Avaya Solution & Interoperability Test Lab

Application Notes for Polycom VVX Series Business IP Phones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.1

Abstract

These Application Notes describe the configuration steps required to integrate the Polycom VVX Series Business IP Phones with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The following Polycom VVX Business IP Phones were verified during the compliance test: VVX 401, VVX 601, VVX 250, and VVX 450. The Polycom VVX Series Business IP Phones registered with Avaya Aura® Session Manager as SIP endpoints. Although the compliance test was completed with and without TLS/SRTP, these Application Notes will describe the configuration with TLS/SRTP enabled.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate the Polycom VVX Series Business IP Phones with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The following Polycom VVX Business IP Phones were verified during the compliance test: VVX 401, VVX 601, VVX 250, and VVX 450. The Polycom VVX Series Business IP Phones registered with Avaya Aura® Session Manager as SIP endpoints. Although the compliance test was completed with and without TLS/SRTP, these Application Notes will describe the configuration with TLS/SRTP enabled.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Polycom VVX deskphones, Avaya SIP/H.323 deskphones and the PSTN, and exercising basic telephony features, such as hold, mute, call transfer and conference. Additional telephony features, such as call forward, follow me, call park/unpark, and call pickup were also verified using Communication Manager Features Access Codes (FACs).

The serviceability testing focused on verifying that VVX deskphones returned to service after re-connecting the Ethernet cable or rebooting the VVX deskphones.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the interface between Avaya systems and Polycom VVX Series Business IP Phones utilized enabled capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of VVX with Session Manager
- Calls between VVX and Avaya SIP/H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between VVX and the PSTN.
- UDP and TLS transport protocols.
- Calls with TLS/SRTP enabled and disabled.
- Support of G.711, G.729, and G.722 codecs.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, blind/attended transfer, attended conference, and long duration calls.
- Extended telephony features using Communication Manager FACs for Call Forward, Follow Me, Call Park/Unpark, and Call Pickup.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve voice messages.
- Proper system recovery after a restart of VVX and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observations noted:

- Polycom VVX does not support blind conference, but it does support attended conference.

- This solution is supported with and without TLS/SRTP enabled.

- Polycom VVX does not support sips. Therefore, the **Enforce SIPS URI for SRTP** option in the SIP signaling group for the SIP trunk between Communication Manager and Session Manager needs to be disabled.

- Polycom VVX does not support SDP Capability Negotiation (RFC5939) so the **IP Codec Set** form on Communication Manager should only be set for one Media Encryption method (i.e., *1-srtp-aescm128-hmac80*); otherwise, SRTP would not be negotiated for the call. To support calls with other Avaya IP deskphones (e.g., Avaya 1600 Series IP Deskphones) that don't support SRTP, a separate IP Network Region with a different IP Codec Set should be used. In this case, the call leg between Polycom VVX and Communication Manager will have SRTP enabled and the call leg between the other party and Communication Manager will not have SRTP enabled. In this case, the call is not shuffled (i.e., not direct IP-IP media). The other party could also support an Avaya proprietary encryption method, such as AES.

- Polycom VVX should be configured with the **Require SRTP** option enabled if TLS/SRTP is required. The **Offer SRTP** option is not supported because Polycom VVX encodes the SDP with secure media stream and an unsecure media description (i.e., dual m-line approach to best effort SRTP), which is not support by Communication Manager. Communication Manager supports SDP Capability Negotiation (RFC5939).

- If TLS/SRTP is enabled, the **Initial IP-IP Direct Media** option in the SIP signaling group of the SIP trunk group between Communication Manager and Session Manager needs to be disabled to avoid failures in some blind transfer scenarios and to allow Polycom VVX to hear audio prompts from Avaya Aura® Messaging. If non-secure media is being used, the **Initial IP-IP Direct Media** option may be enabled.

2.3. Support

For technical support on the Polycom VVX Series Business IP Phones, contact Polycom Support via phone or website.

- **Phone:** +1 (800) POLYCOM
- **Web:** http://www.polycom.com/collaboration-services.html#customer-support

3. Reference Configuration

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

- Avaya Aura® Communication Manager running in a virtual environment with an Avaya G450 Media Gateway. Avaya G450 Media Gateway was connected to the PSTN via an ISDN-PRI trunk (not shown).
- Media resources in the Avaya G450 Media Gateway and Avaya Aura® Media Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP deskphones.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya 96x1 Series H.323 and SIP Deskphones.
- Polycom VVX 401, VVX 601, VVX 250 and VVX 450 Business IP Phones.

Polycom VVX Series Business IP Phones registered with Session Manager and were configured as Off-PBX Stations (OPS) on Communication Manager.

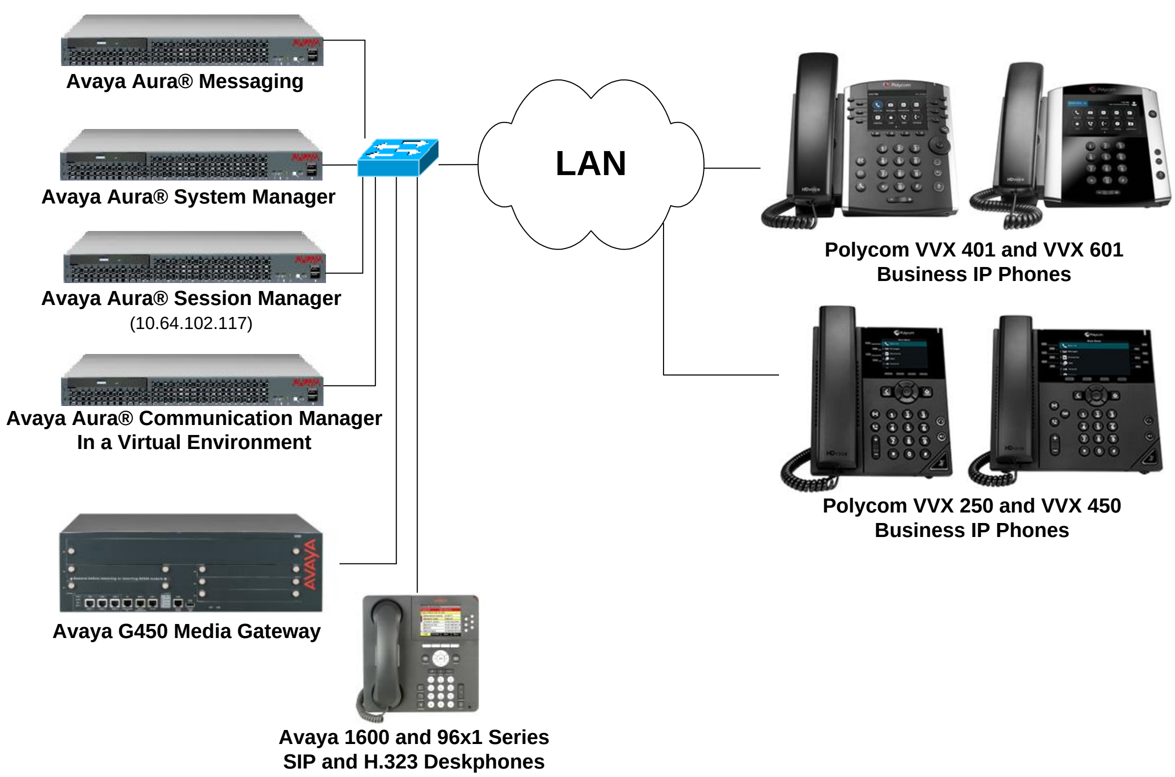


Figure 1: Avaya SIP Network with Polycom VVX Series Business IP Phones

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	8.0 SP1 (R018x.00.0.822.0 with Patch 24796)
Avaya G450 Media Gateway	FW 38.21.1
Avaya Aura® Media Server	v.7.8.0.393
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0 Build No. – 8.0.0.0.931077
Avaya Aura® Messaging	7.1.3.1.0-FP3SP1
Avaya 96x1 Series IP Deskphone	6.6506 (H.323) 7.1.1.0.9 (SIP)
Avaya 1600 Series IP Deskphone	1.3120 (H.323)
Polycom VVX Series Business IP Phones	5.8.1.6389

5. Configure Avaya Aura® Communication Manager

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

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

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

Note: It is assumed that basic configuration, such as voicemail coverage, has already been configured. The SIP station configuration for Polycom VVX Series Business IP Phones is configured through Avaya Aura® System Manager in **Section 6.2**.

5.1. Verify 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 that will be deployed.

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

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

                                                              USED
                                Platform Maximum Ports: 48000    62
                                      Maximum Stations: 36000 24
                              Maximum XMOBILE Stations: 36000 0
                    Maximum Off-PBX Telephones - EC500: 41000 0
                    Maximum Off-PBX Telephones -   OPS: 41000 15
                    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.)
```

On **Page 5**, verify that the **Media Encryption Over IP** option is enabled.

```
change system-parameters customer-options                       Page   5 of  12
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (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 (*lz-asm*). 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 Network Region and IP Codec Set

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 or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name:                       Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 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
```

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to VVX. 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. VVX was tested using G.711, G.722 and G.729 codecs. Specify the desired codecs in the **IP Codec Set** form as per customer requirements.

```
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:
```

To enable SRTP, set **Media Encryption** to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** to *best-effort*. Note that only one Media Encryption method should be listed for Polycom VVX.

Note: To support calls with other IP endpoints (e.g., Avaya 1600 Series IP Deskphones) that don't support this Media Encryption method, these IP endpoints should join a different IP Network Region associated with an IP Codec Set that includes no media encryption or media encryption methods supported by the IP endpoints. For example, for the 1600 Series IP Deskphones, the IP Codec Set included *aes* and *none* under Media Encryption. The **IP Network Map** form may be used to associate certain IP endpoints with a specific IP Network Region. Avaya 96x1 Series H.323/SIP Deskphones do support the media encryption in this IP Codec Set.

```
     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

5.4. Administer SIP Trunk to Session Manager

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

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Set the **Enforce SIPS URI for SRTP** field to *n*.
- Specify Communication Manager (*procr*) 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 are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Disable **Initial IP-IP Direct Media**.

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

```
add signaling-group 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
 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 Polycom VVX, Avaya SIP deskphones, and Avaya Aura® Messaging. 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. Configure the other fields in bold and accept the default values for the remaining fields.

```
add trunk-group 10                                                  Page   1 of  22
                                TRUNK GROUP

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

5.5. AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits beginning with “78” to route pattern 10 as shown below.

```
change aar analysis 78                                                 Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    78                    5    5     10        lev0         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
```

6. Configure Avaya Aura® Session Manager

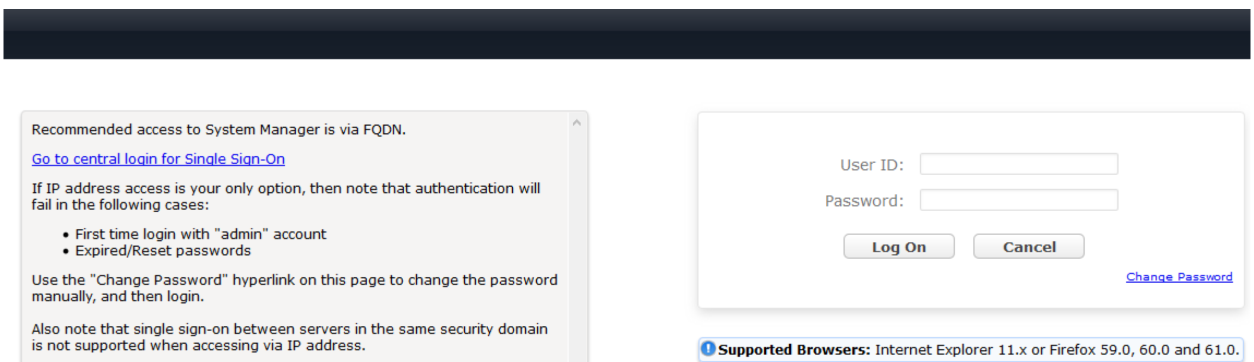
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for Polycom VVX Series Business IP Phones
- Administer SIP User

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of a SIP user for Polycom VVX Series Business IP Phones.

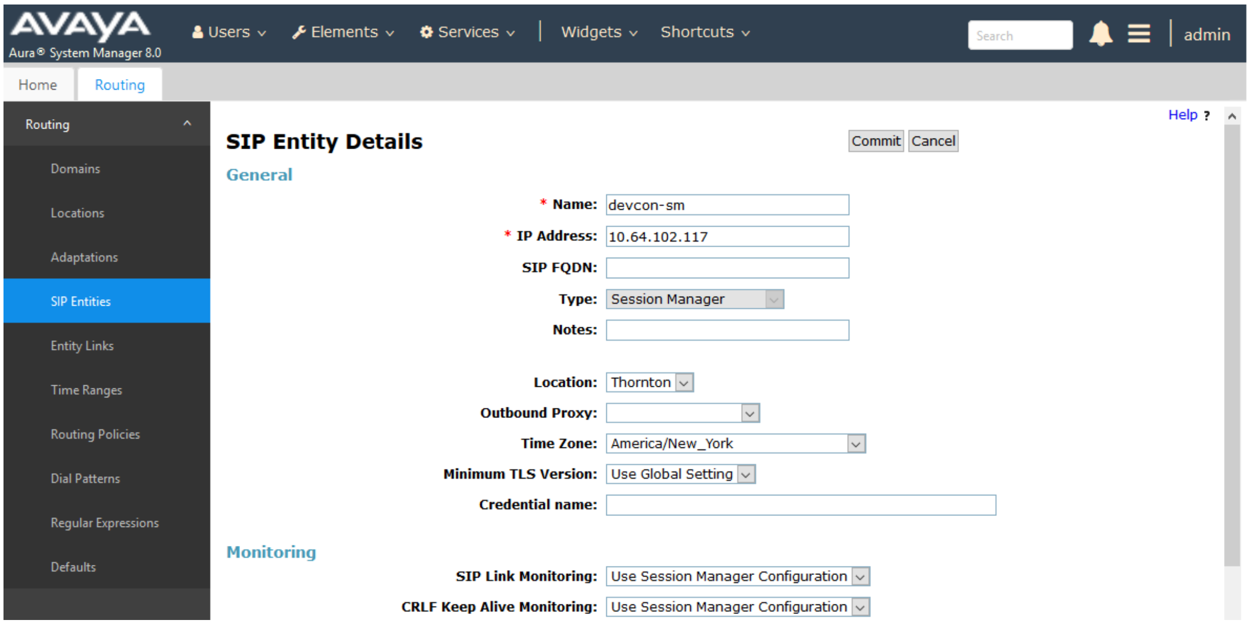
6.1. Launch System Manager

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

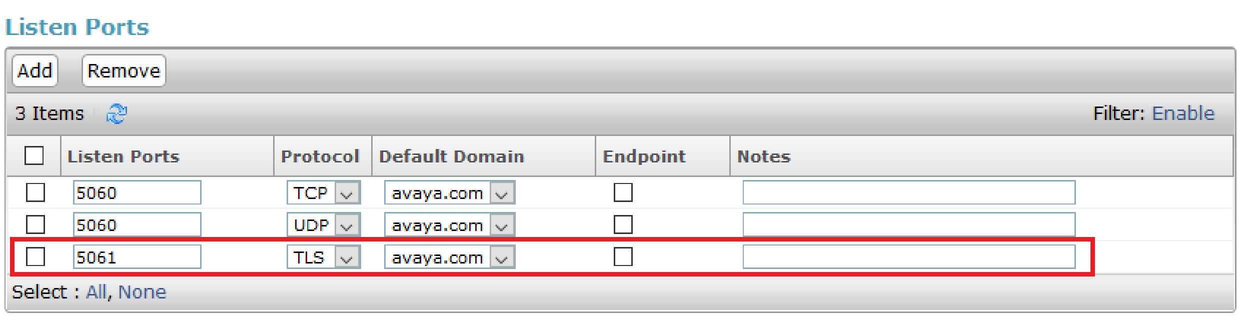


6.2. Set Network Transport Protocol for Polycom VVX Series Business IP Phones

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

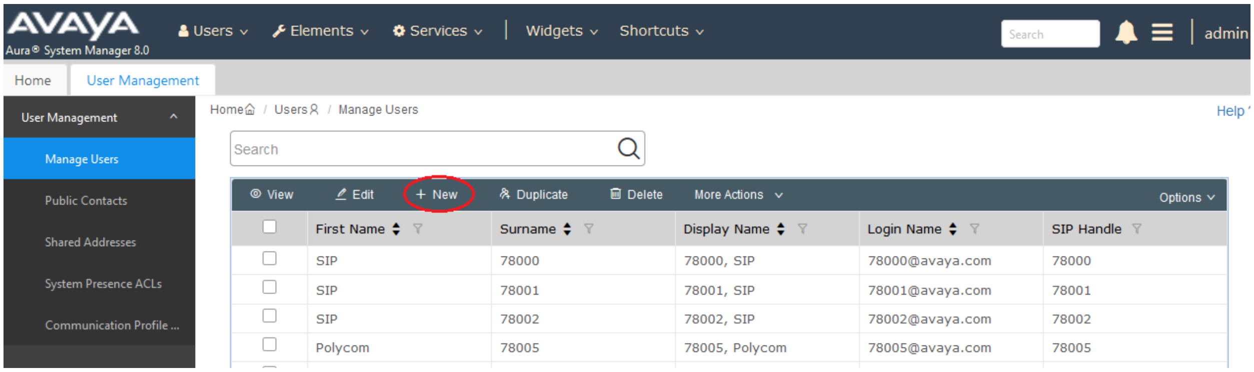


Scroll down to the **Listen Ports** section and verify that the transport network protocol used by VVX deskphones is specified in the list below. For the compliance test, the solution used TLS network transport.



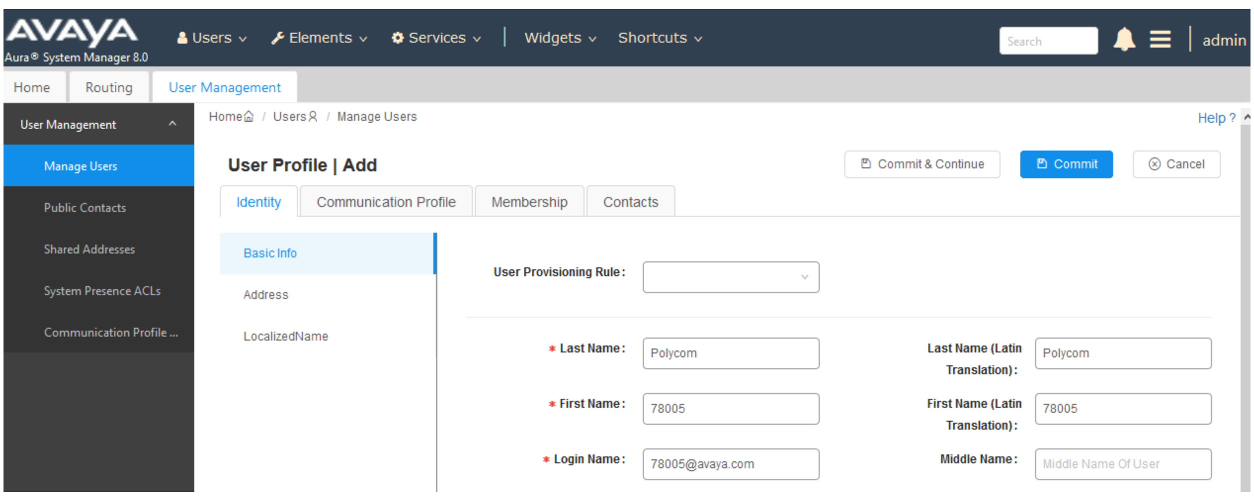
6.3. Administer SIP User

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



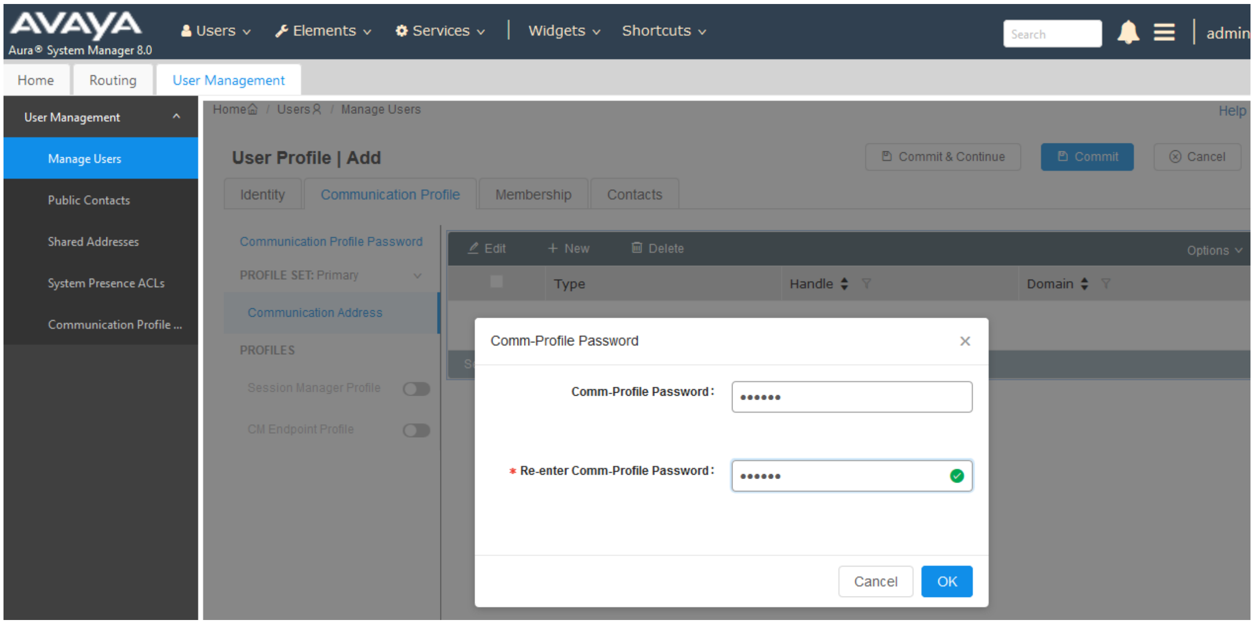
6.3.1. Identity

The **User Profile | Add** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter "*<ext>@<domain>*", where "*<ext>*" is the desired VVX SIP extension and "*<domain>*" is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.



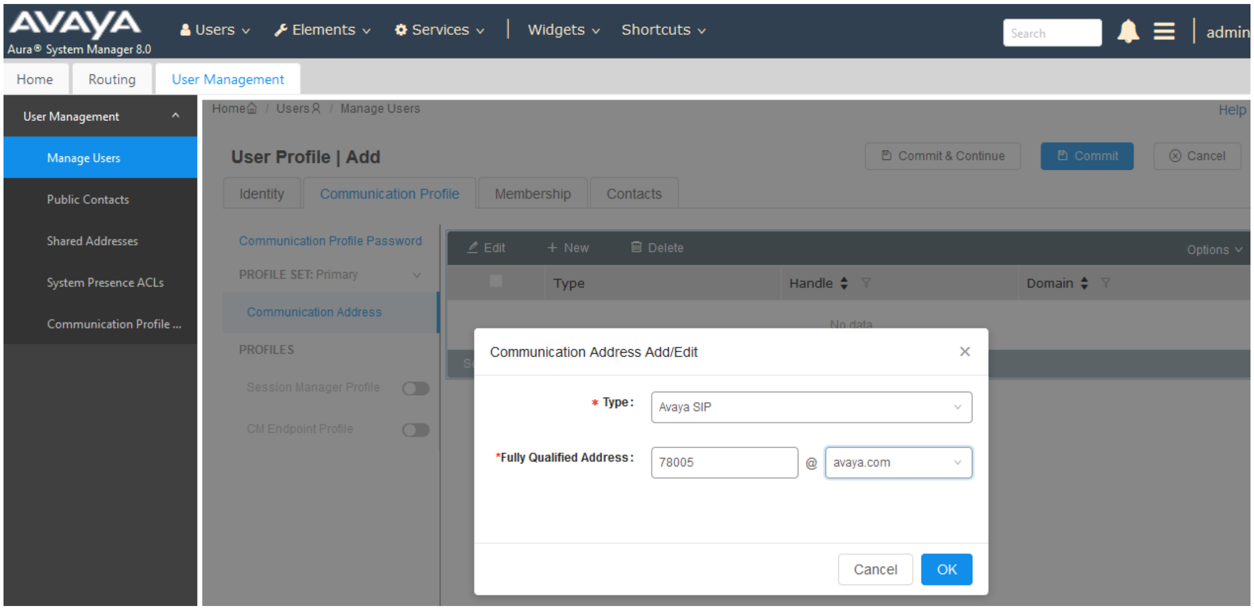
6.3.2. Communication Profile

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. Click **OK**.



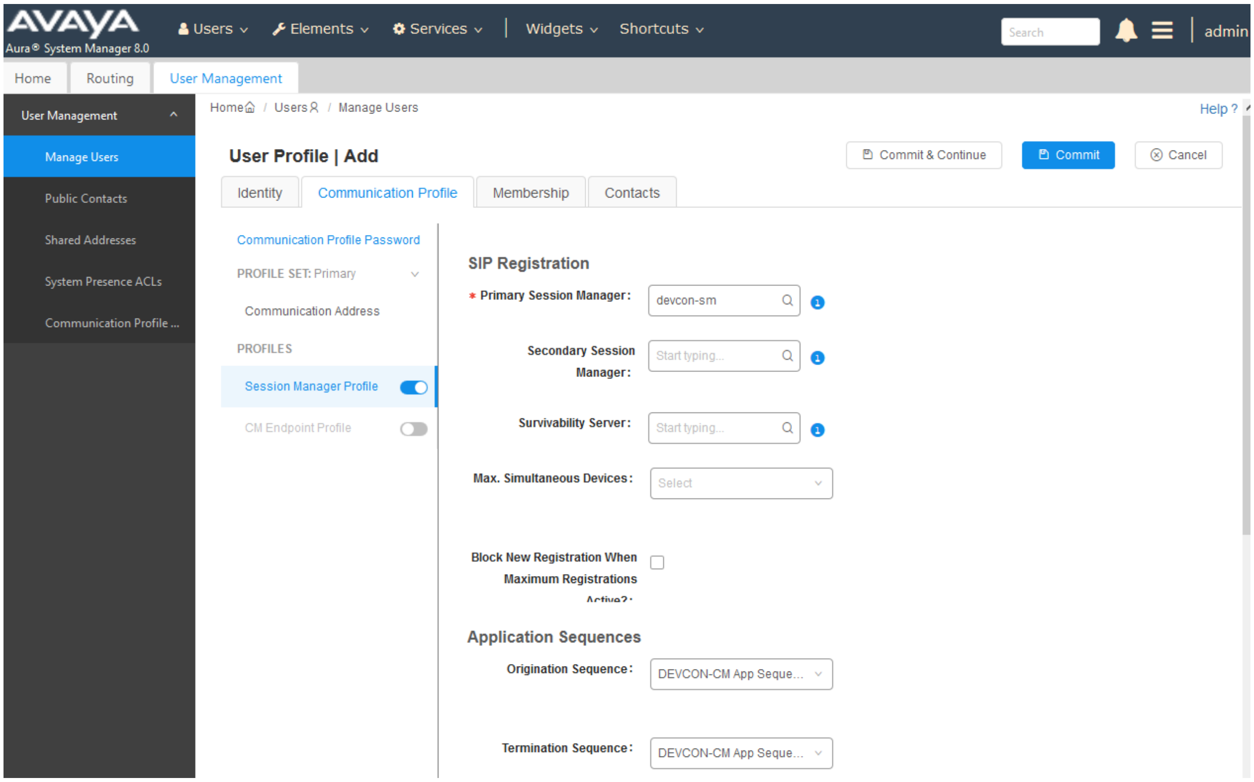
6.3.3. Communication Address

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**, select *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**.

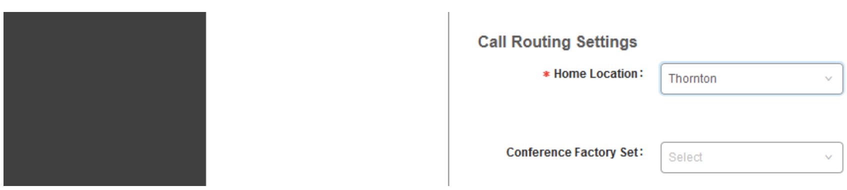


6.3.4. Session Manager Profile

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

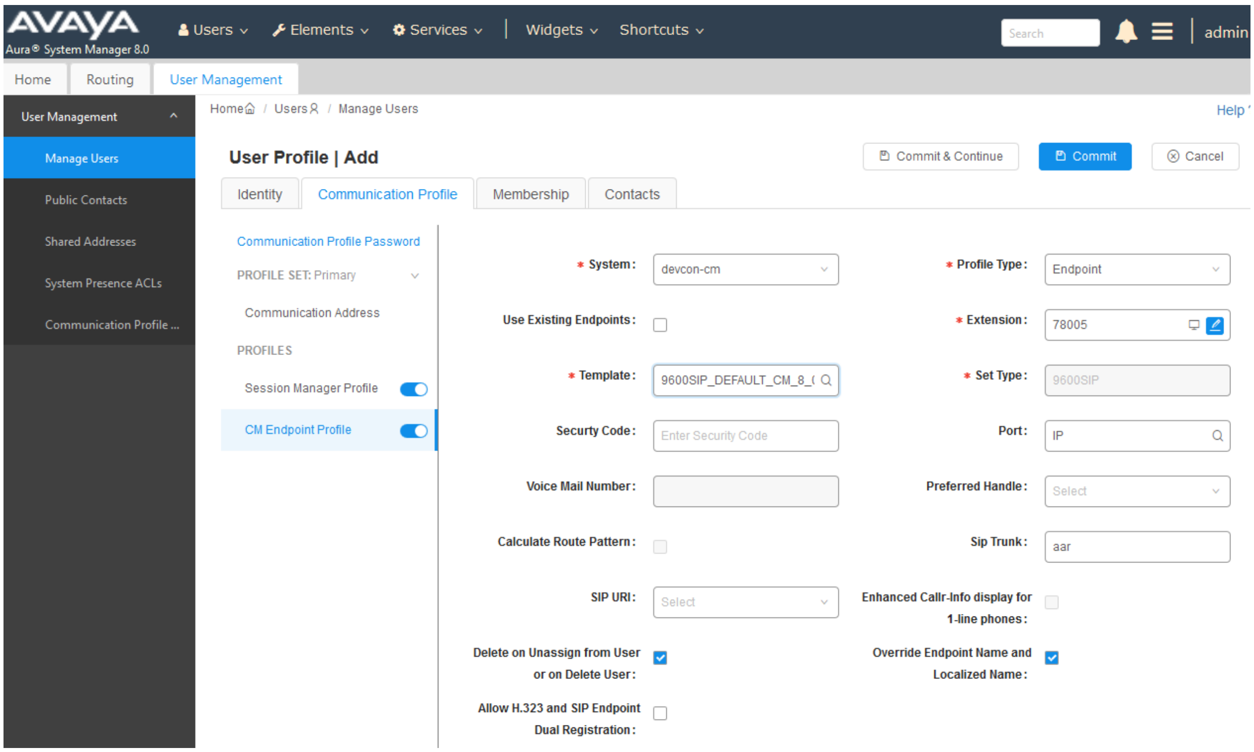


Scroll down to the **Call Routing Settings** section to configure the **Home Location**.

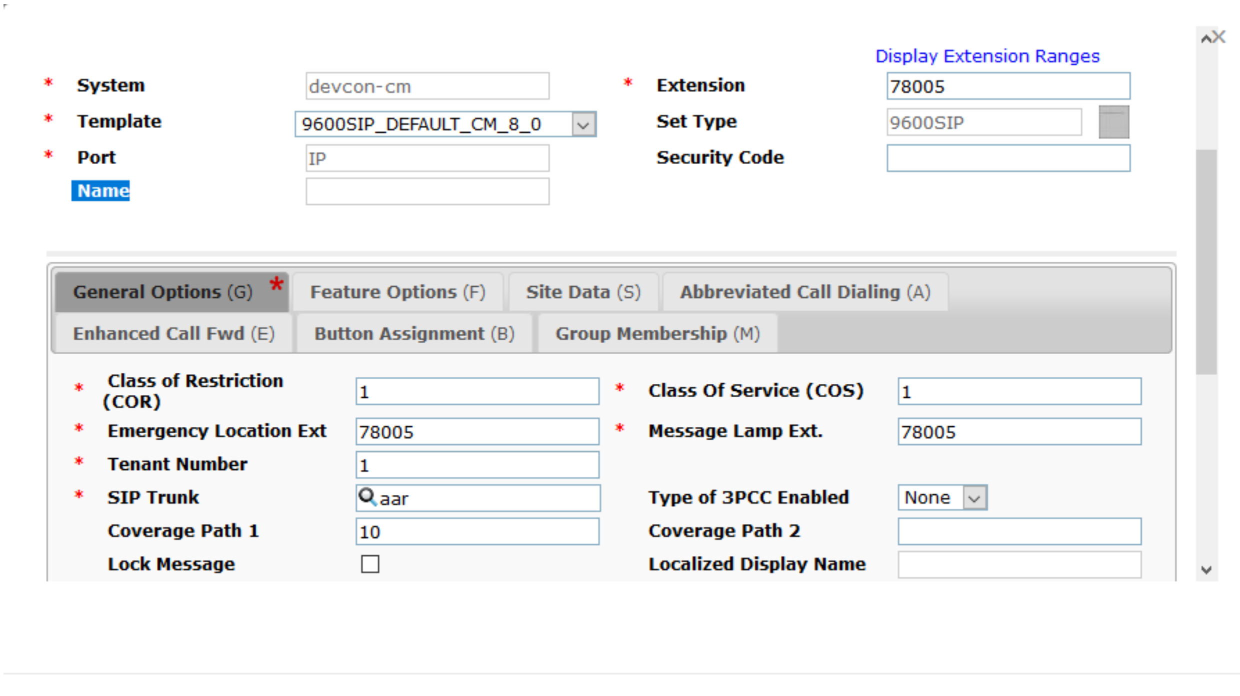


6.3.5. CM Endpoint Profile

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_0*. For **Port**, click and select *IP*. Retain the default values in the remaining fields. Click on the 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. Click **Done** (not shown) to return to the previous web page and then **Commit** to save the configuration (not shown).



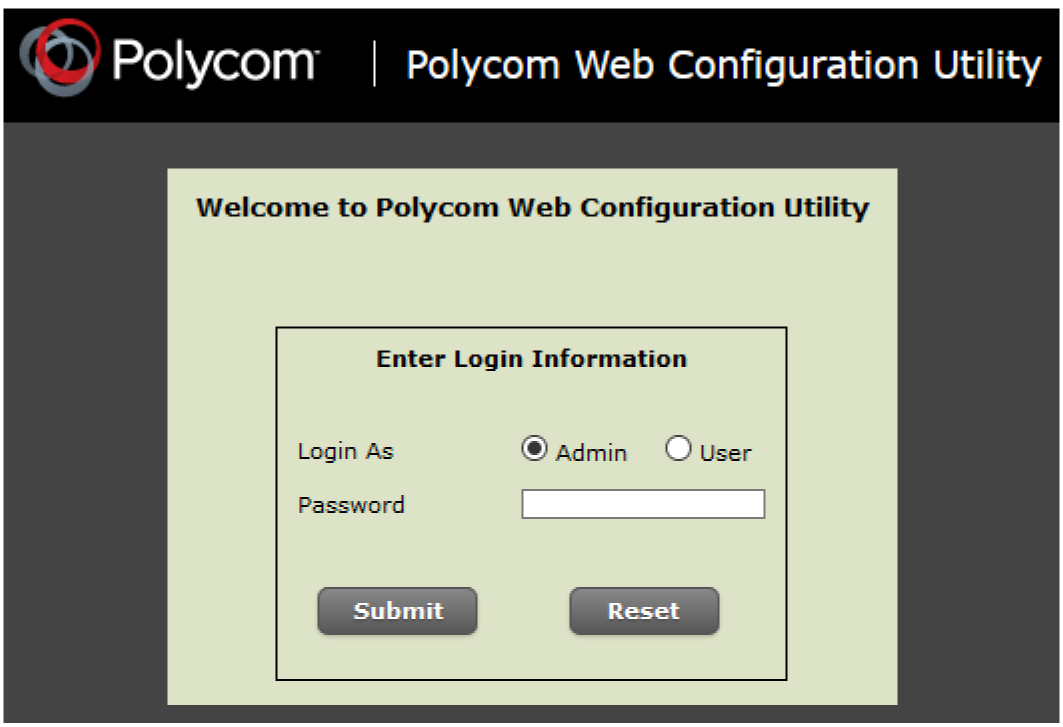
7. Configure Polycom VVX Series Business IP Phones

This section covers the configuration of the Polycom VVX Series Business IP Phones using the Polycom Web Configuration Utility. Note that a provisioning server could have also been used to build the configuration described in this section. Refer to [4] for more information. The configuration covers the following areas:

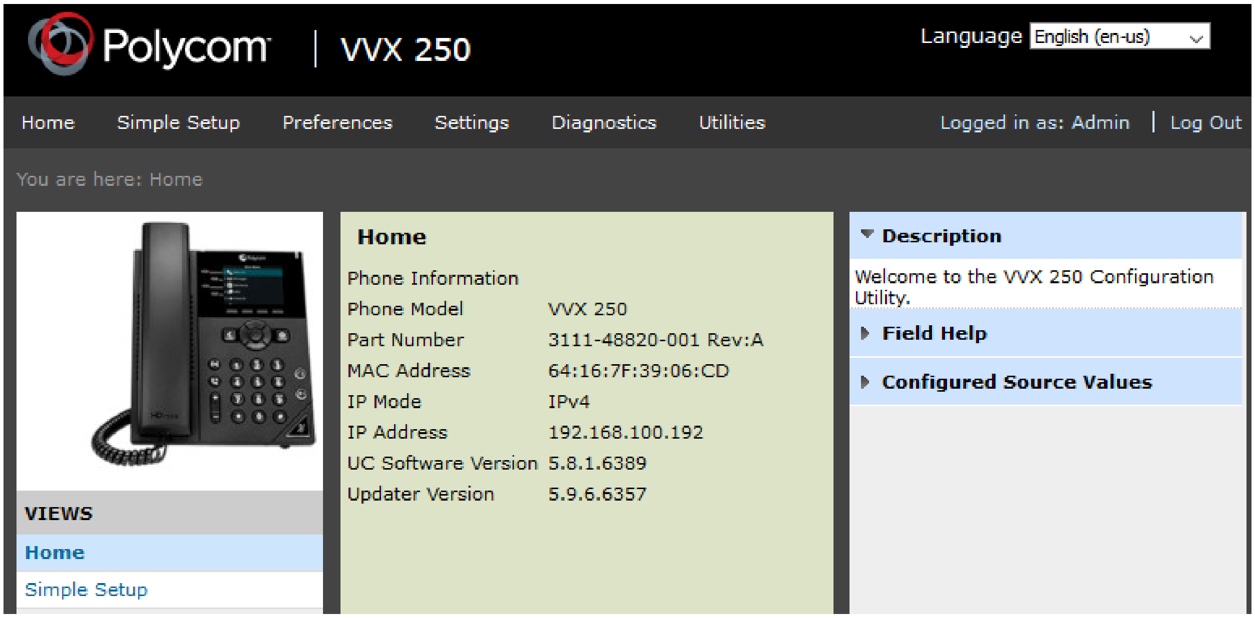
- Log into the Polycom Web Configuration Utility
- Configure SIP for the Polycom VVX Series Business IP Phone
- Configure SIP settings
- Configure Message Center for MWI
- Configure Audio Codec Priority
- Import the TLS certificate from Session Manager (i.e., the root CA)

7.1. Log into the Polycom Web Configuration Utility

From a web browser, enter the URL https://ip-address, where "ip-address" is the VVX IP address. The web configuration utility login webpage displayed as shown below. Select the **Admin** radio button and type in the default password of *456*. Click **Submit** to display the homepage of the configuration utility.



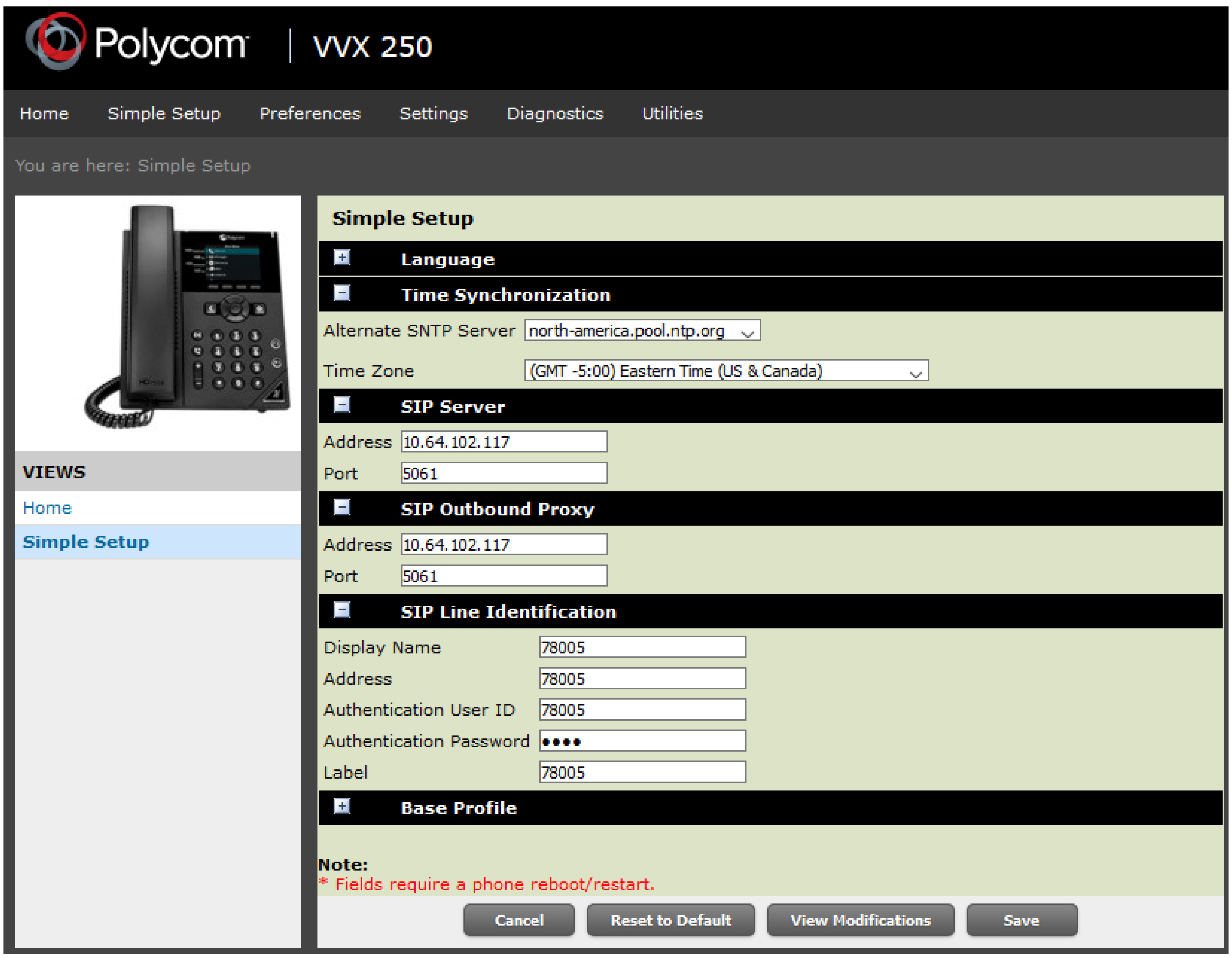
The homepage of the configuration utility is displayed below.



7.2. Configure SIP for the Polycom VVX Series Business IP Phone

Click on **Simple Setup** to configure the SIP parameters to allow the VVX deskphone to register with Session Manager. The **Simple Setup** is displayed as shown below. Configure the following fields and then click **Save**.

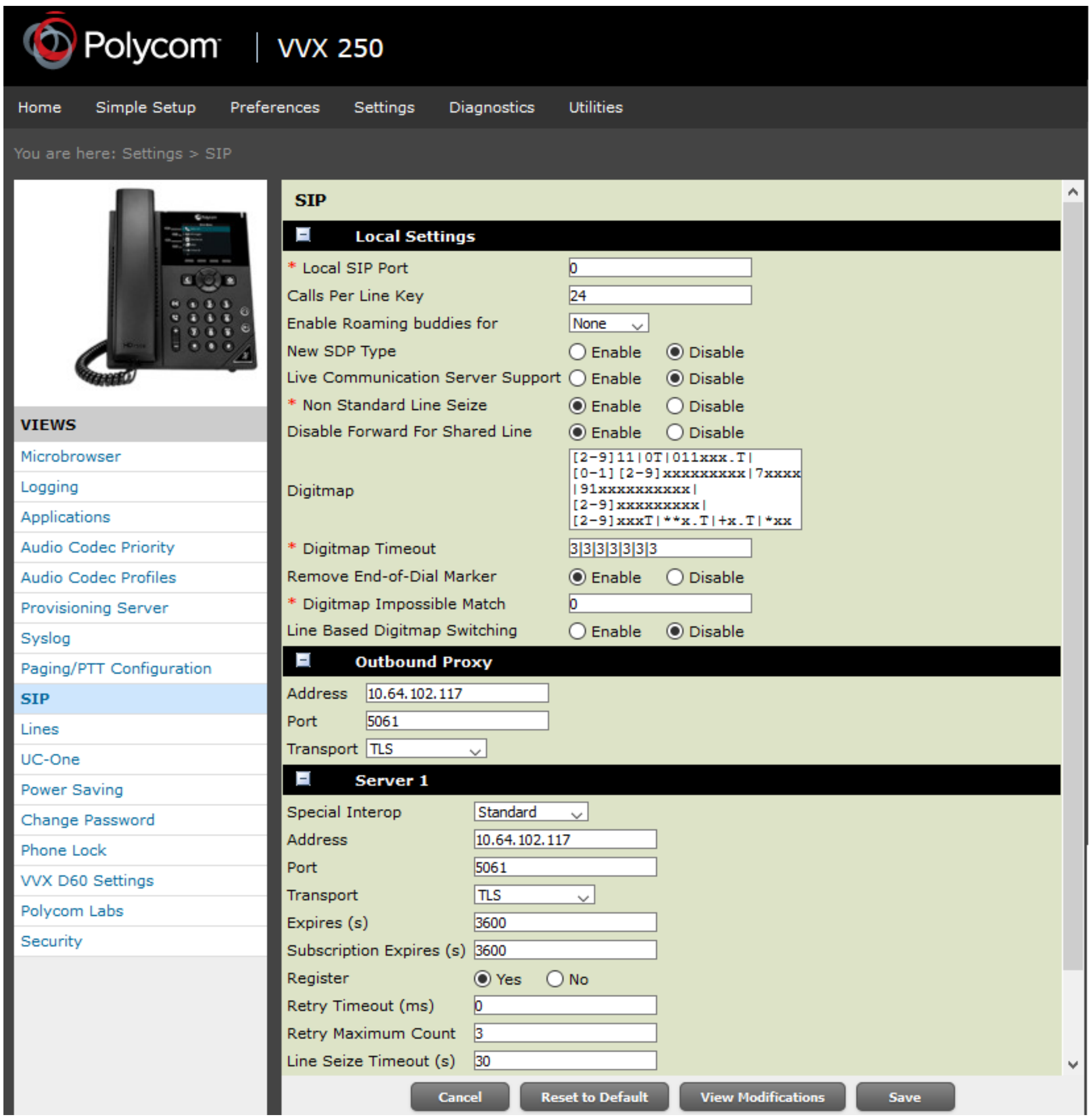
- In the **Time Synchronization** section, select an **Alternate SNTP Server** and specify the appropriate **Time Zone**.
- In the **SIP Server** section, specify the Session Manager IP address and the SIP port (e.g., *5061* for TLS). If SIP port is set to *0*, the port will default to 5061.
- In the **SIP Outbound Proxy** section, specify the Session Manager IP address and the SIP port.
- In the **SIP Line Identification** section, specify the **Authentication User ID** (e.g., *78005*) and **Authentication Password** of the SIP user configured in **Section 6.3**.



7.3. Configure SIP Settings

Navigate to **Settings → SIP** and configure the following fields and then click **Save**:

- In the **Local Settings** section, leave the **Local SIP Port** at *0*. This will default to port 5061. The **Digitmap** field may include other dial patterns that the user may dial, such as 5-digit extensions starting with '7' (e.g., *7xxxx*) or PSTN numbers (e.g., 91xxxxxxxxxx).
- In the **Outbound Proxy** section, specify the Session Manager IP address, the SIP port (e.g., *5061* or *0*, which will default to 5061), and the transport protocol to *TLS*.
- In the **Server1** section, specify the Session Manager IP address, the SIP port, and the transport protocol to *TLS*.

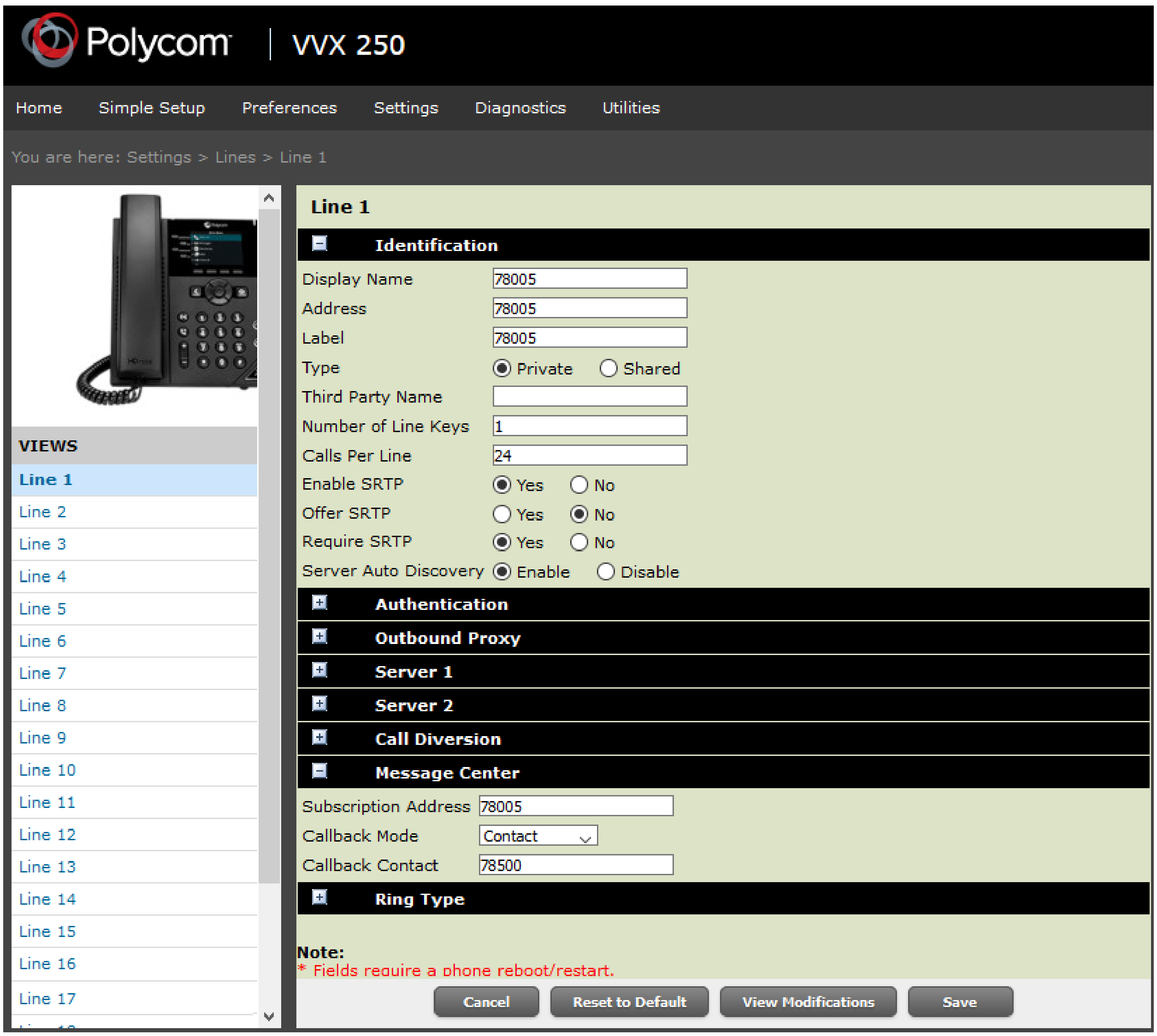


7.4. Configure Message Center for MWI

Navigate to **Settings → Lines** and expand the **Identification** section. Enable **Require SRTP**. **Offer SRTP** should be disabled.

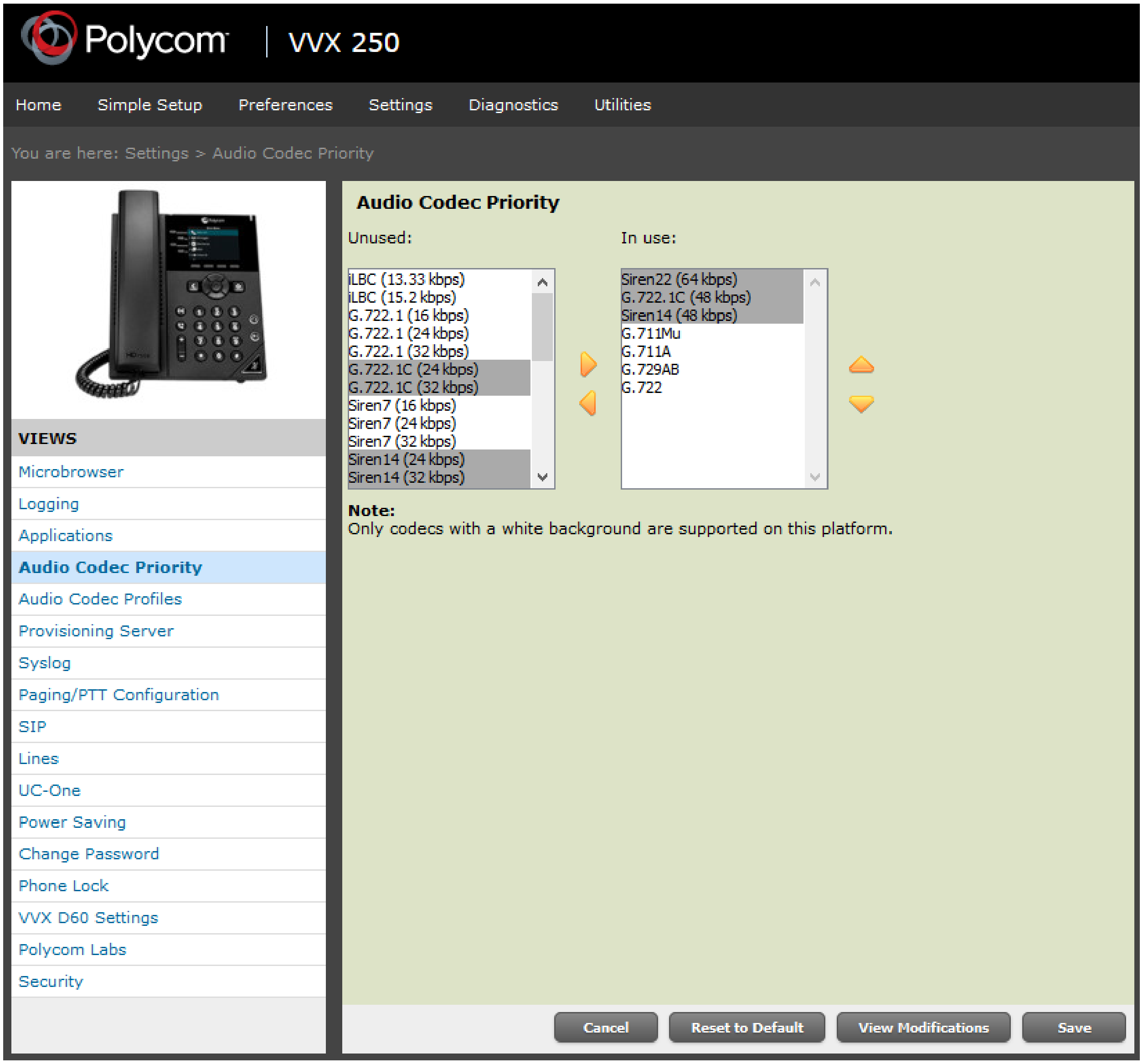
Next, expand the **Message Center** section. Configure the following fields to allow VVX to subscribe to MWI and then click **Save**.

- Set **Subscription Address** to the SIP extension (e.g., *78005*).
- Set **Callback Mode** to *Contact*.
- Set **Callback Contact** to the voicemail pilot number (e.g., *78500*).



7.5. Configure Audio Codec Priority

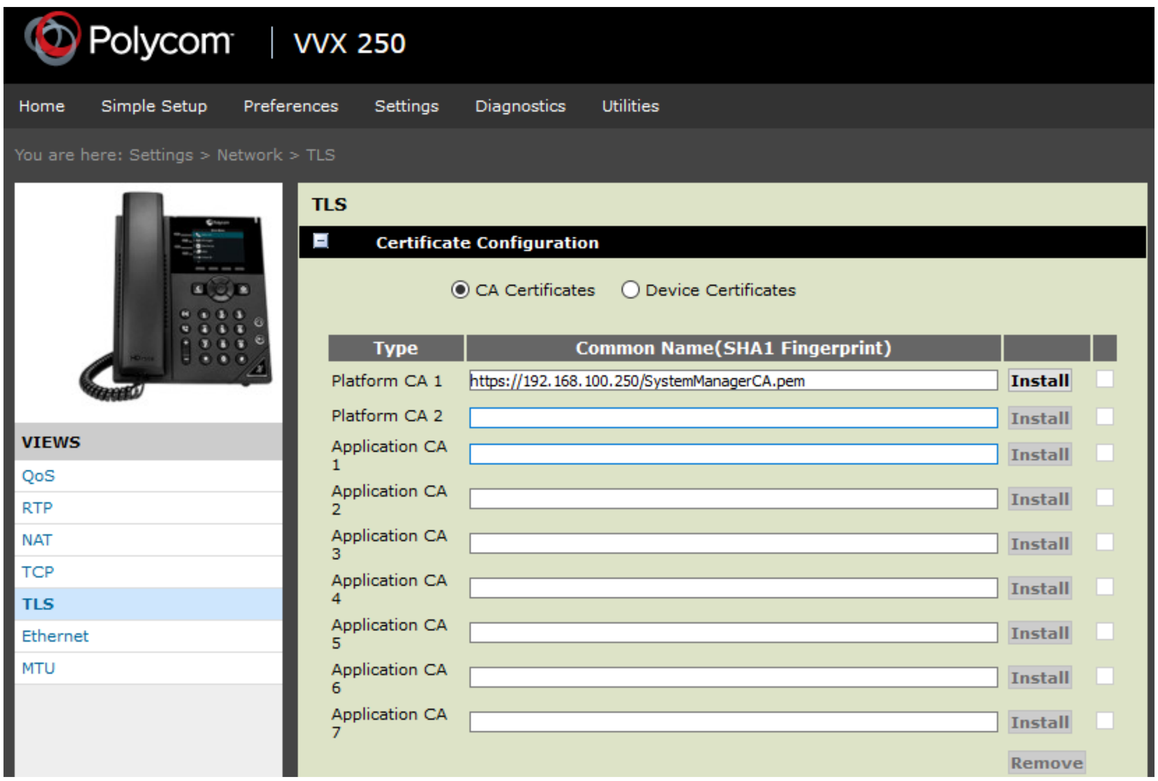
Navigate to **Settings → Audio Codec Priority** and select the codecs (in priority order) to be supported. For the compliance test, G.711, G.729 and G.722 were verified. Click **Save**.



7.6. Import the TLS Certificate from Session Manager

Add a custom/self-signed certificate, if customer is using a self-signed certificate, or a certificate that is signed by a root CA that the VVX deskphones do not inherently trust. For the compliance test, System Manager served as the root CA. The root CA certificate was exported from System Manager and imported into the VVX deskphones. To import the TLS certificate, follow these steps:

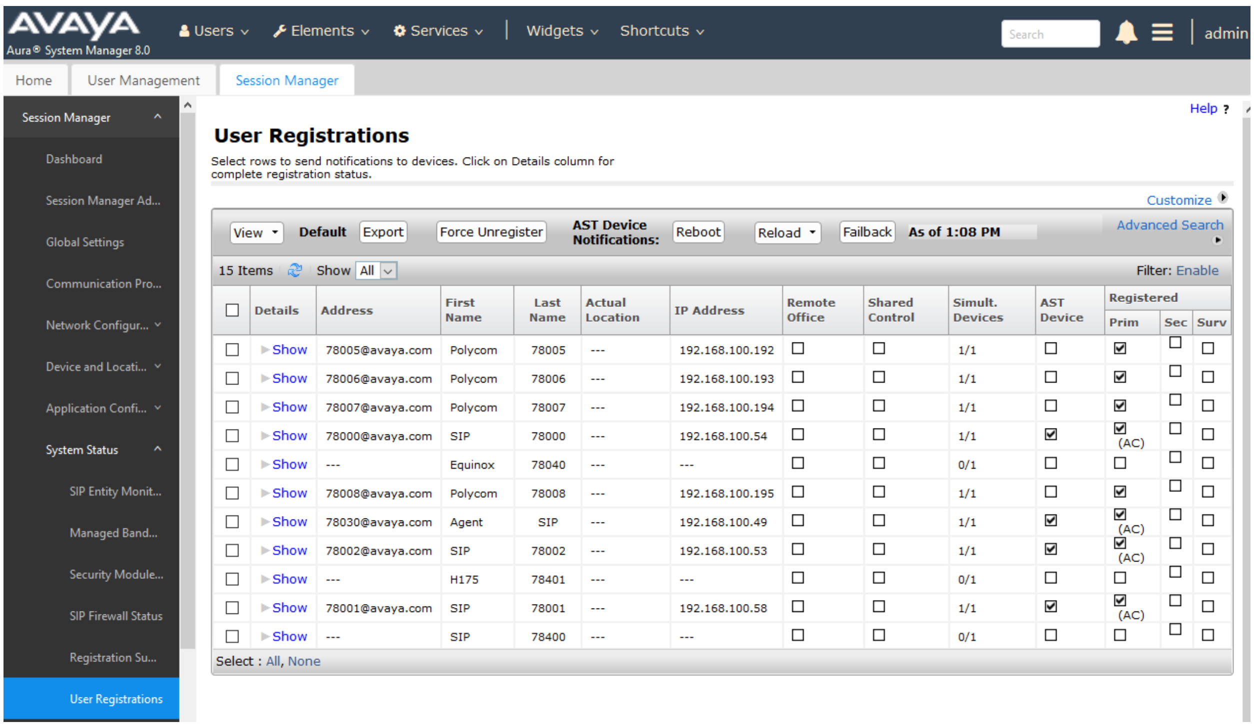
1. Store the root CA certificate on a HTTP server.
2. Navigate to **Settings → Network → TLS** in the web configuration utility. Under **Certificate Configuration**, enter the URL of the certificate file on the HTTP server (e.g. https://192.168.100.250/SystemManagerCA.pem) in the **Platform CA 1** field. Click **Install**. The default values for the **TLS Profiles** and **TLS Applications** sections (not shown) may be used.



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 Polycom VVX Series Business IP Phones.

1. Verify that VVX deskphones have successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status.



2. Establish a call between Polycom VVX and a local Avaya deskphone. The **status trunk** command may be used to view the active call status. The trunk that is being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call. On **Page 2**, **Audio Connection Type** will set to *ip-direct* if the call is shuffled. The **Codec Type** is also displayed.

```
status trunk 10/1                                            Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                           Port
   Near-end:  10.64.102.115                      : 5061
    Far-end:  10.64.102.117                      : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                           Port
   Near-end:  192.168.100.58                     : 5004
    Far-end:  192.168.100.192                    : 2258

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

Page 3 will indicate if SRTP is enabled for the call as shown below.

```
status trunk 10/1                                            Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00001
T00001:TX:192.168.100.192:2258/g711u/20ms/1-srtp-aescm128-hmac80
T00005:RX:192.168.100.58:5004/g711u/20ms/1-srtp-aescm128-hmac80

Dest port: T00005
```

3. While the call is active, basic telephony features can be exercised to verify proper operation.

9. Conclusion

These Application Notes described the configuration steps required to integrate Polycom VVX Series Business IP Phones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Polycom VVX Series Business IP Phones were able to establish calls with Avaya H.323 / SIP deskphones and the PSTN with TLS/SRTP enabled. In addition, basic telephony features were verified. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1, July 2018.

[2] *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0, Issue 4, September 2018.

[3] *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2, July 2018.

[4] *Polycom UC Software Administrator Guide 5.8.0.*

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.