Avaya Solution & Interoperability Test Lab

Application Notes for CounterPath Bria Mobile v3.6 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the steps required to integrate the CounterPath Bria Mobile v3.6 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface. CounterPath Bria Mobile v3.6 supports video along with audio and runs mobile devices.

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 steps required to integrate the CounterPath Bria Mobile v3.6 with Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager) using a SIP interface. Bria Mobile v3.6 supports video along with audio and runs on mobile devices. During the compliance testing the following mobile devices were used:

- Apple iPhone
- Apple iPad
- Google Nexus 7

2. General Test Approach and Test Results

To verify interoperability of the Bria Mobile v3.6 with Communication Manager and Session Manager, video calls were made between Bria Mobile v3.6, Avaya one-X® Communicator (H.323), Avaya Communicator (SIP) and Avaya H175 Video Collaboration Station (SIP). In addition, voice calls were made using similar end points. Additional features were exercised on Bria Mobile v3.6.

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.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of Bria Mobile v3.6 with Session Manager.
- Video calls between Bria Mobile v3.6, and Avaya one-X® Communicator with a H.323 interface, Avaya Communicator with a SIP interface and Avaya H175 Video Collaboration Station with a SIP interface.
- Voice calls between Bria Mobile v3.6 and Avaya one-X® Communicator, Avaya Communicator, and Avaya IP telephones (SIP and H.323).
- G.711MU, G.711A, G.729A and G722-64k codec support.
- Caller ID display on Avaya and Bria Mobile v3.6.
- Call Hold, Mute, Transfer and Conference.
- Proper system recovery after a restart of Bria Mobile v3.6 and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following observations:

- When a call is place on hold and un-held, video is not available. Fix for this issue is scheduled to be supported in Bria Mobile v3.7.1.
- When there are two calls on Bria Mobile v3.6, toggling between them makes the video unavailable. This issue is related to the one mentioned above.
- In a scenario where Bria Mobile v3.6 calls PSTN and call is transferred back into Avaya Environment, video is not able to active. Avaya is currently troubleshooting this issue.

2.3 Support

For technical support on Bria Mobile v3.6 can be obtained via following means:

- **Phone:** 1.877.818.3777
- **Web:** https://support.counterpath.com/
- **Email:** support@counterpath.com

Note: Please contact your CounterPath Sales Representative if you do not have a CounterPath Support Agreement

3. Reference Configuration

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

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones and video endpoints.
- Avaya Aura® System Manager used to configure Session Manager.

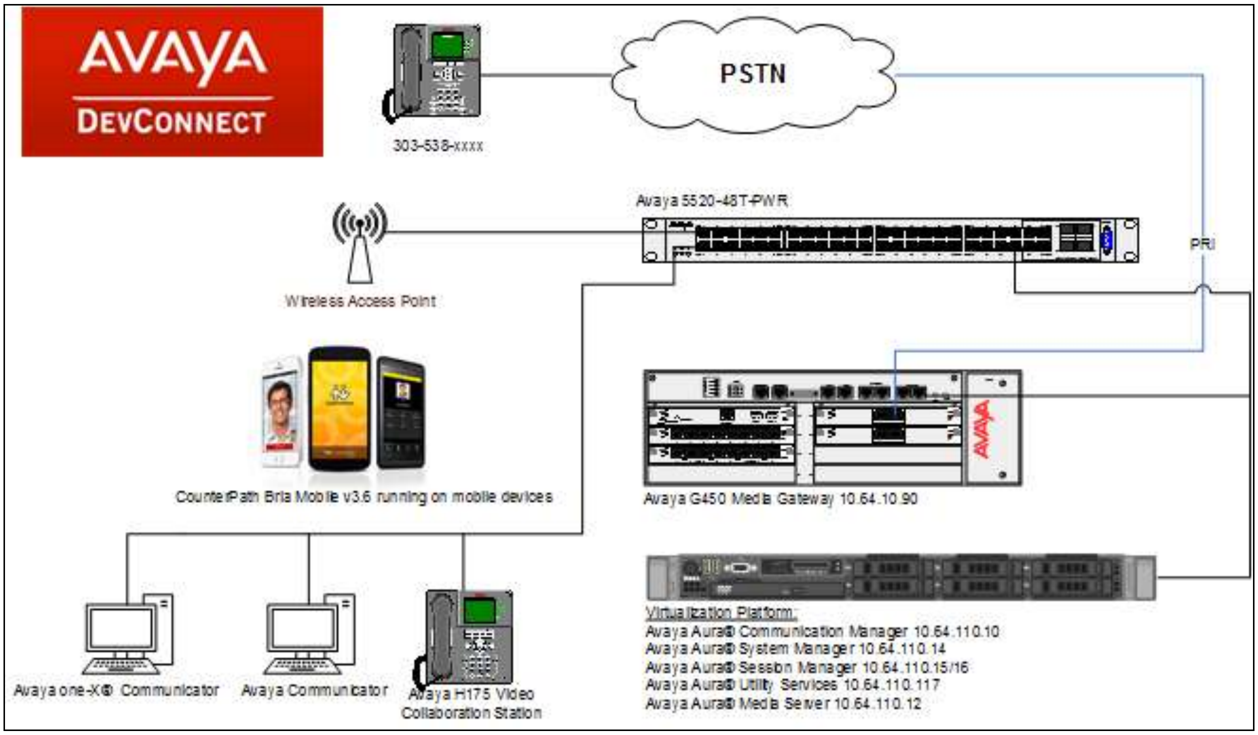


Figure 1: Avaya SIP Network with the Bria Mobile v3.6

4. Equipment and Software Validated

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

Hardware Component	Version
Avaya Aura® Session Manager	7.0.1.0.701007
Avaya Aura® System Manager	7.0.1.0.064859
Avaya Aura® Communication Manager	7.0.1.0.0.441.23012
Avaya Aura® Media Server	7.7.0.334 A15
Avaya G450 Media Gateway	37.38.0
Avaya one-X® Communicator	6.2 SP11
Avaya 9600 Series IP Telephones	3.101 (H.323) 2.6 (SIP)
Avaya H175 Video Collaboration Station	1.0.2
CounterPath Bria Mobile	iOS 3.6.5 build 34728 Android 3.6.4

5. Configure Communication Manager

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

- Verify Communication Manager license
- Configure Bria Mobile v3.6 as an Off-PBX Station (OPS)
- Configure a SIP trunk between Communication Manager and Session Manager

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

5.1 Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS), video capable endpoints, and SIP Trunk options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                    Page   1 of  11
                                        OPTIONAL FEATURES

     G3 Version: V17                              Software Package: Enterprise
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 6400  82
                                      Maximum Stations: 2400  27
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  5
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
                    Maximum Off-PBX Telephones - PVFMC: 9600  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options** form, verify that the number of video capable endpoints and SIP trunks supported by the system is sufficient.

```
display system-parameters customer-options                      Page   2 of  11
OPTIONAL FEATURES

IP PORT CAPACITIES                                                  USED
                     Maximum Administered H.323 Trunks: 4000  30
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  12
                       Maximum Administered SIP Trunks: 4000  10
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2 Configure SIP Trunk

In the **IP Node Names** form, assign an IP address and host name Session Manager SIP interface. The host names will be used throughout the other configuration screens of Communication Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
acms                10.64.110.18
aes                 10.64.110.15
ams                 10.64.110.16
asm                 10.64.110.13
biscom              10.64.101.152
cms17               10.64.10.85
default             0.0.0.0
egw1                10.64.110.200
egw2                10.64.110.201
procr               10.64.110.10
procr6              ::

( 11 of 11  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
```

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 the Avaya G450 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group.

```
change ip-network-region 1                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       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? y
   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
```

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to Bria Mobile v3.6. 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 above. The default settings of the **IP Codec Set** form are shown below. Additional codecs can be added on this page as well.

```
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:
 3:
 4:
 5:
 6:
 7:
```

Configure **Page 2** of the **IP Codec Set** form as follows.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  4096:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  4096:Kbits

                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

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*.
- Set the **Transport Method** field to *tls*.
- Set the **IP Video** field to *y*. This is an important setting required for video calls.
- Specify the procr interface and the Session Manager 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 were 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 **Direct IP-IP Audio Connections** field was enabled on this form.
- The default values for the other fields may be used.

```
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? 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: asm
 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 calls to SIP endpoints. 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. Configure the other fields in bold and accept the default values for the remaining fields.

```
add trunk-group 1                                                  Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: asm                         COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

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

```
trunk-group 1                                                  Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y

 DSN Term? n                         SIP ANAT Supported? n
```

Configure the **Public Numbering 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 '1' whose calls are routed over any trunk group, including SIP trunk group "1", have the extension sent to the far-end for display purposes.

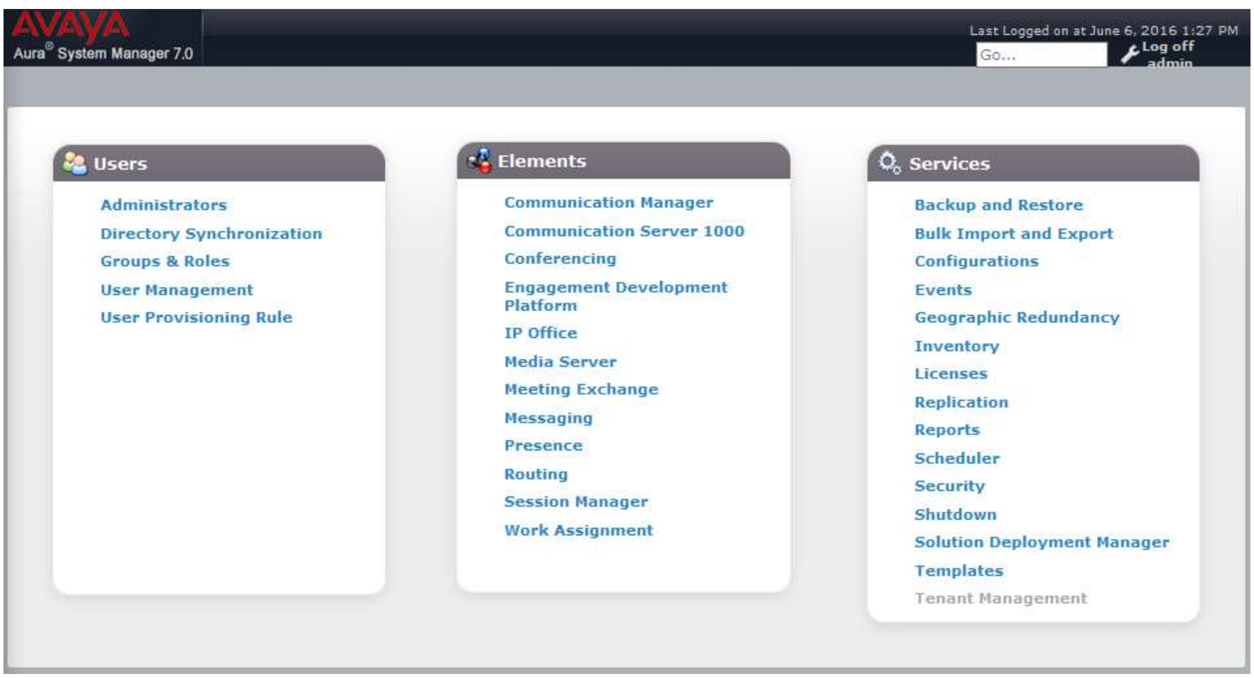
```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                  Total Administered: 3
 5  1                                       5        Maximum Entries: 240
 10 3                                       10
 11 1                                       11    Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.

                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

6. Configure Session Manager

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

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Application Sequence
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager
- Add SIP User

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. The initial screen is displayed as shown below. The configuration in this section will be performed under **Routing** and **Session Manager** listed within the **Elements** box.



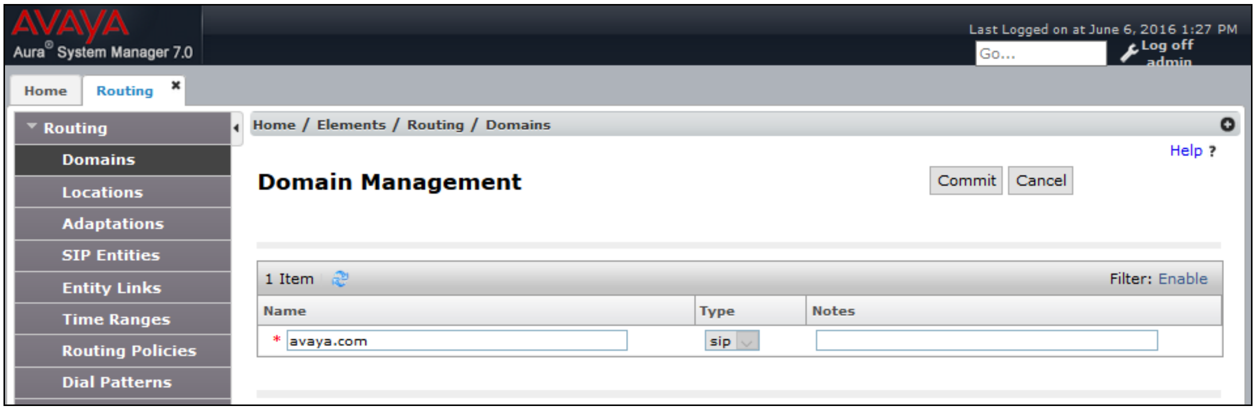
6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Routing → Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *avaya.com*)
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.



6.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

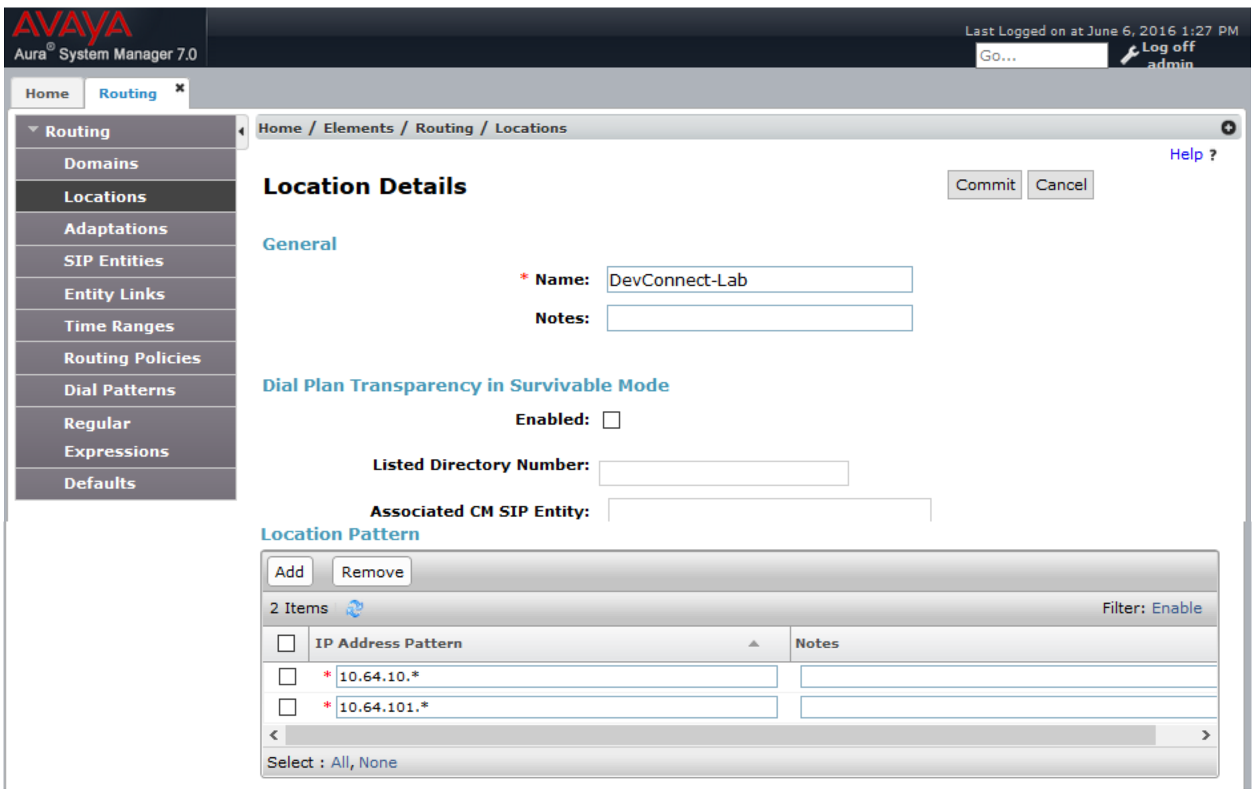
Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the *DevConnect-Lab* location, which includes the Communication Manager and Session Manager. Click **Commit** to save the Location definition.



6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and Communication Manager.

6.3.1 Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

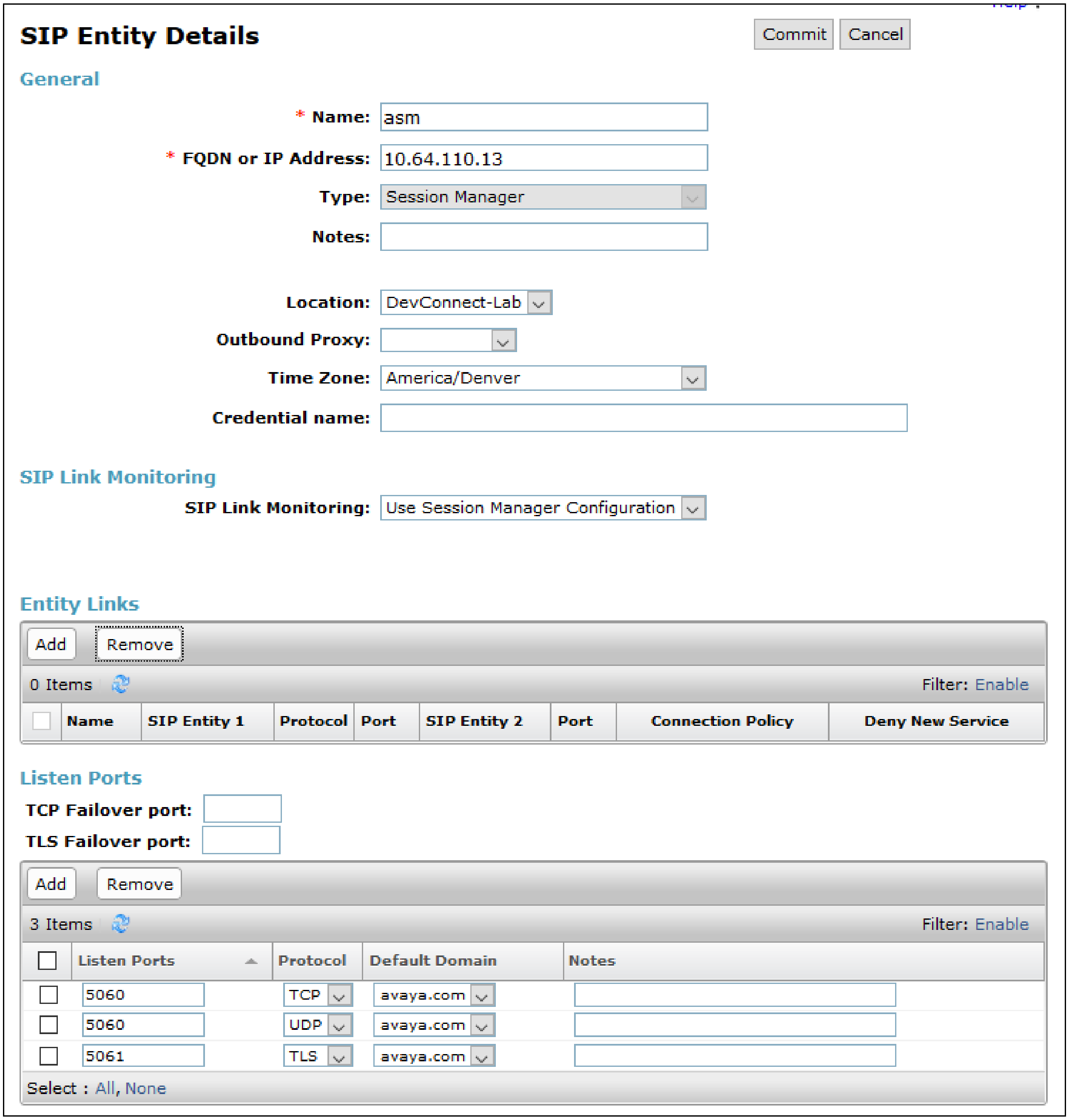
Under *General*:

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

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., *avaya.com*).

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


SIP Entity Details
Commit
Cancel
General
* Name: asm
* FQDN or IP Address: 10.64.110.13
Type: Session Manager
Notes:
Location: DevConnect-Lab
Outbound Proxy:
Time Zone: America/Denver
Credential name:
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration
Entity Links
Add
Remove
0 Items
Filter: Enable
Name
SIP Entity 1
Protocol
Port
SIP Entity 2
Port
Connection Policy
Deny New Service
Listen Ports
TCP Failover port:
TLS Failover port:
Add
Remove
3 Items
Filter: Enable
Listen Ports
Protocol
Default Domain
Notes
5060 TCP avaya.com
5060 UDP avaya.com
5061 TLS avaya.com
Select : All, None

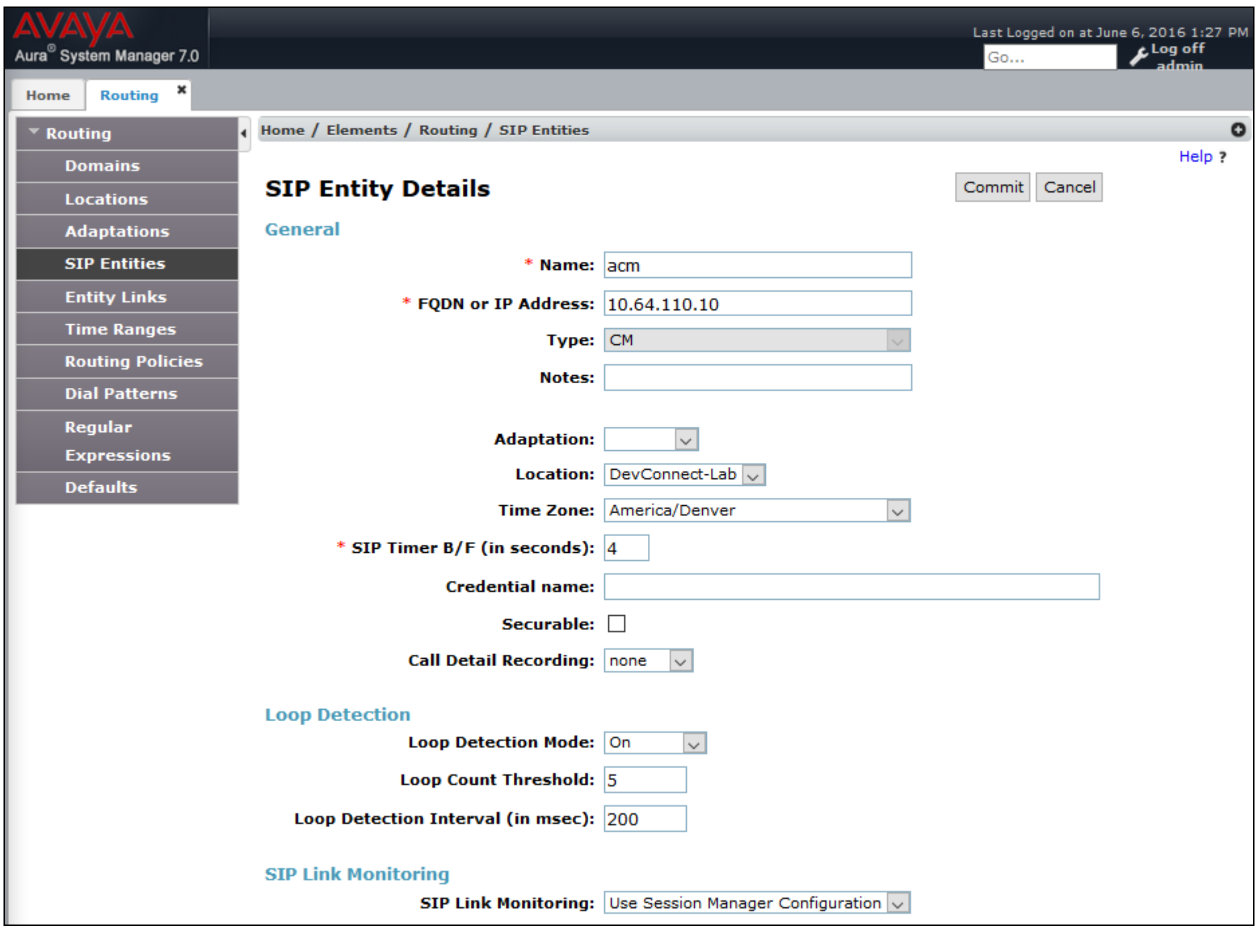
6.3.2 Communication Manager

A SIP Entity must be added for the Communication Manager. To add a SIP Entity, select **SIP Entities** 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*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of Communication Manager
- **Type:** Select *CM*.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

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

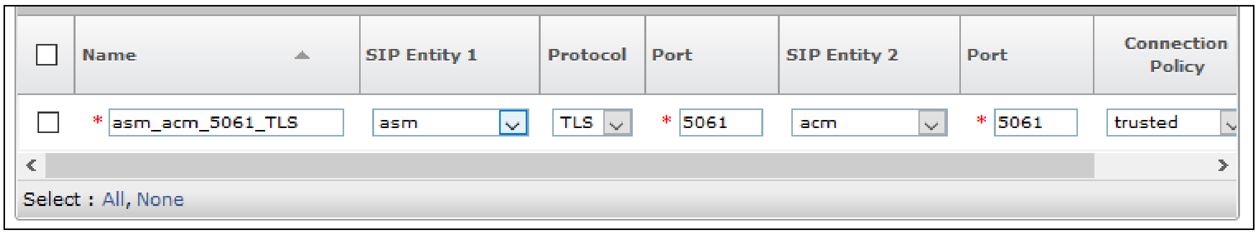


6.4 Add Entity Link

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

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **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.

Click **Commit** (not shown) to save the Entity Link definition.



6.5 Define Communication Manager as Managed Element

Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

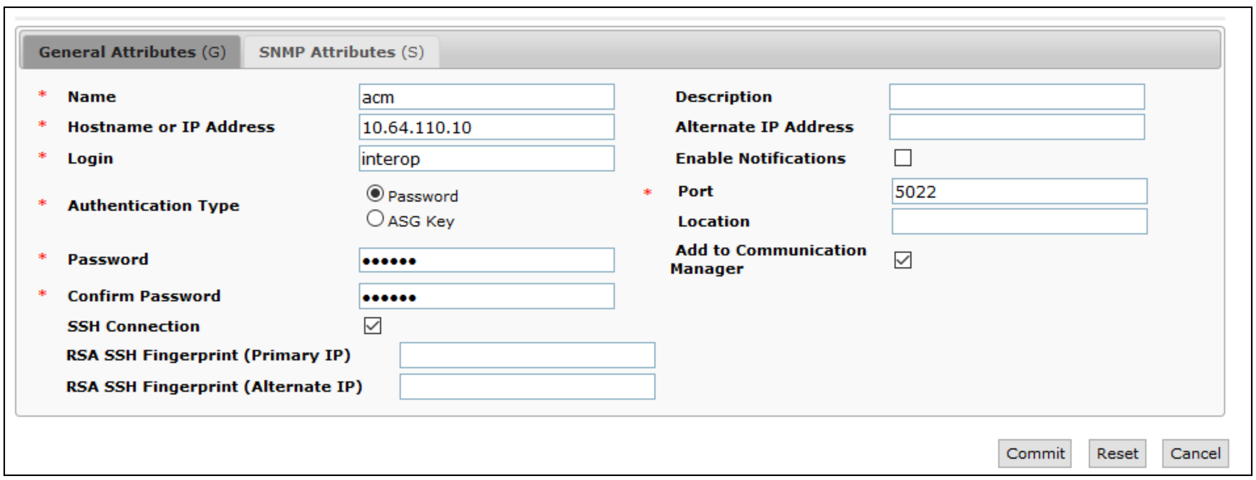
To define Communication Manager as a managed element, select **Home → Inventory → Manage Elements** on the left and click on the **New** button (not shown) on the right. In the **New Entities Instance** screen (not shown), select *Communication Manager* in the **Type** field can click **Commit**.

In the **New CM Instance** screen, fill in the following fields as follows:

In the *Application* tab:

- **Name:** Enter an identifier for Communication Manager.
- **Hostname or IP Address:** Enter the IP address of Communication Manager.
- **Login / Password:** Enter the login and password used for administration access.
- **Port:** Enter the port number for SSH administration access (5022).

Defaults can be used for the remaining fields. Click **Commit** to save the settings.

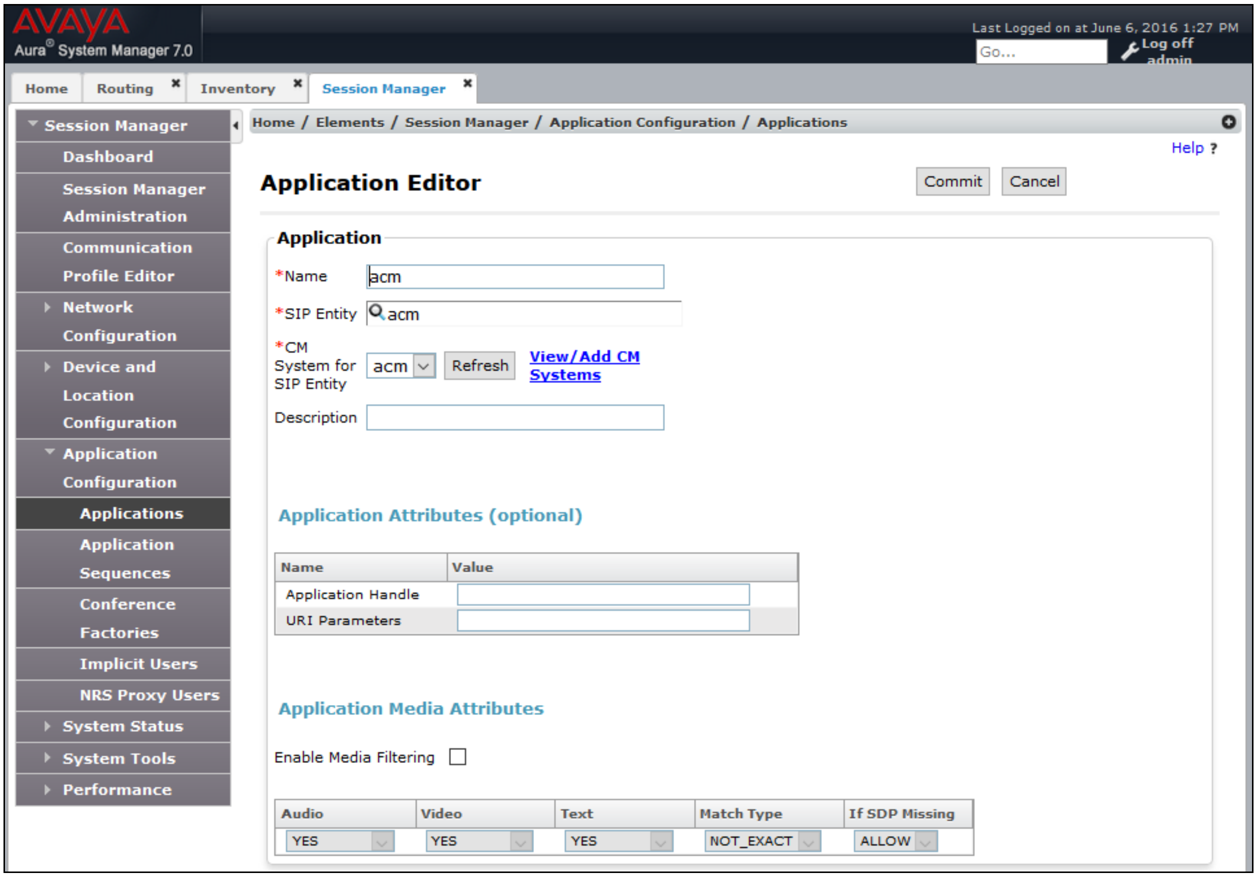


6.6 Add Application Sequence

To define an application for Communication Manager, navigate to **Home → Session Manager → Application Configuration → Applications** on the left and select **New** button (not shown) on the right. Fill in the following fields:

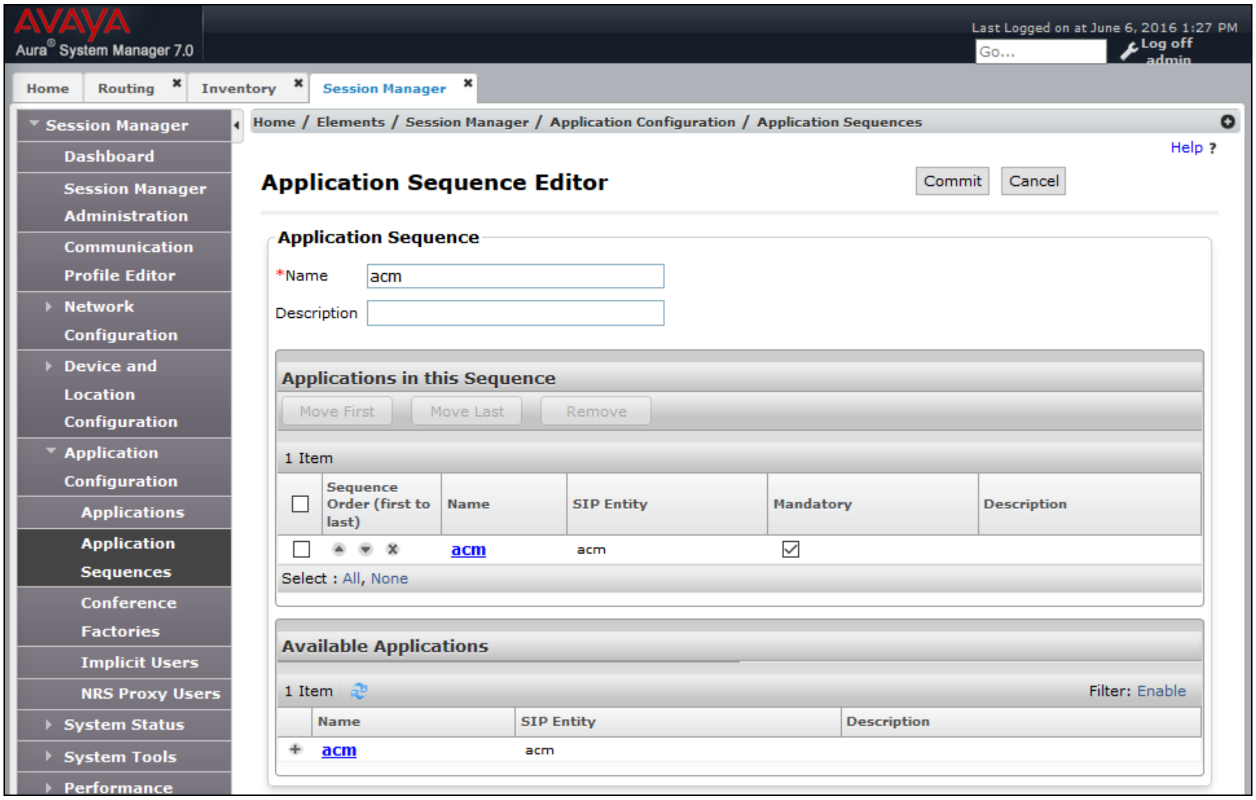
- **Name:** Enter name for application.
- **SIP Entity:** Select the Communication Manager SIP entity.
- **CM System for SIP Entity** Select the Communication Manager managed element.

Click **Commit** to save the Application definition.



Next, navigate to **Elements → Session Manager → Application Configuration → Application Sequences** to define the Application Sequence for Communication Manager as shown below. Provide a **Name** (e.g., *acm*) for the Application Sequence and under **Available Applications**, click on the plus (+) sign by *acm* to add it under the **Application in this sequence** section.

Verify a new entry is added to the **Applications in this Sequence** table and the **Mandatory** column is ☑ as shown below.



6.7 Add SIP User

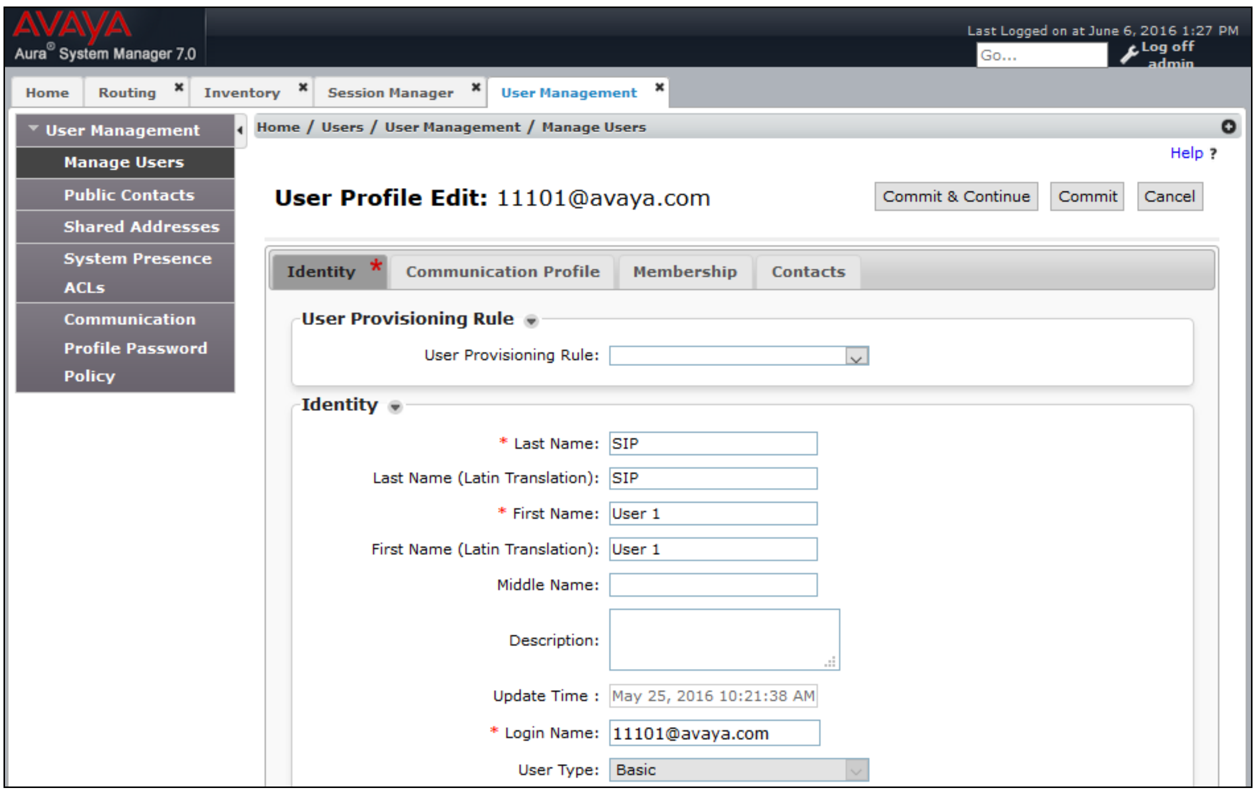
Add a SIP user for Bria Mobile v3.6**.** The following configuration will automatically create the SIP station on Communication Manager Evolution Server.

To add new SIP users, navigate to **Home → User Management → Manage Users** from the left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **Identity** tab of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter *<extension>@<sip domain>* of the user (e.g., 11101@avaya.com).

The screen below shows the information when adding a new SIP user to the sample configuration.



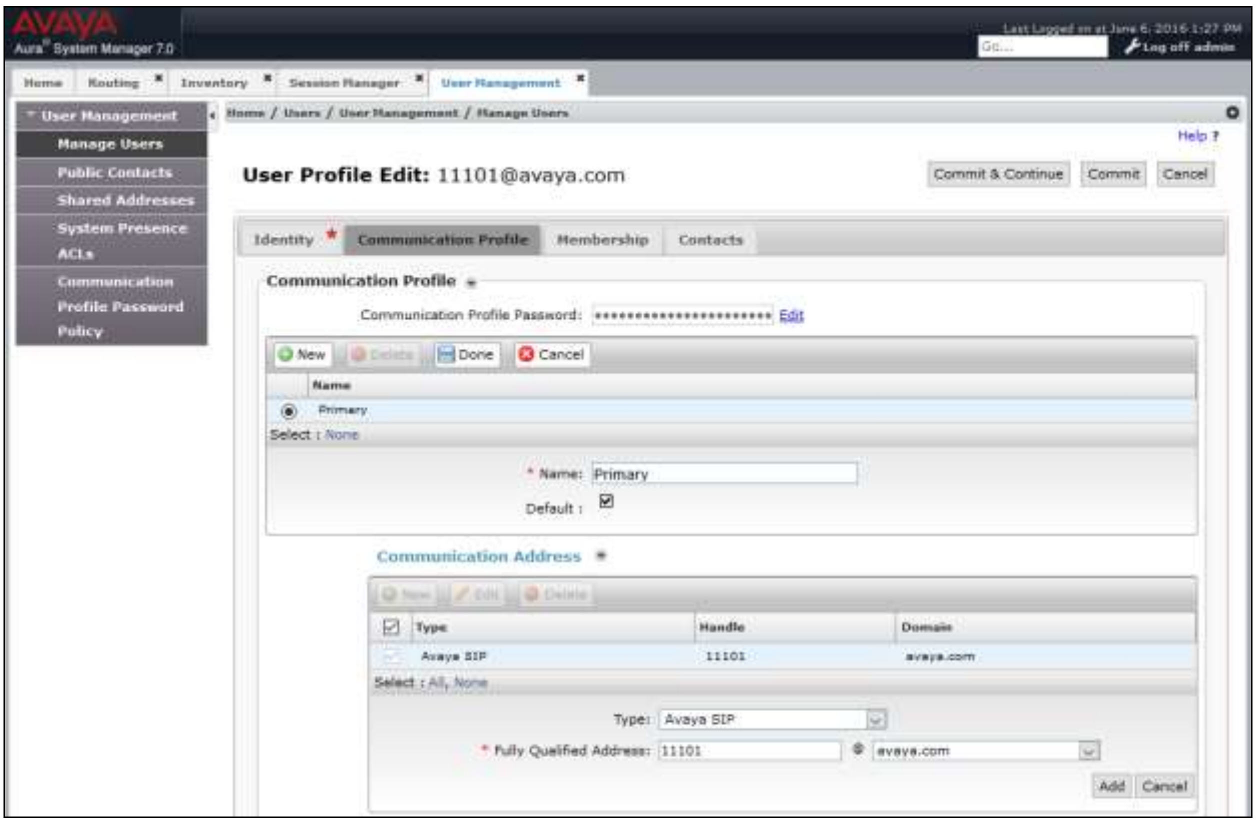
Enter values for the following required attributes for a new SIP user in the **Communication Profile** tab of the new user form.

- **Communication Profile Password:** Enter the password which will be used by Bria Mobile v3.6 to register with Session Manager.
- **Confirm Password:** Re-enter the password from above.

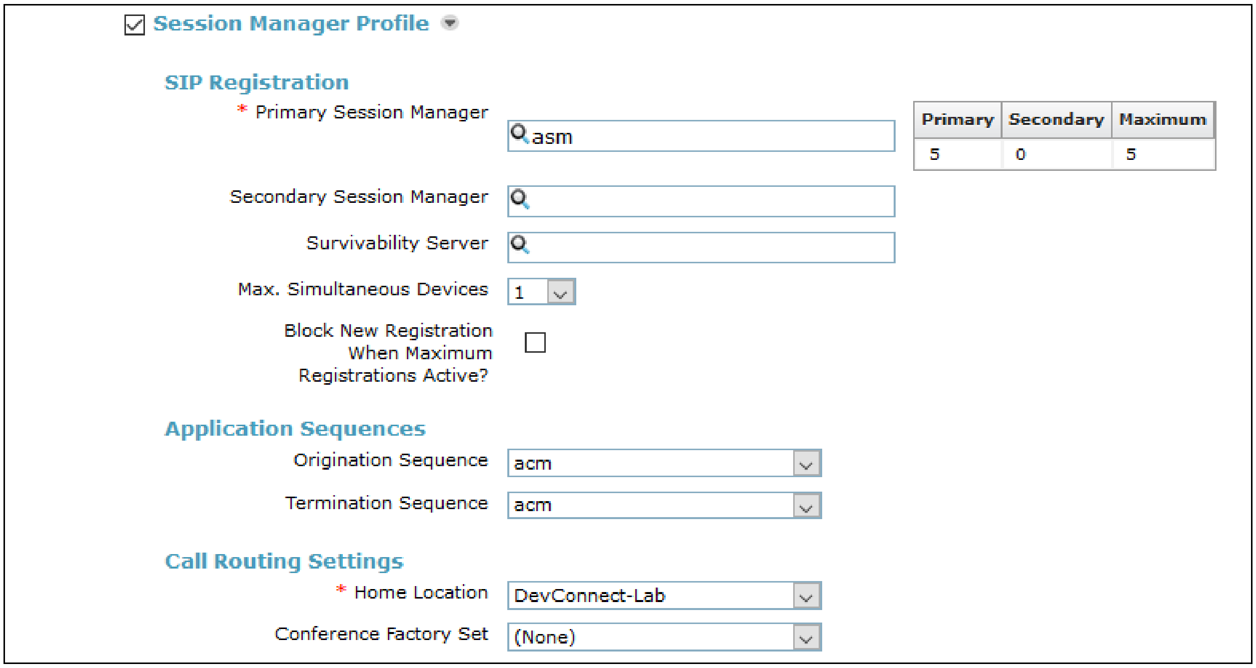
Scroll down to the **Communication Address** section and select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select a SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.

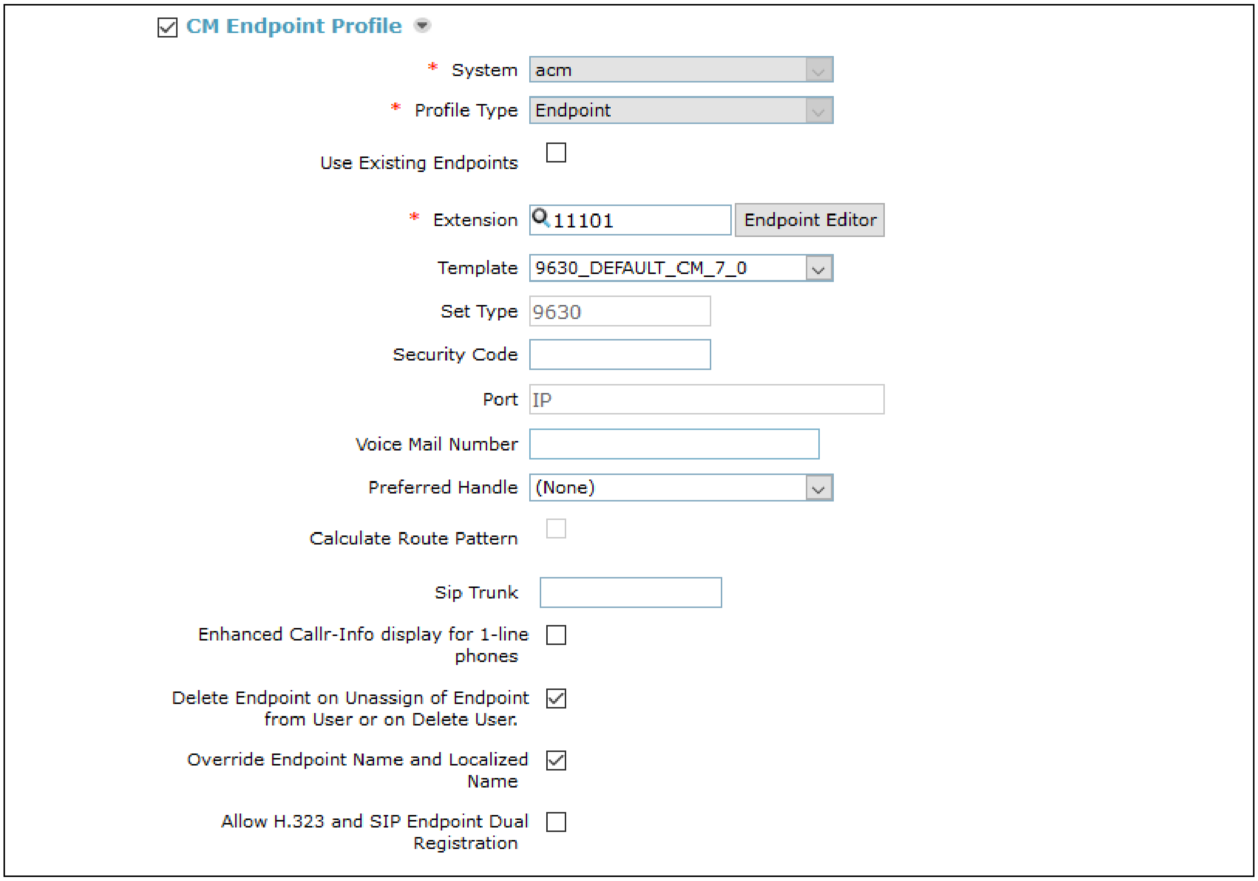


In the *Session Manager Profile* section, specify the Session Manager entity from **Section 6.3.1** for **Primary Session Manager** and assign the **Application Sequence** defined in **Section 6.5** to the new SIP user as part of defining the **SIP Communication Profile**. The **Application Sequence** can be used for both the originating and terminating sequence. Set the **Home Location** field to the **Location** configured in **Section 6.2**.

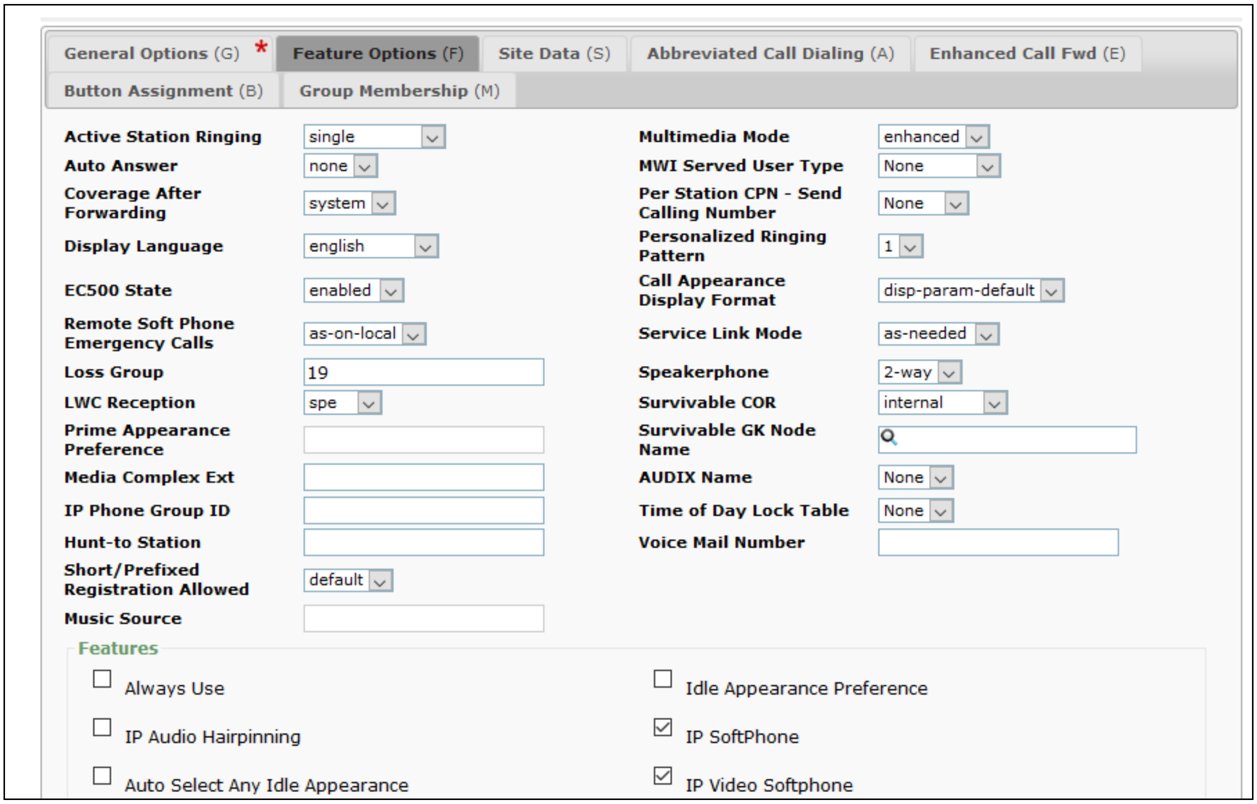


In the **CM Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type** Select *Endpoint*.
- **Use Existing Stations:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for type of SIP phone.



Next, click on the **Endpoint Editor** button by the **Extension** field. The following screen is displayed. In the **Feature Options** section, select **IP Softphone** and **IP Video Softphone** and click **Done**. The user will be returned to the previous screen. Click the **Commit** button to save the new SIP user profile.



6.8 Add Session Manager

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

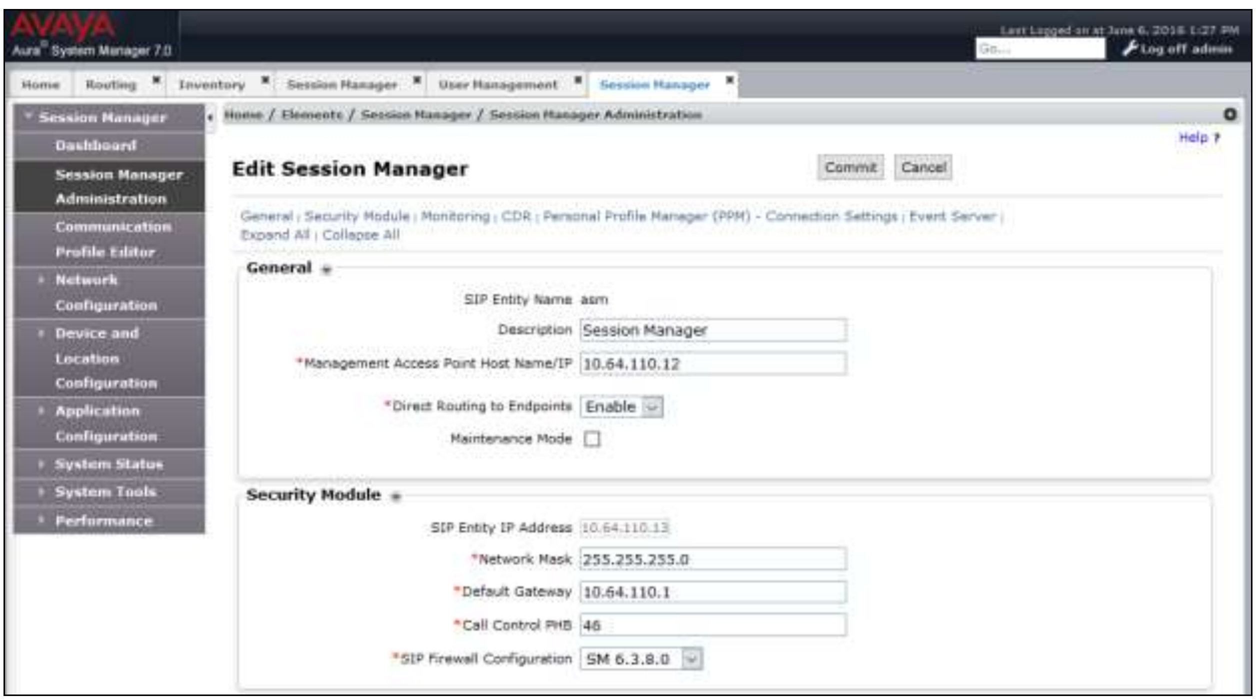
Under *General*:

- **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*:

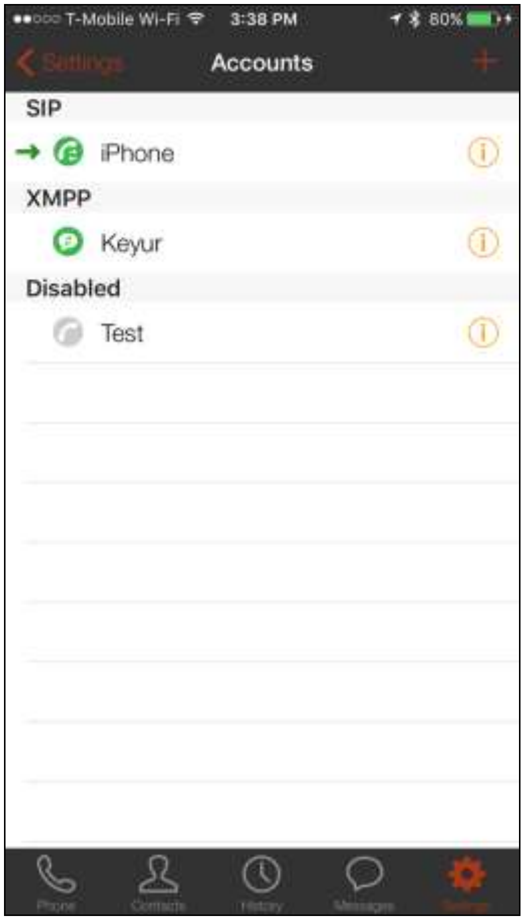
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

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

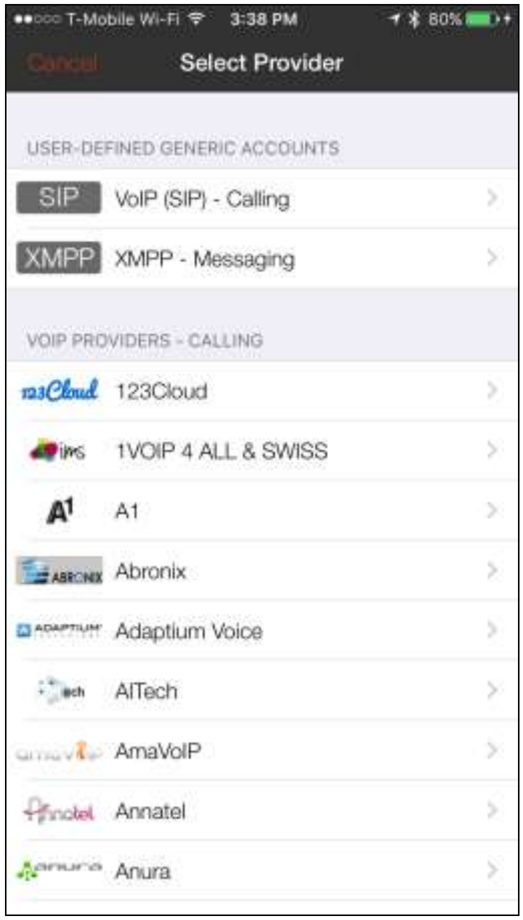


7. Configure Bria Mobile v3.6

Configuration for Bria Mobile v3.6 on iOS and Android is similar. In this document, configuration for Bria Mobile v3.6 for iOS is shown. Once the Bria app is downloaded from the app store, open it and navigate to **Setting → Accounts**. Select **+** to add a new account.



Select **Voice (SIP) – Calling**.



On the **New SIP Account** screen:

- Type in a desired name in the **Display as** field.
- For the **Username** and **Password** fields, provide information from **Section 6.7.**
- Type in the domain from **Section 6.1.**

Continuing from above, scroll down and select **Account Advanced.**

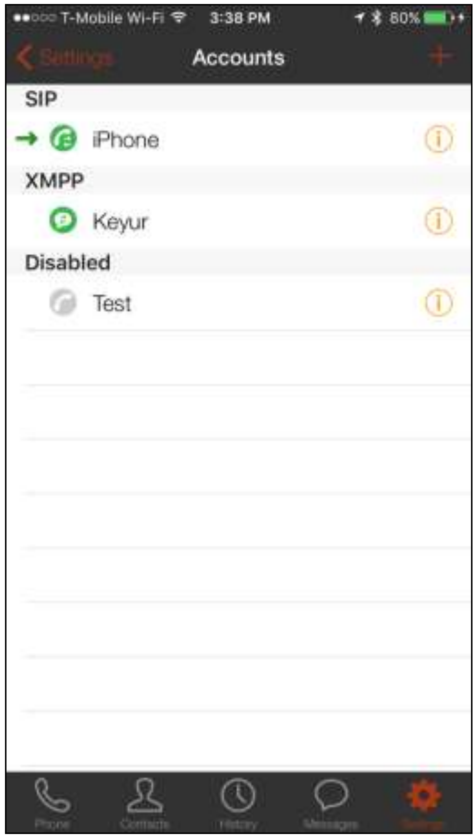
Under **ACCOUNT ADDITIONAL,** type in the Session Manager SIP IP address in **Out. Proxy** and select **Done.**

On the **New SIP Account** screen, toggle the **Enabled** switch and select **Save**.

8. Verification Steps

This section provides the steps that may be performed to verify proper configuration of the Bria Mobile v3.6 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

On the Bria Mobile v3.6, if the registration is successful, the icon on the left of Account Name will turn green.



1. Place an outgoing video call from Bria Mobile v3.6 to another video system registered with Session Manager and verify that the video completes with 2-way audio and video.

2. Place an outgoing voice call from Bria Mobile v3.6 to an Avaya IP telephone and verify that the voice call completes with 2-way audio.

9. Conclusion

These Application Notes have described the administration steps required to integrate the Bria Mobile v3.6 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Bria Mobile v3.6 successfully registered with Session Manager and voice and video calls were established with Avaya one-X® Communicator and Avaya IP telephones. All test cases passed with observations noted in **Section 2.2**.

10. References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager, Release 7.0.1, 03-300509, Issue 2, May 2016*.

[2] *Administering Avaya Aura® Session Manager, Release 7.0.1, Issue 2, May 2016*

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.