Avaya Solution & Interoperability Test Lab

Application Notes for Talkaphone VOIP-220 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Talkaphone VOIP-220 Series IP Call Stations 7.3.3.0 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Talkaphone VOIP-220 Series IP Call Stations are a family of indoor and outdoor-rated (ruggedized) VoIP emergency/information phones for use in locations such as parking facilities, college campuses, medical centers and industrial parks. Talkaphone VOIP-220 Series IP Call Stations register with Avaya Aura® Session Manager as a SIP endpoint. For the compliance test, a Talkaphone VOIP-220C IP Call Station was used.

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 Talkaphone VOIP-220 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Talkaphone VOIP-220 Series IP Call Stations are a family of indoor- and outdoor-rated (ruggedized) VoIP emergency/information phones for use in locations such as parking facilities, college campuses, medical centers and industrial parks. Talkaphone VOIP-220 Series IP Call Stations register with Avaya Aura® Session Manager as a SIP endpoint. For the compliance test, a Talkaphone VOIP-220C IP Call Station was used. See **Attachment 1** for other models in the same series. Some models include a camera, but the video is not established as part of the voice call and was not tested.

Talkaphone VOIP-220 Series IP Call Stations incorporate Zenitel components and use the Zenitel GUI for configuration, under license from Zenitel USA, Inc.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Talkaphone VOIP-220 Series IP Call Stations, Avaya SIP / H.323 deskphones, and the PSTN, and exercising basic telephony features, such as hold, mute, transfer, and conference, from the Avaya IP deskphones. Additional telephony features, such as call forward and call coverage, initiated from Avaya IP deskphones were also verified.

The serviceability testing focused on verifying that the Talkaphone VOIP-220 Series IP Call Stations come back into service after re-connecting the Ethernet cable or rebooting the IP Call Station.

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 Talkaphone VOIP-220 Series IP Call Stations used TLS/SRTP encryption features.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of VOIP-220C with Session Manager.
- Calls between VOIP-220C and Avaya SIP / H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled. Shuffling allows IP endpoints to send audio RTP packets directly to each other without using media resources on the Avaya Media Gateway or Avaya Aura® Media Server.
- Calls between VOIP-220C and the PSTN.
- Use of call button on VOIP-220C to place an outgoing call to Avaya IP deskphones and the PSTN.
- Use of Ring List on VOIP-220C to try multiple numbers for incoming calls.
- Playing a recording on VOIP-220C when a specific DTMF digit is entered by the connected party.
- G.711 and G.729 codec support.
- Support of TLS/SRTP using one-way authentication, TLS 1.3, and a secure PFS cipher.
- Support of UDP/RTP.
- Basic telephony features, including hold, mute, redial, call forwarding, transfer, and 3-way conference, initiated from Avaya IP deskphones.
- Call answer and termination on VOIP-220C via call button.
- Auto answer and manual answer on VOIP-220C.
- Call coverage on VOIP-220C.
- Long duration calls with VOIP-220C.
- Proper system recovery after a restart of VOIP-220C Station and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observation:

- Dialing Feature Access Codes (FACs) or Feature Name Extensions (FNEs) to activate telephony features are not applicable to Talkaphone VOIP-220 Series IP Call Stations.

2.3. Support

For technical support and information on Talkaphone VOIP-220 Series IP Call Stations, contact Talkaphone Technical Support at:

- Phone: 1-773-539-1100
- Email: support@talkaphone.com
- Website: https://www.talkaphone.com/contact-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 virtualized environment with a G430 and G450 Media Gateway and Avaya Aura® Media Server.
- Media resources in the Avaya 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 telephones.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya Messaging serving as the voicemail system.
- Avaya 96x1 Series SIP and H.323 deskphones.
- Avaya J100 Series SIP Phones.
- Talkaphone VOIP-220C IP Call Station.

Talkaphone VOIP-220 Series IP Call Station registered with Session Manager and was configured as Off-PBX Stations (OPS) on Communication Manager.

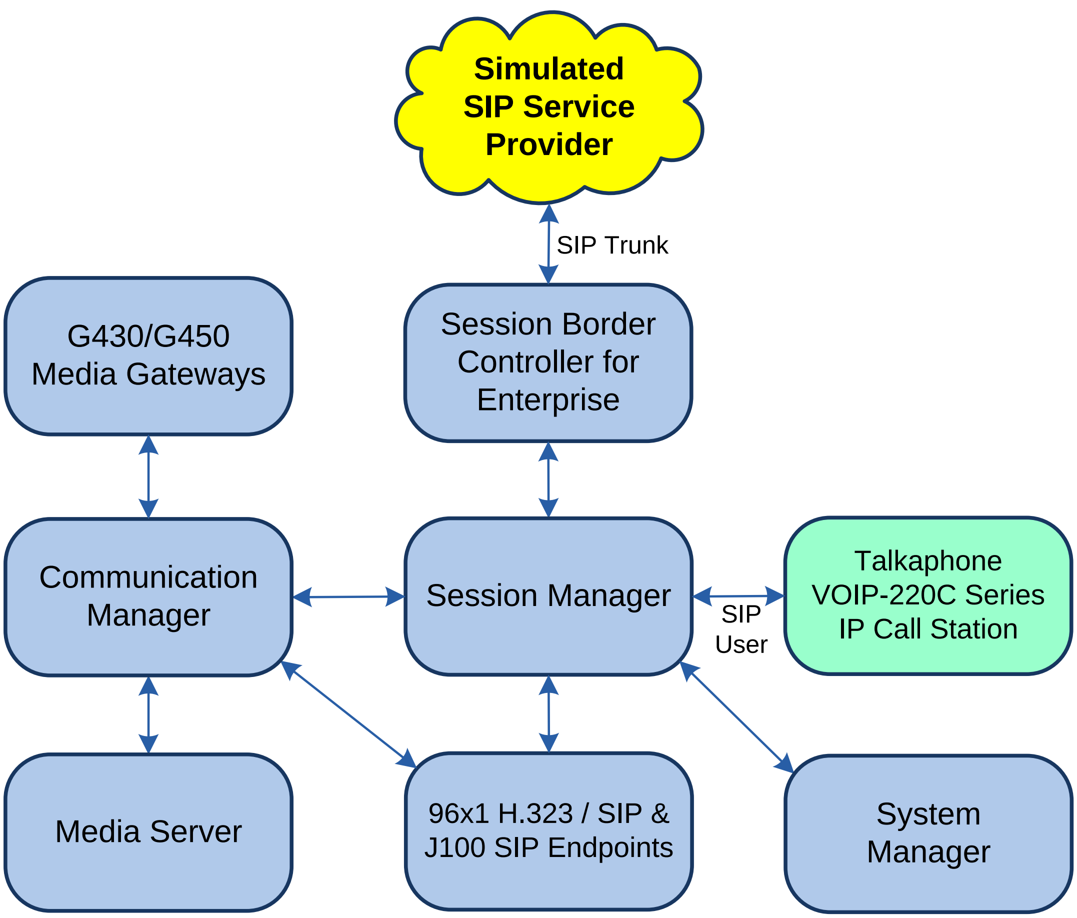


Figure 1: Avaya SIP Network with Talkaphone VOIP-220 Series IP Call Station

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	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.8.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media-Server	v.10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 Series IP Phones	4.0.13.0.6 (SIP)
Talkaphone VOIP-220C IP Call Station	7.3.3.0

5. Configure Avaya Aura® Communication Manager

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

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

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

Note: The SIP station configuration for the Talkaphone IP Call Stations is configured through Avaya Aura® System Manager in **Section 6.3**.

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: V20                              Software Package: Enterprise
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                                USED
                                Platform Maximum Ports: 48000    131
                                      Maximum Stations: 36000     37
                              Maximum XMOBILE Stations: 36000      0
                    Maximum Off-PBX Telephones - EC500: 41000      0
                    Maximum Off-PBX Telephones -   OPS: 41000     23
                    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 Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya 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: SIP Enterprise        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
```

5.4. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to VOIP-220C. 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 section above. VOIP-220C was tested using G.711 and G.729 codecs.

To enable SRTP, **Media Encryption** was set to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** was left at the default value of *best-effort*. Note that RTP, which would be indicated by *none* under **Media Encryption**, must not be included so that Communication Manager enforces SRTP.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

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

     Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3:
 4:
 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 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*.
- Enable **Initial IP-IP Direct Media**.

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

```
add signaling-group 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? y
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to/from VOIP-220C 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. Configure the other fields in bold and 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
```

5.6. Administer AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with "78" to route pattern "10" as shown below. VOIP-220C was assigned extension 78400.

```
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

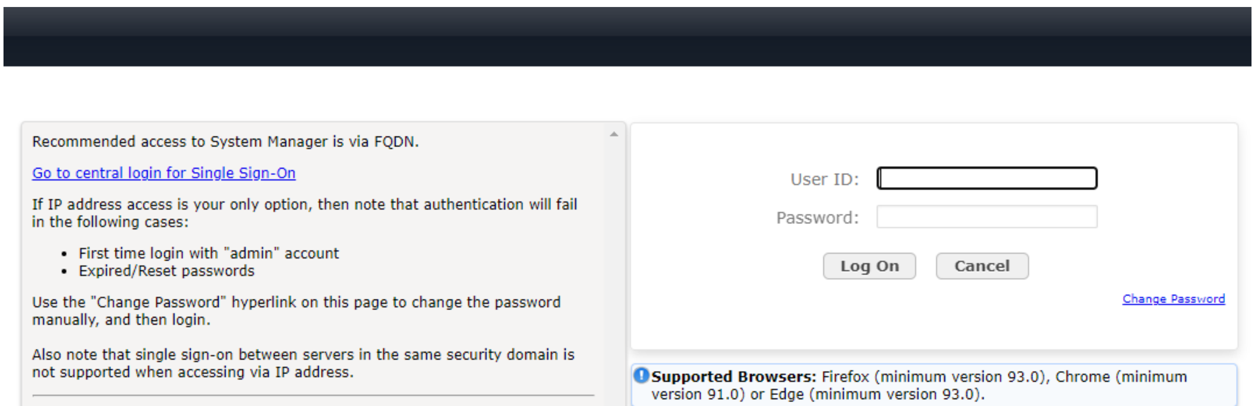
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol
- 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 the Talkaphone IP Call Station.

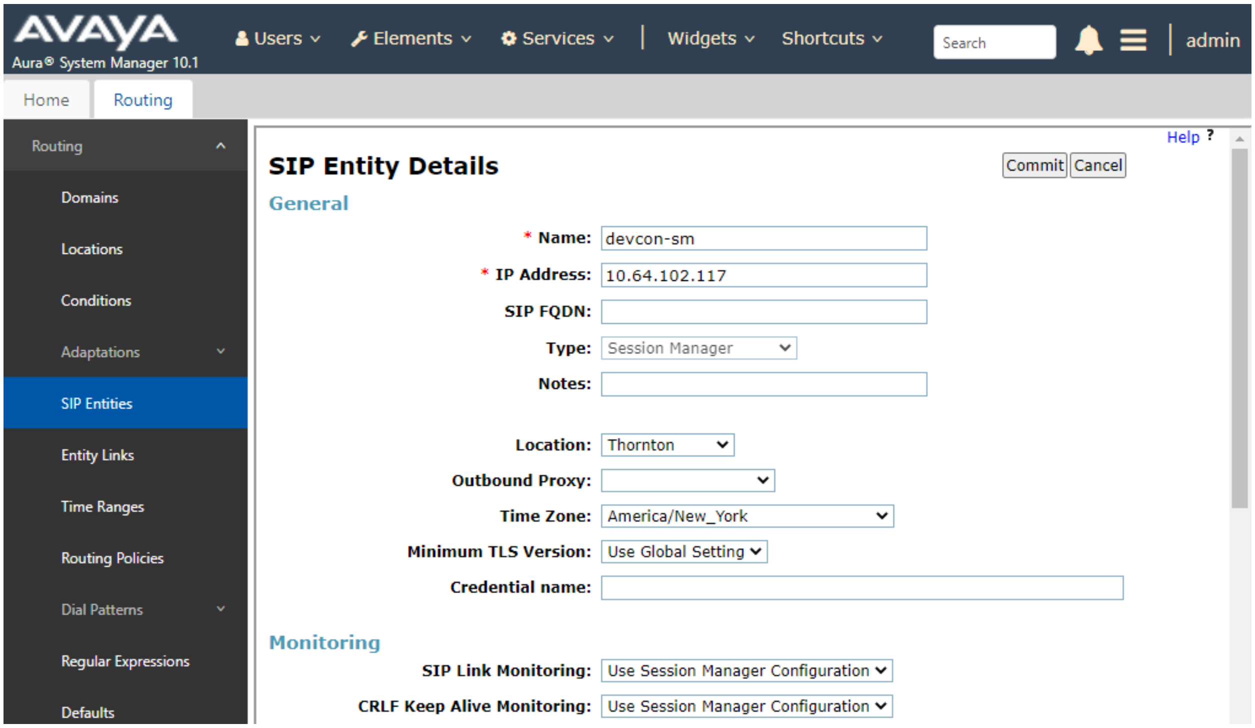
6.1. Launch System Manager

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.

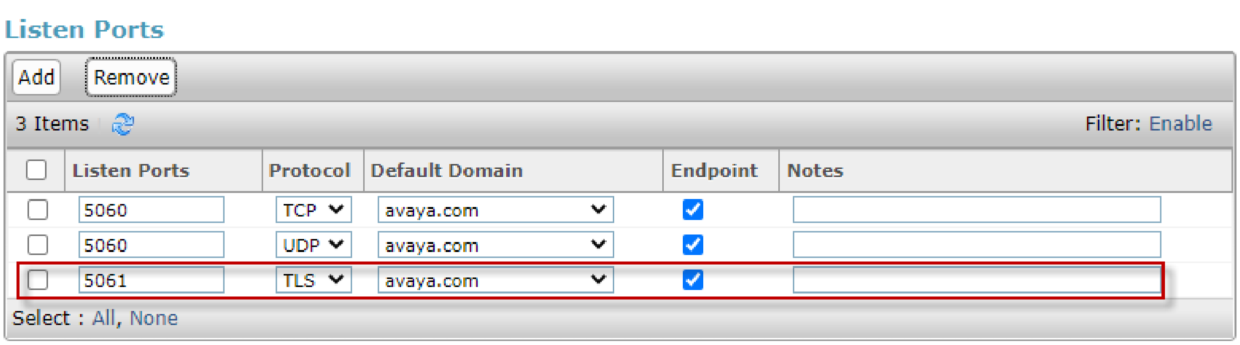


6.2. Set Network Transport Protocol

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

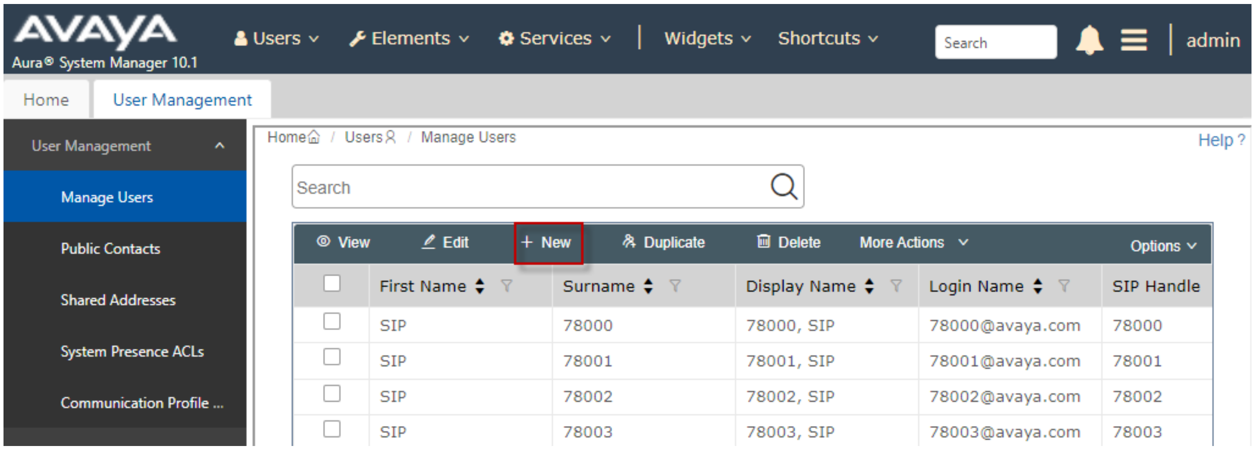


Scroll down to the **Listen Ports** section and verify that the transport network protocol used by Talkaphone IP Call Station is specified in the list below. For the compliance test, the solution used TLS network transport although UDP is also supported with VOIP-220C.



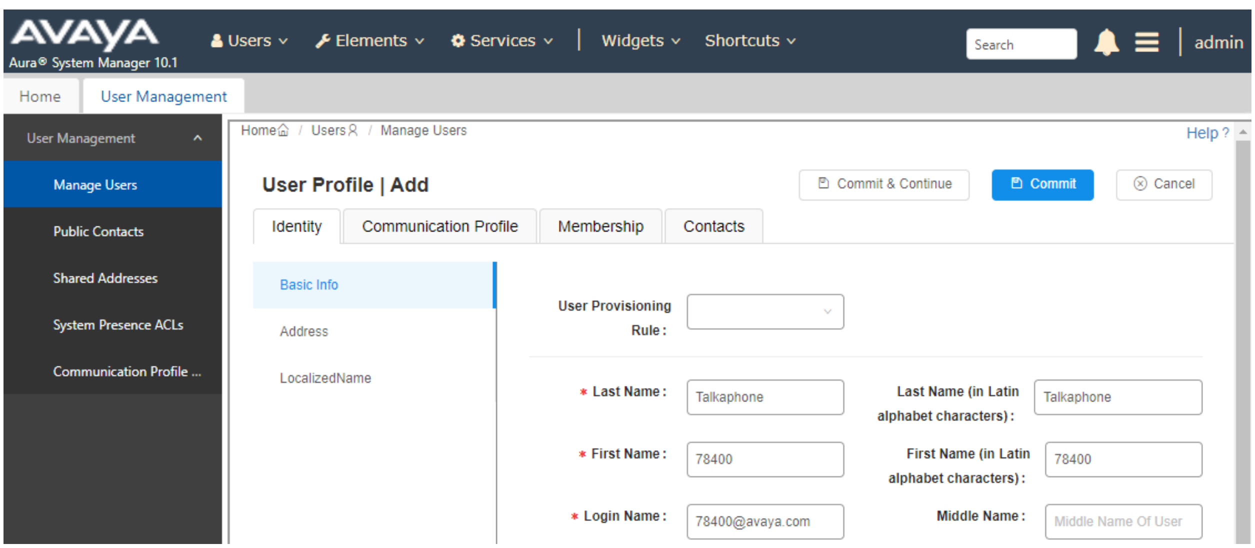
6.3. Administer SIP User

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.



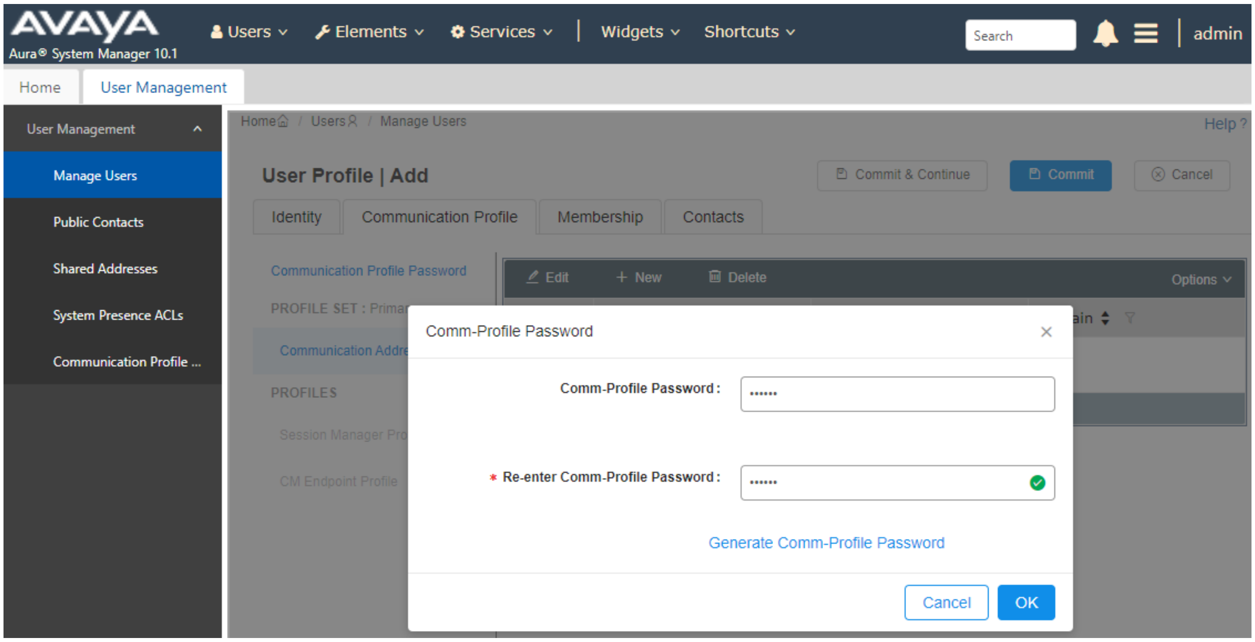
6.3.1. Identity

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 VOIP-220C SIP extension and "*<domain>*" is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.



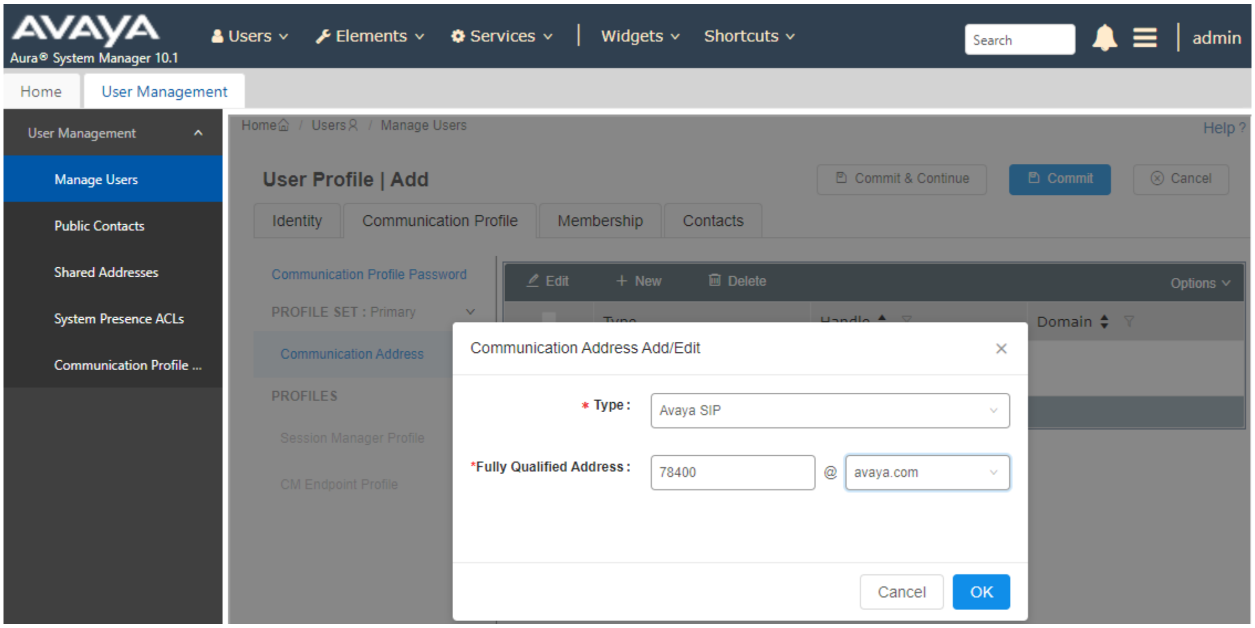
6.3.2. Communication Profile

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**.



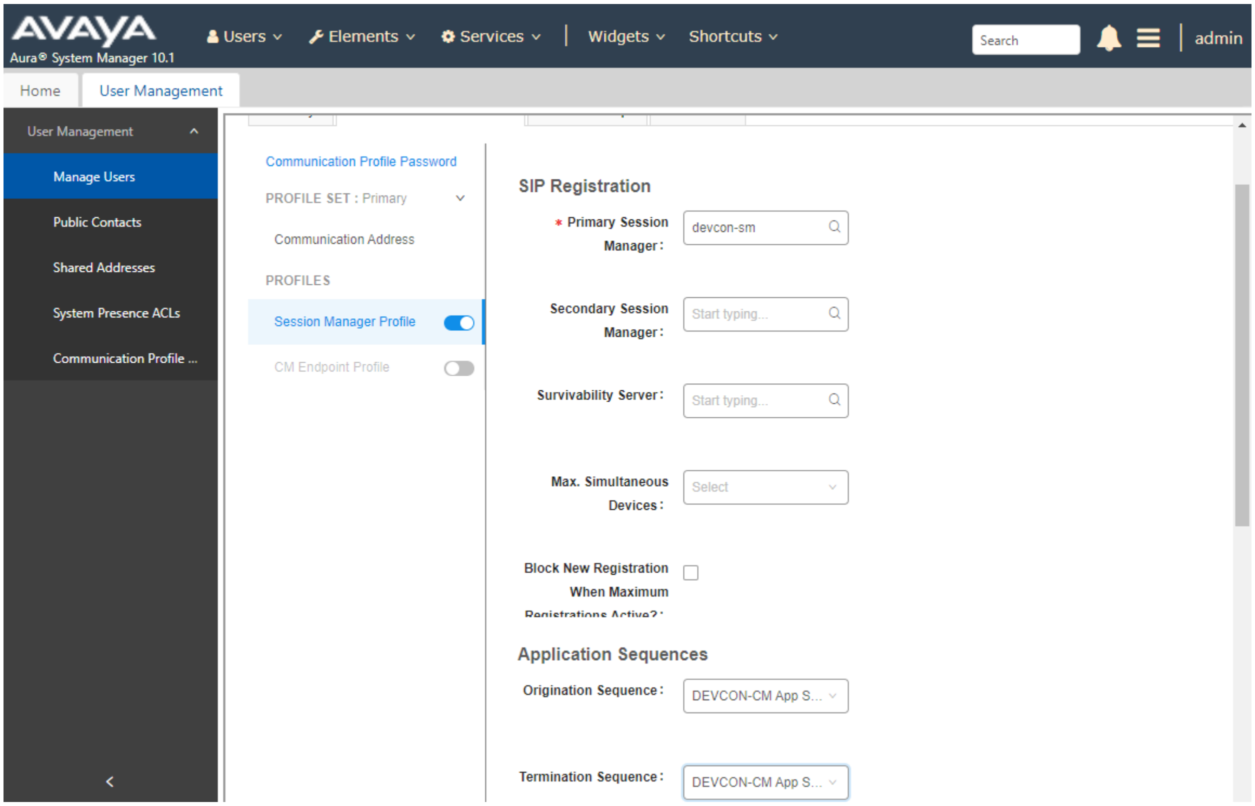
6.3.3. Communication Address

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**.

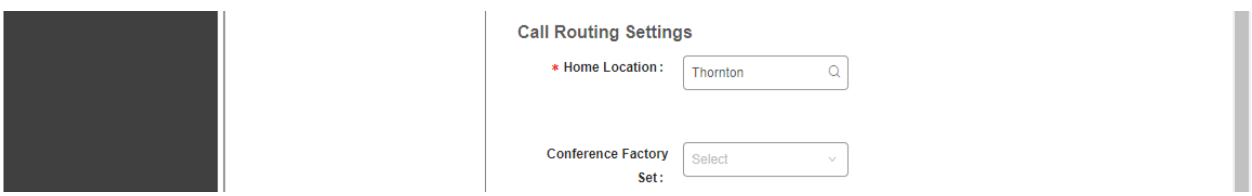


6.3.4. Session Manager Profile

Click on 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.

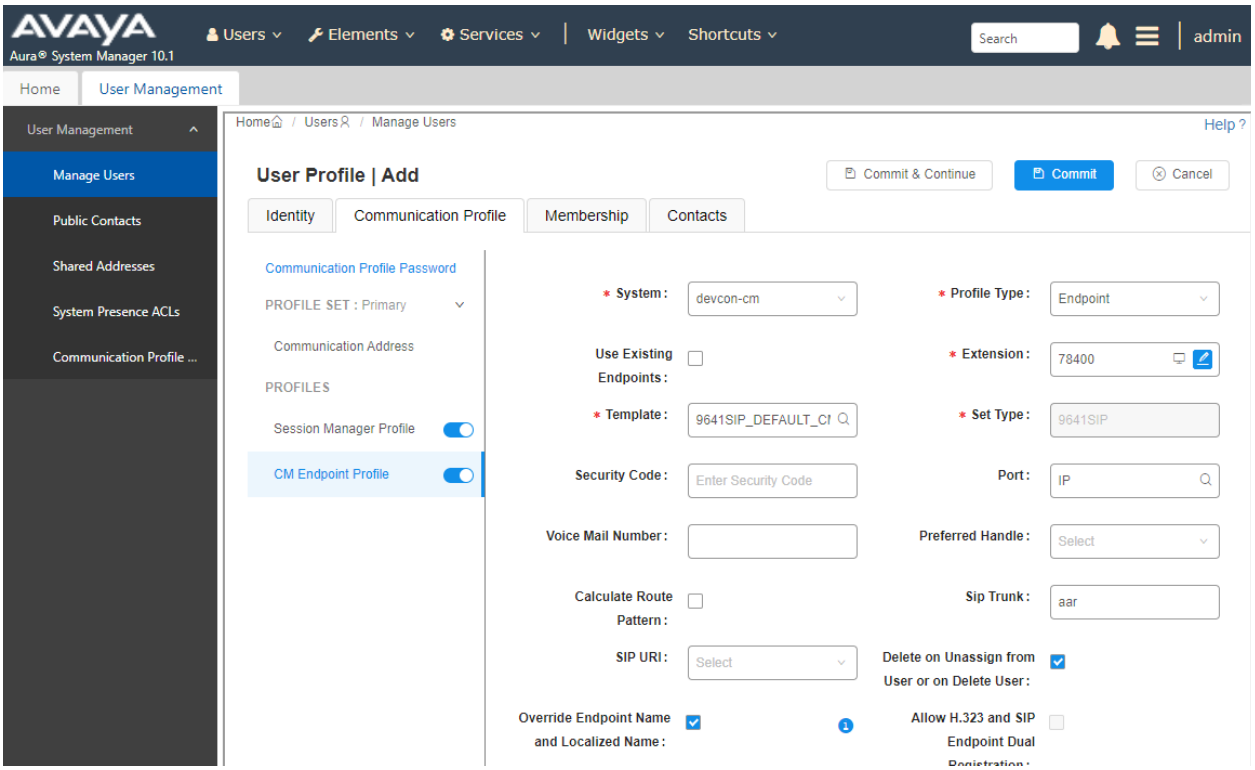


Scroll down to the **Call Routing Settings** section to configure the **Home Location**.



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 *9641SIP_DEFAULT_CM_8_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields.



7. Configure Talkaphone VOIP-220 Series IP Call Station

This section covers the configuration of the Talkaphone VOIP-220 Series IP Call Station. The following procedures are covered:

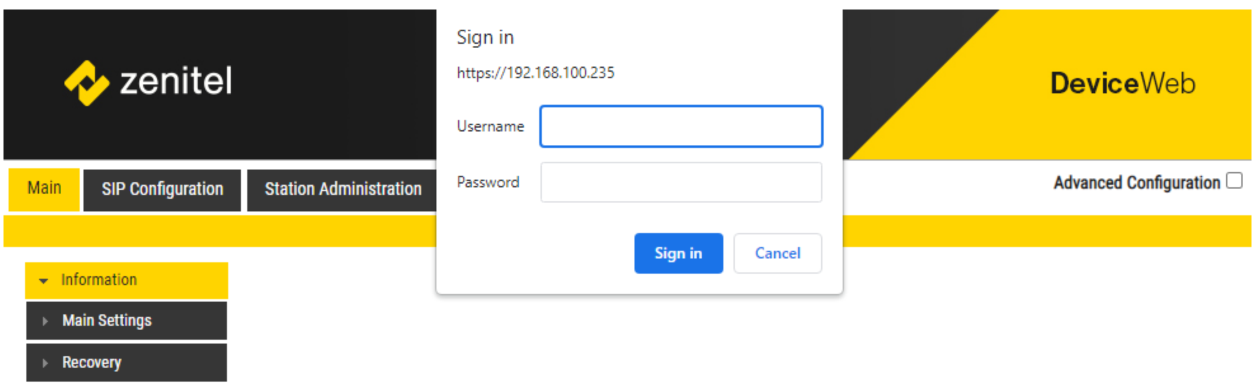
- Launching the Web Administration Interface
- Network Configuration
- SIP Configuration
- Configure Direct Access Keys
- Upload TLS Certificate

7.1. Launching the Web Administration Interface

Talkaphone IP Call Stations are pre-configured with the following default values:

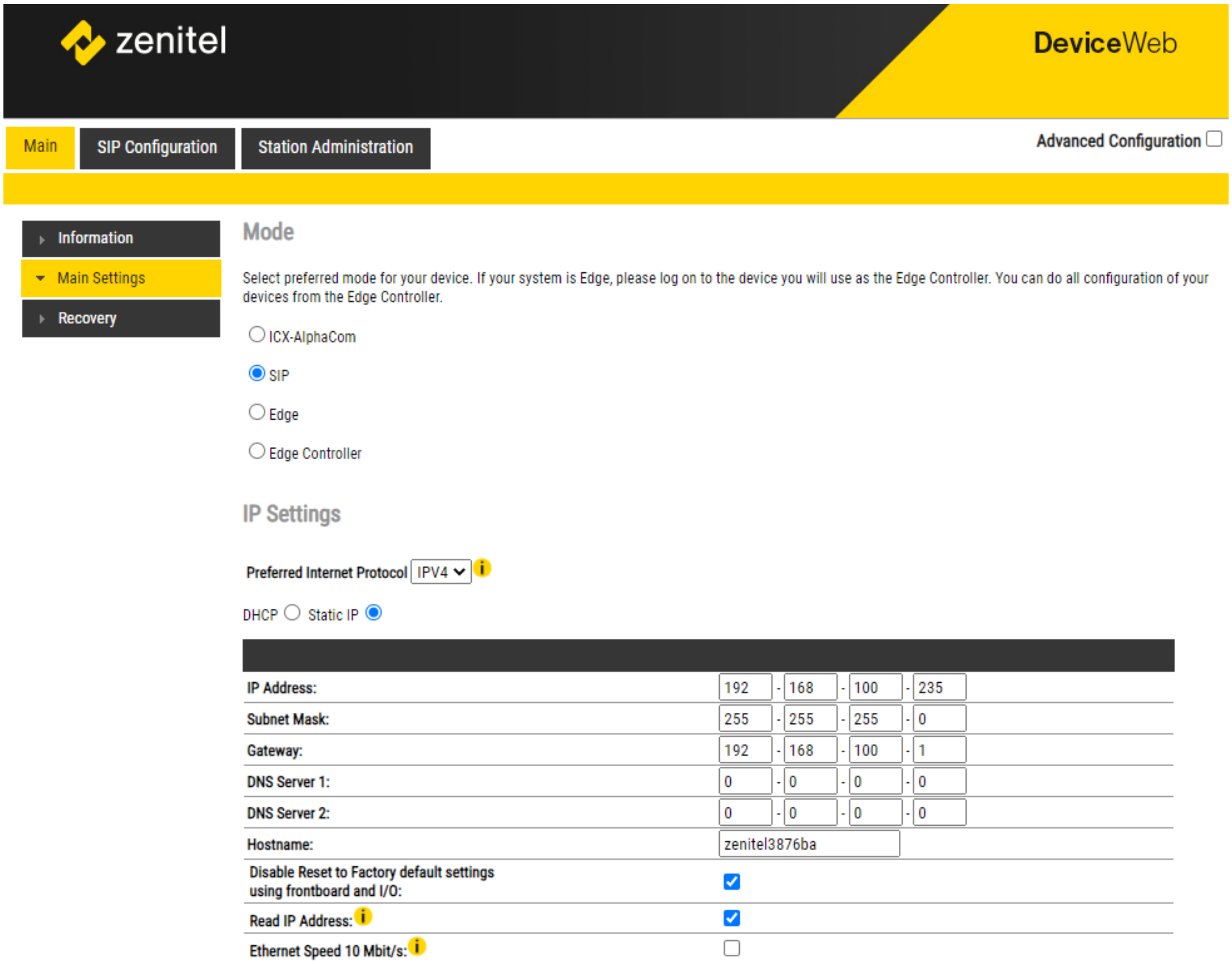
- **IP Address:** 192.168.1.10
- **Username:** admin
- **Password:** alphaadmin

Ensure that the administration PC and Talkaphone IP Call Station are connected to the LAN. Open a web browser and enter the default IP address of the Talkaphone IP Call Station in the URL field. The browser prompts for authentication. Log in with the appropriate credentials.



7.2. Network Configuration

To modify the IP network configuration of VOIP-220C navigate to the **Main → Main Settings** page. Verify that the **Mode** is set to *SIP*. Configure the IP settings so that it conforms to the customer network requirements.



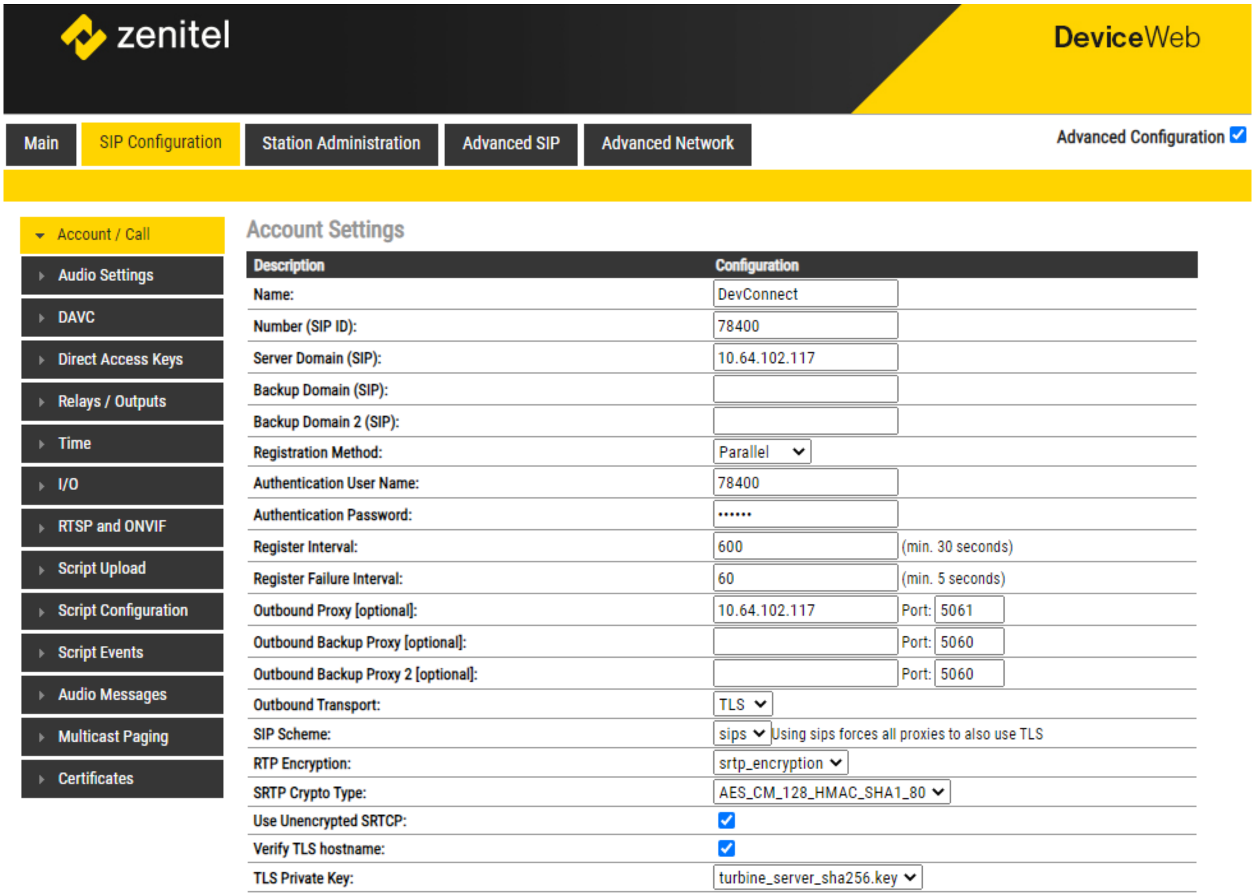
7.3. SIP Configuration

Navigate to **SIP Configuration → Account / Call** to configure the SIP settings of VOIP-220C. The following SIP configuration enables TLS/SRTP; however, UDP/RTP is also supported. Configure the following parameters.

Under **Account Settings**:

- **Name:** Specify a display name (e.g., *DevConnect*).
- **Number (SIP ID):** Specify the SIP number (e.g., *78400*) configured in **Section** Error! Reference source not found..
- **Server Domain:** Specify the IP address of Session Manager (e.g., *10.64.102.117*).
- **Authentication User Name:** Specify the SIP number VOIP-220C (e.g., *78400*).
- **Authentication Password:** Specify the SIP password configured in **Section 6.3.2**.
- **Register Interval:** Set the SIP registration interval (e.g., *600* seconds). Session Manager was configured to accept a minimum of 600 seconds.
- **Outbound Proxy 1**
- **(optional):** Specify the IP address of Session Manager (e.g., *10.64.102.117*).
- **Port:** Specify the SIP port (e.g., *5061*).
- **Outbound Transport:** Set to *TLS*.
- **SIP Scheme:** Select *sip* or *sips*. *sips* was used for the compliance test.
- **RTP Encryption:** Select *srtp_encryption* to enable SRTP.
- **SRTP Crypto Type:** Select *AES_CM_128_HMAC_SHA1_80*. To match the **Crypto Suite** configured in Communication Manager in **Section 5.4**.
- **Use Unencrypted SRTCP:** Enable unencrypted SRTCP. Avaya H.323 phones do not support encrypted SRTCP.
- **Verify TLS hostname:** Enable TLS hostname verification.
- **TLS Private Key:** Accept default value of *turbine_server_sha256.key*.

Note: The TLS certificate is uploaded in **Section 7.5**.


zenitel
DeviceWeb
Main
SIP Configuration
Station Administration
Advanced SIP
Advanced Network
Advanced Configuration
Account / Call
Audio Settings
DAVC
Direct Access Keys
Relays / Outputs
Time
I/O
RTSP and ONVIF
Script Upload
Script Configuration
Script Events
Audio Messages
Multicast Paging
Certificates
Account Settings
Description
Configuration
Name:
DevConnect
Number (SIP ID):
78400
Server Domain (SIP):
10.64.102.117
Backup Domain (SIP):
Backup Domain 2 (SIP):
Registration Method:
Parallel
Authentication User Name:
78400
Authentication Password:
••••••
Register Interval:
600
(min. 30 seconds)
Register Failure Interval:
60
(min. 5 seconds)
Outbound Proxy [optional]:
10.64.102.117
Port: 5061
Outbound Backup Proxy [optional]:
Port: 5060
Outbound Backup Proxy 2 [optional]:
Port: 5060
Outbound Transport:
TLS
SIP Scheme:
sips
Using sips forces all proxies to also use TLS
RTP Encryption:
srtp_encryption
SRTP Crypto Type:
AES_CM_128_HMAC_SHA1_80
Use Unencrypted SRTCP:
Verify TLS hostname:
TLS Private Key:
turbine_server_sha256.key

In the **Call Settings** section, enable auto answer, if desired. To view additional call settings, select the **Advanced Configuration** checkbox as shown above.

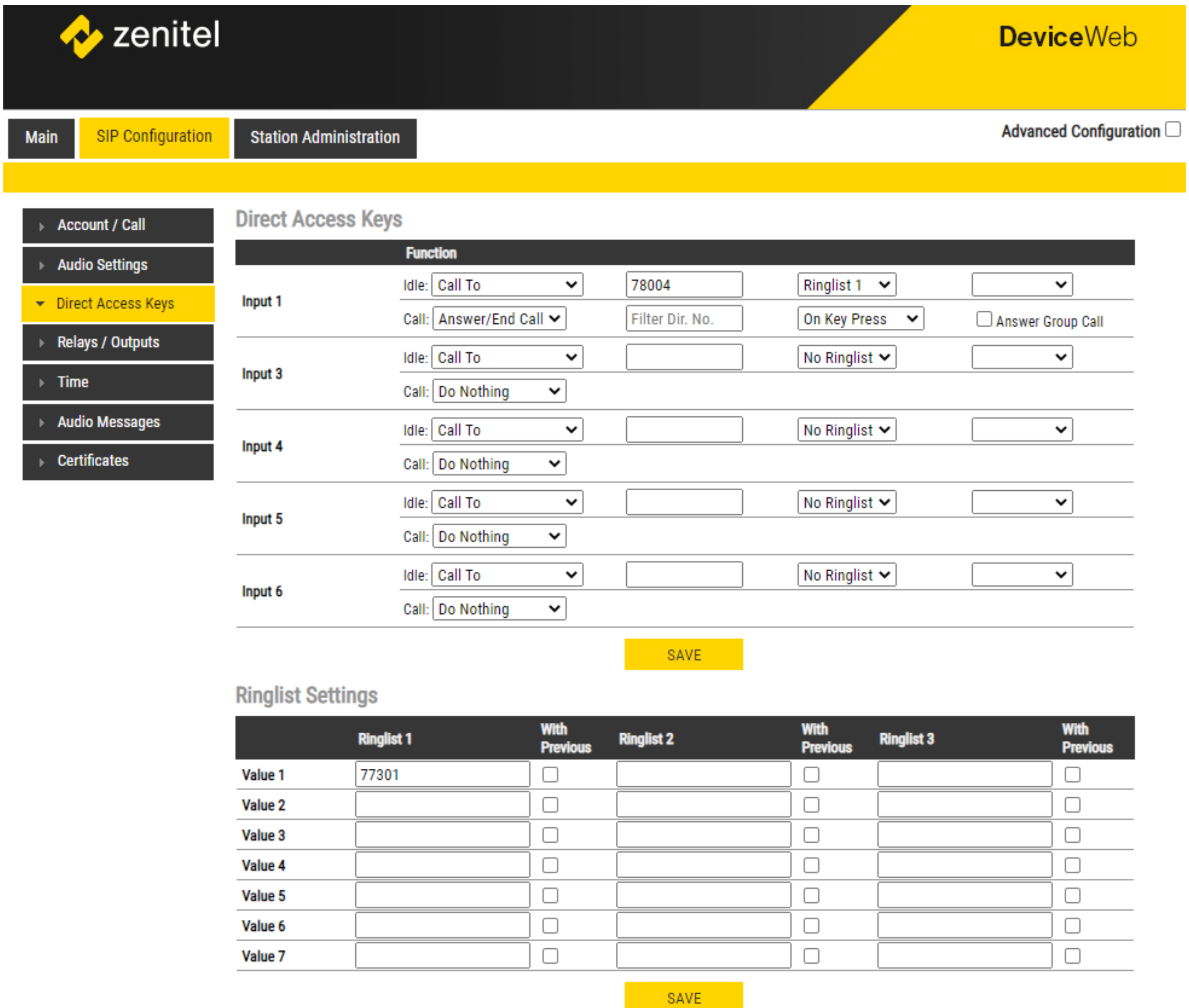
All of the default settings were used for the compliance testing, but this section also shows the codec configuration and is displayed for informational purposes.

Call Settings

Description	Configuration
Enable Auto Answer:	☑
Auto Answer Delay:	0 seconds. Max 30 seconds.
Press and Hold Time:	0 seconds. Max 60 seconds. Defines how long a DAK key/Input must be pressed before the call is established.
Max Trying Time:	15 How long to wait on response before hanging up.
Max Ringing Time:	120 How long a call can be ringing before hanging up.
Max Conversation Time:	3600 How long a call can be in conversation before hanging up.
Max MP114 Speech Time:	0 How long between MP114 speech start/end before hanging up.
Max Queued Time:	20 How long a call can be queued before hanging up.
Max Queued Calls:	4 How many incoming calls can be queued. Max 5.
Use NAT Keep Alive:	☐
Dialing Method:	Enbloc Dialing
Enbloc Dialing Timeout:	No Timeout
DTMF method:	SIP INFO
Conversation Mode:	Duplex
PTT Mode:	Mic and speaker is controlled by PTT button
Resume Call Automatically:	☑ Resume Call On-Hold Automatically After Emergency Priority Ends
Remote Controlled Audio Direction:	☐ (Received DTMF * to listen, DTMF # to talk, DTMF 0 for open duplex)
SIP Message Controlled Audio Direction:	☐ (SIP MESSAGE controls audio direction)
Boost Volume on Push To Talk:	☐
Override Remote Push To Talk:	☐
Force Open Duplex Using DTMF:	-
Send DTMF */# with M key:	☑
RTP Timeout value:	0 seconds. 0 = RTP Timeout Disabled.
SIP OPTIONS Timeout value:	0 seconds. 0 = SIP OPTIONS Timeout Disabled.
Codec g729:	Medium Priority
Codec g722:	High Priority
Codec g711a:	Medium Priority
Codec g711u:	Low Priority
Tone Volume:	0 (-1)=disabled, 0=default, [1..4]=[-22..-1]dB

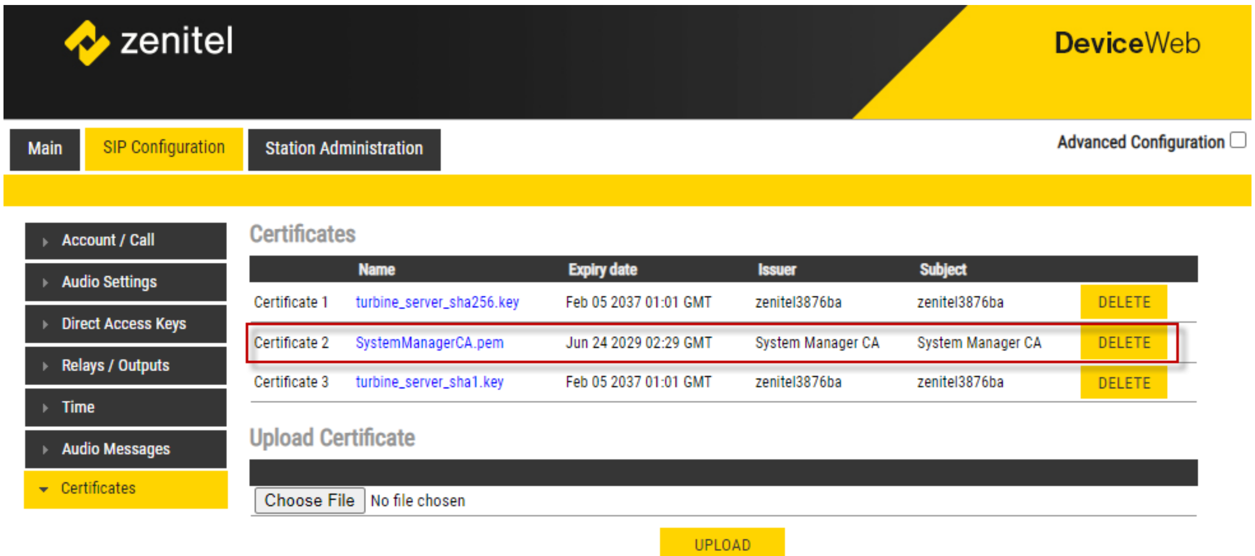
7.4. Configure Direct Access Keys

Navigate to **SIP Configuration → Direct Access Keys** to configure the behavior of VOIP-220C button. **Input 1** is configured to place a *Call To* the specified number, *78004*, when VOIP-220C is **Idle** and is associated with *Ringlist 1*. For incoming calls and active calls, the VOIP-220C button is configured to *Answer/End Call*. In the **Ringlist Settings** section, **Ringlist 1** is configured to try another number, *77301*, if the first call attempt to *78004* is not answered.



7.5. Upload TLS Certificate

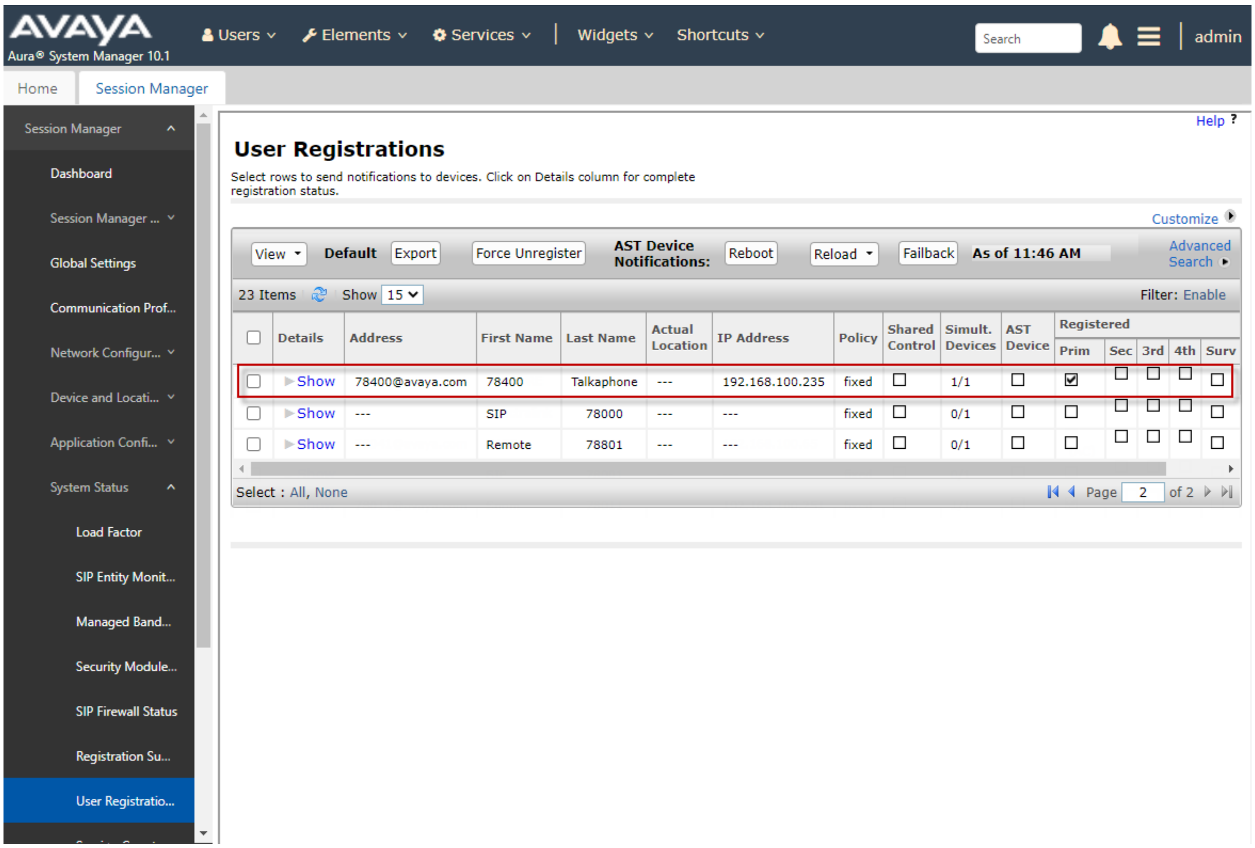
To upload the TLS certificate to VOIP-220C, navigate to **SIP Configuration → Certificates** and upload the certificate in the **Upload Certificate** section. The installed certificate is shown below in the **Certificates** section. For the compliance test, the TLS certificate was obtained from the System Manager CA.



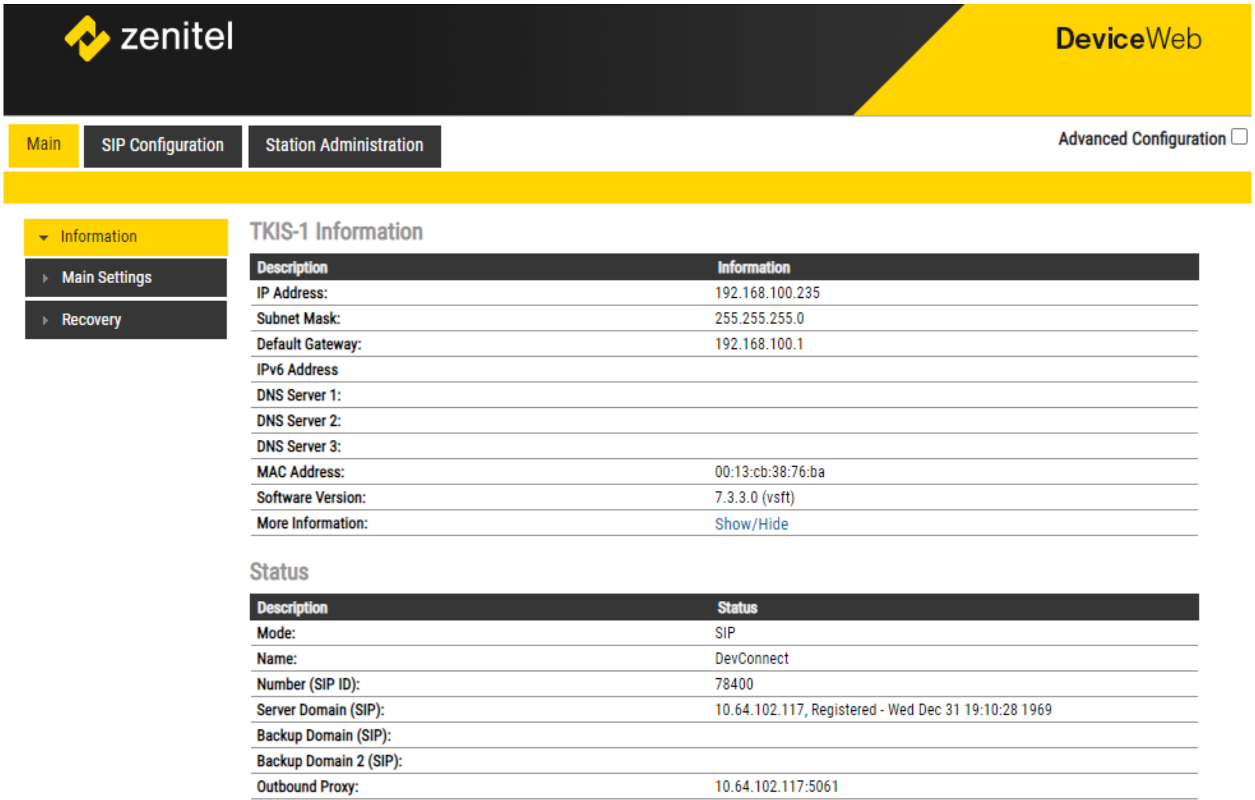
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Talkaphone VOIP-220 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

1. Verify that VOIP-220C has successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status (i.e., registered with the primary Session Manager per the checkbox).



2. Alternatively, the VOIP-220C registration status may be viewed on the VOIP-220C web interface. Navigate to **Main → Information** and verify that VOIP-220C is *Registered* in the **Server Domain (SIP)** field.



3. Place an incoming/outgoing call to to/from VOIP-220C, verify 2-way audio and proper call termination.

9. Conclusion

These Application Notes have described the administration steps required to integrate the Talkaphone VOIP-220 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Talkaphone IP Call Stations successfully registered with Session Manager and basic telephony features were verified. All test cases passed with observations noted in **Section 2.2**.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 3, December 2022, available at http://support.avaya.com.

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

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

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

ATTACHMENT 1

TALKAPHONE

7530 North Natchez Avenue
Niles, Illinois 60714

T: 773-539-1100
F: 773-539-1241
talkaphone.com

February 20, 2023

Re: Common Platform for VOIP-200 Series Compact IP Call Stations

Avaya Inc.
350 Mt. Kemble Avenue
Morristown, NJ 07960

Attn: Avaya DevConnect Program

To Whom It May Concern:

Talkaphone's **VOIP-220 Series Compact IP Call Stations** incorporate a common SIP (Session Initiation Protocol) audio intercom PCBA (printed circuit board assembly) and firmware. This SIP audio intercom board is the Zenitel TKIS-1 VoIP Intercom Module and is incorporated under license from Zenitel USA, Inc.

Signage—The signage options outlined on p.7 of the VOIP-220 datasheet (revised on Aug. 17, 2022) only relates to the ADA-compliant features of the faceplate (i.e. the raised lettering and braille) and have no bearing with respect to any SIP interoperability testing.

It should be noted that the nomenclature for signage has carried over from the predecessor product, the VOIP-200 Series, and also applies to that product line.

Camera—Moreover, the camera included with certain VOIP-220 models also has no bearing with respect to the SIP interoperability testing. The camera is a standalone component and does not interact directly with the SIP audio intercom PCBA (i.e. the camera is packaged within a shared enclosure).

It should be noted that this camera arrangement has always been the case and also applies to the predecessor product, the VOIP-200 Series.

If there are further inquiries or concerns, please do not hesitate to contact us.

Sincerely,

Clarence Wong

Clarence Wong
Vice President – Product Management

Encl. (1)