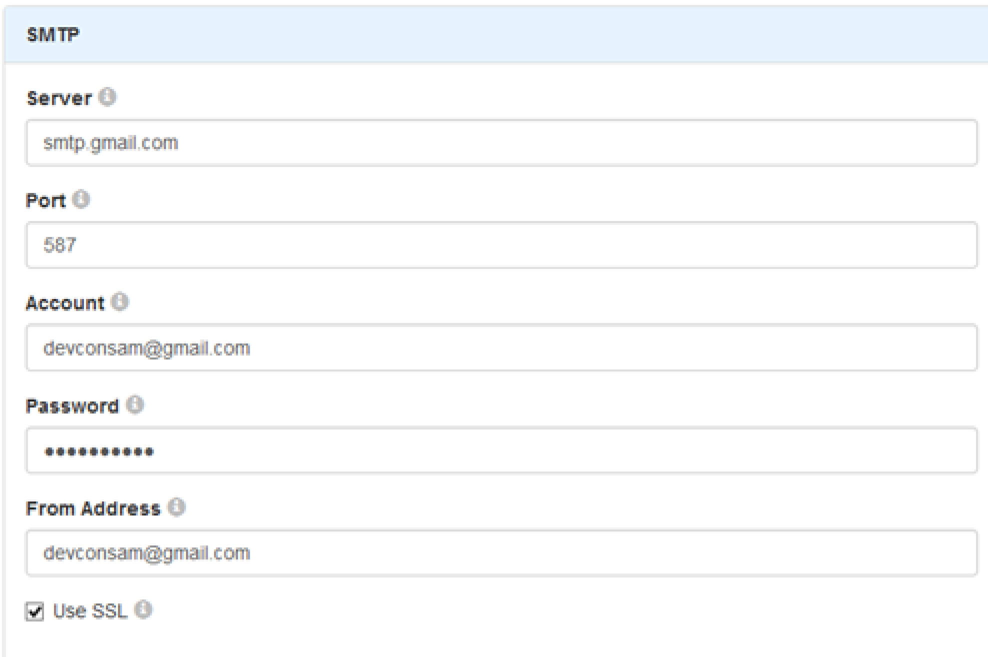
7.4 Configure SAM Tenant

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.

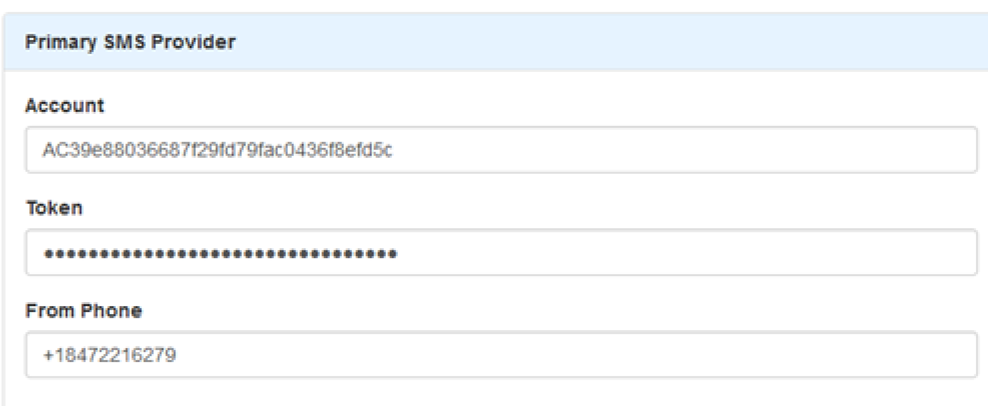


Scroll down to the **SMTP** section and configure the following fields:

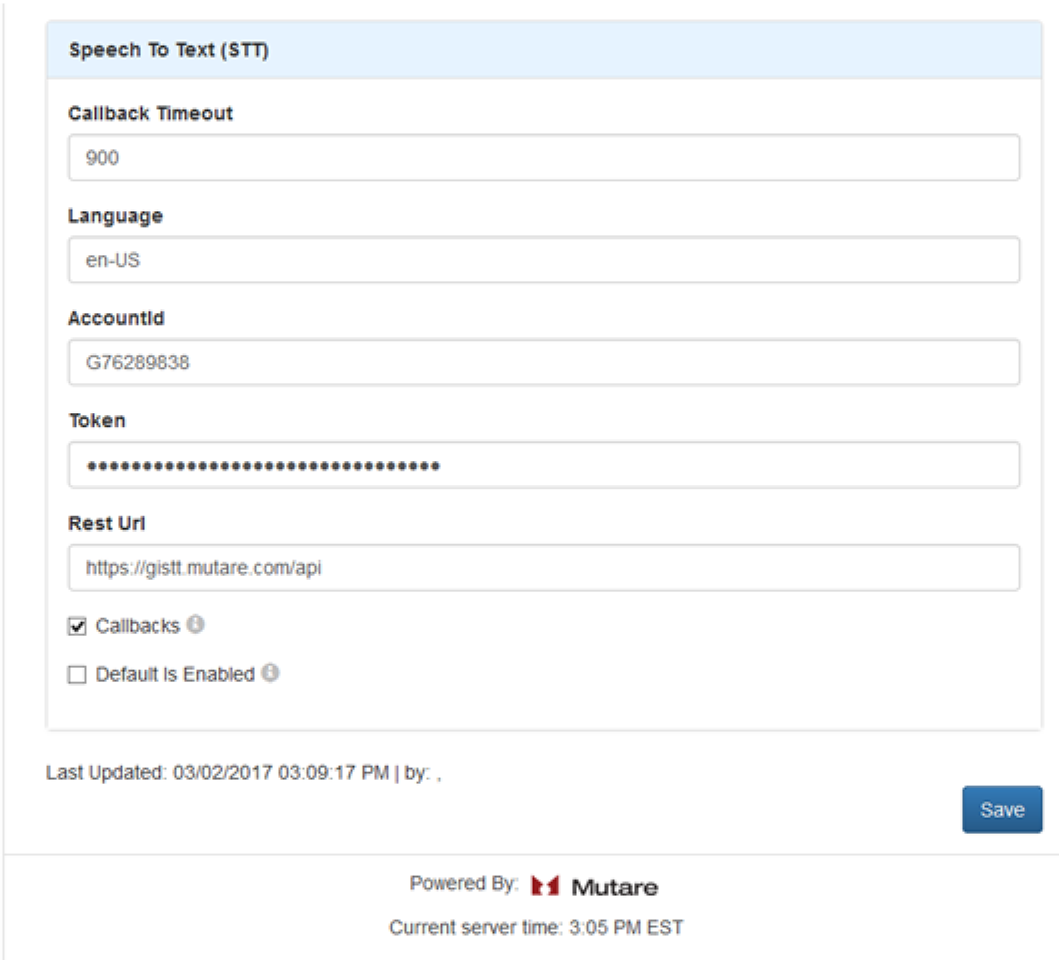
- **Server:** SMTP server to use for this tenant
- **Port:** SMTP port to use for this tenant
- **Account:** SMTP user account to authenticate with
- **Password:** SMTP user account password to authenticate this tenant
- **From Address:** SMTP from address. Should match the account SMS Provider
- **Use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



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.



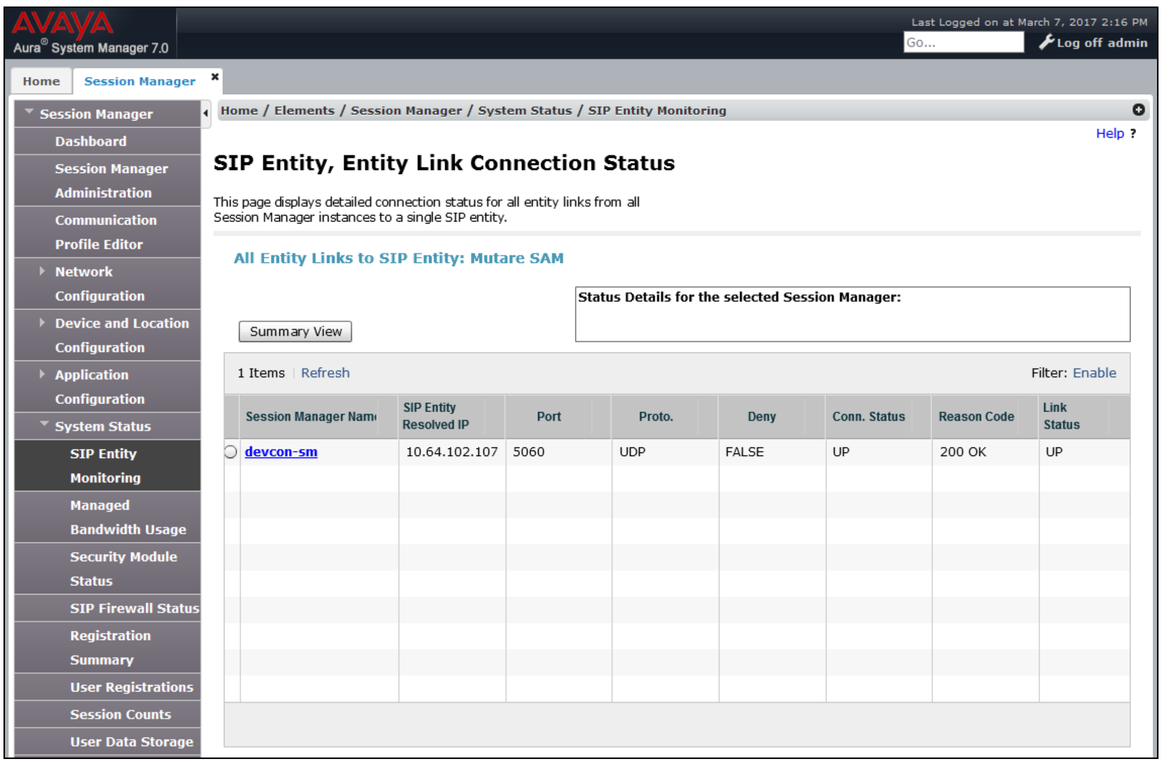
Scroll down to the **Speech to Text (STT)** section and configure the **Callback Timeout**, **Language**, **AccountId**, **Token**, and **Rest URL** fields as directed by the Mutare giSTT administrator. Click **Save**.



8 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 SAM 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 SAM indicating that the **Link Status** is *UP*.



2. Place a call to a SAM user and let the call cover to SAM. Leave a voice message for the SAM user.

3. Verify that an email and SMS text notification were left for the SAM user.

9 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**.

10 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] *Administering Avaya Aura® Messaging*, Release 6.3.2, Issue 2, March 2015.
[2] *Mutare SAM Admin Guide*, Last Updated: 1/31/2017, Release 1.2.0.

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