Avaya Solution & Interoperability Test Lab

Application Notes for Mobile Heartbeat Voice Gateway with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Mobile Heartbeat Voice Gateway 20.5.1 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Mobile Heartbeat Voice Gateway is a proxy/registrar for Mobile Heartbeat endpoints used for clinical communications in a healthcare environment. Mobile Heartbeat Voice Gateway connects to an Avaya Aura® Session Manager using a SIP trunk to route calls between the Avaya SIP network and Mobile Heartbeat endpoints.

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

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 Mobile Heartbeat Voice Gateway (MH-VGW) 20.5.1 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Mobile Heartbeat Voice Gateway is a proxy/registrar for Mobile Heartbeat endpoints used for clinical communications in a healthcare environment. Mobile Heartbeat Voice Gateway connects to an Avaya Aura® Session Manager using a SIP trunk to route calls between the Avaya SIP network and Mobile Heartbeat endpoints. For the compliance test, Mobile Heartbeat endpoints were smartphones running Mobile Heartbeat MH-CURE client, which registered with Mobile Heartbeat Voice Gateway as SIP endpoints.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between MH-CURE clients registered to MH-VGW, Avaya SIP / H.323 IP Deskphones, and the PSTN, and exercising telephony features, such as hold/resume, mute/unmute, call transfer, and 3-way conference.

The serviceability testing focused on verifying that MH-VGW came back into service after reconnecting the network connection or a reboot.

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 Mobile Heartbeat Voice Gateway did not include use of any specific encryption features as requested by Mobile Heartbeat.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between MH-VGW and Session Manager and verifying the exchange of SIP Options messages.
- Calls between MH-CURE clients registered to MH-VGW and Avaya H.323/SIP endpoints with Direct IP Media (Shuffling) enabled and disabled. Shuffling allows IP endpoints to send audio RTP packets directly to each other without using media resources on Avaya Media Gateway or Avaya Aura® Media Server.
- Support of G.711 mu-law codec.
- Basic telephony features, including hold/resume, mute/unmute, multiple calls, blind and attended transfer, and 3-way conference.
- Long duration PSTN calls and outbound calls from MH-VGW that were rejected due to dialing an invalid number or a busy endpoint.
- Proper system recovery after re-establishing network connectivity to MH-VGW or restarting MH-VGW server.

2.2. Test Results

All test cases passed with the following observations:

- When MH-VGW initiated a blind transfer, ringback tone was not heard while the transferred-to party was ringing.
- All MH-VGW calls were routed through Session Manager and Communication Manager.
- Although compliance testing took place with Direct IP-IP Audio Connections (shuffling) enabled, and no issues were encountered, Mobile Heartbeat recommends that it be disabled if audio quality issues are encountered. Shuffling may be disabled in the IP Network Region in **Section 5.2** or in the Signaling Group in **Section 5.4**.
- With shuffling enabled, Avaya Media Gateway and Avaya Media server resources were released. MH-Cure initiated calls routed audio through MH-VGW as opposed to MH-Cure endpoints during compliance tests. MH-VGW can be configured to route audio directly to MH-CURE endpoints. See **Section 7**.
- If an outgoing call from an MH-CURE client doesn't complete for any reason (e.g., invalid number, busy, or call blocked), related tones are not played; the call simply disappears on the client. For an invalid number, "All circuits are busy now, please try again later" is echoed to the caller.

2.3. Support

For Mobile Heartbeat Voice Gateway technical support, contact Mobile Heartbeat technical support via phone or website.

- **Phone:** 1 (781) 238-0000
- **Web:** https://www.mobileheartbeat.com/contact-us/

3. Reference Configuration

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

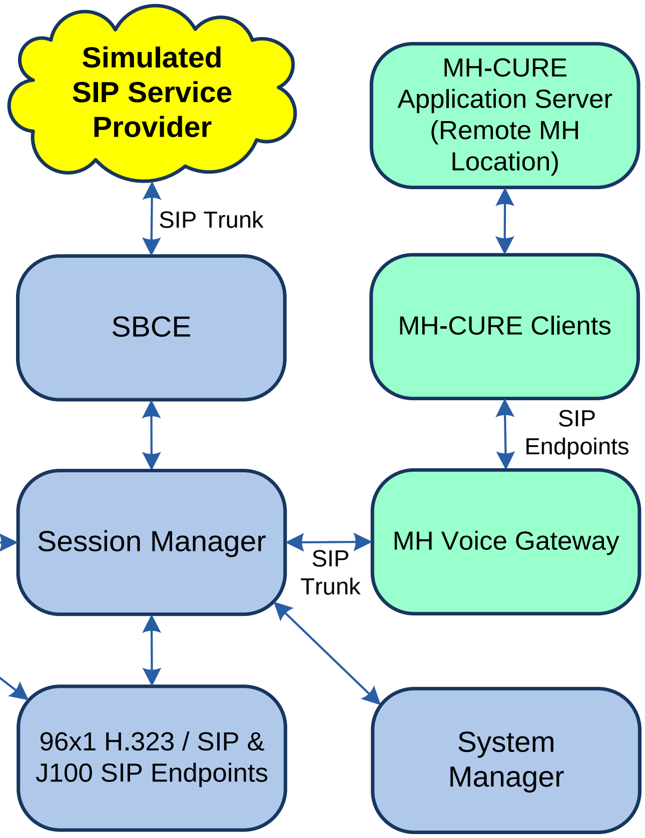


Figure 1: Avaya SIP Network with Mobile Heartbeat Voice Gateway

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 running on Virtualized Environment	10.1.0.2-SP2 01.0.974.0-27607
Avaya G450 Media Gateway	42.7.0
Avaya Aura® Media Server running on Virtualized Environment	10.1.0.101
Avaya Aura® System Manager running on Virtualized Environment	10.1.0.2 Service Pack 2 10.1.0.2.0715160
Avaya Aura® Session Manager running on Virtualized Environment	10.1.0.2 Service Pack 2 10.1.0.02.1010215
Avaya Session Border Controller for Enterprise running on Virtualized Environment	10.1.0.0-32-21432
Avaya 9641G IP Deskphone	6.8.5.3.2 (H.323)
Avaya J179 IP Phone	4.0.13.0.6 (SIP)
MH-CURE Client running on iOS 15.7.1 Smartphone	20.5.2.12
MH-CURE Application Server running on Windows Server 2016	20.5.1.3
Mobile Heartbeat Voice Gateway	3.4.0.20190211

5. Configure Avaya Aura® Communication Manager

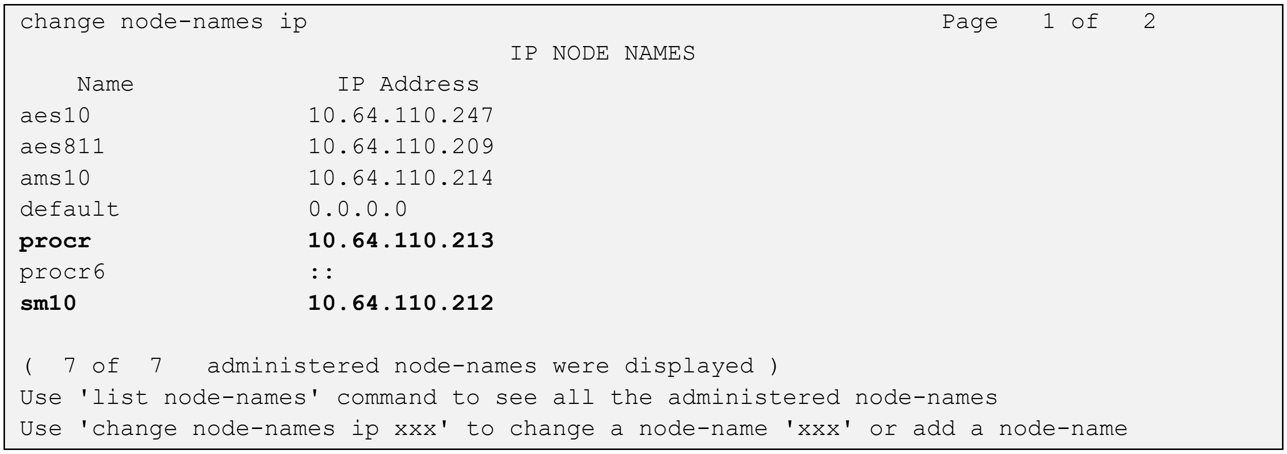
This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer SIP Trunk Group to Session Manager
- Administer AAR Call Routing

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

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 (*sm10*). These 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
aes10               10.64.110.247
aes811              10.64.110.209
ams10               10.64.110.214
default             0.0.0.0
procr               10.64.110.213
procr6              ::
sm10                10.64.110.212

(  7 of  7   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2. Administer IP Network Region

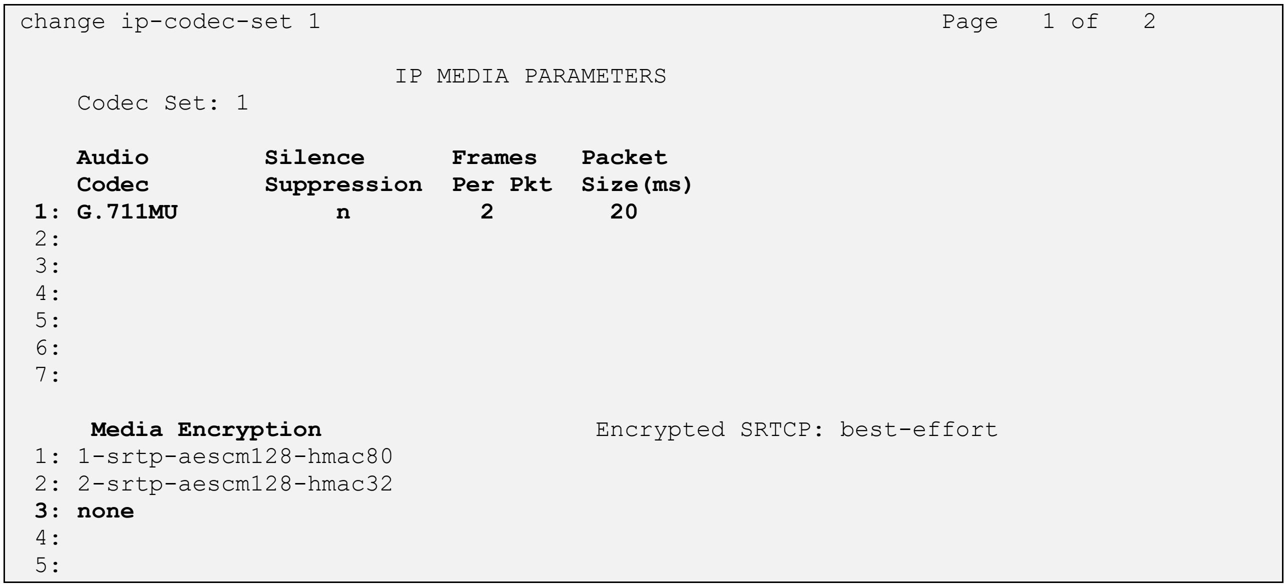
In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in Avaya G450 Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. The UDP port range is also specified in this form.

Note: If media resources are required to maintain call quality, shuffling may be disabled in the IP Network Region in **Section 5.2** or Signaling Group form in **Section 5.4**. For this solution, all MH-VGW calls are routed through Communication Manager.

```
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: yes
      Codec Set: 1           Inter-region IP-IP Direct Audio: yes
   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
```

5.3. Administer IP Codec Set

In the **IP Codec Set** form, the audio codec type supported for calls routed over the SIP trunk to MH-VGW is specified. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set 1 was specified in IP Network Region 1 shown in **Section 5.2**. The default settings of the **IP Codec Set** form are shown below. MH-VGW supports the G.711 codec. In the **Media Encryption** section, *none* should be specified to allow RTP, which is supported by MH-VGW.



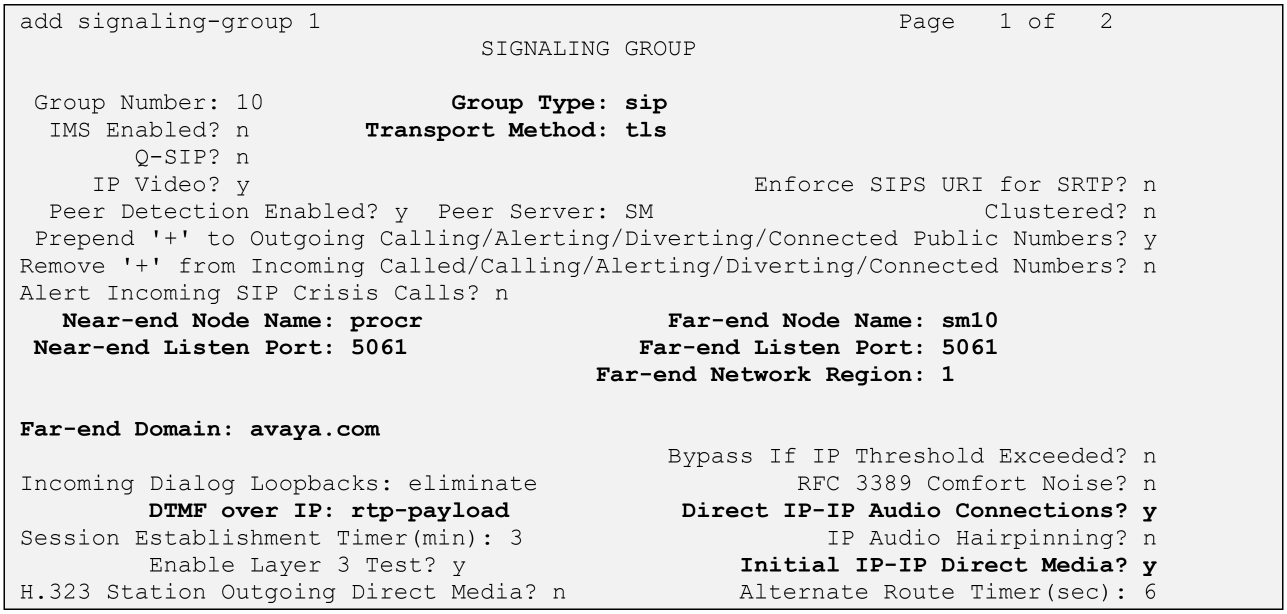
```
change ip-codec-set 1                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

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

     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
 4:
 5:
```

5.4. Administer SIP Trunk Group 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*.
- Set the **Enforce SIPS URI for SRTP** field to *n*.
- Specify Communication Manager (*procr*) and the Session Manager (*sm10*) 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 **Direct IP-IP Audio Connections** field was enabled on this form.
  Note: If media resources are required to maintain call quality, shuffling may also be disabled in the IP Network Region in **Section 5.2** or Signaling Group in **Section 5.4**. For this solution, all MH-VGW calls are routed through Communication Manager.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Enable **Initial IP-IP Direct Media**.

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



```
add signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y                                   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: sm10
 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? y
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/from MH-VGW, Avaya SIP Deskphones, and the PSTN. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie* or *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. Configure the fields in bold and accept the default values for the remaining fields.

```
add trunk-group 1                                            Page   1 of  22
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SM Trunk 1                  COR: 1        TN: 1        TAC: 1010
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

Page 5 of the SIP trunk group was configured as follows.

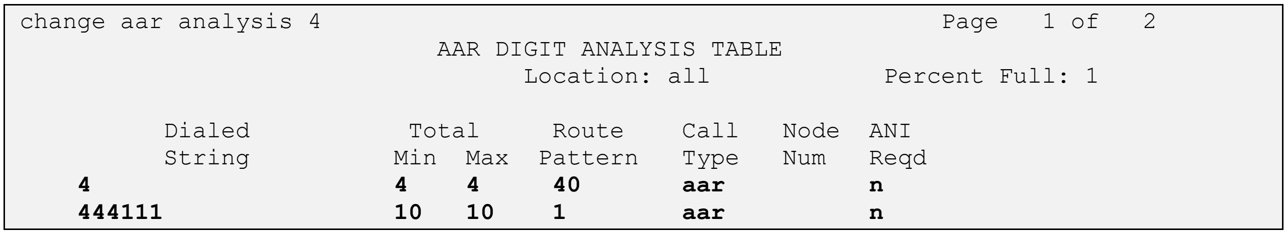
```
change trunk-group 1                                         Page   5 of   5
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? 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 AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. The MH-Clients were assigned extensions 4001 through 4003. In addition, these extensions also mapped to the following 10-digit numbers, 4441114001 through 4441114003, respectively. Therefore, AAR was configured to allow dialing the 4-digit extension or 10-digit number.

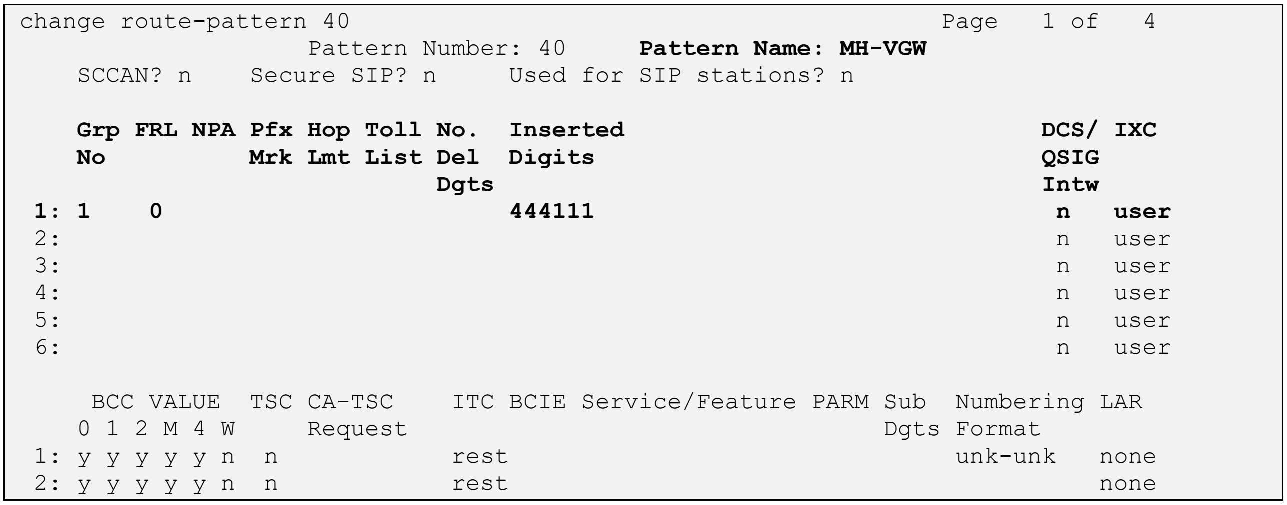
Configure the AAR analysis form and add an entry that routes 4-digit numbers beginning with “4” to route pattern 40 as shown below, which will prepend 444111 to complete the 10-digit number. Add a second entry that routes 10-digit number beginning with “444111” to route pattern 1, which performs no digit manipulation.

Note: 4-digit extensions beginning with “4” were configured with a **Call Type** of *aar* in the Dial Plan Analysis form. This allowed this dial string to be routed via AAR without using a Feature Access Code (FAC).



```
change aar analysis 4                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    4                     4    4     40       aar          n
    444111                10   10    1        aar          n
```

Configure a preference in **Route Pattern** 40 to route calls over SIP trunk group 1 as shown below. This route pattern prepends 444111 to convert the 4-digit extension to a 10-digit number.



```
change route-pattern 40                                         Page   1 of   4
                    Pattern Number: 40     Pattern Name: MH-VGW
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                               DCS/ IXC
    No          Mrk Lmt List Del  Digits                                 QSIG
                             Dgts                                        Intw
 1: 1    0                        444111                                  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
```

Configure a preference in **Route Pattern** 1 to route calls over SIP trunk group 1 as shown below.

```
change route-pattern 1                                          Page   1 of   4
                    Pattern Number: 1      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: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
```

Incoming calls from the PSTN to MH-VGW use DID numbers in the format of 1 + 10-digit number (e.g., 14441114001). The Incoming Call Handling Table for trunk group 10 is used to delete the leading 7 digits to convert the 11-digit number to a 4-digit extension (e.g., 4001). This extension is then routed via AAR as described above. The Incoming Call Handling Table for trunk group 1 appears as follows.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 Tie               11 14441114         7
```

6. Configure Avaya Aura® Session Manager

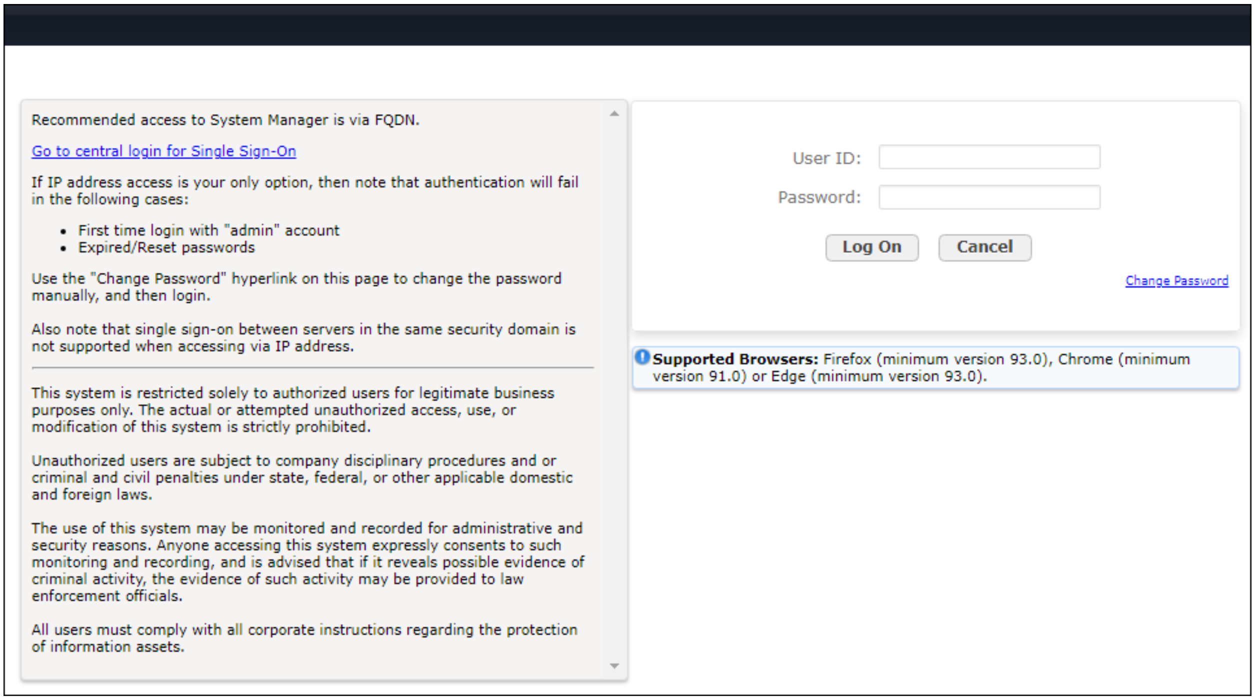
This section provides the procedure for configuring Session Manager to establish a SIP trunk to MH-VGW and to route calls. The procedures include the following areas:

- Launch System Manager
- Administer SIP Entities for Session Manager and MH-VGW
- Administer Entity Link between Session Manager and MH-VGW
- Add Routing Policy
- Add Dial Pattern
- Enable Monitoring on Session Manager

Note: It is assumed that basic configuration of Session Manager has already been performed.

6.1. Launch System Manager

Access the System Manager Web interface by using the URL *https://<ip-address>* in an Internet browser window, where *<ip-address>* is the IP address of the System Manager server. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

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

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

Administer SIP Entities

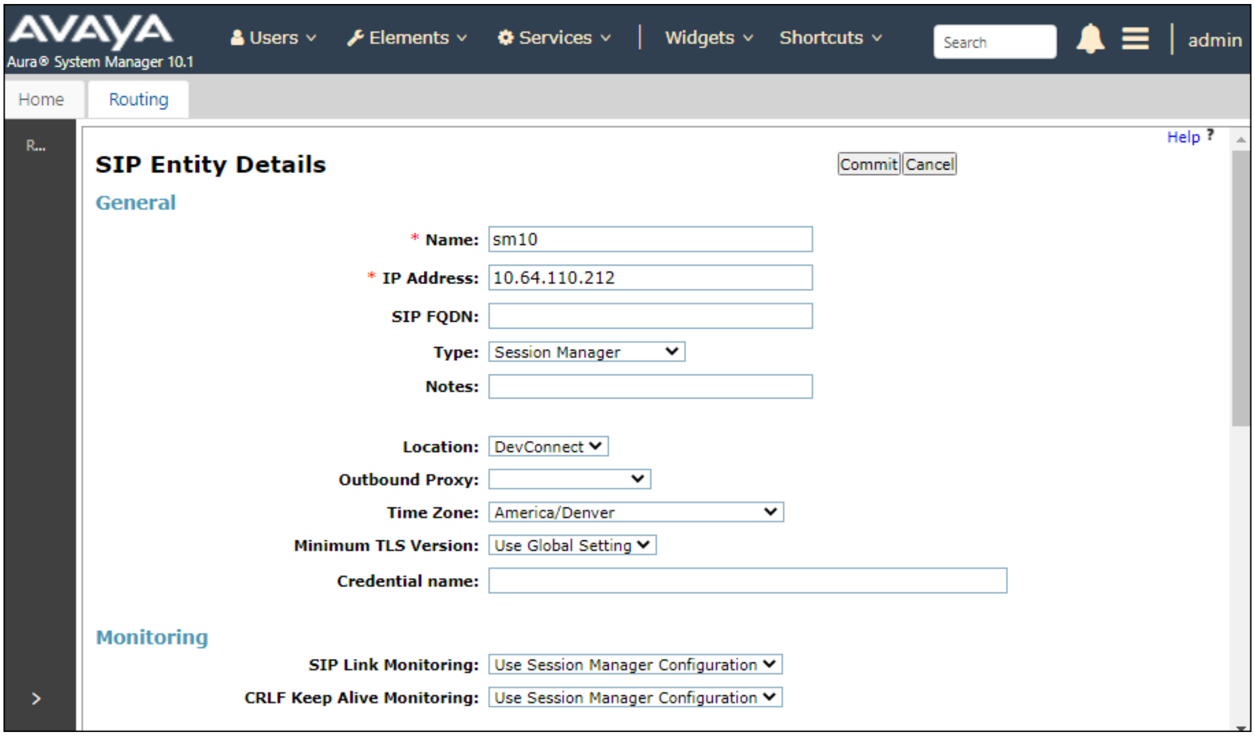
This section covers the configuration of SIP Entities for Session Manager and MH-VGW.

6.1.1. Avaya Aura® Session Manager

From the System Manager **Home** screen, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.



SIP Entity Details

General

* Name: sm10
* IP Address: 10.64.110.212
SIP FQDN:
Type: Session Manager
Notes:
Location: DevConnect
Outbound Proxy:
Time Zone: America/Denver
Minimum TLS Version: Use Global Setting
Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration
CRLF Keep Alive Monitoring: Use Session Manager Configuration

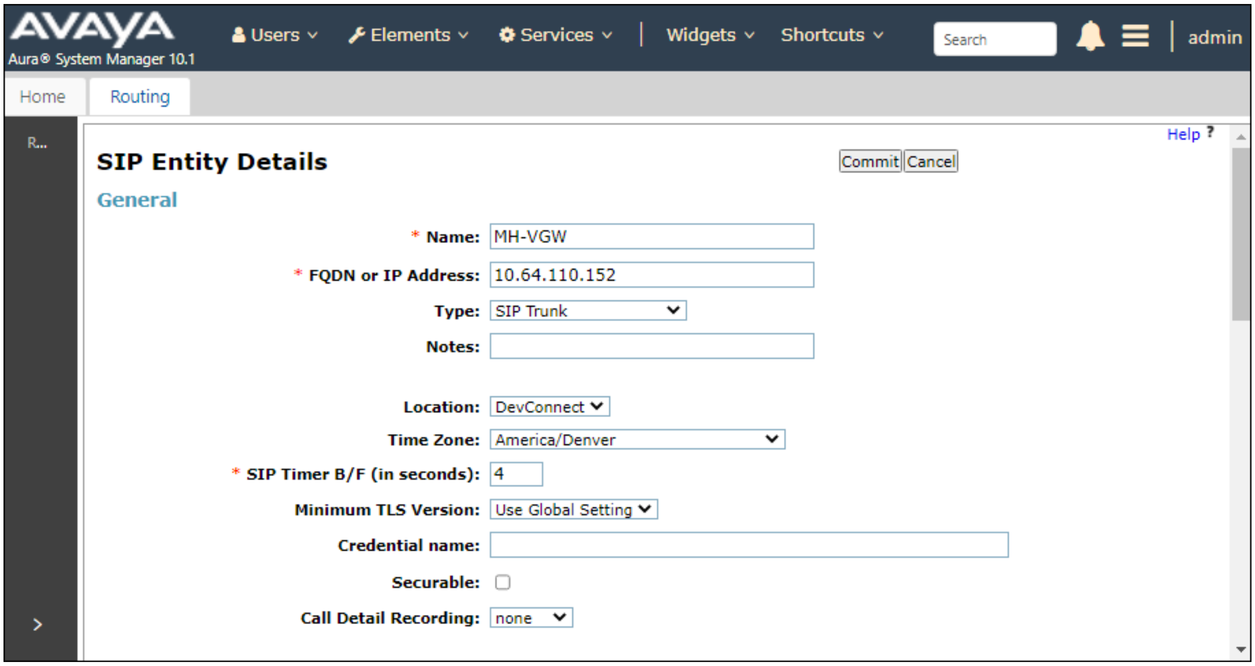
6.1.2. Mobile Heartbeat Voice Gateway

A SIP Entity must be added for MH-VGW. To add a SIP Entity, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

Name:	A descriptive name.
FQDN or IP Address:	MH-VGW IP address.
Type:	Select *SIP Trunk*.
Location:	Select one of the locations previously defined.
Time Zone:	Time zone for this location.

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



SIP Entity Details

General

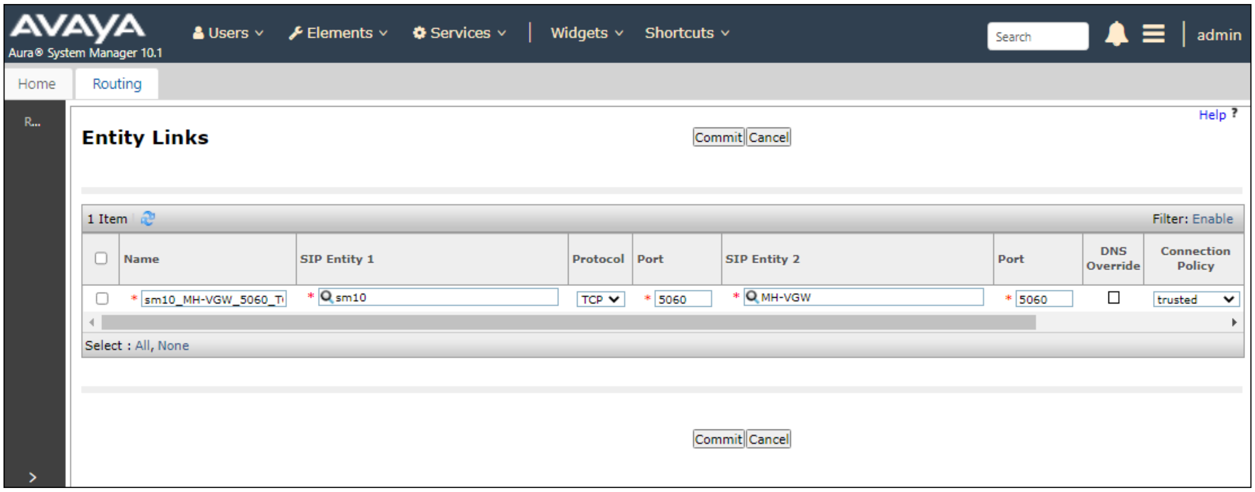
* Name:	MH-VGW
* FQDN or IP Address:	10.64.110.152
Type:	SIP Trunk
Notes:	
Location:	DevConnect
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	none

6.2. Administer Entity Link between Session Manager and MH-VGW

The SIP trunk between Session Manager and MH-VGW 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., *sm10_MH-VGW_5060_TCP_IPv4*).
- **SIP Entity 1:** Select the Session Manager SIP entity.
- **Protocol:** Select TCP transport protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the *MH-VGW* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in* ***Section 6.1*** *will be denied.*

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



Entity Links

1 Item

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
☐	* sm10_MH-VGW_5060_T	* sm10	TCP	* 5060	* MH-VGW	* 5060	☐	trusted

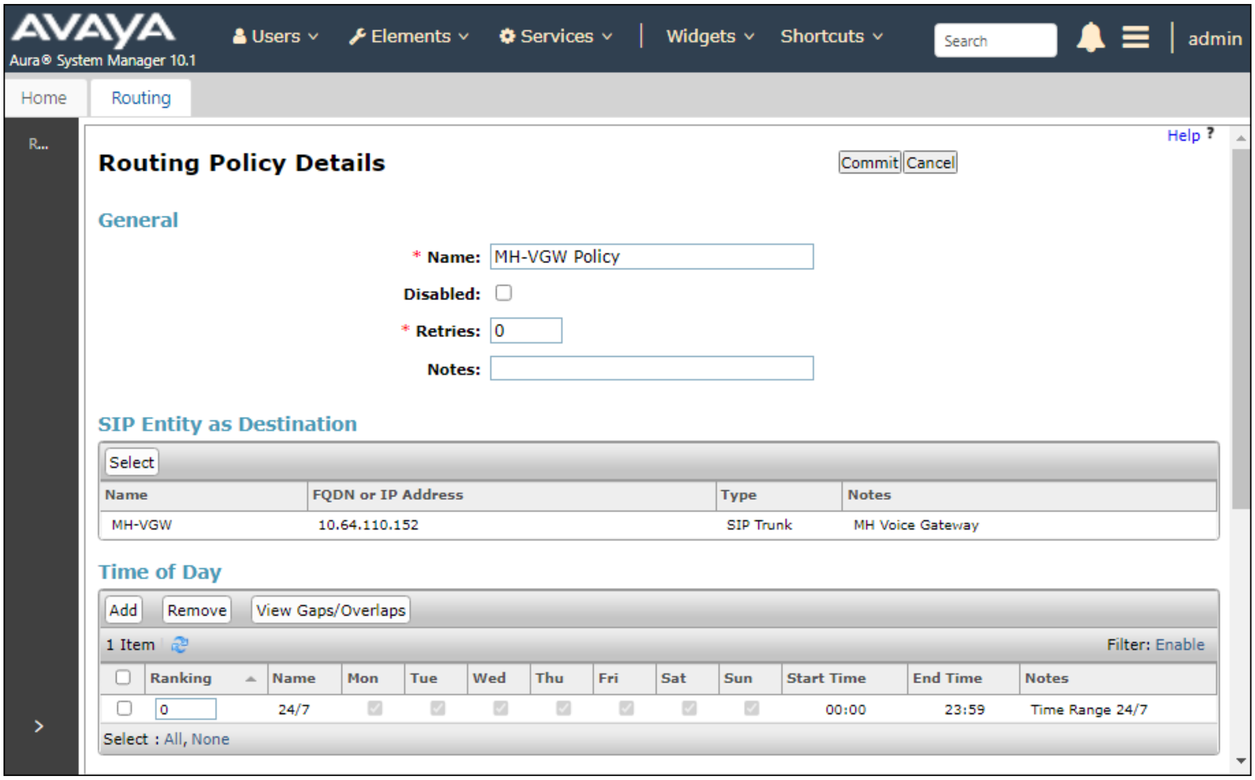
6.3. Add Routing Policy

A routing policy describes the conditions under which calls will be routed to the MH-VGW SIP entity. To add a routing policy, navigate to **Elements → Routing → Routing Policies** and click on the **New** button (not shown). 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 each Routing Policy definition. The following screen shows the Routing Policy for MH-VGW.



Routing Policy Details

General

* Name: MH-VGW Policy

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
MH-VGW	10.64.110.152	SIP Trunk	MH Voice Gateway

Time of Day

1 Item

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

6.4. Add Dial Pattern

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, three Dial Patterns were used for routing calls from local endpoints to MH-VGW, from the PSTN to MH-VGW, and from MH-VGW to the PSTN. For local calls, Communication Manager will send the corresponding 10-digit number (e.g., 4441114001) assigned to MH_CURE clients to Session Manager, which in turn will route the call to MH-VGW. For incoming PSTN calls, 11-digit numbers (e.g., 14441114001) will be received from the PSTN and routed through Communication Manager before terminating on MH-VGW. For MH-VGW calls to the PSTN, the ARS access code (e.g., 9) will dialed first, followed by 1 + 10-digits number assigned to MH-CURE clients. PSTN calls are routed through Communication Manager.

To add a dial pattern, navigate to **Elements → Routing → Dial Patterns** and click on the **New** button (not shown). Fill in the following:

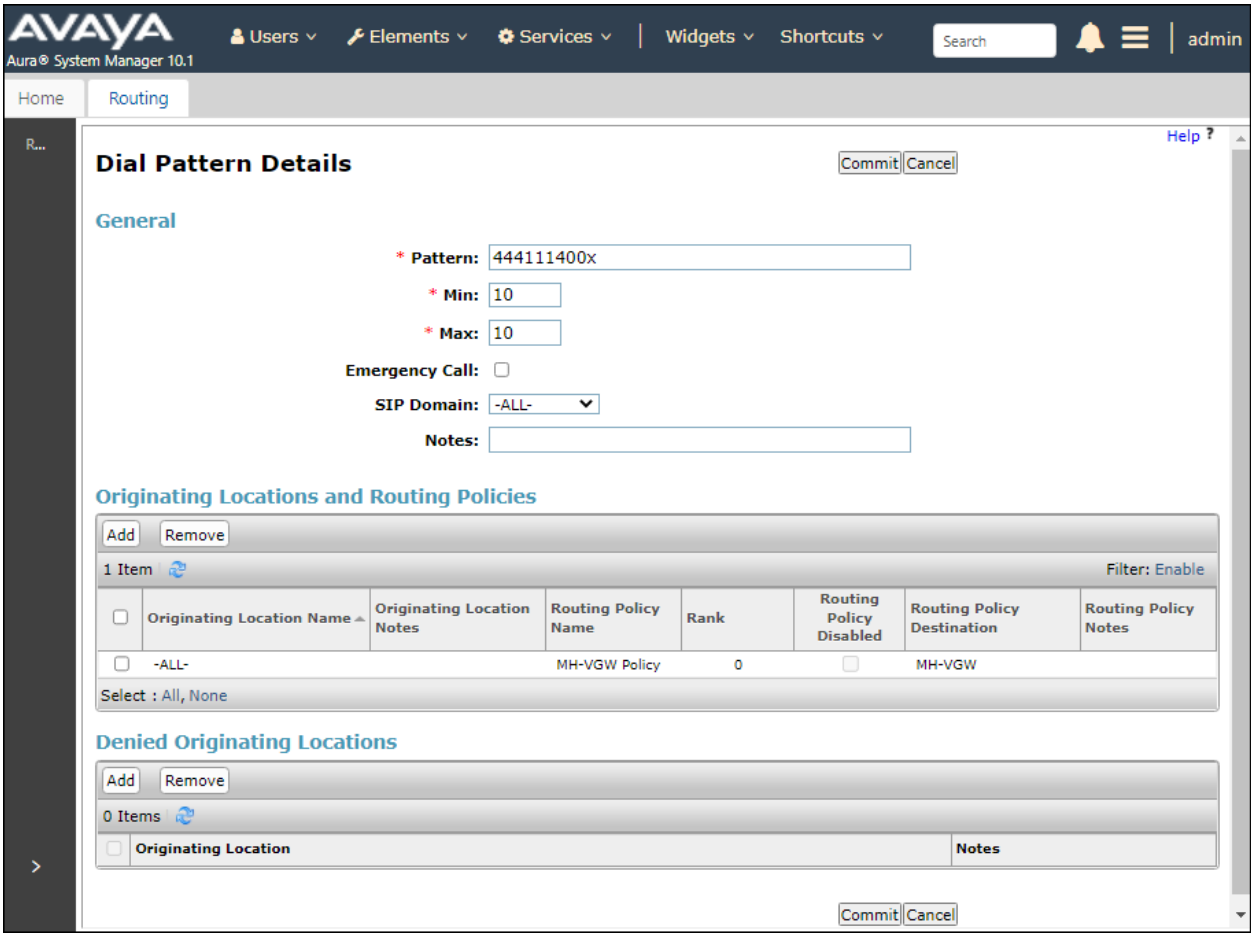
Under *General*:

- **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 local calls to MH-VGW.



Dial Pattern Details

General

* Pattern:	444111400x
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

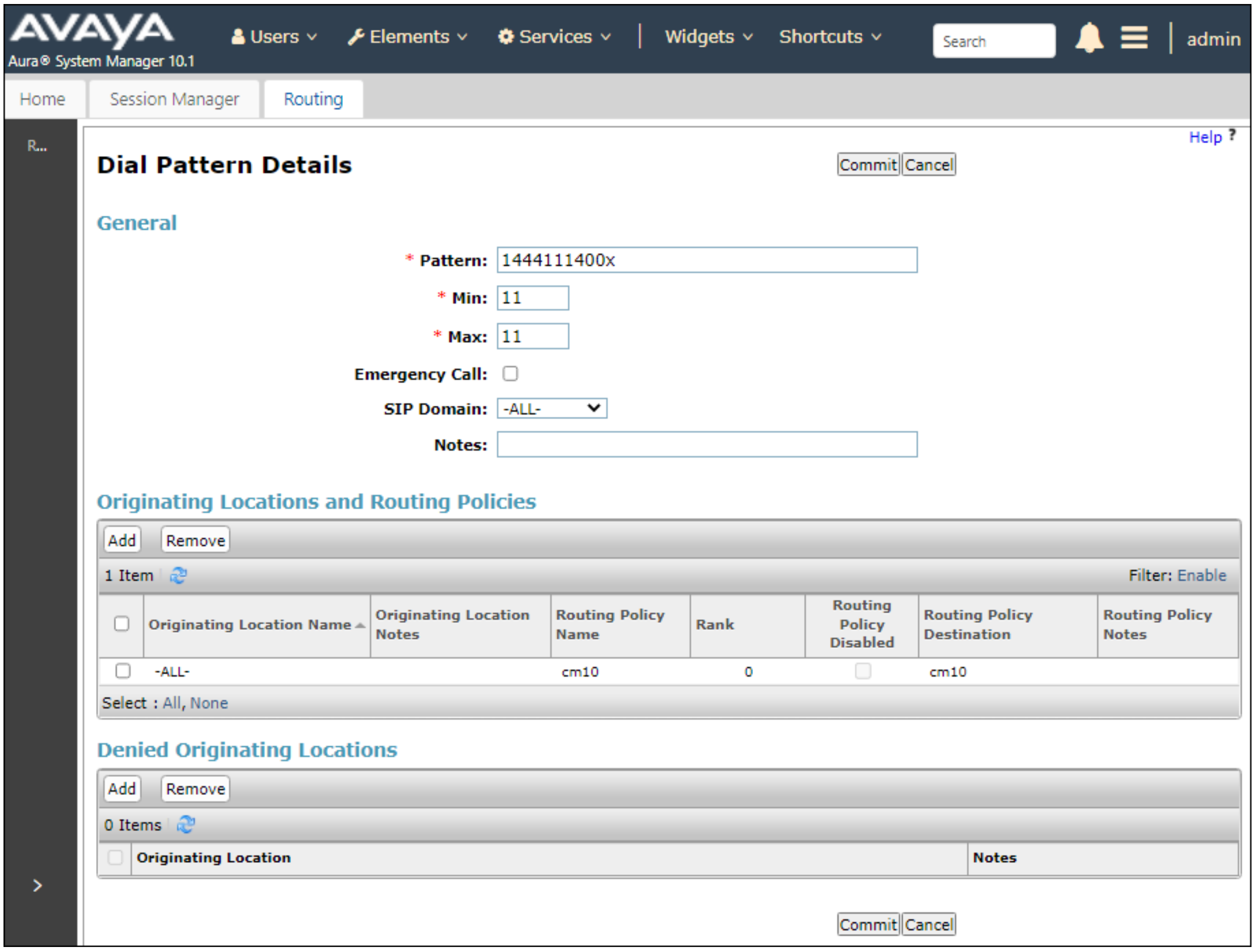
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		MH-VGW Policy	0	□	MH-VGW	

Select : All, None

Denied Originating Locations

□	Originating Location	Notes

The following screen shows the dial pattern definition for routing PSTN calls to MH-VGW. This call is routed as follows: PSTN → SBCE → Session Manager → Communication Manager → Session Manager → MH-VGW.



Dial Pattern Details

Commit Cancel

General

* Pattern:	1444111400x
* Min:	11
* Max:	11
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		cm10	0	□	cm10	

Select : All, None

Denied Originating Locations

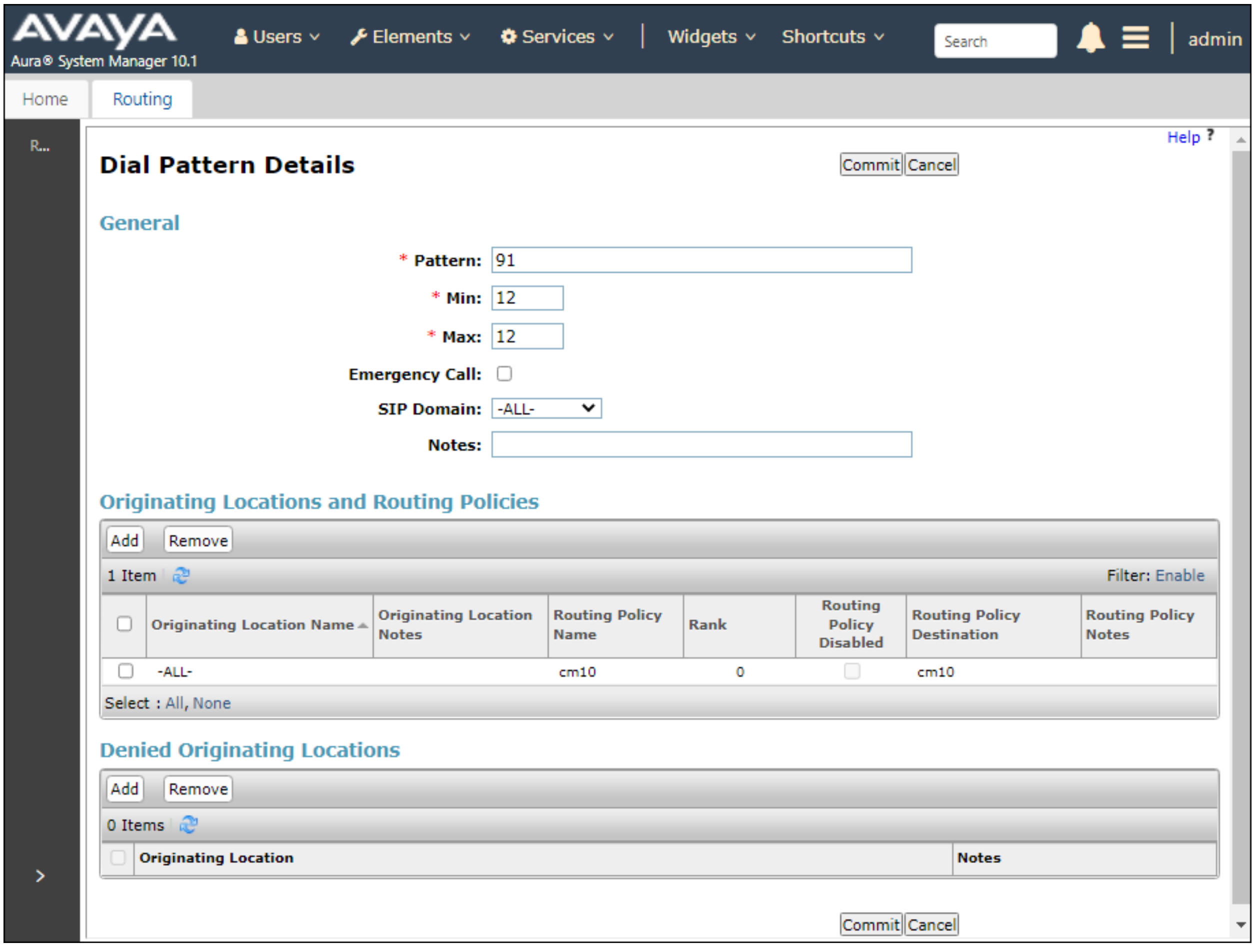
Add Remove

0 Items

□	Originating Location	Notes

Commit Cancel

The following screen shows the dial pattern definition for routing calls from MH-VGW to the PSTN. This call is routed as follows: MH-VGW → Session Manager → Communication Manager → Session Manager → SBCE → PSTN.



Dial Pattern Details

General

* Pattern:	91
* Min:	12
* Max:	12
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		cm10	0	□	cm10	

Select : All, None

Denied Originating Locations

Add Remove

0 Items

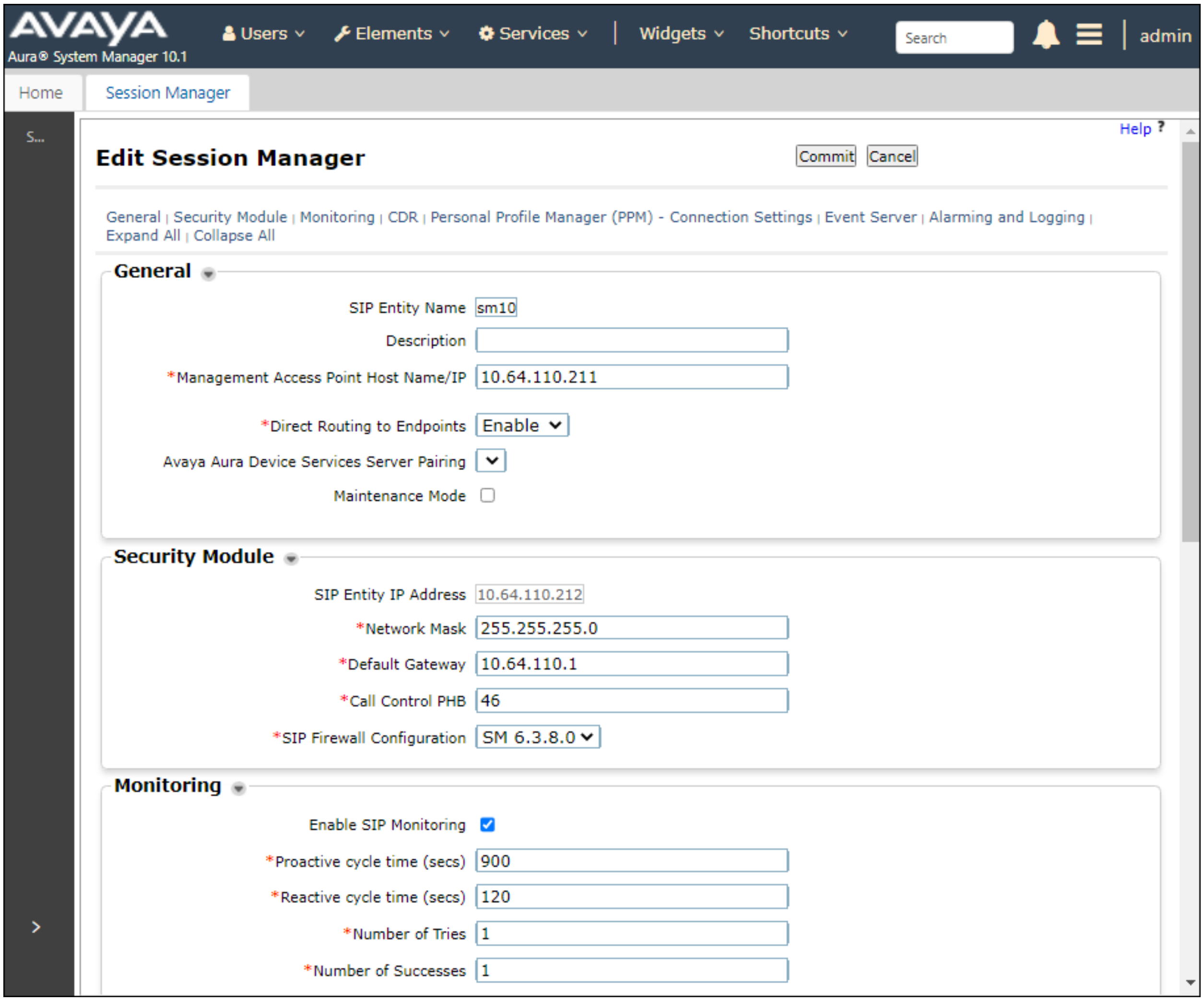
□	Originating Location	Notes

Commit Cancel

6.5. Enable Monitoring on Avaya Aura® Session Manager

Verify that monitoring is enabled for Session Manager. Navigate to **Elements → Session Manager → Session Manager Administration**, select the appropriate Session Manager and click **Edit** (not shown). This assumes that Session Manager has already been configured for System Manager.

Next, scroll down to the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to MH-VGW. Ensure that monitoring is enabled and 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 900 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.


AVAYA
Aura® System Manager 10.1
Users
Elements
Services
Widgets
Shortcuts
Search
admin
Home
Session Manager
S...
Help ?
Commit
Cancel
General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Alarming and Logging |
Expand All | Collapse All

Edit Session Manager

General

SIP Entity Name: sm10
Description:
*Management Access Point Host Name/IP: 10.64.110.211
*Direct Routing to Endpoints: Enable
Avaya Aura Device Services Server Pairing:
Maintenance Mode: □

Security Module

SIP Entity IP Address: 10.64.110.212
*Network Mask: 255.255.255.0
*Default Gateway: 10.64.110.1
*Call Control PHB: 46
*SIP Firewall Configuration: SM 6.3.8.0

Monitoring

Enable SIP Monitoring: ☑
*Proactive cycle time (secs): 900
*Reactive cycle time (secs): 120
*Number of Tries: 1
*Number of Successes: 1

7. Configure Mobile Heartbeat Voice Gateway

The configuration of MH-VGW is performed by Mobile Heartbeat. This section is provided for informational purposes. To configure the SIP trunk to Session Manager, the **pjsip_trunks.conf** file located in the **/etc/asterisk** directory in the MH-VGW server needs to be modified as shown below. Note that the SIP Domain and Session Manager IP address is specified here.

```
;
; Mobile Heartbeat(R) MH-CURE(tm) Voice Gateway configuration file
;
; This file was initially generated by default static configuration, it may be edited,
but be aware that
; future versions of Voice Gateway may overwrite it

; File pjsip_trunks.conf initialized Thu, 01 Dec 2022 12:15:35 -0500



; ####################################################################
;
;   Trunk to Hospital
;

;     EXAMPLES - adjust to fit - delete what is not needed etc
;                You must also adjust extensions_trunks.conf to match this
;                Especially routes and such


; ---------------------------------------------------------------------------
; do NOT edit any of this unless special trunk settings are needed - see further down
for actual trunk peer configs

[def-trunk-customer-1-ep](!)
type = endpoint

; By default we enable tcp for trunk, can be changed as needed
transport=transport-tcp-5060
;transport=transport-udp-5060

context=from-trunk-customer-1
send_rpid=yes
send_pai=yes
trust_id_inbound=yes
trust_id_outbound=yes
direct_media=yes
disallow=all
allow=ulaw
; allow=opus
from_domain=avaya.com

[def-trunk-customer-1-aor](!)
type=aor
qualify_frequency=60


; ---------------------------------------------------------------------------

; Here starts the actual trunks - endpoints need aor/contacts for outgoing and ident
for incoming
; so there has to be 3 entries per trunk peer, endpoint, aor, and identify
; REMEMBER to chang the IP address in two places per trunk - in the aor and the
identify


; === Trunk 1-0 ===

[trunk-customer-1-0](def-trunk-customer-1-ep)
aors=trunk-customer-1-0

[trunk-customer-1-0](def-trunk-customer-1-aor)
contact=sip:10.64.110.212:5060

[trunk-customer-1-0]
match=10.64.110.212
type=identify
endpoint=trunk-customer-1-0
```

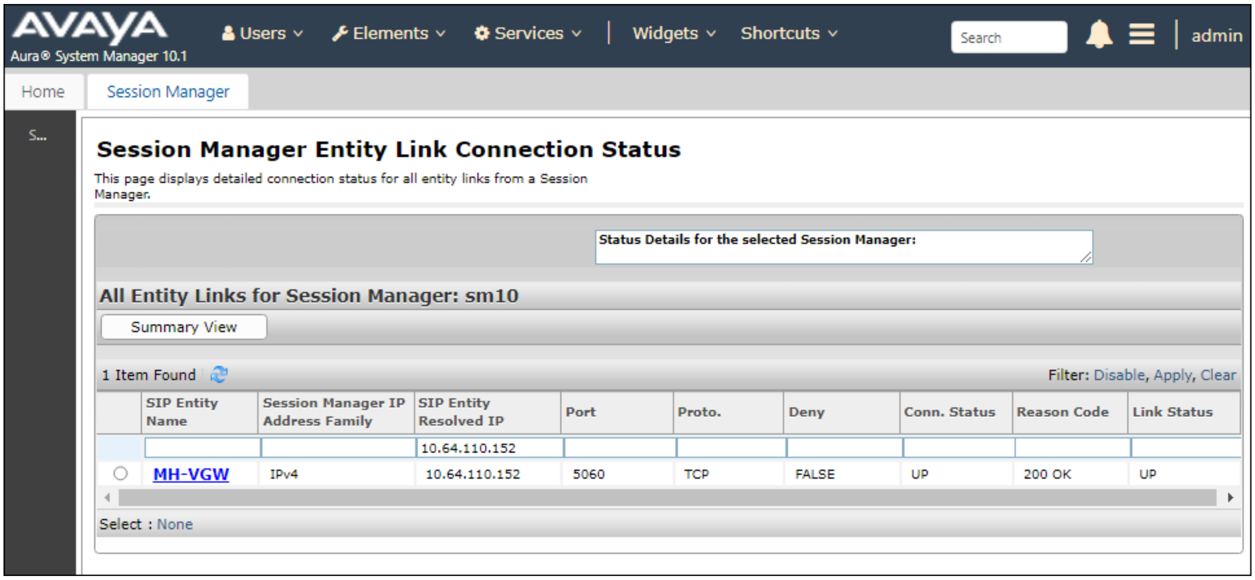
To configure audio path to terminate on MH-CURE endpoint, the **extensions_trunk.conf** file located in the **/etc/asterisk** directory in the MH-VGW server needs the following line in the [macro-dial-trunk] subsection as shown below.

```
[macro-dial-trunk];

exten => s,1,Noop(MACRO_DIAL_TRUNK
${TRUNK_TYPE}/${MACRO_EXTEN}@${TRUNK_GROUP}${TRUNK_CURRENT} : cid ${CALLERID(all)})
  same => n,Dial(${TRUNK_TYPE}/${MACRO_EXTEN}@${TRUNK_GROUP}${TRUNK_CURRENT},60,r)
  same => n,Goto(s-${DIALSTATUS},1)
```

8. Verification Steps

This section provides the tests that may be performed to verify proper configuration of Mobile Heartbeat Voice Gateway with Session Manager and Communication Manager.

1. Verify that the SIP trunk between MH-VGW and Session Manager has been established successfully. In System Manager, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**, and then click on the MH-VGW entity (not shown) to check the Entity Link connection status.



Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: sm10

1 Item Found

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
			10.64.110.152						
○	MH-VGW	IPv4	10.64.110.152	5060	TCP	FALSE	UP	200 OK	UP

Select : None

2. Alternatively, the SIP trunk status may be viewed on MH-VGW via SSH using the **pjsip show contacts** command shown below. Note that the SIP trunk specified by the Session Manager IP address of 10.64.110.212 is *Avail*.

```
milton@avayavgw:/etc/asterisk$ sudo asterisk -rvvv
[sudo] password for milton:
Asterisk certified/13.18-cert3, Copyright (C) 1999 - 2014, Digium, Inc. and othe
rs.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk certified/13.18-cert3 currently running on avayavgw (pid =
1674)
avayavgw*CLI> pjsip show contacts

  Contact:  <Aor/ContactUri.............................> <Hash....> <Status> <
RTT(ms)..>
================================================================================
==========

  Contact:  mhsipcheck/sip:mhsipcheck@127.0.0.1:54650;tran 69115bd46c Unknown
nan
  Contact:  trunk-customer-1-0/sip:10.64.110.212:5060      37112a1513 Avail
13.738

Objects found: 2
```

3. Place incoming and outgoing calls to/from MH-VGW and verify the call is established successfully with two-way audio. Exercise telephony features, such as call transfer or conference. Terminate the call.

9. Conclusion

These Application Notes described the configuration steps required to integrate Mobile Heartbeat Voice Gateway 20.5.1 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Incoming and outgoing calls were placed to/from MH-CURE clients registered to Mobile Heartbeat Voice Gateway and telephony features were exercised. All feature and serviceability test cases were completed with observations as noted in **Section 2.2**.

10. References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 7, September 2022, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022, available at http://support.avaya.com.

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.