**Avaya Solution & Interoperability Test Lab**

# Application Notes for Calix ONT SIP Device with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

## Abstract

These Application Notes describe the configuration of Calix ONT SIP Device with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Session Manager 8.1. The Calix ONT SIP Device runs a native SIP stack and provides analog ports for POTS devices plus Ethernet ports for IP devices. The native SIP stack allows the POTS devices to appear as SIP endpoints and register with Avaya Aura® Session Manager and access telephony features on Avaya Aura® Communication Manager. For the compliance test, a Calix E7 OLT, which serves as an access node, was connected to two Calix 819G ONT SIP Devices via a Gigabit Passive Optical Network (GPON) connection. The Calix E7 OLT also provided Ethernet connectivity to the IP telephony network. This solution is suitable for hotel rooms, where the SIP-enabled POTS phones would reside in the guest rooms.

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 of Calix ONT SIP Device with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Session Manager 8.1. The Calix ONT SIP Device runs a native SIP stack and provides analog ports for POTS devices plus Ethernet ports for IP devices. The native SIP stack allows the POTS devices to appear as SIP endpoints and register with Avaya Aura® Session Manager and access telephony features on Avaya Aura® Communication Manager. For the compliance test, a Calix E7 OLT, which serves as an access node, was connected to two Calix 819G ONT SIP Devices via a Gigabit Passive Optical Network (GPON) connection. The Calix E7 OLT also provided Ethernet connectivity to the IP telephony network.

The Calix E7 OLT (optical line terminal) received SIP and RTP/audio traffic from the IP telephony network and sent the traffic to the appropriate Calix 819G ONT SIP Device, an access endpoint that provides an optical termination at the subscriber premise, and provides subscriber interfaces, such as POTS and Ethernet. This solution is suitable for hotel rooms, where the SIP-enabled POTS phones would reside in the guest rooms.

# 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the POTS phones are the Calix ONT SIP Devices, Avaya H.323 / SIP Deskphones, and the PSTN, and exercising telephony features, such as Hold/Resume, Mute/Unmute, Call Coverage, Call Transfer, and Conference. Additional telephony features, such as Call Forward, Call Pickup, and Call Park/Unpark, were also verified using Communication Manager Feature Access Codes (FACs).

The serviceability testing focused on verifying that Calix ONT SIP Devices would come back into service after rebooting the Calix E7 OLT and Calix ONT SIP Devices, re-connecting the fiber connection to the ONT SIP Devices, and re-connecting re-establishing IP network connectivity to the Calix E7 OLT.

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 this Application Note, the interface between Avaya systems and Calix ONT SIP Devices did not include use of any specific encryption features as requested by Calix.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of the ONT SIP Devices with Session Manager.
- Calls between POTS phones on ONT SIP Devices and Avaya H.323 / SIP Deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between POTS phones on ONT SIP Devices and the PSTN.
- Calls between Avaya H.323 / SIP Deskphones connected to an Ethernet port on the ONT SIP Devices and POTS phones on the ONT SIP Devices.
- G.711 and G.729 codec support.
- Proper recognition of DTMF tones.
- T.38 Fax using a desktop PC connected to a Voice (i.e., POTS) port on the ONT SIP Device using an analog modem.
- Basic telephony features, including Hold, Mute, Redial, multiple calls, Blind and Supervised Transfer, and Attended Conference.
- Extended telephony features using Communication Manager FACs for Call Forward, Call Park/Unpark, and Call Pickup.
- Hospitality features, such as wakeup calls, dialing Housekeeping Status FACs, and Calix Direct Connect (Hot Line) feature.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve voice messages.
- Proper system recovery after restarting the ONT SIP Devices and E7 OLT, re-connecting GPON connection between ONT SIP Devices and E7 OLT, and re-establishing E7 OLT IP network connectivity.

## 2.2. Test Results

All test cases passed with the following observation:

- Direct IP Media (Shuffling) is not supported when Avaya H.323 / SIP Deskphones are connected to an Ethernet port on the Calix ONT SIP Device. If the solution is used in this way, Direct IP Media should be disabled for the SIP user.

## 2.3. Support

For Calix ONT SIP Device technical support, contact Calix Support Services via phone or website.

- **Phone:** 1 (408) 514-3000
- **Web:** https://www.calix.com/services/support-services.html

# 3. Reference Configuration

**Figure 1** illustrates a sample configuration with an Avaya SIP-based network that includes the Calix E7 OLT and two Calix 819G ONT SIP Devices. The Calix E7 OLT receives SIP and RTP/audio traffic from the IP network and routes/terminates it on one of the Calix 819G ONT SIP Devices, where POTS phones are connected. In other words, the SIP connectivity is between Session Manager and the Calix 819G ONT SIP Devices.

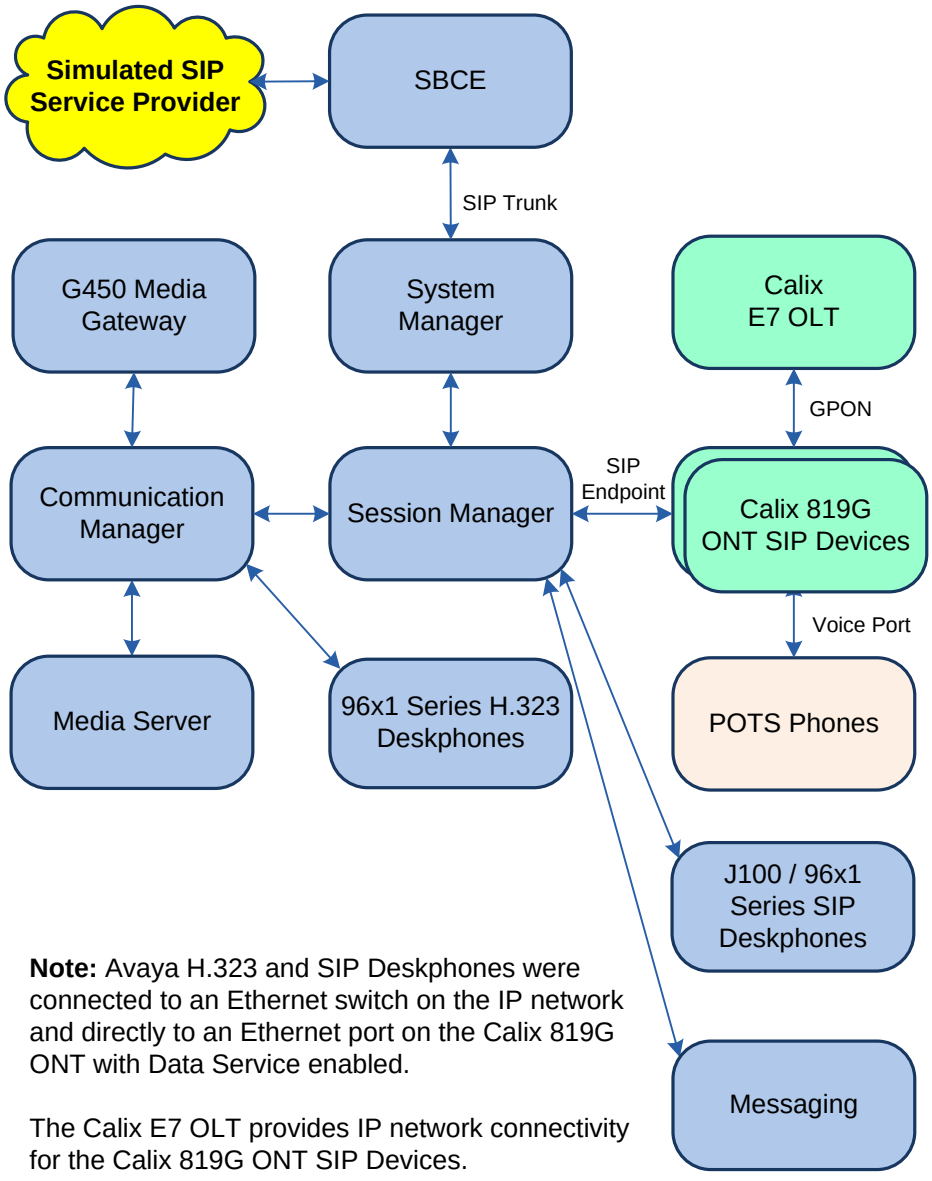



**Figure 1: Avaya SIP Telephony Network with Calix E7 OLT and Calix ONT SIP Devices**

# 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| Avaya Aura® Communication Manager | 8.1.3.1.0-FP3SP1 |
| Avaya G450 Media Gateway | FW 41.24.0 |
| Avaya Aura® Media Server | v.8.0.2.138 |
| Avaya Messaging | 10.8.2 SP1 |
| Avaya Aura® System Manager | 8.1.3.1<br>Build No. – 8.1.0.0.733078<br>Software Update Revision No:<br>8.1.3.1.1012493<br>Service Pack 1 |
| Avaya Aura® Session Manager | 8.1.3.1.813113 |
| Avaya 96x1 Series IP Deskphone | 6.8502 (H.323)<br>7.1.13.0.4 (SIP) |
| Avaya J100 Series SIP Deskphone | 4.0.9.0.4 |
| Calix E7 OLT | 3.4.10.35 |
| Calix 819G ONT SIP Devices | 1.5.4.13.110 |

# 5. Configure Avaya Aura® Communication Manager

This section describes the configuration of a SIP trunk to Session Manager and routing calls to ONT SIP Devices. Administration of Communication Manager was performed using the System Access Terminal (SAT). The following configuration is covered:

- **Optional Features** to verify Communication Manager license.
- **IP Node Names** to associate names with IP addresses.
- **IP Codec Set** to specify the codec type used for calls to ONT SIP Devices.
- **IP Network Region** to specify the SIP domain name, the IP codec set, and enable IP-IP direct audio (i.e., Shuffling).
- **SIP trunk** for calls towards Session Manager and ONT SIP Devices.
- **Private Numbering** to allow the caller's extension to be sent over the SIP trunk.
- **Call Routing** to route calls to ONT SIP Devices using AAR.

## 5.1. Verify Communication Manager License

Using the SAT, verify that the Off-PBX Telephones (OPS) option is 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, including ONT SIP Devices, that will be deployed.

```
display system-parameters customer-options                    Page   1 of  12
                              OPTIONAL FEATURES

     G3 Version: V18                              Software Package: Enterprise
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                          USED
                                 Platform Maximum Ports: 48000   107
                                      Maximum Stations: 36000    36
                                 Maximum XMOBILE Stations: 36000     0
                     Maximum Off-PBX Telephones - EC500: 41000     0
                     Maximum Off-PBX Telephones -   OPS: 41000    22
                     Maximum Off-PBX Telephones - PBFMC: 41000     0
                     Maximum Off-PBX Telephones - PVFMC: 41000     0
                     Maximum Off-PBX Telephones - SCCAN:     0     0
                          Maximum Survivable Processors: 313       0



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

## 5.2. Administer IP Node Names

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

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
devcon-aes          10.64.102.119
devcon-ams          10.64.102.118
devcon-sm           10.64.102.117
procr               10.64.102.115
procr6              ::

( 6  of 6    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

## 5.3. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to ONT SIP Devices. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU and G.729 codecs were verified. The following IP codec set is configured with G.711MU.

Media encryption was enabled for Avaya IP Deskphones. ONT SIP Devices weren't configured to support SRTP, so the *none* option was also included under **Media Encryption**.

```
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: none
 3:
 4:
 5:
```

## 5.4. 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 ONT SIP Devices and IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya 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. 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       NR Group: 1
Location: 1       Authoritative Domain: avaya.com
    Name:                      Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
      Codec Set: 1             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 50999
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

## 5.5. Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify the Ethernet processor (*procr*) of Communication Manager and 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 are taken from the **IP Node Names** form in **Section 5.1**.
- 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.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

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

```
add signaling-group 10                                        Page   1 of   2
                              SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
       Q-SIP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                Far-end Node Name: devcon-sm
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

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

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to ONT SIP Devices and Avaya SIP deskphones. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling**

**Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 10                                          Page   1 of  5
                               TRUNK GROUP

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

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

```
add trunk-group 10                                          Page   3 of  5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y

   Suppress # Outpulsing? n  Numbering Format: private
                                             UUI Treatment: service-provider
                                           Maximum Size of UUI Contents: 128
                                              Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n

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

 Show ANSWERED BY on Display? y
```

On **Page 4** of the trunk group form, the default settings were used as shown below.

```
add trunk-group 10                                          Page   5 of  5
                             PROTOCOL VARIATIONS

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

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

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

## 5.6. Configure Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '7' whose calls are routed over any trunk group, including SIP trunk group 10, have their extension sent.

```
change private-numbering 0                                    Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

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

## 5.7. AAR Call Routing

Configure the uniform dial plan table to route calls using AAR for dialed digits that are 5-digits long and begin with '78'. This would cover call routing to ONT SIP Devices extensions (i.e., 78010 – 78012) and Avaya SIP deskphones.

```
change uniform-dialplan 7                                     Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                            Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits     Net Conv Num
 78              5   0                   aar  n
```

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits beginning with "78" to route pattern 10 as shown below. Note that the **Call Type** was set to *lev0*. This routes calls to Avaya SIP stations and to ONT SIP Devices.

```
change aar analysis 7                                         Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    7                     7    7     254      aar          n
    78                    5    5     10       lev0         n
    8                     7    7     254      aar          n
    9                     7    7     254      aar          n
                                                n
                                                n
```

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

```
change route-pattern 10                                          Page   1 of   3
                  Pattern Number: 10     Pattern Name: To devcon-sm
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                          QSIG
                              Dgts                                Intw
 1: 10   0                                                         n   user
 2:                                                                n   user
 3:                                                                n   user
 4:                                                                n   user
 5:                                                                n   user
 6:                                                                n   user

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

# 6. Configure Avaya Aura® Session Manager

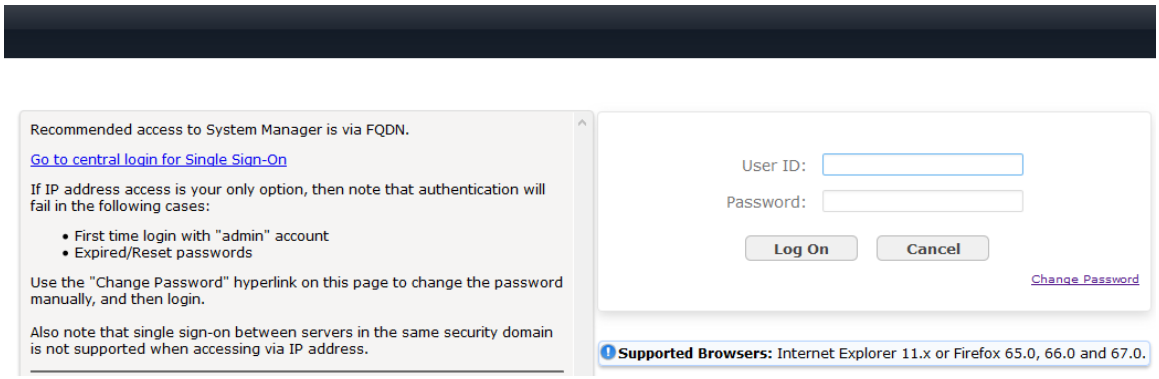
This section covers the procedure for adding a SIP user in Session Manager. The configuration covers:

- Launch System Manager
- Set Network Transport Protocol for ONT SIP Devices
- Administer SIP User

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

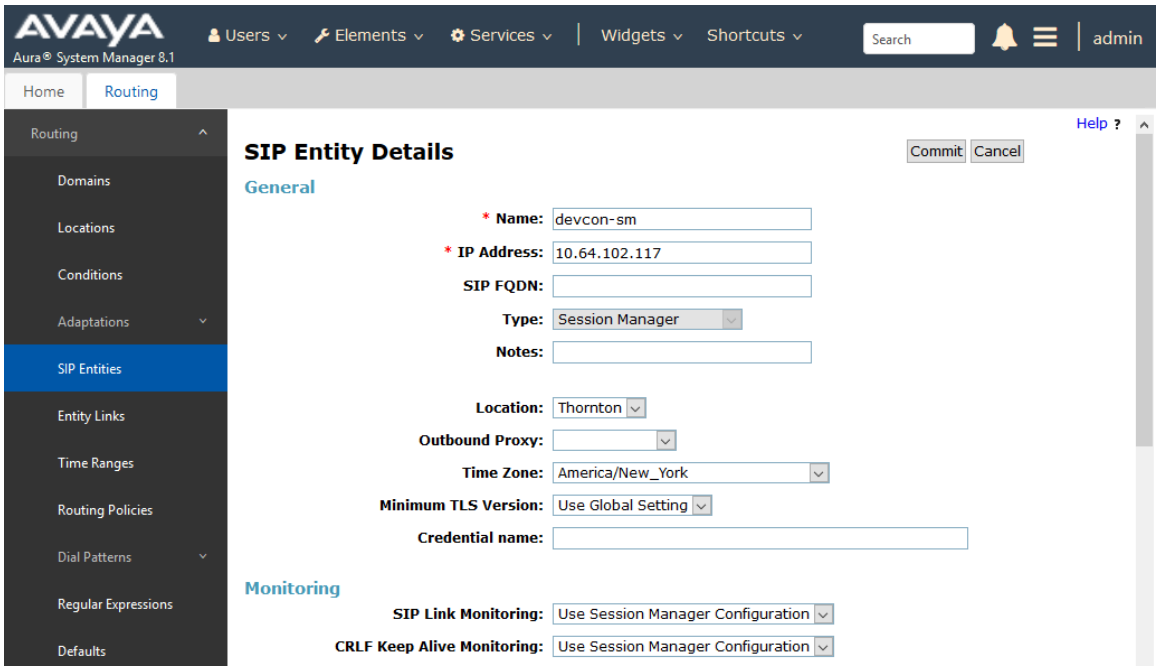
## 6.1. Launch System Manager

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

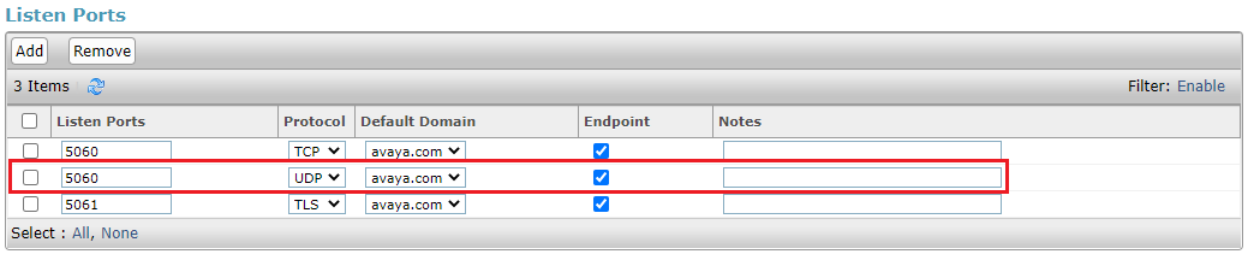


## 6.2. Set Network Transport Protocol for ONT SIP Devices

From the System Manager **Home** screen, select **Elements → Routing → SIP Entities** and edit the SIP Entity for Session Manager shown below.

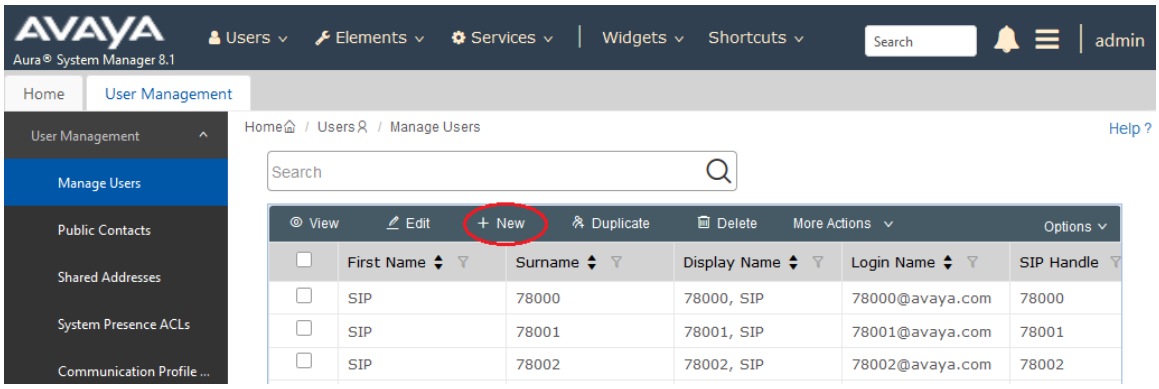



Scroll down to the **Listen Ports** section and verify that the transport network protocol used by ONT SIP Devices is specified in the list below. For the compliance test, the solution used UDP network transport. Avaya SIP deskphones used TLS.



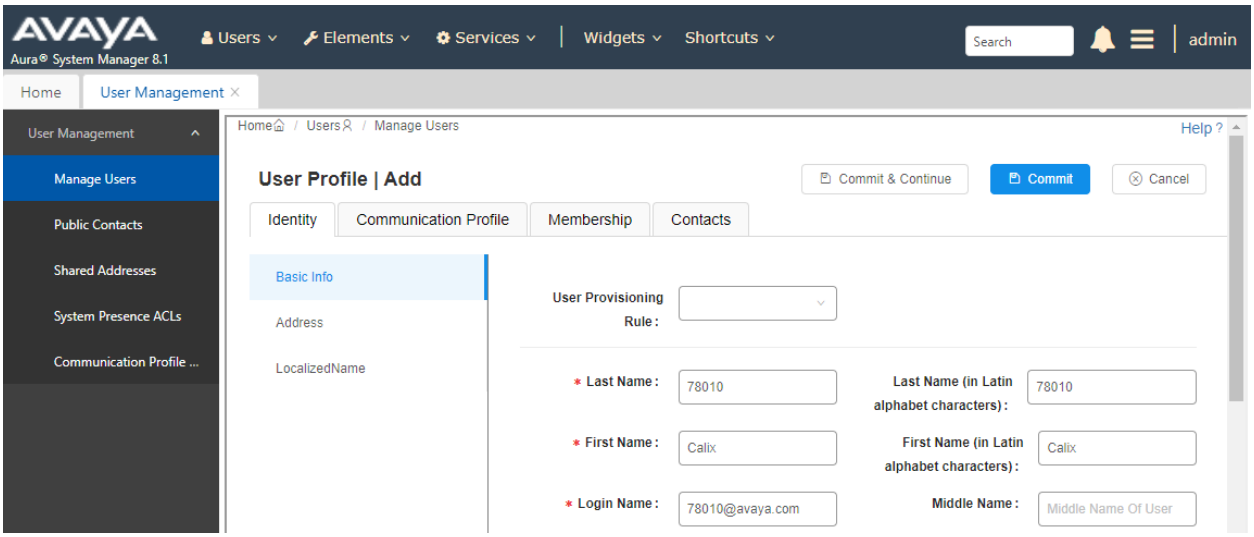
## 6.3. Administer SIP User

In the subsequent screen (not shown), select **Users → User Management → Manage Users** to display the **User Management** screen below. Click **New** to add a user.



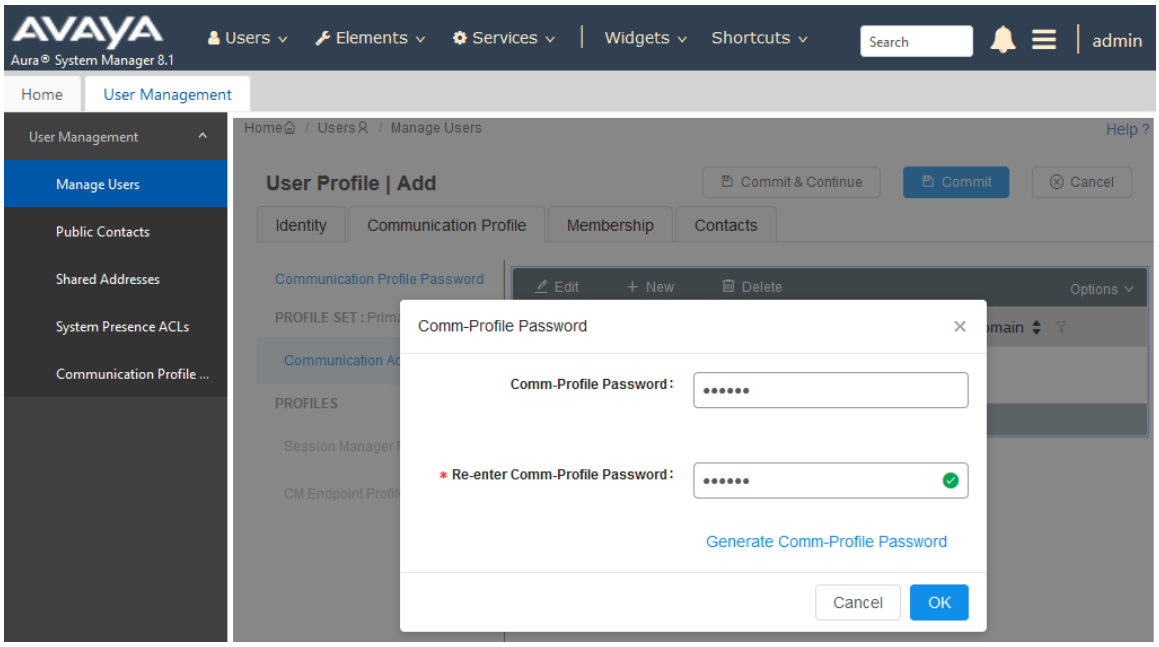

### 6.3.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter *<extension>@<domain>*, where *<extension>* is the desired ONT SIP Device SIP extension and *<domain>* is the applicable SIP domain name from **Section 5.4**. Retain the default values in the remaining fields.



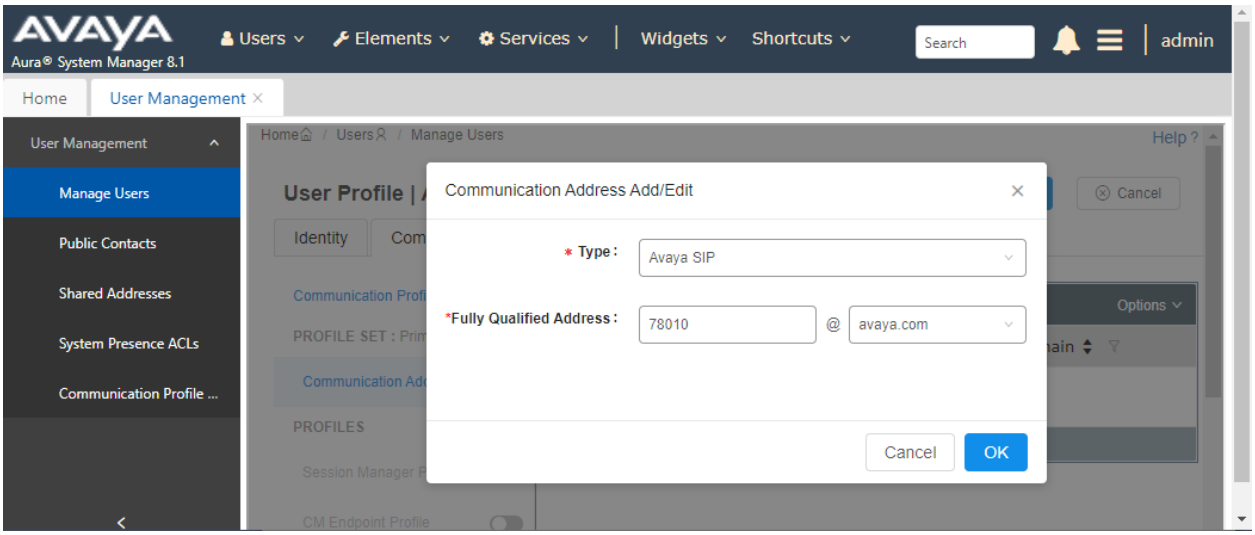
### 6.3.2. Communication Profile

Select the **Communication Profile** tab. Next, click on **Communication Profile Password**. For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user to use for registration to be used in the configuration in **Section 7.4**. Click **OK**.



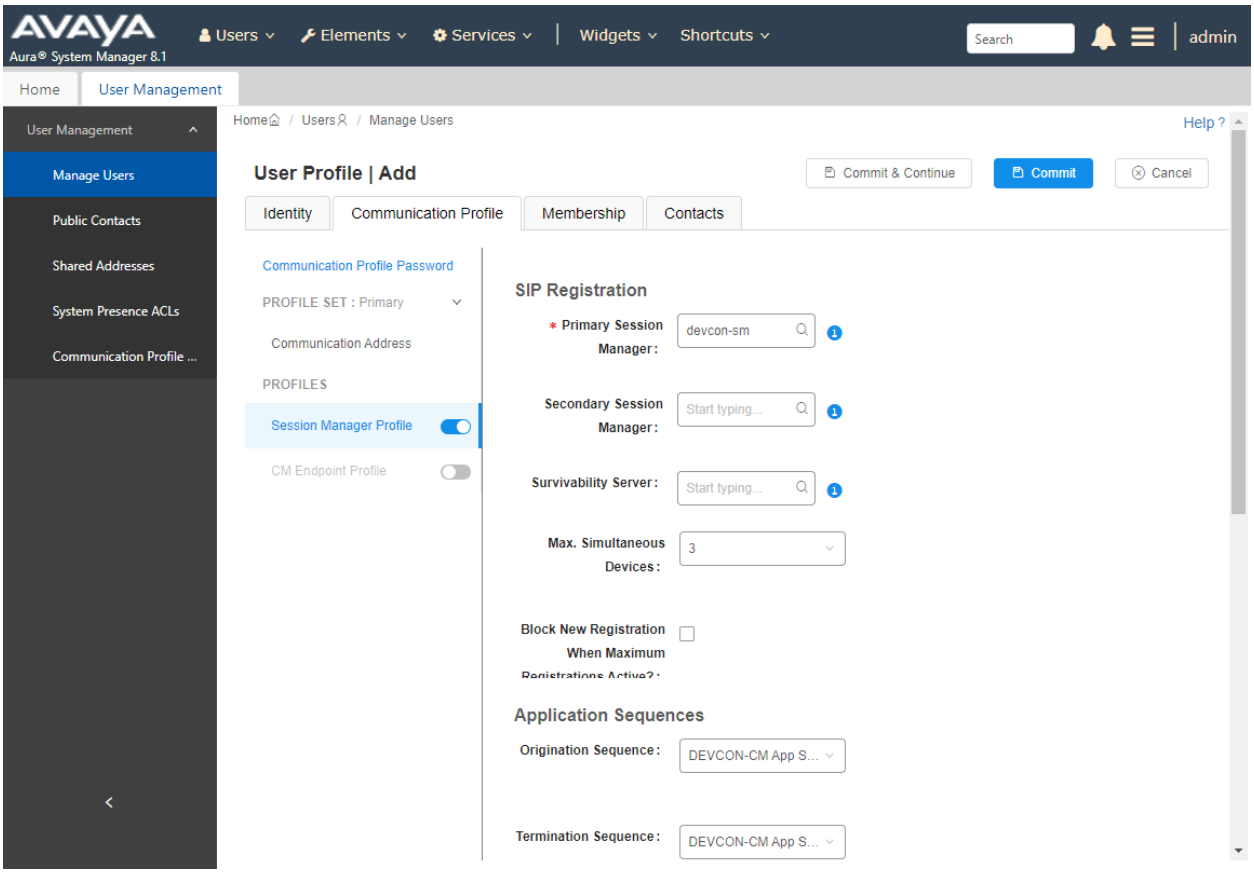
### 6.3.3. Communication Address

Click on **Communication Address** and then click **New** to add a new entry. The **Communication Address Add/Edit** dialog box is displayed as shown below. For **Type**, retain *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension and select the domain name to match the login name from **Section 6.3.1**. Click **OK**.

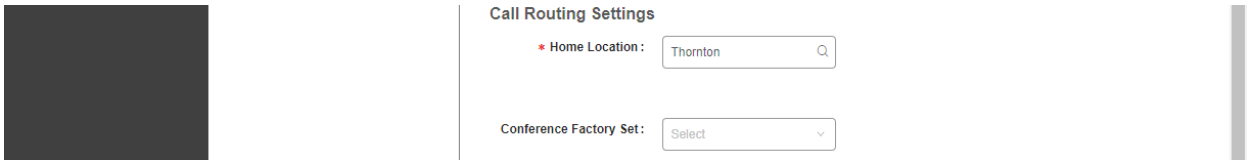


### 6.3.4. Session Manager Profile

Click on toggle button by **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

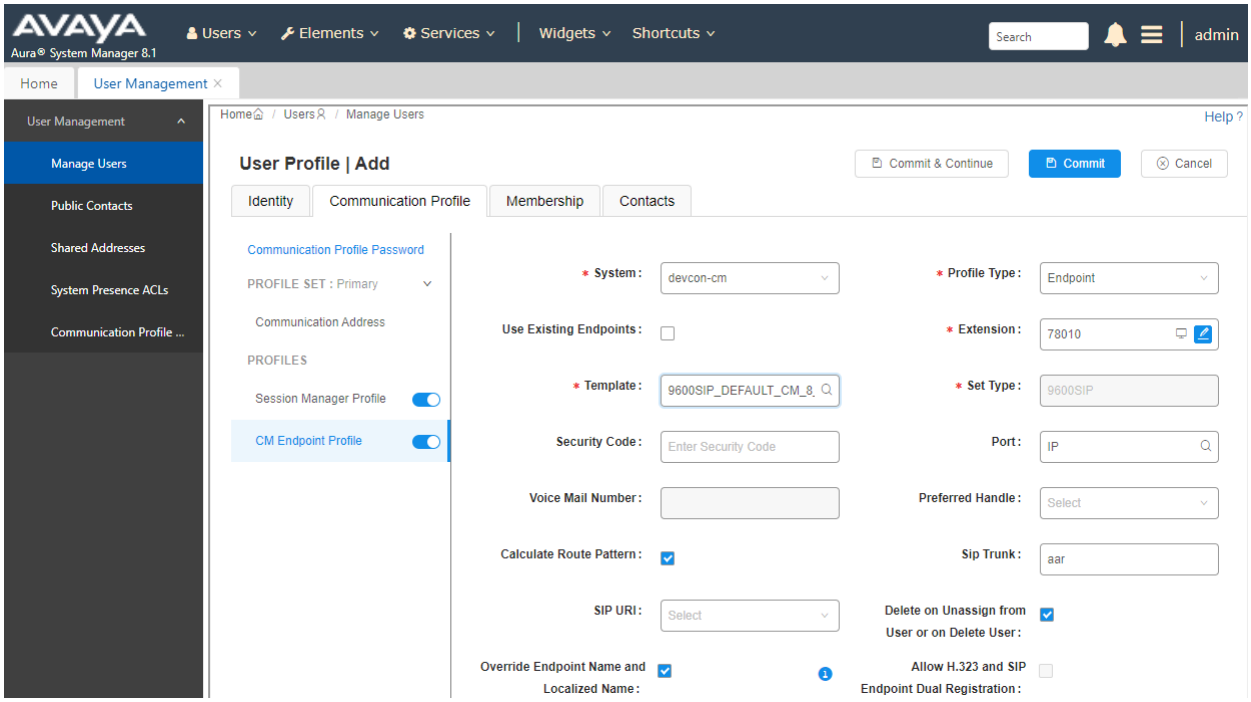



Scroll down to the **Call Routing Settings** section to configure the **Home Location**.

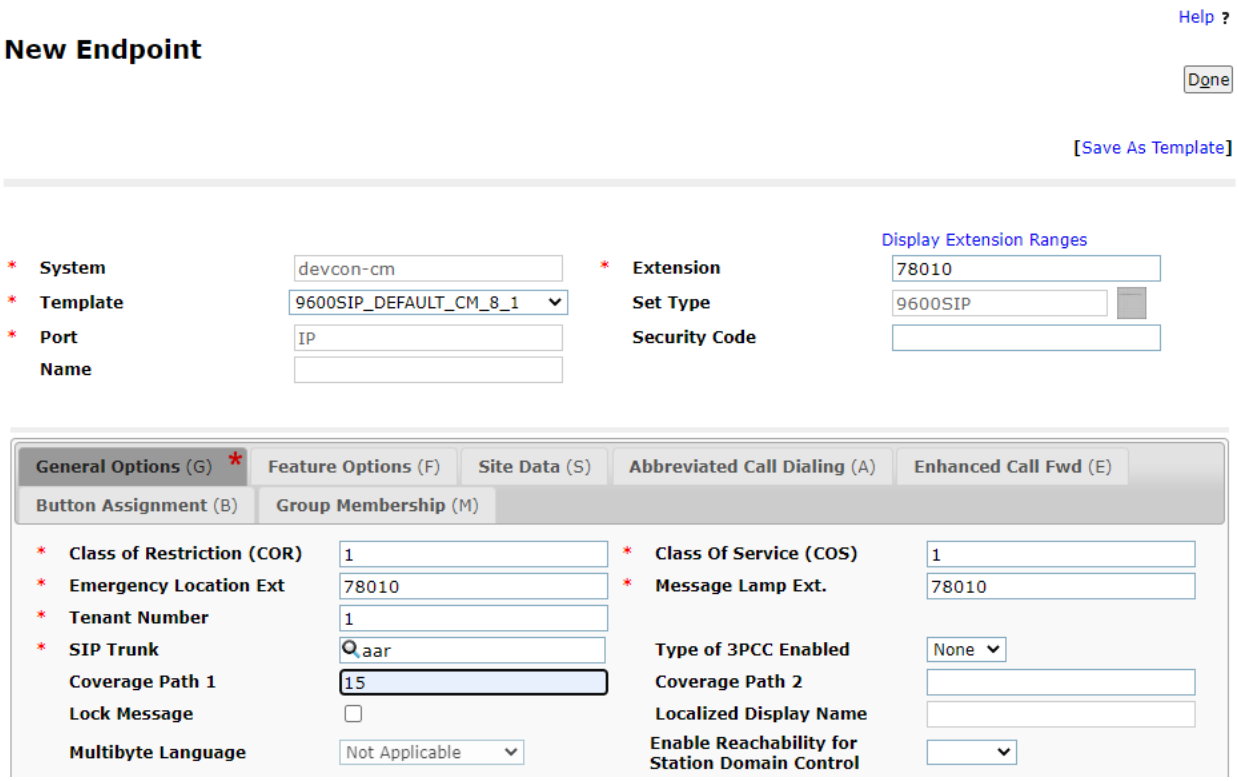


### 6.3.5. CM Endpoint Profile

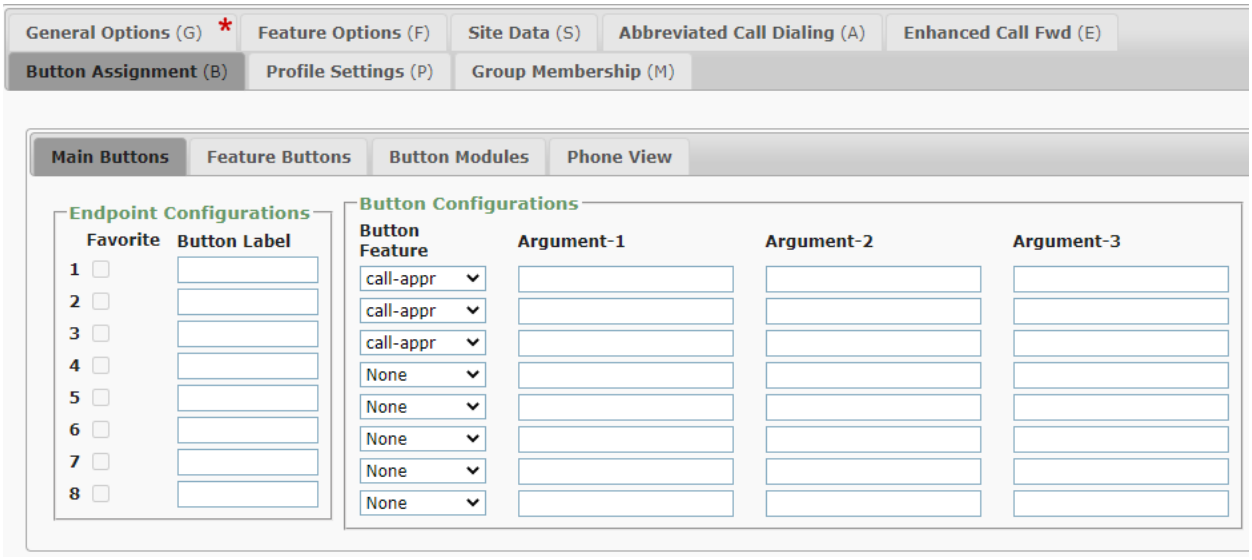
Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.1**. For **Template**, select *9600SIP_DEFAULT_CM_8_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields. Click on **Endpoint Editor** (i.e, Edit icon in **Extension** field) to configure the **Coverage Path**.



Navigate to the **General Options** tab and set the **Coverage Path 1** field to the voicemail coverage path. This provides voicemail coverage for the SIP user. In this example, coverage path 15 was used.




In the **Button Assignment** tab, select the **Main Buttons** sub-tab and accept the default settings with three call appearances.



# 7. Configure Calix ONT SIP Device

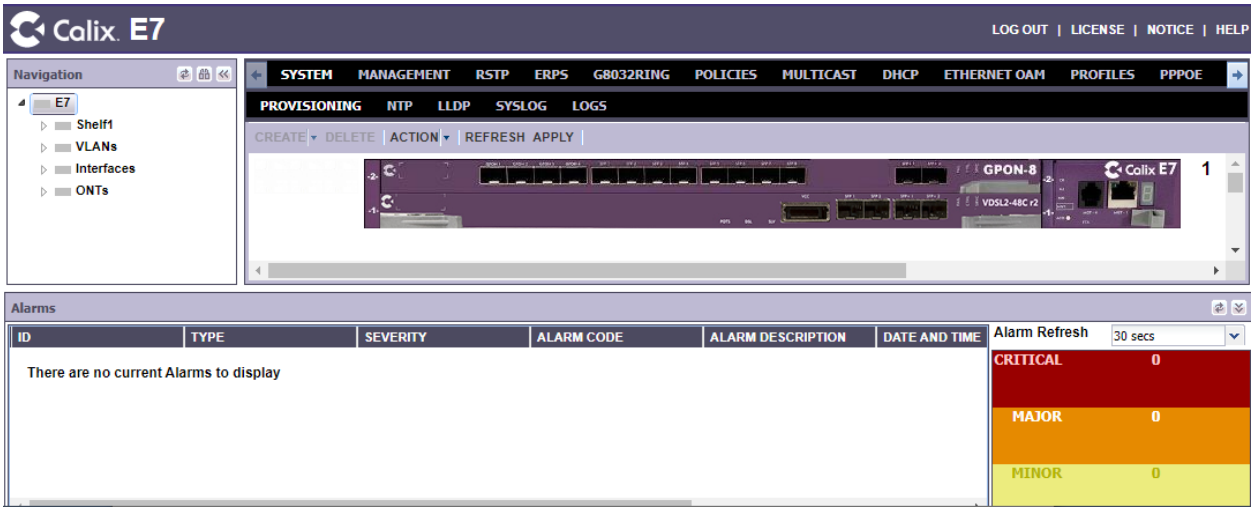
This section provides the procedure for configuring the ONT SIP Device and provide SIP connectivity to Session Manager. Configuration for ONT SIP Device is performed via Calix E7 Unified Access Web Interface.

- Log into Calix E7 Unified Access Web Interface
- Configure ONT SIP Device IP Address
- Configure SIP Gateway
- Configure ONT SIP Device
- Configure Dial Plan

## 7.1. Log into Calix E7 Unified Access Web Interface

Access the Caklix E7 Unified Access Web Interface by using the URL https://<*ip-address*> in an Internet browser, where <*ip-address*> is the E7 OLT IP address. Log in using the appropriate credentials.

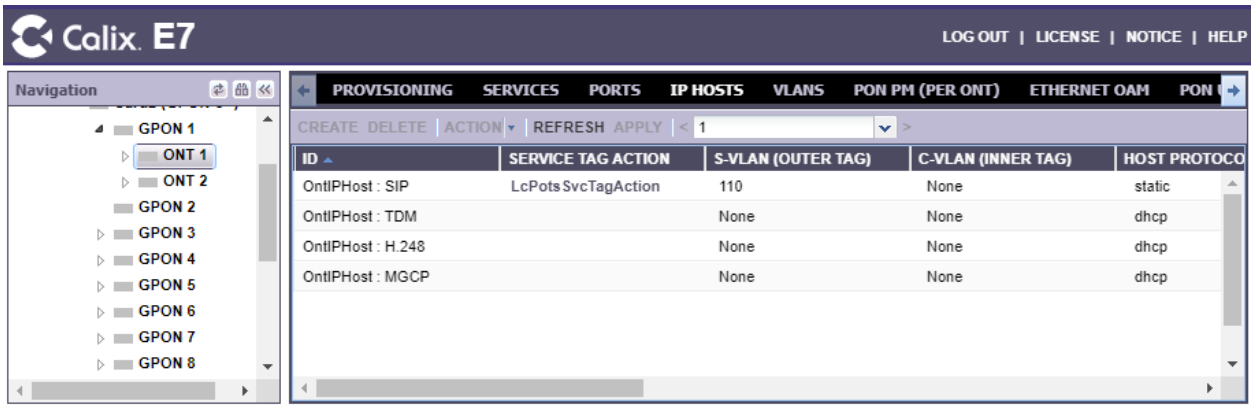
Once logged in, the following screen is displayed.



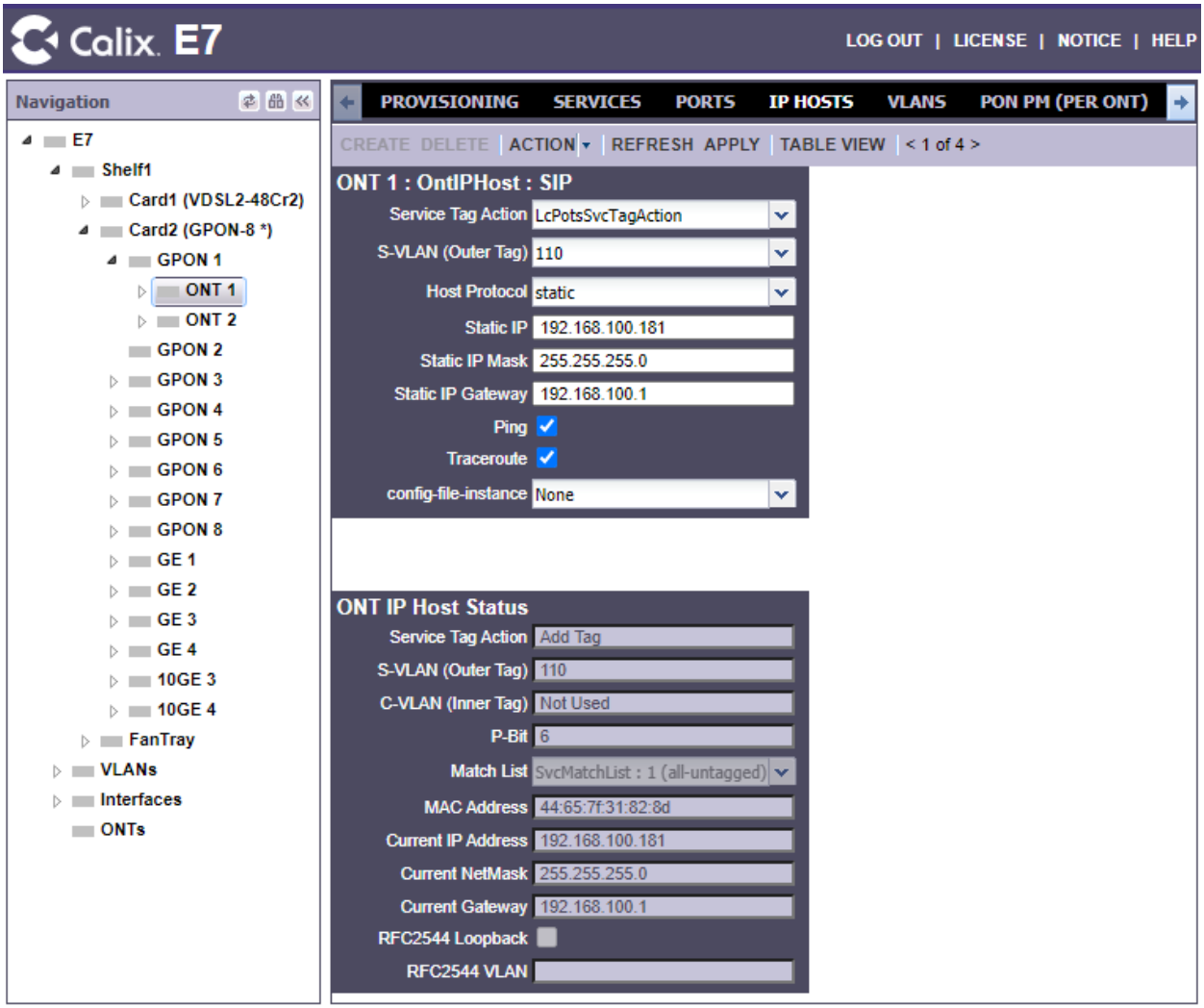
## 7.2. Configure ONT SIP Device IP Address

Configure a **Service Tag Action Profile**. Navigate to **PROFILES → SERVICE → TAGGING → TAG ACTIONS → PROFILES** and click **Create** to add a **Service Tag Action**. Specify a **Name** (e.g., *LcPotsSvcTagAction*) and set the remaining fields as shown below.


In the left pane, navigate to **E7 → Shelf1 → Card2 (GPON-8) → GPON 1 → ONT 1** and click on **IP Hosts** to display the screen below. Click **Create** to add a SIP IP Host associated with the **Service Tag Action**, *LcPotsSvcTagAction*, created above, if it doesn't exist in the list.



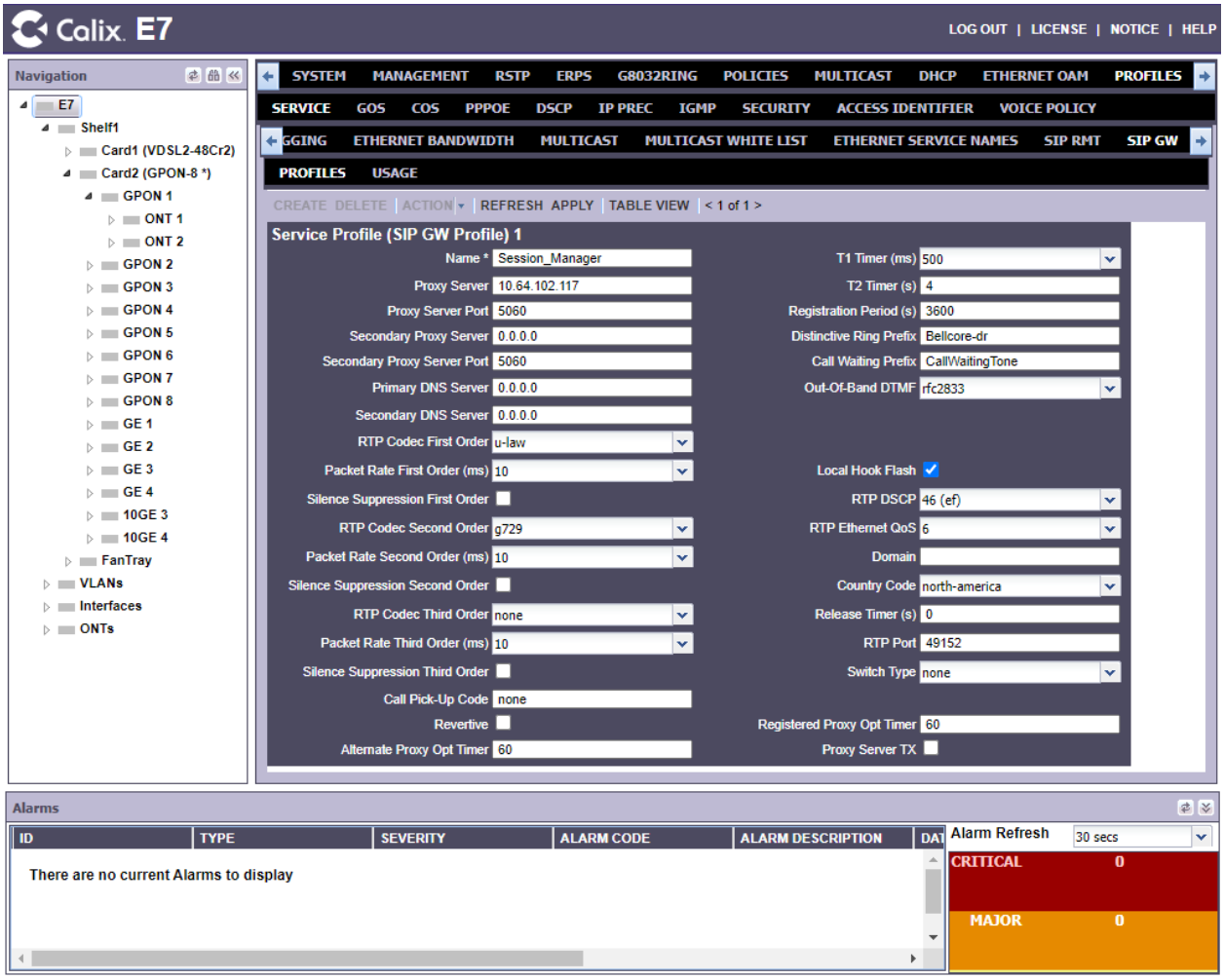
In the SIP IP Host, Set the **Service Tag Action** to *LcPotsSvcTagAction* created above and set the Static IP (e.g., *192.168.100.181*) associated with the ONT SIP Device. Configure the **Static IP Mask** and **Static IP Gateway** as appropriate for the local network.



## 7.3. Configure SIP Gateway

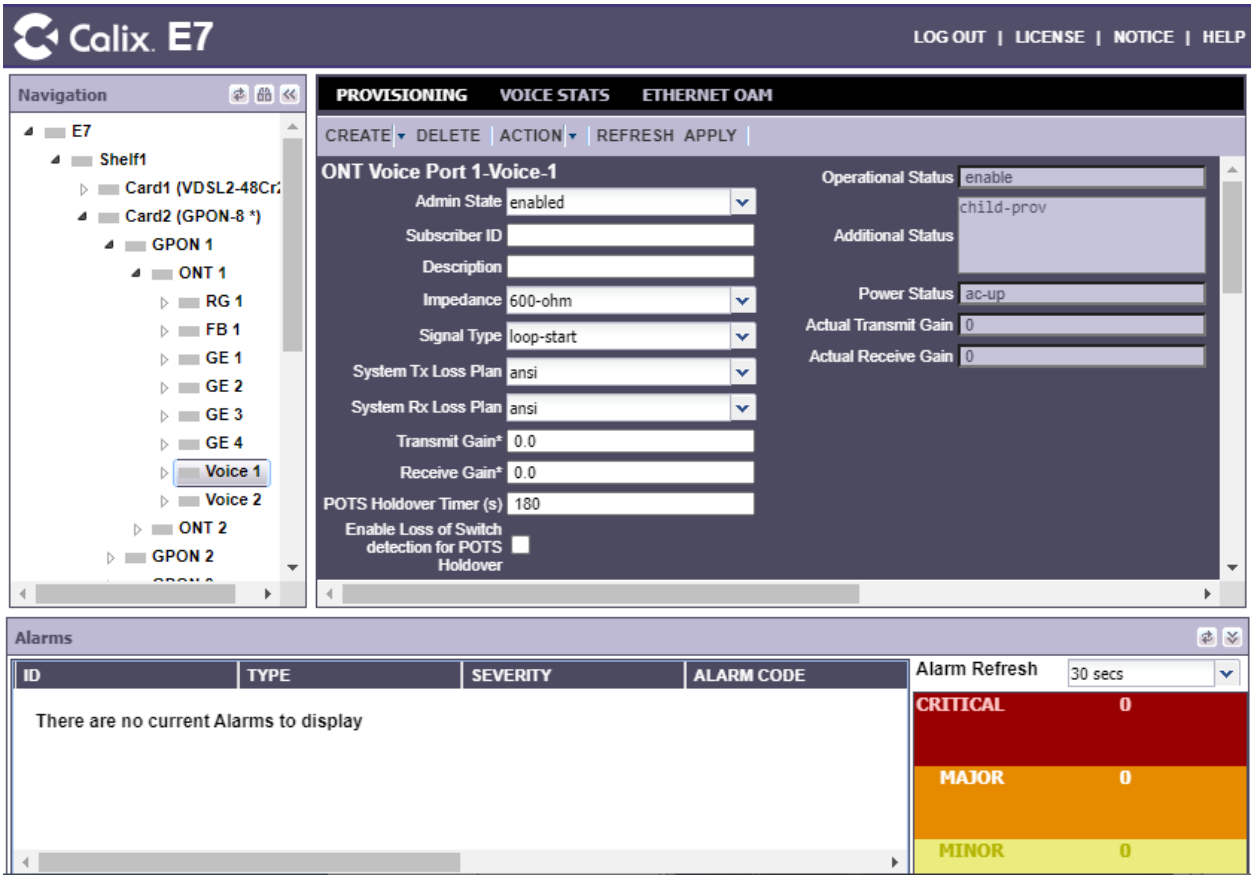
From E7 Unified Access, navigate to **PROFILES → SERVICE → SIP GW** to configure Session Manager as the SIP gateway and specify the supported codecs. On this screen, click **Create** and configure the following parameters:

- **Name:** Provide a descriptive name (e.g., *Session_Manager*).
- **Proxy Server:** Set to Session Manager signaling IP address.
- **Proxy Server Port:** Set to SIP port (e.g., *5060*).
- **RTP Codec First Order:** Set to first preference codec (e.g., *u-law*).
- **RTP Codec Second Order:** Set to second preference codec (e.g., *g729*).
- **Out-of-Band DTMF:** Set to *rfc2833*.
- **Release Timer (s):** Set to *0* so that call is dropped immediately when the POTS phone on the ONT SIP Device hangs up.



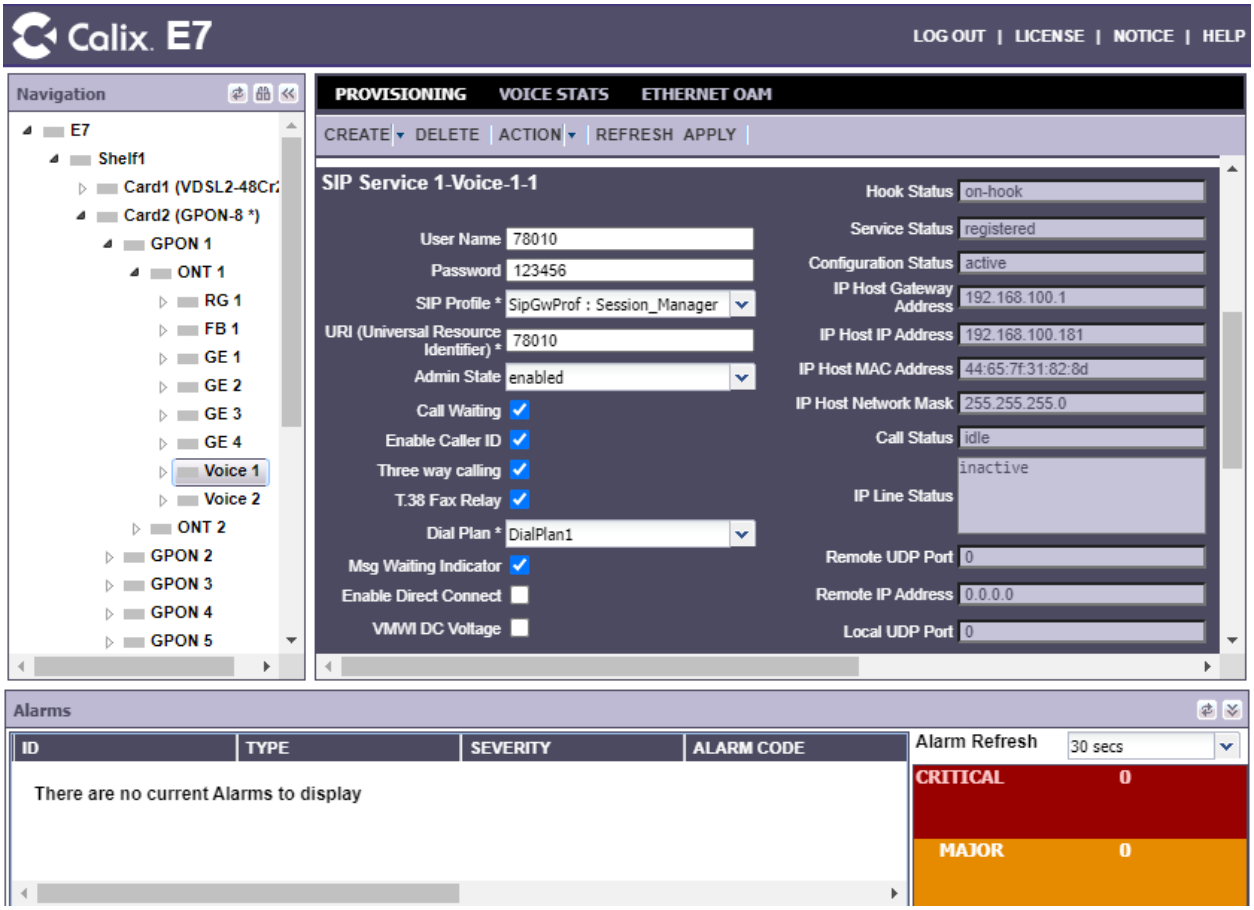
## 7.4. Configure ONT SIP Device

In the left pane, navigate to **E7 →Shelf1 →Card2 (GPON-8) → ONT 1 → Voice 1** to configure the ONT SIP Device SIP extension and features. In the **ONT Voice Port 1-Voice 1** section, set the **Admin State** to *enabled* as shown below.



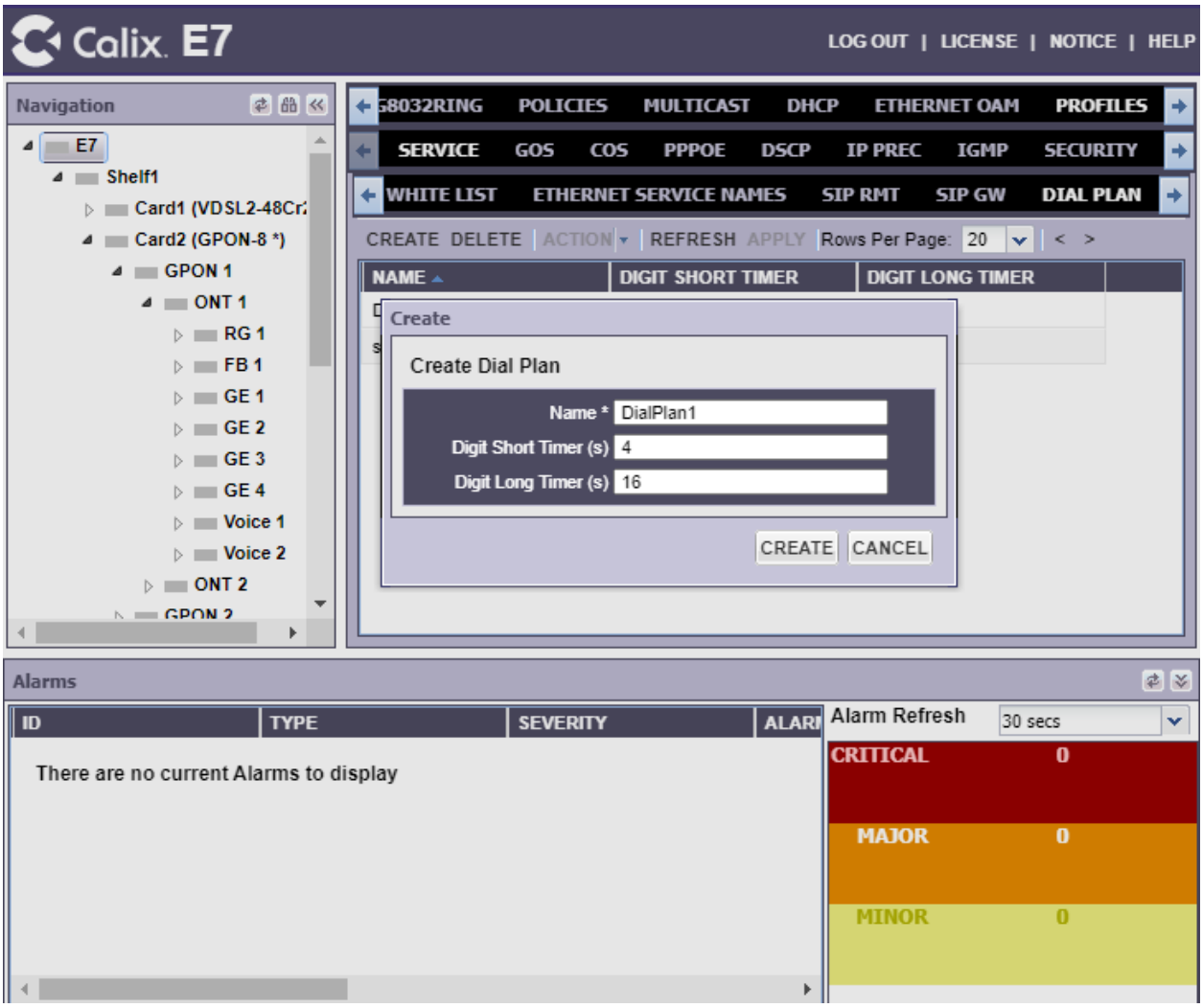
Scroll down to the **SIP Service 1-Voice 1** section and set the following parameters:

- **User Name:** Set to SIP extension (e.g., *78010*).
- **Password:** Specify SIP password configured in **Section 6.3.2**.
- **SIP Profile:** Select the SIP Gateway Profile configured in **Section 7.2**.
- **URI (Universal Resource Identifier):** Set to SIP extension (e.g., *78010*).
- **Admin State:** Set to *enabled*.
- **Call Waiting:** Enable Call Waiting.
- **Enable Caller ID:** Enable Caller ID.
- **Three way calling:** Enable Three way calling.
- **T.38 Fax Relay:** Enable T.38 Fax Relay.
- **Dial Plan:** Select the Dial Plan configured in **Section 7.5**.
- **Msg Waiting Indicator:** Enable MWI.
- **Enable Direct Connect:** Enable Direct Connect, if desired. If enabled, Three way calling must be disabled. Direct Connect allows the POTS device to automatically connect to a specified number when it goes off-hook.

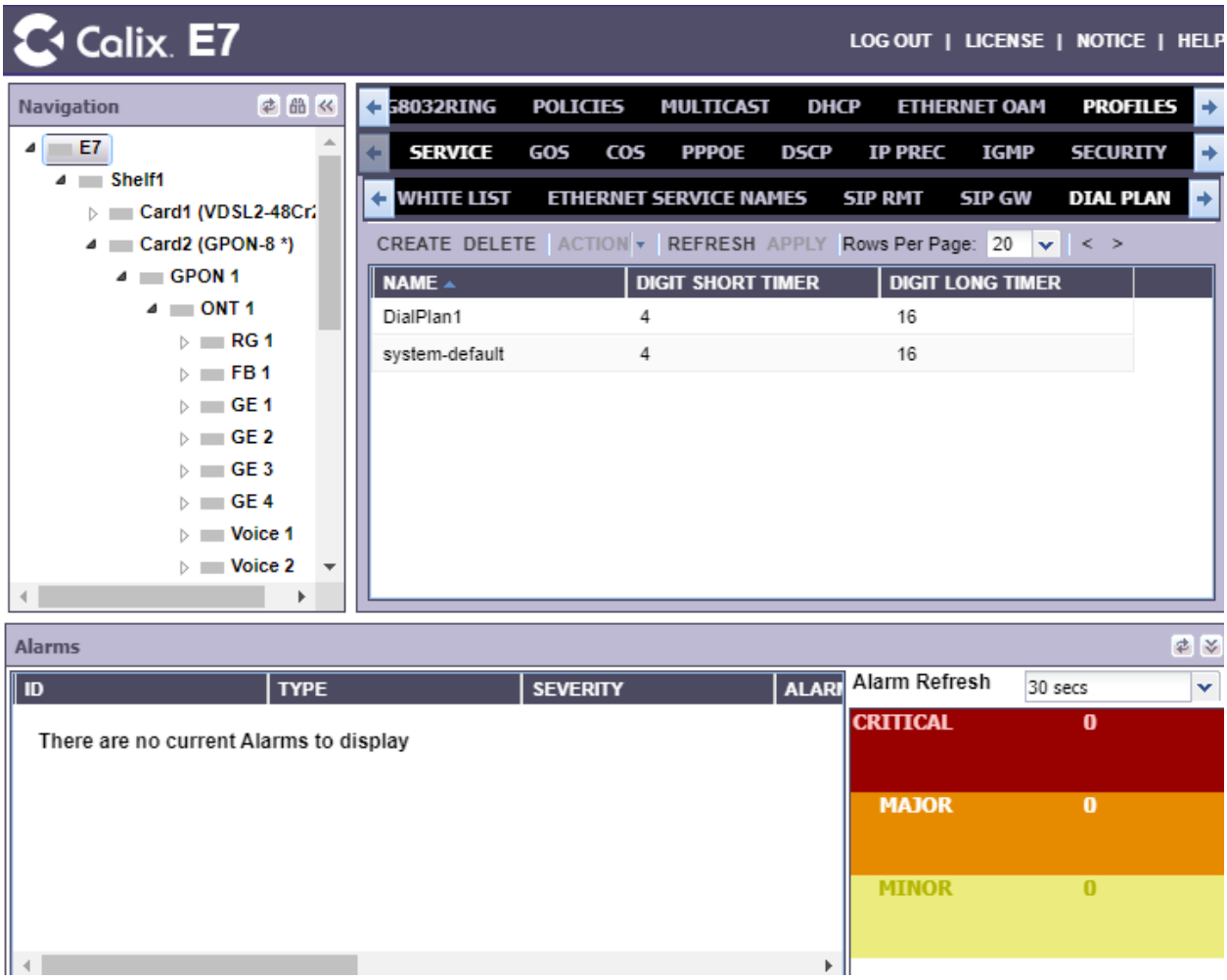


## 7.5. Configure Dial Plan

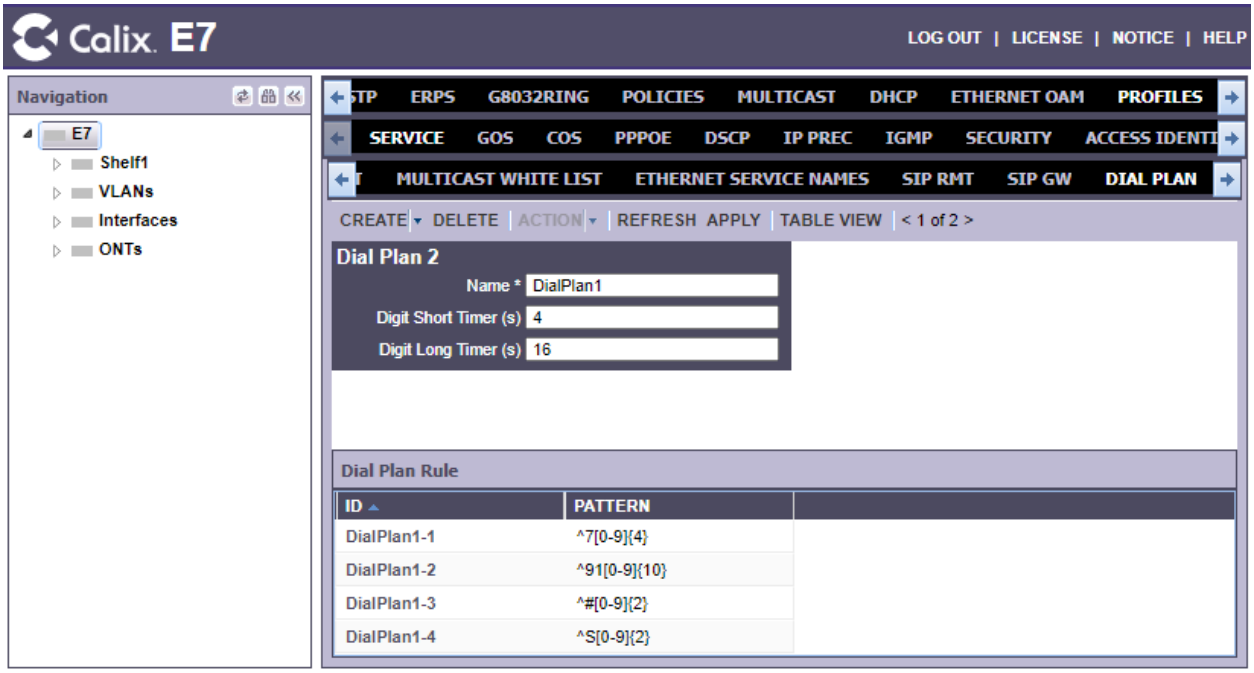
Navigate to **PROFILES → SERVICE → DIAL PLAN**. Click **Create** to add a new dial plan. In the Create Dial Plan dialog box, provide a **Name**, such as *DialPlan1* as shown below.



The **Dial Plan** screen, displays the new dial plan as shown below. Double-click on the new dial plan.



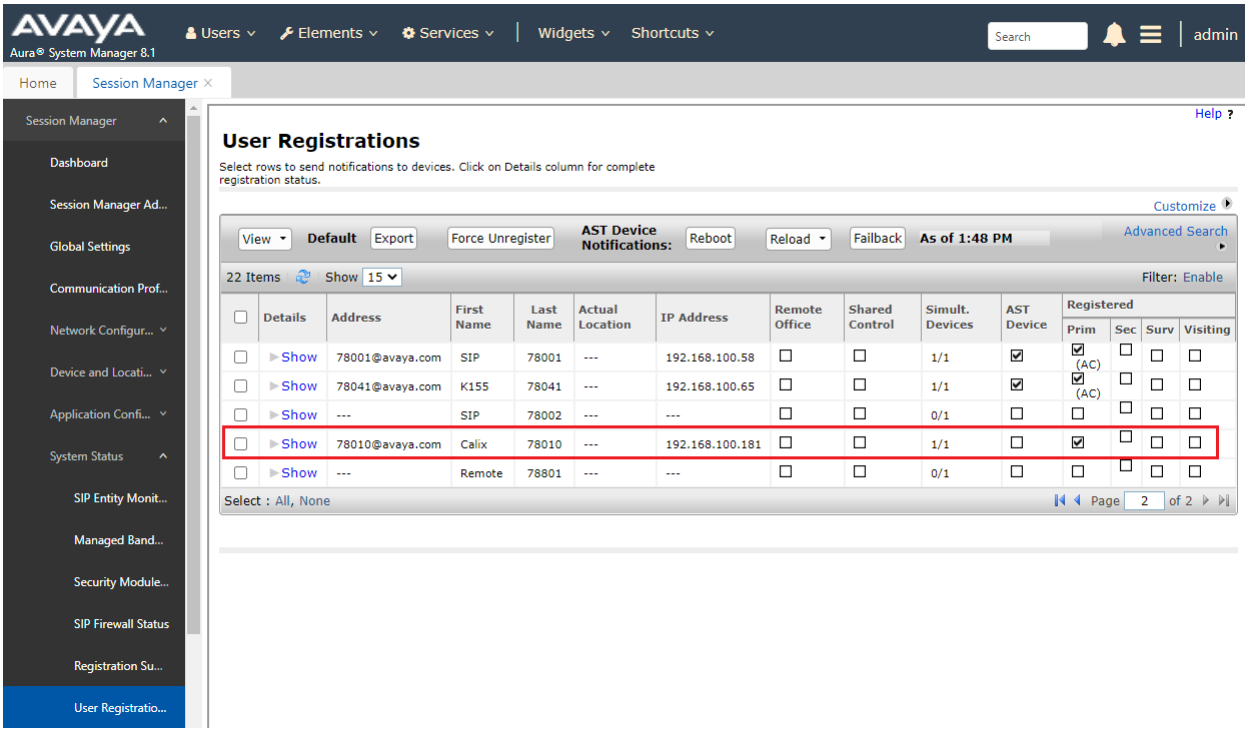
Add Dial Plan Rules as necessary. In the following example, four dial plan rules were added for for 5-digit numbers beginning with ‘7’, 10-digit number prepended with ‘91’, FACs beginning with ‘#”, and FACs beginning with ‘*’. Note that the ‘S’ indicates a ‘*’.



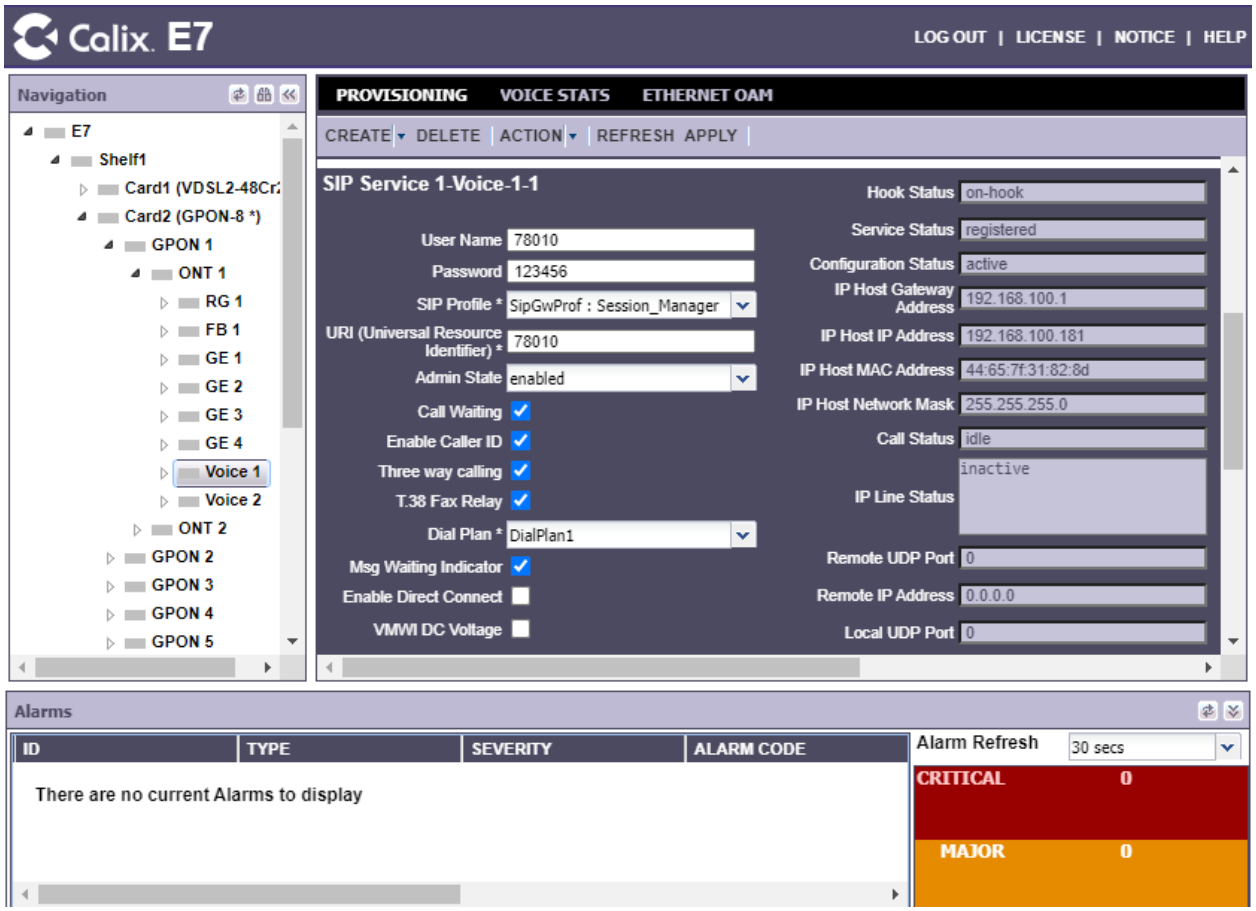
# 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Calix ONT SIP Devices.

1. Verify that ONT SIP Devices have successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status as shown below.



2. Alternatively, from the **E7 Unified Access Web Interface**, Navigate to **E7 → Shelf1 → Card2 (GPON-8) → ONT 1 → Voice 1** and verify that the **Service Status** is displayed as *registered*, as shown below, to verify that the ONT SIP Device has registered with Session Manager.




3. Establish a call from a POTS phone on the ONT SIP Device to an Avaya IP deskphone. While the call is active, verify two-way audio and exercise basic telephony features.

# 9. Conclusion

These Application Notes describe the integration of Calix ONT SIP Device with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Calix ONT SIP Device successfully registered with Avaya Aura® Session Manager as a SIP endpoint. Incoming and outgoing calls were placed to/from Calix ONT SIP Devices and telephony features were exercised. All test cases passed with observations noted in **Section 2.2**.

# 10. References

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


[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 10, March 2021, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 11, April 2021, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at http://support.avaya.com.

[4] *Calix EXA R3.x GPON Applications Guide*, available online at https://www.calix.com/content/calix/en/site-prod/library-html/systems-products/e-series/sysop/e7-ud/r3x/gpon/index.htm?toc36798167.htm?38367.htm

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.