Avaya Solution & Interoperability Test Lab

Application Notes for Spok Care Connect Speech R1.9 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Session Manager 8.1 via SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Spok Care Connect Speech with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The solution used Avaya Aura® Session Manager to route calls between Avaya Aura® Communication Manager and Care Connect Speech. The overall objective of the interoperability compliance testing was to verify the basic telephony features, DTMF, speech recognition, and blind transfer with Spok Care Connect Speech with Avaya Aura® Communication Manager using a SIP trunk.

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 procedures to integrate the Spok Care Connect Speech (CCS) application with Avaya Aura® Communication Manager via a SIP trunk configured on Avaya Aura® Session Manager. Avaya Aura® Session Manager provides SIP trunking and network routing service to route calls between Avaya Aura ® Communication Manager and the Care Connect Speech server.

2. General Test Approach and Test Results

The general test approach was to verify test calls made from Avaya Aura® Communication Manager to Care Connect Speech to exercise basic features such as DTMF, speech recognition, and blind call transfer.

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 Session Manager and Connect Care Speech utilized enabled capabilities of TLS and SRTP encryption.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunks between Session Manager and Care Connect Speech server.
- Basic features on the speech server: DTMF, speech recognition and blind transfer.
- Basic telephony features on Communication Manager: hold and retrieve call, voice mail.
- Transfer calls off-net.
- Codecs: G.711A and G.711MU.
- Recovery from temporary network interruption

2.2. Test Results

The interoperability testing did not include:

- Codecs other than G.711 and any codec negotiation
- Attended transfer and conferencing as they are not supported

One observation noted is Care Connect Speech busy or invalid transferred to extensions did not drop the caller. Avaya does provide call busy information via NOTIFY SIP messages. Care Connect Speech call flow designs can provide appropriate behavior.

2.3. Support

Technical support for the Spok CCS Speech solution can be obtained by contacting Spok:

- URL – http://www.spok.com
- Phone – +1 (888) 797-7487

3. Reference Configuration

The diagram below illustrates a sample test configuration.

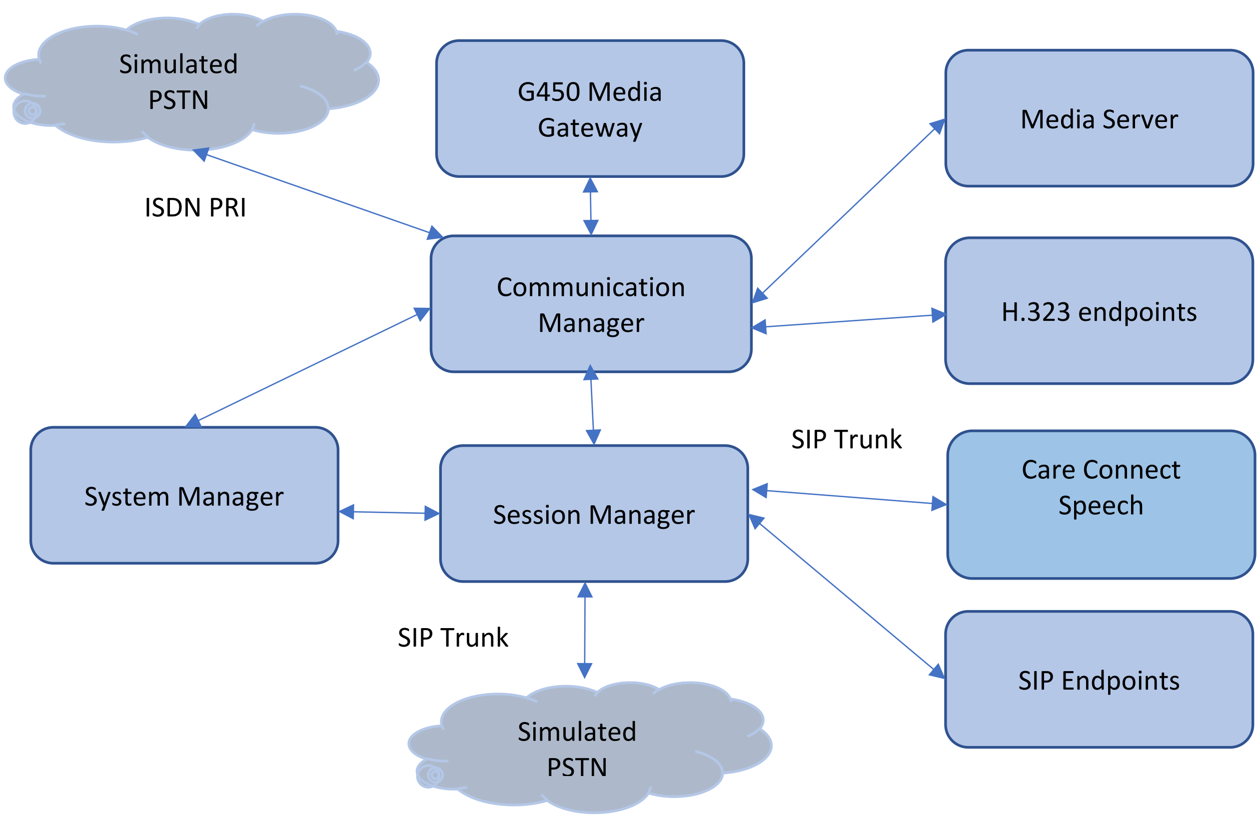


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the interoperability test:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.0.1.1.890.25763
Avaya Aura® Session Manager	8.1.0.0.811021
Avaya Media Gateway G450	41.24.0/2
Avaya Aura® Media Server	8.0.0.21
Avaya IP 96xx1series (H.323)	6.8.3
Avaya IP J100 series (SIP)	4.0.6.0
Spok Care Connect Speech	R1.9

5. Configure Avaya Aura® Communication Manager

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (Note: During Compliance Testing, all inputs not highlighted in **Bold** were left as Default)

- Verify License
- Configure IP Node Names
- Configure IP codec set
- Configure IP network region
- Configure SIP signaling group
- Configure SIP trunk group
- Configure route pattern
- Configure Dial Plan
- Configure Uniform Dial Plan
- Configure AAR analysis

5.1. Verify Avaya Aura® Communication Manager License

Use the "display system-parameters customer-options" command. Navigate to Page 2 and verify that there is sufficient remaining capacity for SIP trunks by comparing the Maximum Administered SIP Trunks field value with the corresponding value in the USED column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 2
                   Maximum Video Capable IP Softphones: 18000 19
                       Maximum Administered SIP Trunks: 12000 10
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```

5.2. Configure IP Node Names

Use the “change node-names ip” command and add an entry for Session Manager. In this case, **sm81** and **10.64.110.212** are entered as **Name** and **IP Address**, respectively. Note the **procr** and **10.64.110.213** entry, which is the node **Name** and **IP Address** for the processor board. These values will be used later to configure the signaling group **Section 5.5**.

```
change node-names ip                                            Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
aes81               10.64.110.215
ams81               10.64.110.214
procr               10.64.110.213
sm81                10.64.110.212
```

5.3. Configure IP Codec Set

Use the “change ip-codec-set n” command to update the audio codec types in the **Audio Codec** fields as necessary. Configure the codec as shown below. Note SRTP was specified as mentioned in **Section 2**.

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

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU       n         2        20
 2:
Media Encryption                   Encrypted SRTCP: best-effort
 1:1-srtp-aescm128-hmac80
 2:
 3:
 4:
 5:
```

5.4. Configure IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.5**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter the codec set number from **Section 5.3.**

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name: Main                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
```

5.5. Configure SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** “sip”.
- **Transport Method:** “tls”.
- **Near-end Node Name:** An existing C-LAN node name or “procr” from **Section 5.2**.
- **Far-end Node Name:** The existing node name for Session Manager from **Section 5.2**.
- **Near-end Listen Port:** An available port for integration with Session Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** The network region from **Section 5.4**.
- **Direct IP-IP Audio Connections?:** “y”
- **DTMF over IP:** “y” **RFC2833 for DTMF**

```
add signaling-group 1                                          Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority 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: sm81
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

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

5.6. Configure SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** “sip”.
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”.
- **Signaling Group:** The signaling group number from **Section 5.5**.
- **Number of Members:** The desired number of members, in this case “10”.

```
add trunk-group 1                                           Page   1 of   5
                                TRUNK GROUP

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: SM Trunk                    COR: 1        TN: 1        TAC: 101
   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
```

Navigate to **Page 3** and enter “private” for **Numbering Format**.

```
add trunk-group 1                                           Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: both
                                                         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: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

5.7. Configure Route Pattern

Use the "change route-pattern n" command, where "n" is an existing route pattern number to be used to reach Care Connect Speech, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format**: Set to "**lev0-pvt**".

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
 1: y y y y y n  n            rest                              lev0-pvt  none
```

5.8. Configure Dial Plan Analysis

This section provides sample Dial Plan Analysis used for routing calls with dialed digits 59994 to Connect Care Speech. Note that other methods of routing may be used. Use the "change dial plan analysis" command, and add an entry to specify use of UDP dial plan for routing of digit 59994. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

Dialed String: Dialed prefix digits to match on, in this case "59994"
Total Length: Length of the full dialed number, in this case "5"
Call Type: "udp"

```
change dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
 1             3   dac
 2             5   ext
 3             5   ext
 4             5   aar
 59994         5   udp
```

5.9. Configure Uniform Dial Plan

Use the "**change uniform-dialplan 0**" command and add an entry of 59994 and specify "**aar**" as the routing method in the **Net** column for this dial pattern. Note that other routing methods may be used.

```
change uniform-dialplan 0                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                   Insert               Node
  Pattern       Len Del      Digits     Net Conv Num
59994           5   0                  aar  n
```

5.10. Configure AAR Analysis

Use the "change aar analysis 0" command and add an entry to specify how to route calls to 59994. In the example shown below, calls with digits 59994 will be routed as an AAR call using route pattern "1" from **Section 5.7**.

```
change aar analysis 59994                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total      Route     Call   Node  ANI
          String         Min  Max   Pattern    Type   Num   Reqd
    59994                  5    5      1         aar          n
```

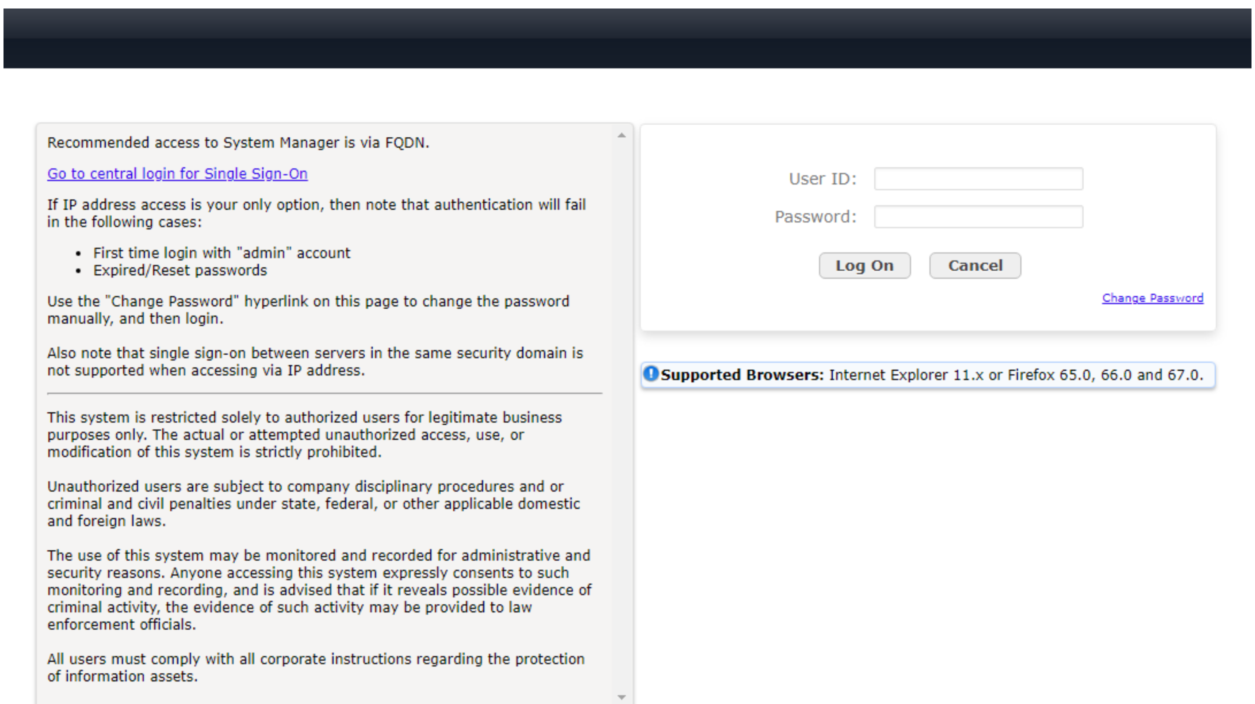
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Configure SIP Domain
- Configure Locations
- Configure SIP Entities
- Configure Entity Links
- Configure Routing Policy
- Configure Dial Patterns

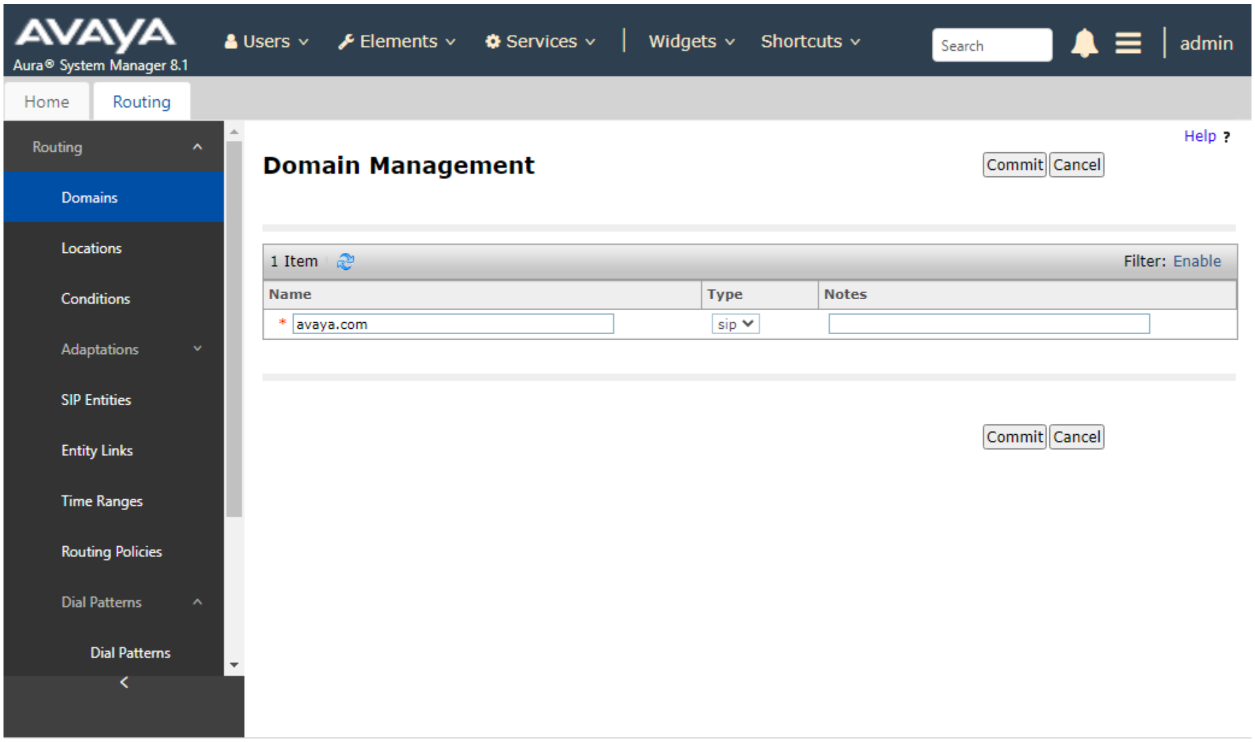
6.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address/SMGR" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



6.2. Configure SIP Domain

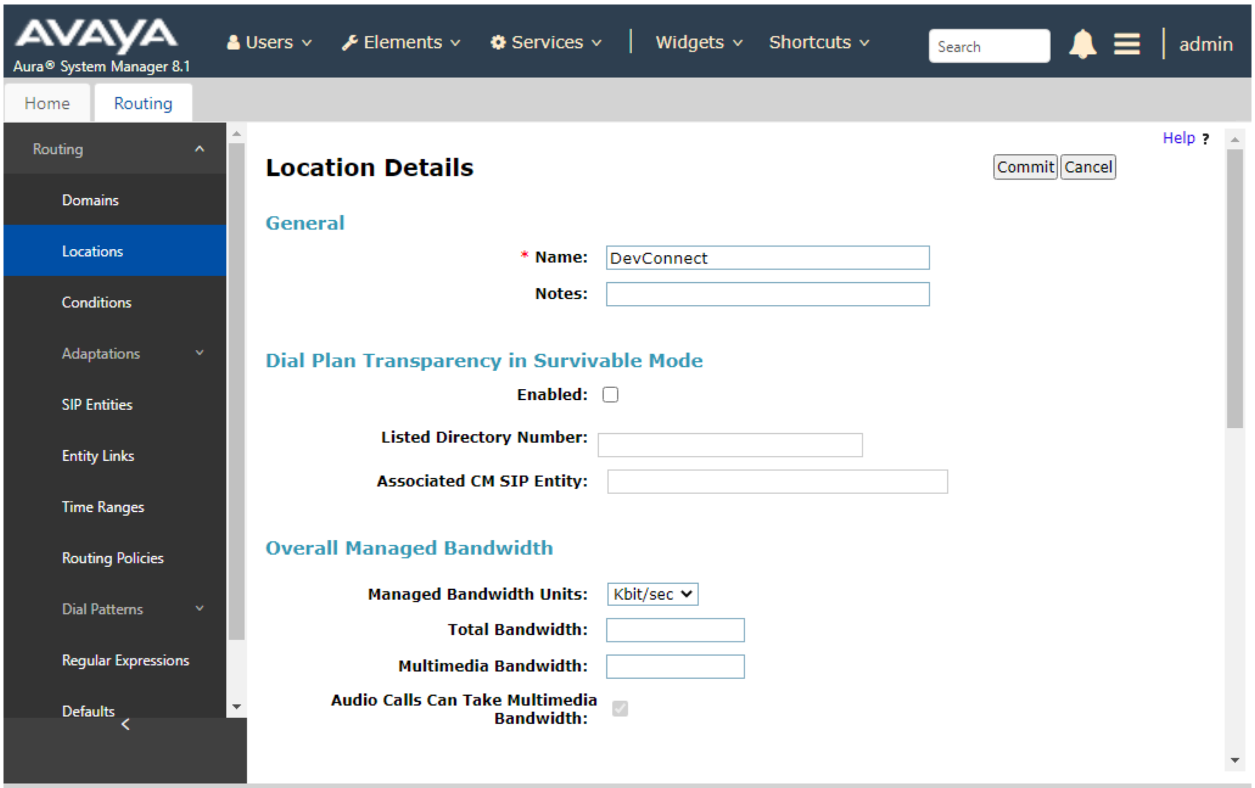
Select **Routing → Domains** from the left pane, and click **New** in the subsequent screen to add a new domain. The **Domain Management** screen is displayed. In the **Name** field, enter the domain name. Select "sip" from the **Type** drop down menu and provide any optional **Notes**.



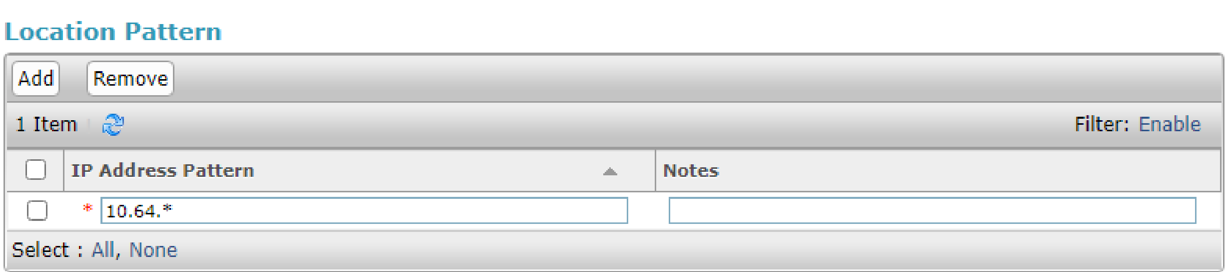
6.3. Configure Locations

Select **Routing → Locations** from the left pane and click **New** in the subsequent screen (not shown).

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.



Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.



6.4. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk. During the compliance test the following SIP Entities were configured:

- Session Manager
- Communication Manager
- Care Connect Speech

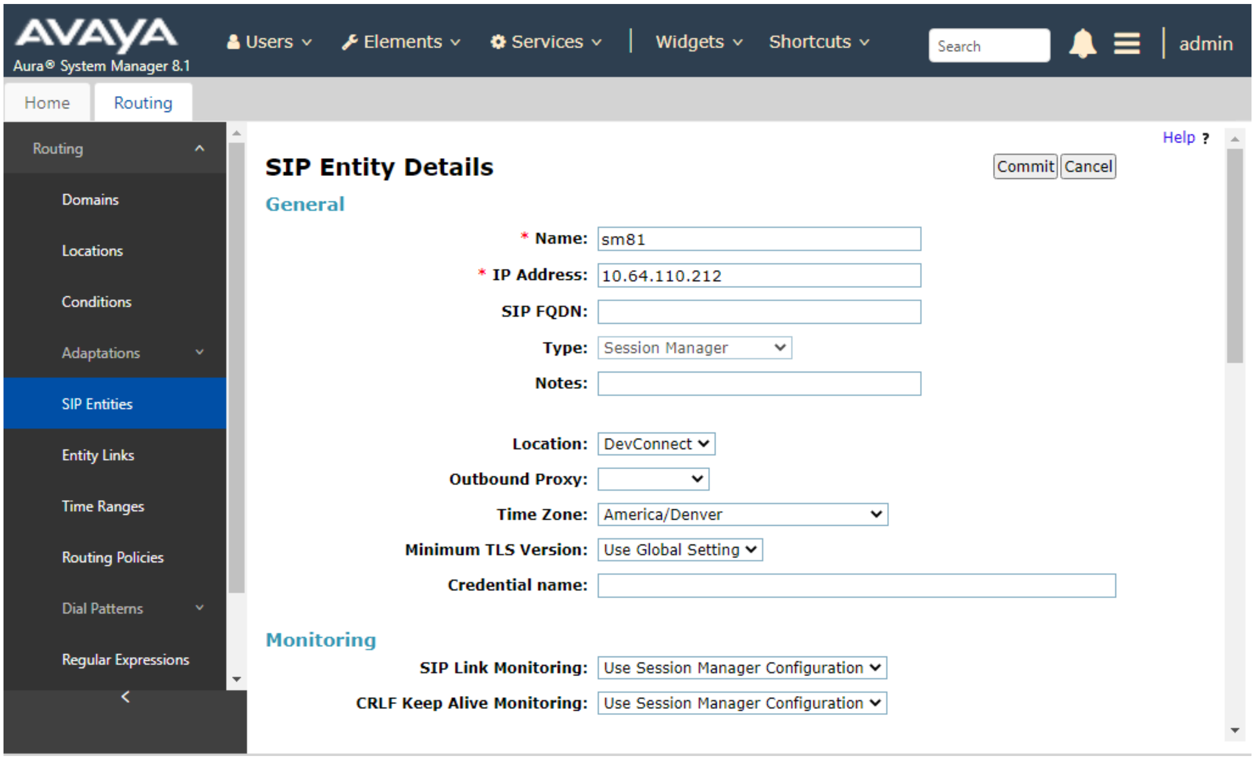
Navigate to Routing →SIP Entities and click on the New button to create a new SIP entity (screen not shown). Provide the following information:

General section
Enter the following and use default values for the remaining fields: **Name**: Enter a descriptive name. **FQDN** or **IP Address**: Enter the IP address of the signaling interface on each:

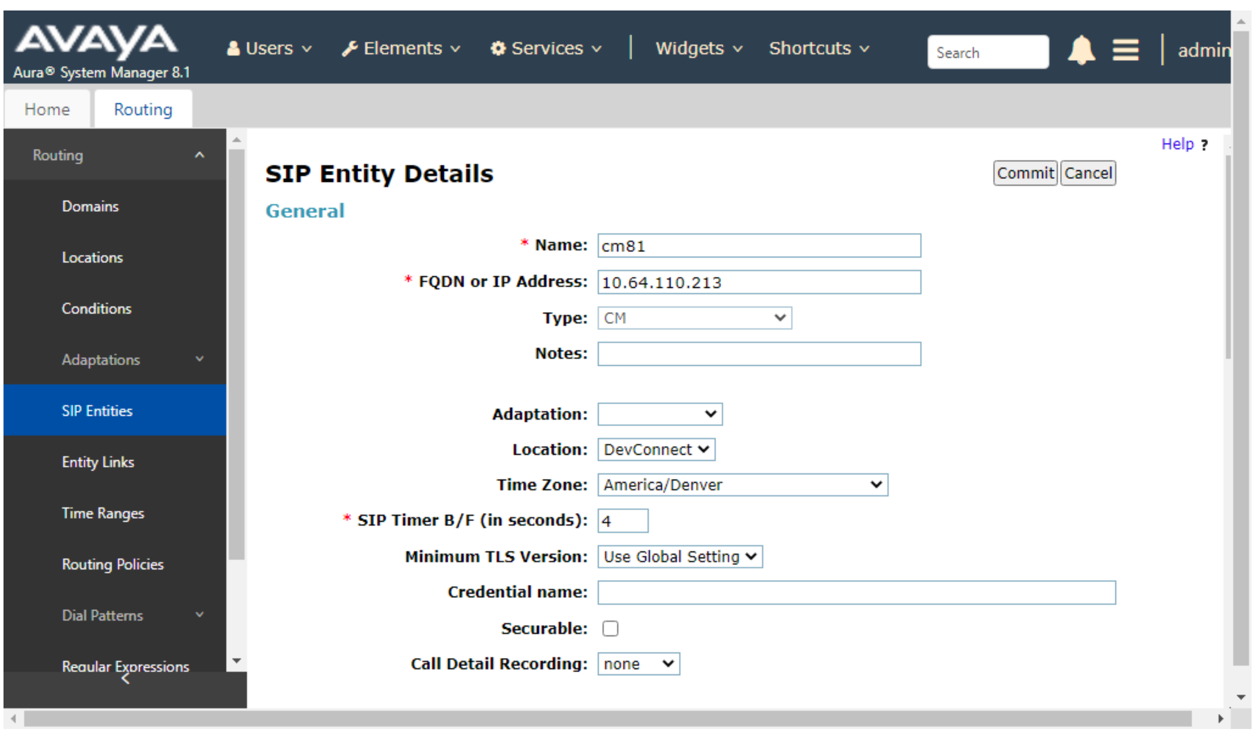
- Communication Manager: 10.64.110.213
- Signaling Session Manager: 10.64.110.212
- Care Connect Speech: 10.64.110.229
- From the **Type** drop down menu, select a type that best matches the SIP Entity:
- For Communication Manager Gateway: select "CM"
- For Session Manager, select "Session Manager"
- For Care Connect Speech, select "Other"
- Enter a description in the **Notes** field if desired.
- Select the appropriate **time zone**.
- **Listen Ports** (only available in the SM SIP Entity): Add port 5060 for TCP and UDP, and 5061 for TLS protocols (not shown), and select the location from **Section 6.3** in the location column for each added port. Accept the other default values.

Click on the Commit button to save each SIP entity. Repeat all the steps for each new entity.

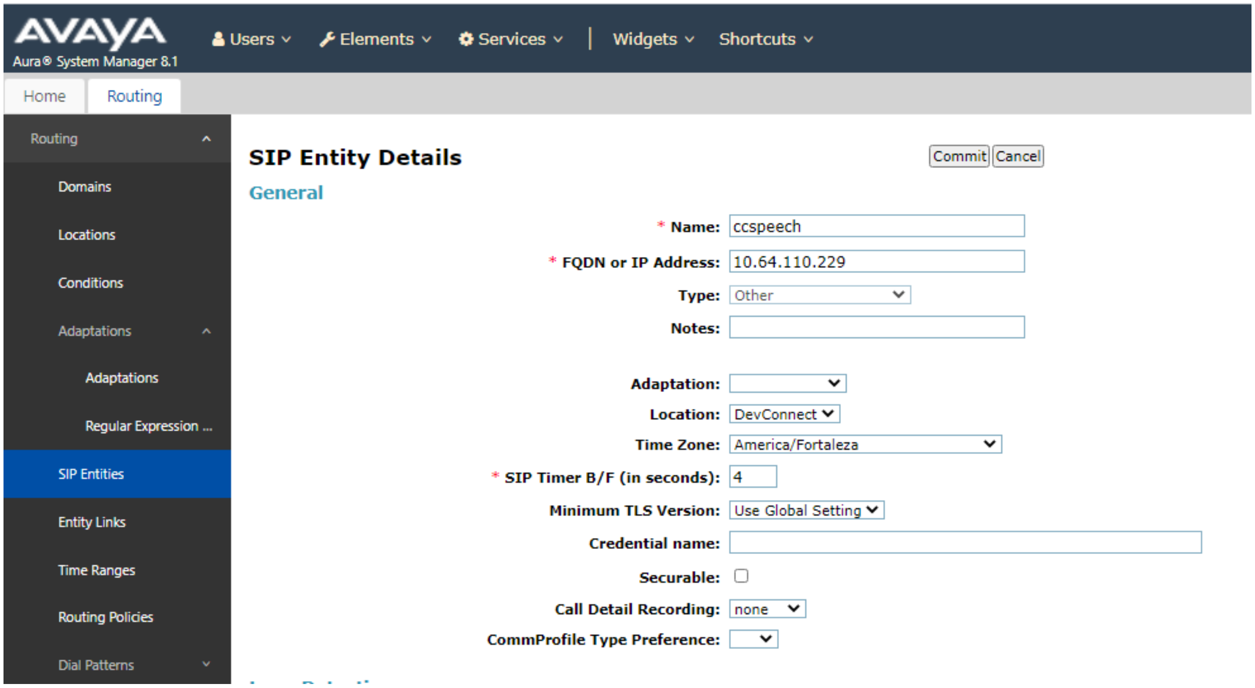
The screen below shows the detail of the Session Manager SIP Entity.



The screen below shows the detail of the Communication Manager SIP Entity.



The screen below shows the detail of the Care Connect Speech SIP Entity.



6.5. Configure Entity Links

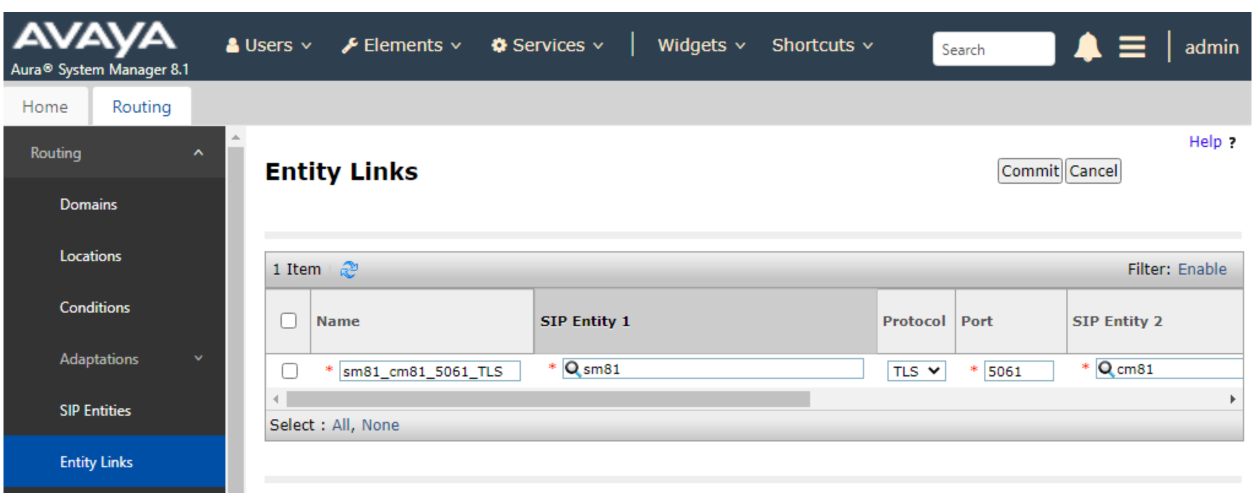
Entity Links define the connections between the SIP Entities. In the compliance test, the following entity links are defined from System Manager.

- Session Manager and Communication Manager
- Session Manager and Care Connect Speech Server

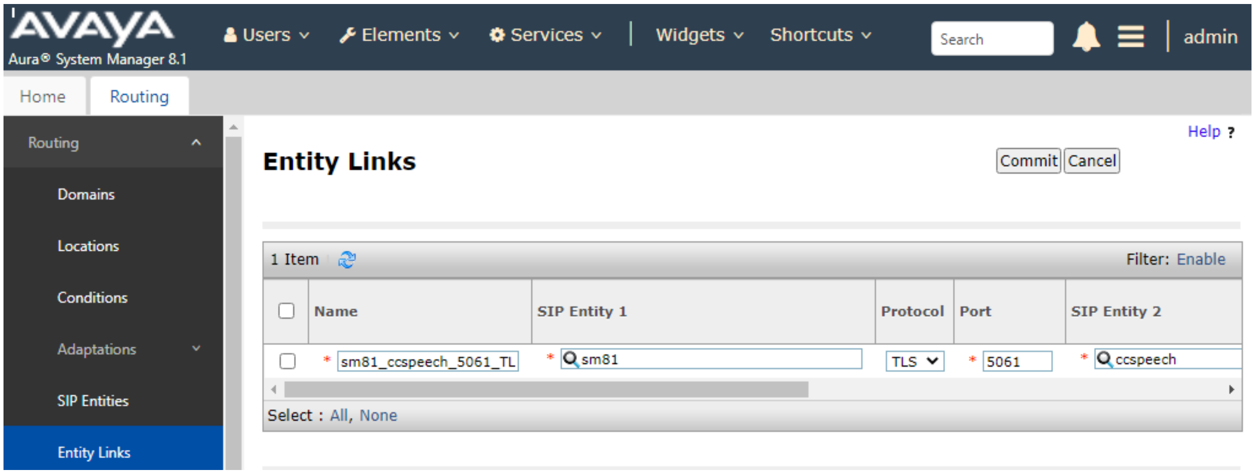
Navigate to Routing → Entity Links and click on the New button to create a new entity link (screen not shown). Provide the following information:

- **Name**: Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 6.4** (e.g. sm81).
- In the **Protocol** drop down menu, select the TLS protocol.
- In the **Port** field, enter the port to be used (e.g. 5061).
- In the **SIP Entity 2** drop down menu, select cm81 for the entity links between Session Manager and Communication Manager and select Care Connect-Speech (e.g. ccspeech) for the entity links between Session Manager and Care Connect Speech.
- In the **Port** field, enter the port to be used (e.g. 5061).
- In the **Connection Policy** column, select Trusted from the dropdown list.
- Enter a description in the **Notes** field if desired.
- Click on the Commit button to save each Entity Link definition. Repeat all the steps for each SIP Entity Link.

The screen below shows the detail of the entity link between Session Manager and Communication Manager.



The screen below shows the detail of the entity link between Session Manager and Care Connect Speech.



6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.4**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for: Inbound calls to Communication Manager and inbound calls to Care Connect Speech.

To add a Routing Policy, navigate to Routing → Routing Policies and click on the New button on the right (screen not shown). Provide the following information:

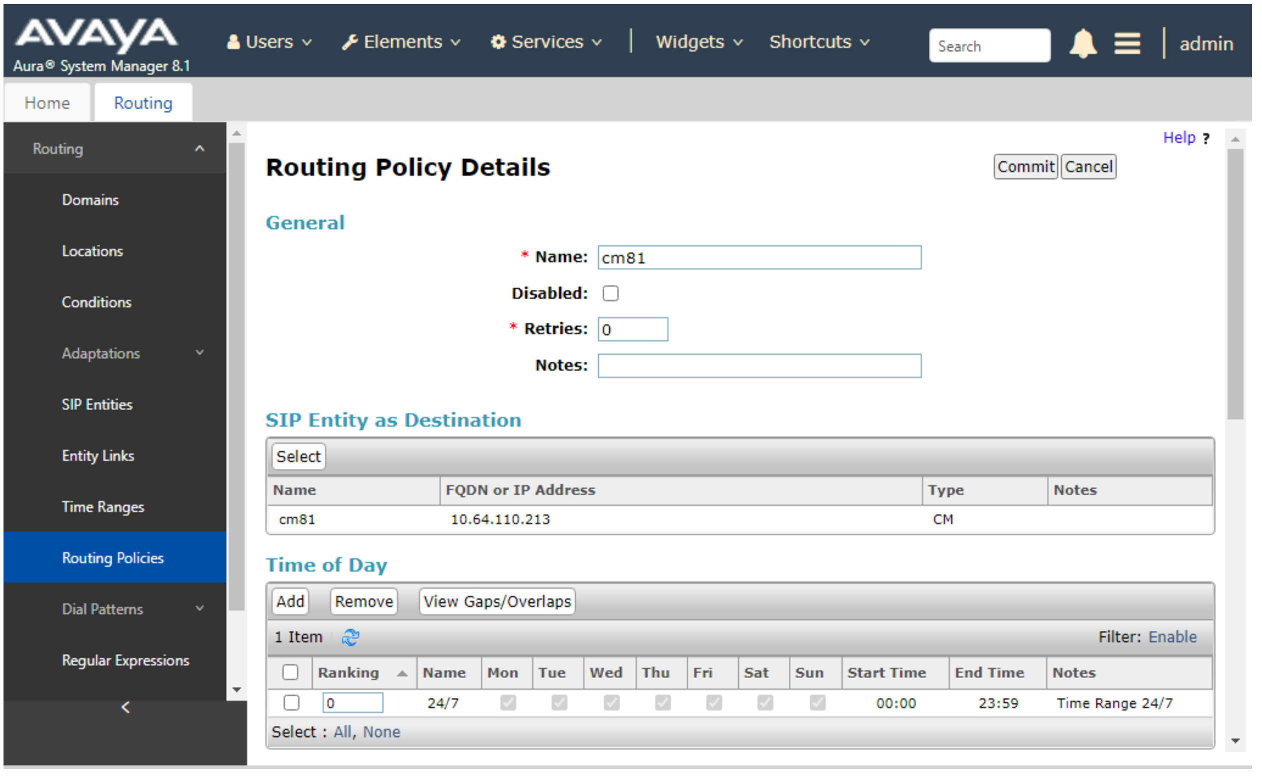
General Section:

- Enter a descriptive name in the **Name** field (e.g. cm81, ccspeech).
- Enter a description in the **Notes** field if desired.

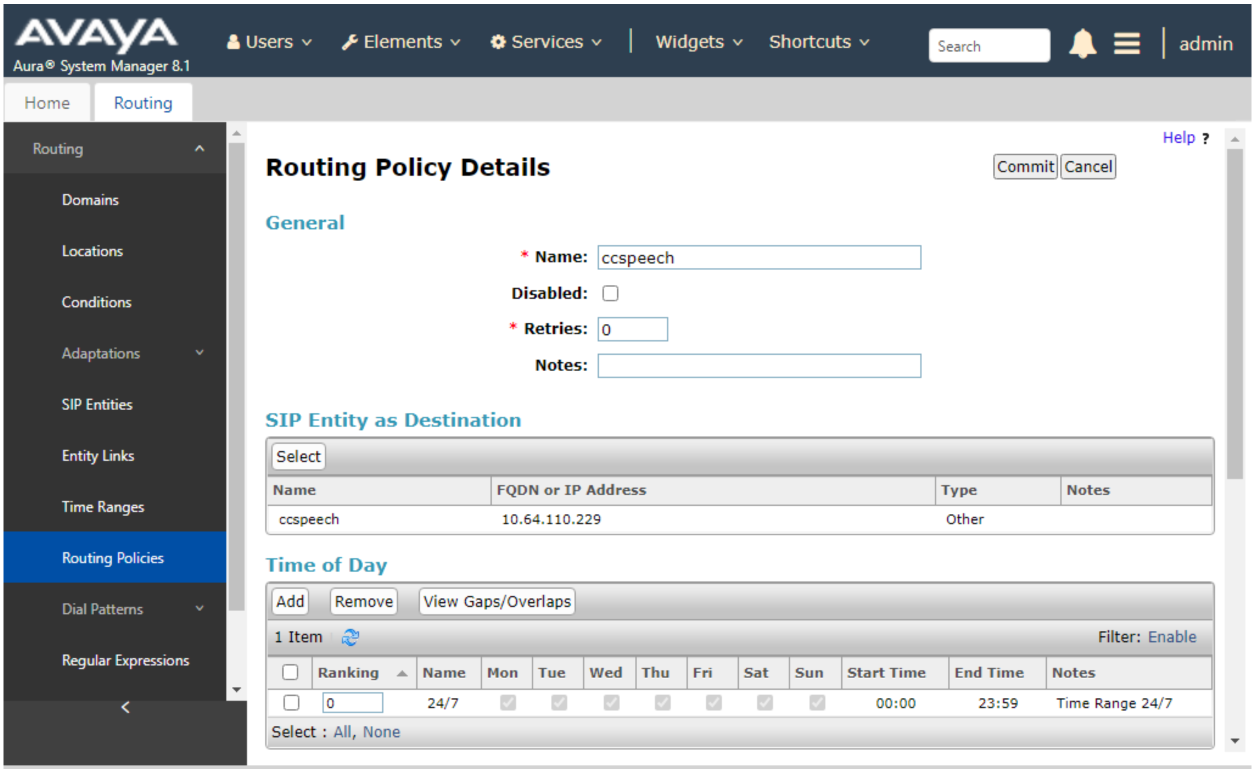
SIP Entity as Destination Section:

- Click the Select button.
- Select the SIP Entity **Name** that will be the destination for this call.
- Click the Select button.

Click Commit to save Routing Policy definition. Repeat the steps for each new Routing Policy. The following screen shows the Routing Policy used for Communication Manager during the compliance test.



The following screen shows the Routing Policy used for Care Connect Speech during the compliance test.



6.7. Configure Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- 70xxx – dial pattern used to route calls to Communication Manager.
- 59994 – dial pattern used to route to Care Connect Speech.

To add a Dial Pattern, select Routing →Dial Patterns and click on the New button (screen not shown) on the right pane. Provide the following information:

General Section:

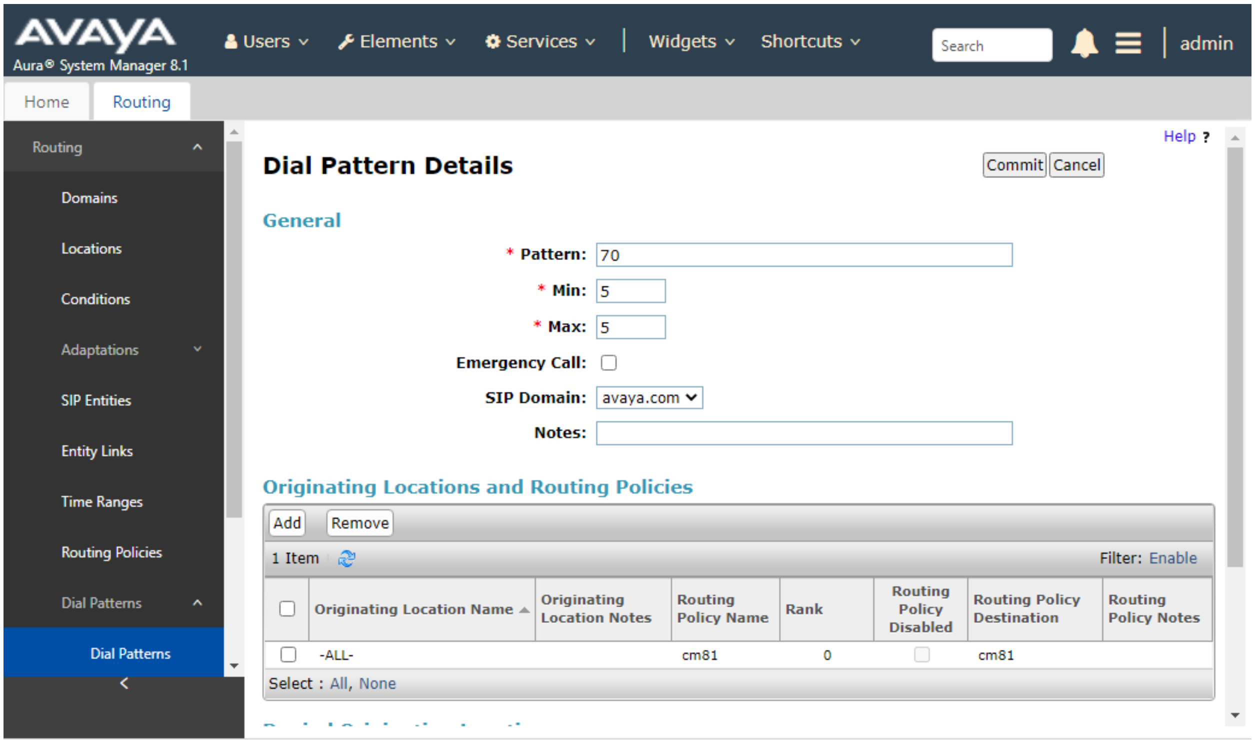
- Enter a unique pattern in the **Pattern** field (e.g. 70).
- In the **Min** field enter the minimum number of digits (e.g. 5).
- In the **Max** field enter the maximum number of digits (e.g. 5).
- In the **SIP Domain** drop down menu select the domain defined in Section 6.1. In compliance testing, the value of'-ALL- was used.

Originating Locations and Routing Policies Section:

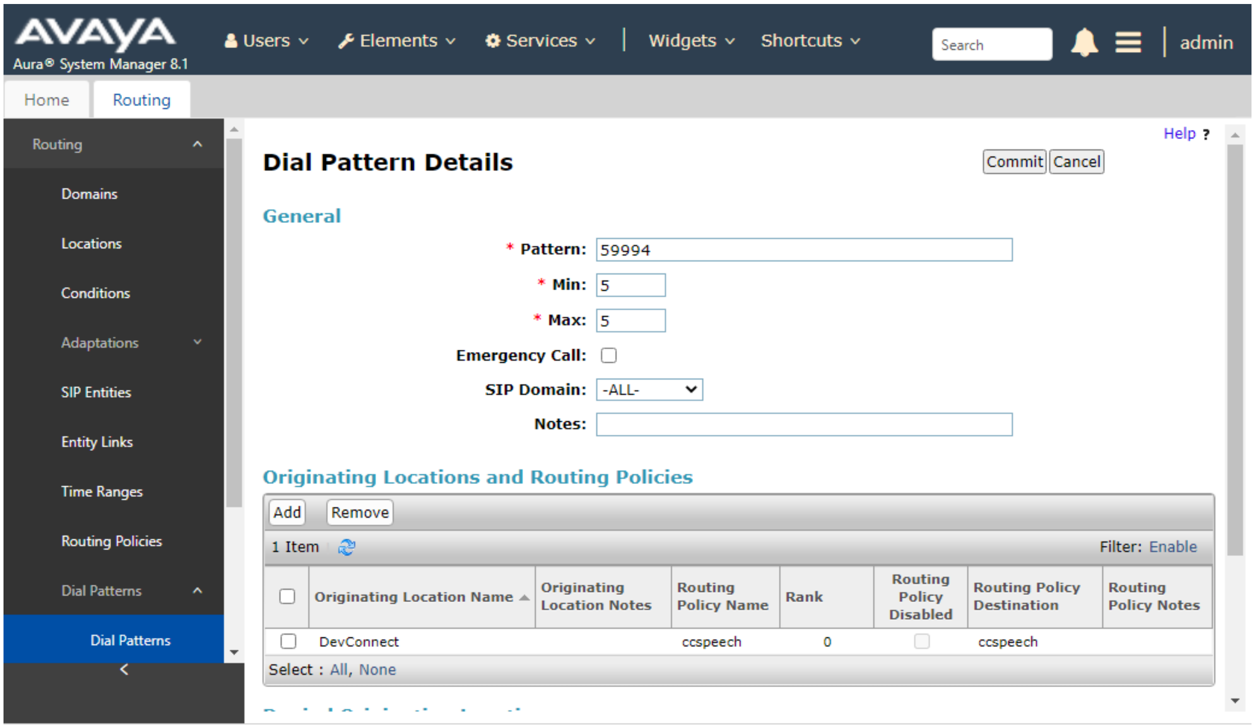
- Click on the Add button and a window will open (screen not shown).
- Click on the box for the appropriate **Originating Locations**, and **Routing Policies** (see **Section 6.6**) that pertain to this Dial Pattern.
- Select the **Originating Location** to apply the selected routing policies to All.
- Select appropriate **Routing Policies**.
- Click on the Select button and return to the Dial Pattern page.

Click the Commit button to save the new definition. Repeat steps for the remaining Dial Patterns.

The following screen shows the dial pattern **70** used to route calls to Communication Manager during the compliance test.



The following screen shows the dial pattern **59994** used to route calls to Care Connect Speech during the compliance test.



7. Configure Spok Connect Care Speech

Spok installs, configures, and customizes the Spok CCS Applications for their end customers.

7.1. Configuring Care Connect Speech System Settings

To access Care Connect Suite Speech configuration settings:

- Log in to Care Connect Web.
- Click Administration, and then click Speech.
- To edit the available configuration settings, click Edit.
- After settings are updated, click Save and then restart the Care Connect Speech server. Note: Saved configuration settings do not take effect until the server is restarted.

The following configuration areas are available:

- Speech Configuration
- FreeSWITCH Settings

7.1.1. Speech Configuration

The following Care Connect Speech server configuration settings ensure other components of Care Connect Suite are integrated properly with the Speech server.

- Server Name: Enter the name or IP address of the server on which Care Connect Speech is installed.
- Server Port: Enter the port number on which the Care Connect Speech server listens for connections from other Care Connect Suite components.

Note: If these settings are updated, the Care Connect Suite IIS Application Pool (SpokServiceAppPool) is reset, which also resets the web apps and causes the core service to use the new settings when communicating with the Speech server.

7.1.2. FreeSWITCH Settings

- Outbound Caller ID Name: Enter the desired name to appear on a recipient's Caller ID when an outbound call is made.
- Outbound Caller ID Number: Enter the desired number to appear on a recipient's Caller ID when an outbound call is made. Only numeric values are allowed.
- Max Outbound Calls: Enter the maximum number of simultaneous outbound calls the system can initiate.
- Max Inbound Calls: Enter the maximum number of simultaneous inbound calls the system can accept.

Note: The value of the maximum and minimum number of simultaneous inbound calls are each commonly set as half the number of total ports. This ensures that the system can accommodate the same number of maximum inbound and outbound calls simultaneously.

- Make Call Timeout :Enter the duration, in seconds, for the system to wait for someone to answer an outbound call before it is ended.
- Music On Hold: Enter the name of the audio file to play when a caller is placed on hold. This file must be in wave format with a .wav extension and must exist in the \Spok\Care Connect\Speech\Prompts\ folder on the Care Connect Speech server.
- Parked Call Timeout: Enter the duration, in seconds, a parked call waits to be connected with no answer from the recipient before the alternate action specified in the call flow is executed.
- Record Silence Hits: Enter the duration, in seconds, of silence to elapse before the in progress greeting recording is automatically stopped. The greeting recording prompts the caller to record a short message to be played to the recipient before they accept or decline an inbound call.
- Record Silence Threshold: Enter a numeric value for the threshold of what is considered "silence" by the system. The lower the value, the quieter the line must be in order for the system to consider the line to be "silent." The default value is 200. This configuration setting works in conjunction with the value of the Record Silence Hits field. If the threshold for what the system considers to be "silence" is reached for the duration specified in the Record Silence Hits field, the system stops the recording. Update this value to troubleshoot instances where the system either stops recording prematurely when soft-spoken callers are recording a message because the silence threshold has been met, or continues recording because background noise is being picked up and the silence threshold is not met even though the caller has stopped speaking.

- Hold Before Transfer:Select this option to place calls on hold before transferring. Otherwise, calls are immediately transferred, which may involve a risk of a call being dropped.
- Hold Delay Before Transfer:Enter the duration, in milliseconds, a call is on hold before being transferred when Hold Before Transfer is enabled. The default value is 1000, or 1 second.
- Use TLS:Select to secure the telephony network with Transfer Layer Security Protocol (TLS).
- SIP IP:Enter the SIP IP address of the switch to connect to. This can then be used as a variable in the Outbound and Transfer Call Patterns: {SIPTRUNKIP}
- SIP Port: Enter the SIP port number to connect to. This can then be used as a variable in the Outbound and Transfer Call Patterns: {SIPTRUNKPORT}

7.2. Configuring the FreeSWITCH Engine

FreeSWITCH is a component of Care Connect Speech and must be configured as part of the Care Connect implementation.
FreeSWITCH is used for telephony connectivity and media control. In order for FreeSWITCH to accept inbound calls, modify the acl.conf.xml file with the IP addresses of the PBX or SIP Gateway to allow to access FreeSWITCH:

7.2.1. Allowing Gateway/Trunk Access to FreeSWITCH

- Access the acl.conf.xml file. In most cases, this file can be found in the following location: C:\Program Files\FreeSWITCH\conf\autoload_configs\acl.conf.xml.
- Open the file via text editor.
- Replace the cidr value XXX.XXX.XXX.XXX/XX with the IP address of the PBX\Gateway to be allowed access to this server. For example, if the PBX IP is 192.168.0.0, the cidr value is 192.168.0.0/24. The section of the value after the IP address (/24) represents the bit length of the subnet mask. Typically, /24 is the default. In this example, 192.168.0.0/24, the /24 allows for any address between 192.168.0.0 and 192.168.0.255 to access this server. If using multiple gateways, either add additional nodes, repeating step 3, or make sure that the IP address range is within the specified cidr value.

7.2.2. Applying FreeSWITCH Changes

There are several ways to apply the above changes, but the easiest solution is to restart the FreeSWITCH Service. However, at times there may be a need to apply changes to an active system that is taking calls. For this purpose, it is best to use the **FreeSWITCH Client Console** and issue a few commands to get things to take effect.

- Locate the **fs_cli.exe**. In most cases, this can be found in the following location: **C:\Program Files\FreeSWITCH**
- Execute the **fs_cli.exe**. A DOS command prompt opens.

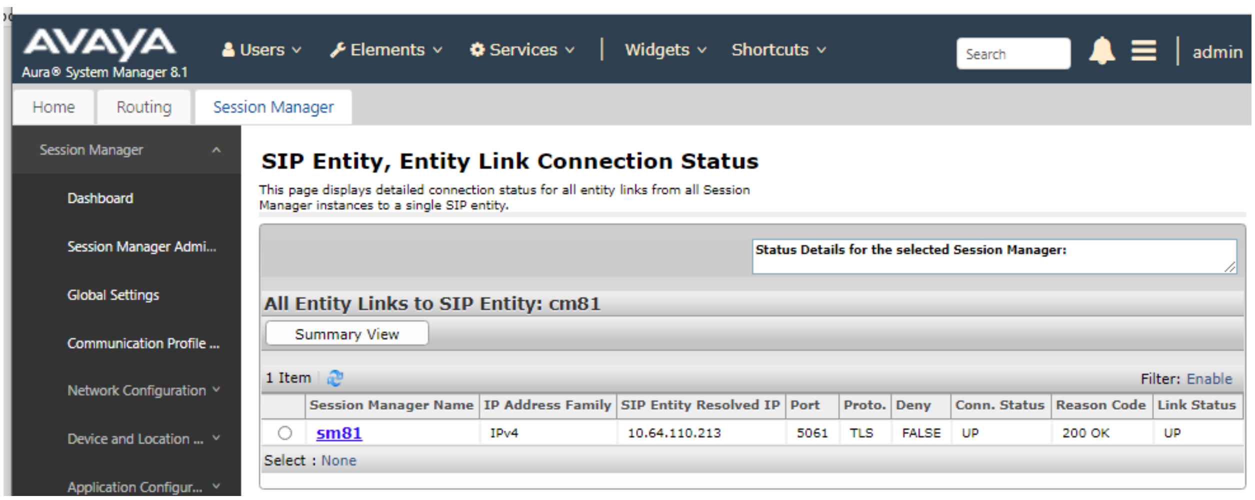
- To reload dialplan (**public.xml** and **dialplan.xml**) files, type **RELOADXML** and press **Enter**.
- Log information appears in the command prompt. Green text output indicates a successful **RELOADXML**. Error information in red text indicates an unsuccessful reload.
- Once successful, exit out of the **fs_cli.exe**. **NOTE:** To reload the **acl.conf**, repeat the reload procedure, using the **RELOADACL** command instead.

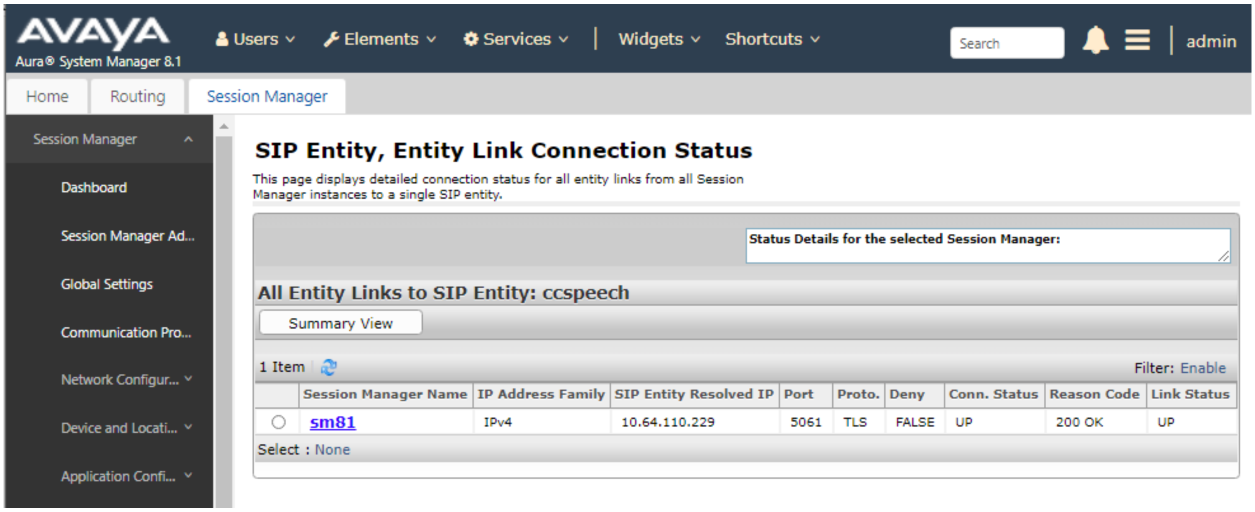
8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Care Connect Speech.

8.1. Verify Session Manager

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Verify that the state of the Session Manager links to Communication Manager and Care Connect Speech by selecting the SIP Entity names.





9. Conclusion

These Application Notes described the administration steps required to integrate Care Connect Speech with Avaya Aura® Communication Manager via SIP trunk configured on the Avaya Aura® Session Manager. All test cases passed. Refer to **Section 2.2** for additional details and observations.

10. Additional References

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

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020
[2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, August 2020

Product information for Spok products may be found at http://knowledge.spok.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.