Avaya Solution & Interoperability Test Lab

Application Notes for Conex 4.9.0 from Voxtronic to interoperate with Avaya Session Border Controller for Enterprise R10.1 and Avaya Aura® Application Enablement Services R10.1 for Call Recording - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Voxtronic Conex to successfully interoperate with Avaya Session Border for Enterprise and Avaya Aura® Application Enablement Services. Conex integrates with Avaya Session Border Controller for Enterprise using SIP Recording and Avaya Aura® Application Enablement Services using TSAPI to record various types of calls.

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 for Voxtronic Conex to successfully interoperate with Avaya Session Border for Enterprise and Avaya Aura® Application Enablement Services. Conex integrates with Avaya Session Border Controller for Enterprise using SIP Recording and Avaya Aura® Application Enablement Services using TSAPI to record various types of calls.

Conex can be configured to monitor specific local endpoints and record calls made to or from those endpoints. Calls between or among local endpoints which are each monitored produce multiple voice files, one for each monitored endpoint. Incoming calls to the Call Center via vector directory numbers (VDN) can also be recorded including any announcements that may be played before the call is routed to the dispatcher.

Conex is fully integrated into a LAN (Local Area Network) and includes easy-to-use web-based application.

Note: The term "VoIP Recorder" in this document refers to a system or unit within Conex for the purpose of recording VoIP.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Conex to carry out call recording in a variety of scenarios using SIP Recording on the Avaya Session Border Controller for Enterprise (ASBCE).

Compliance testing focused on using Implicit Users and Application Sequencing to allow calls to VDN's to be recorded from the moment the call arrives at the VDN. This is achieved by routing the call to the SBCE and back to the VDN again, basically "looping in" the Session Border Controller to allow the call to be recorded.

For compliance testing all "dispatchers" were Avaya SIP endpoints registered as Remote Workers via the Session Border Controller. Bridged Appearances were used to route the calls to the dispatchers. Each remote worker phone can have several bridged appearance buttons added. These can be the same bridged appearance extensions for all dispatchers allowing each VDN call to appear to several dispatchers at once. The Vector is programmed to route the call to bridged appearance A first and then B, then C and so on. For compliance testing two remote workers were setup with two bridged Appearance buttons each. Each dispatcher was configured with the same bridged appearance number and when the call hit that number all the dispatcher's phones rang at the same time was answered by whoever was either free or first to answer to call.

For compliance testing an announcement was played before the call was routed to the bridged appearance number, this announcement was recorded along with the conversation with the dispatcher. The connection to Application Enablement Services using TSAPI allowed Conex to make sense of the SIP Recordings using the UUI data from the initial ISDN caller and other call events that are passed from Application Enablement Services.

Recording of a call routed through a VDN:

- Call coming in at G450 (with UUI-data), VDN in CM is first touchpoint.
- Routing from CM to SM.
- Application Sequencing to ASBCE (to initiate SIPREC to the VoIP Recorder) and back to CM.
- Via AES-TSAPI monitoring, UUI-data are sent to the VoIP Recorder.
- CM Announcement and routing to SIP-Stations.
- As long as the call is active in CM, the call will be recorded via SIPREC.
- AES TSAPI delivers metadata from the call to the VoIP Recorder.

Recording of Remote Worker (SIP-Phone registered at ASBCE):

- SIPREC is set to the Remote Worker configuration at ASBCE.
- All incoming and outgoing calls from Remote Worker Station will be sent as SIPREC-Stream to the VoIP Recorder.
- Using AES, all additional call information is sent to the VoIP Recorder.
- As long as the Remote Worker Station has an active call, this will be recorded via SIPREC.
- AES TSAPI delivers metadata from the call to the VoIP Recorder.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Conex did not make use of any specific encryption features, as per the request of Voxtronic.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Recording of Inbound calls directly to Remote Workers** – Test call recording for inbound calls to remote workers both from other Avaya endpoints and from PSTN callers.
- **Recording of Outbound calls from Remote Workers** – Test call recording for outbound calls from remote workers both to other Avaya endpoints and to PSTN endpoints.
- **Recording of VDN calls from PSTN** - Test call recording for calls made to a VDN with an announcement played and then routed to the remote worker phones.
- **Recording of transferred/conferenced calls** - Test call recording for calls that are transferred or conferenced.
- **Serviceability testing** - The behavior of Conex under different simulated LAN failure conditions.

The serviceability testing focused on verifying the ability of Conex to recover from disconnection and reconnection to the Avaya solution.

The following Extensions and VDN's were used for compliance testing.

- Remote Worker 3172, set as Dispatcher 1.
- Remote Worker 3173, set as Dispatcher 2.
- Calls to VDN 3950 were routed to Implicit User 7253951 using Vector 50.
- Calls were routed back to VDN 3951 using an Adaptation on Session Manager.
- Calls to VDN 3951 were routed to Bridged Appearances 3050 and 3051 using Vector 51.
- Remote Workers assigned Bridged Appearances 3050 and 3051.

2.2. Test Results

All functionality and serviceability test cases were completed successfully, with the following observations.

1. The connection to Conex used UDP as the transport protocol. When an attempt was made to connect using TCP, the connection was made successfully but an issue with the SBCE meant that some messages were being sent over UDP, even though TCP was the selected protocol. Avaya are investigating this issue.
2. If a CODEC is renegotiated using REINVITE during the setup of the call, this REINVITE is not sent to the VoIP Recorder. Avaya are investigating this issue but is currently stated to be "as per design".

2.3. Support

Technical support can be obtained for Conex from Voxtronic as follows:

- Email: support@voxtronic.com
- Website: http://www.voxtronic.com
- Phone: +43 1 8174846 600

3. Reference Configuration

Figure 1 shows the network topology during interoperability testing. The setup show the Remote Workers connected to the Avaya platform using the SBCE. "Dispatchers" using the Remote Worker phones have bridged appearance buttons configured on them. This is how the calls are routed to the dispatchers.

When a call comes into VDN 3950, the call is then routed to 7253951, this is routed to Session Manager where Implicit User 7253951 uses Application Sequencing to loop in the Session Border Controller and the recording starts. The call is then routed back to Communication Manager stripping the first three digits leaving the number 3951 which is a VDN on Communication Manager.

VDN 3951 then routes the call to the Bridged Appearance buttons on the Remote Workers effectively delivering the caller to the Remote Worker dispatchers all configured with the same Bridged Appearance buttons depending on the initial VDN called.

RTP is sent to Conex using SIP Recording on SBCE, the call events from the TSAPI connection to AES allows the VoIP Recorder to formulate the calls and give information on the call at hand.

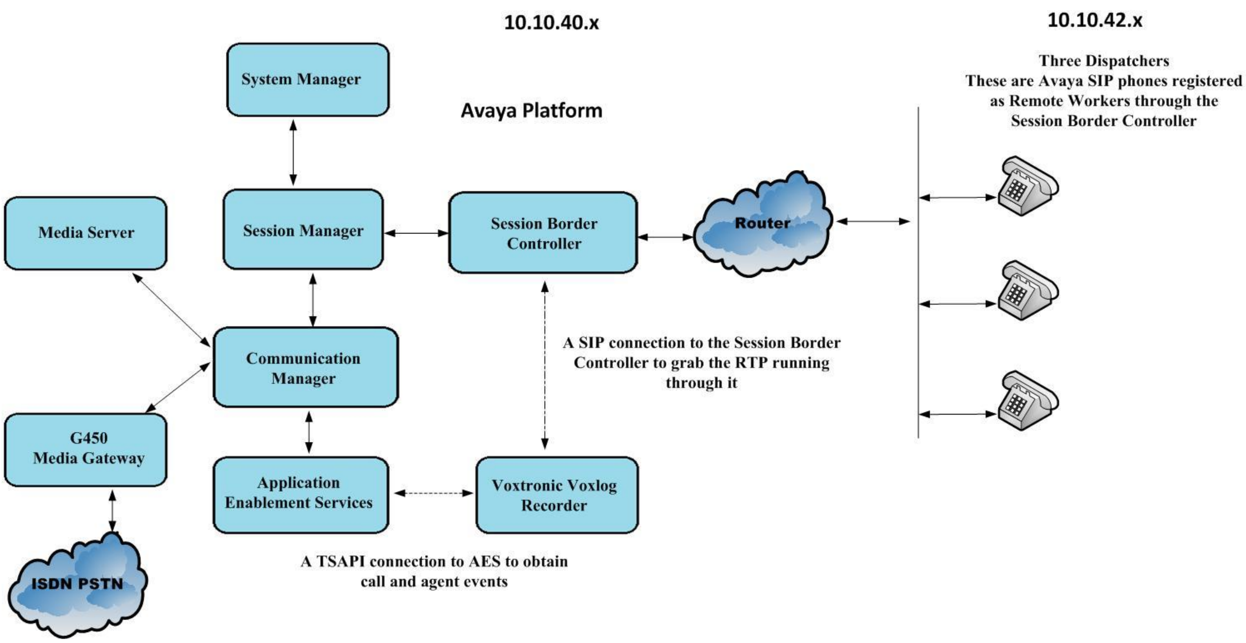


Figure 1: Avaya Session Border Controller for Enterprise R10.1 with Avaya Aura® Application Enablement Services R10.1 and Conex from Voxtronic

4. Equipment and Software Validated

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

Equipment/Software	Release/ Version
Avaya Aura® Application Enablement Services	R10.1 10.1.0.2.0.12-0
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432 10.1.0.0-34-22640-hotfix-11102022 SBCE Version 10.1.0.0-32-21432 Kernel 3.10.0-1160.76.1.el7.AV1 Config API 10.1.0.0-22609 GUI 10.1.0.0-22609 Application 10.1.0.0-22640 Database 10.1.0.0-21413 ICU 10.1.0.0-22552 PCF Module 10.1.0.0-22491
Avaya Aura® System Manager	System Manager 10.1.0.2 SP2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160
Avaya Aura® Session Manager	Session Manager R10.1 SP2 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Media Gateway G450	42.7.0/2
Avaya J100 Series (H323)	6.8502
Avaya J100 Series (SIP)	4.0.7.0
Avaya 9408 Digital Deskphone	V2.0
Voxtronic Conex	4.9.0

Note: All equipments were running on Virtual Servers.

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 12**.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters and Features
- Configure SIP Trunk
- Configure Call Routing for Voxtronic
- Configure Connection to AES
- Configure VDNs and Vectors for Voxtronic

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

5.1. Verify System Parameters and Features

Each Communication Manager system will have its own setup with different System Parameters and Features configured depending on the requirement of the customer. Here is a snapshot of some of these values that were configured on the DevConnect lab for compliance testing.

5.1.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call uses a minimum of one SIP trunk. Calls that are routed back to stations on Communication Manager or calls that are routed back to Communication Manager to access the PSTN will use two SIP trunks.

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

IP PORT CAPACITIES                                          USED
                 Maximum Administered H.323 Trunks: 12000     10
       Maximum Concurrently Registered IP Stations:  2400     11
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations:  2400      0
          Maximum Concurrently Registered IP eCons:  128       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  36000     1
               Maximum Video Capable IP Softphones:   1150     3
                   Maximum Administered SIP Trunks: 12000     65
  Max Administered Ad-hoc Video Conferencing Ports: 12000      0
   Max Number of DS1 Boards with Echo Cancellation: 688    0
```

On **Page 4**, ensure that both **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

On **Page 6**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                   Page   6 of  12
                                OPTIONAL FEATURES

            Multinational Locations? n             Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y    Station as Virtual Extension? y
                    Multiple Locations? n
                                          System Management Data Transfer? n
         Personal Station Access (PSA)? y             Tenant Partitioning? y
                      PNC Duplication? n     Terminal Trans. Init. (TTI)? y
                  Port Network Support? y             Time of Day Routing? y
                      Posted Messages? y     TN2501 VAL Maximum Capacity? y
                                                     Uniform Dialing Plan? y
                   Private Networking? y   Usage Allocation Enhancements? y
             Processor and System MSP? y
                   Processor Ethernet? y              Wideband Switching? y
                                                                Wireless? n
                        Remote Office? y
         Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

5.1.2. Configure System Features

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 12** for supporting documentation.

```
display system-parameters features                            Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n

             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

5.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the processor interface of Communication Manager (**procr)** and the Session Manager (**sm101x**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name                IP Address
sm101x                10.10.40.12
aespri101x            10.10.40.16
aessec101x            10.10.40.46
g450                  10.10.40.15
procr                 10.10.40.13
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1.1**. In this configuration, the domain name is **greeneyp.sil6.avaya.com**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```
display ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: greaneyp.sil6.avaya.com
    Name: Default region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
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 codecs supported for calls routed over the SIP trunk. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by Voxtronic Conex. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media.

```
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.711A            n         2        20
 2: G.711MU           n         2        20
 3: G.722-64K         n         2        20
 4:

     Media Encryption                Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

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

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm101x**).
- Ensure that the recommended TLS port value of **5062** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              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: sm101x
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 1

Far-end Domain: greaneyp.sil6.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
                                                  Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Session Manager. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. 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.

```
change trunk-group 1                                           Page   1 of  4
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP TRK                     COR: 1        TN: 1     TAC: *801
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                     Signaling Group: 1
                                                   Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Voxtronic to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **120** was used.

```
change trunk-group 1                                           Page   2 of  4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 120

 Disconnect Supervision - In? y  Out? y


           XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

```
change trunk-group 1                                          Page   3 of  4
                                TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



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

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Settings on **Page 4** are as follows.

```
change trunk-group 1                                         Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                      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
```

5.3. Configure Call Routing for Voxtronic

For compliance testing, all callers were initially routed to 7253951 to allow the call to be recorded by the SBCE. When calls come into the VDN 3950 from the PSTN, the Vector associated with this VDN routes the call to Session Manager and on to the SBCE to allow calls to be recorded. Automatic alternate routing (aar) was used to route the calls to Session Manager.

5.3.1. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 725 with a total length of 7 digits were to be sent across the SIP trunk to Session Manager. Type **change dialplan analysis**, to make changes to the dial plan. Ensure that **725** is added with a **Total Length** of **7** and a **Call Type** of **udp**.

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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           4   udp
   2           4   udp
   3           4   ext
   4           4   ext
   725         7   udp
   8           1   fac
   9           1   fac
   *           3   fac
```

5.3.2. Administer Route Selection for Voxtronic Calls

As digits **725xxxx** were defined in the dial plan as udp (**Section 5.3.1**), use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **725** that are **7** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 725                                    Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits      Net Conv Num
  725            7   0                    aar   n
                                                n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to Session Manager begin with **725** and are matched with the **aar** entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 4                                           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
    725                  7     7     1         aar            n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**. This is the SIP Trunk configured in **Section 5.2**.

```
change route-pattern 1                                        Page   1 of   4
               Pattern Number: 1   Pattern Name: SIPTRK
           SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                               n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM   No.  Numbering  LAR
    0 1 2 M 4 W     Request                                  Dgts  Format
 1: y y y y y n  n            unre                                 lev0-pvt  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
```

5.4. Configure Connection to Avaya Aura® Application Enablement Services

It is assumed that a connection to AES is already in place and that the TSAPI connection and switch connection between Communication Manager and AES is fully working. The following section outlines the connection that was setup for compliance testing.

5.4.1. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the IP addresses by using the command **display node-names ip** and noting the IP address for the **procr** and the AES.

```
display node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
sm101x                  10.10.40.12
aespri101x              10.10.40.16
aessec101x              10.10.40.46
g450                    10.10.40.15
procr                   10.10.40.13
```

5.4.2. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES, use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**
- **Enabled:** Set to **y**
- **Local Node:** Set to the node name assigned for the procr in **Section 5.4.1**
- **Local Port:** Retain the default value of **8765**

```
change ip-services                                            Page   1 of   3

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS         y           procr        8765
```

Go to **Page 3** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aespri101x**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 8.2**. The **AE Services Server** must match the administered name for the AES server; this is created as part of the AES installation and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

```
change ip-services                                           Page   3 of   3
                            AE Services Administration

   Server ID    AE Services        Password           Enabled    Status
                   Server
      1:        aespri101x         ********           y          idle
      2:
      3:
```

5.4.3. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                               Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 1990
     Type: ADJ-IP
                                                                      COR: 1
     Name: aespri101x
```

5.5. Configure VDNs and Vectors for Voxtronic

There are two VDNs and two Vectors added to route calls to the SBCE and Remote Workers. The Vector associated with VDN 3950 routes the call to Session Manager, when the call is routed back into Communication Manager again to the second VDN 3951, the call is then routed to the dispatcher via Bridged Appearance buttons that are added on each Remote Workers phone.

5.5.1. Adding VDNs

VDN 3950 is added as the initial number that is called by the PSTN caller, **Vector 50** is associated with the VDN. This Vector is used to route the caller out to Session Manager.

```
add vdn 3950                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                         Extension: 3950                      Unicode Name? n
                             Name*: Voxtronic-PSTN
                       Destination: Vector Number        50
               Attendant Vectoring? n
              Meet-me Conferencing? n
                Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none     Report Adjunct Calls as ACD*? n

        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
SIP URI:
```

Same command is used to **add VDN 3951** and this will use Vector **51**.

```
add vdn 3951                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                         Extension: 3951                      Unicode Name? n
                             Name*: Voxtronic-Implicit
                       Destination: Vector Number        51
               Attendant Vectoring? n
              Meet-me Conferencing? n
                Allow VDN Override? n
                               COR: 1
                               TN*: 1
                          Measured: none     Report Adjunct Calls as ACD*? n


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
SIP URI:

* Follows VDN Override Rules
```

5.5.2. Adding Vectors

VDN 3050 on the previous page uses **Vector 50** to route the call out to the Implicit User configured in **Section 6.2.3**. This will then loop in the SBCE and allow the call to be recorded before being routed back into Communication Manager and onto VDN 3951.

```
change vector 50                                                Page   1 of   6
                                  CALL VECTOR

    Number: 50               Name: Voxtronic Route Implicit
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y  ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing ringback
02 route-to     number 7253951                 cov n if unconditionally
03 wait-time    60   secs hearing ringback
04
05
06
07
08
09
10
```

VDN 3951 uses the following **Vector 51** which plays the announcement and then routes the call to the Bridged Appearance numbers that are assigned to the Remote Workers phones, as shown in **Section 6.4**.

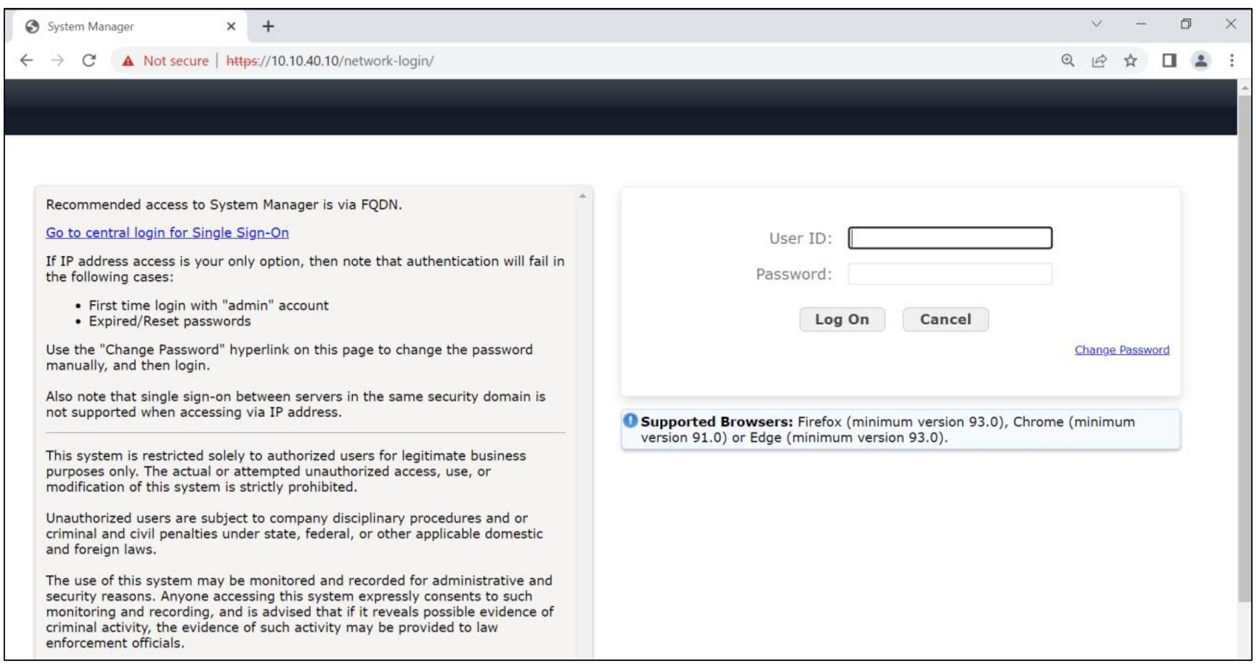
```
change vector 51                                               Page   1 of   6
                                  CALL VECTOR

    Number: 51               Name: Voxtronic-Routing
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n         Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 announcement 3331
02 route-to     number 3050                    cov n if unconditionally
03 wait-time    5   secs hearing ringback
04 route-to     number 3051                    cov n if unconditionally
05 wait-time    60  secs hearing ringback
06
07
08
09
10
```

6. Configure Avaya Aura® Session Manager

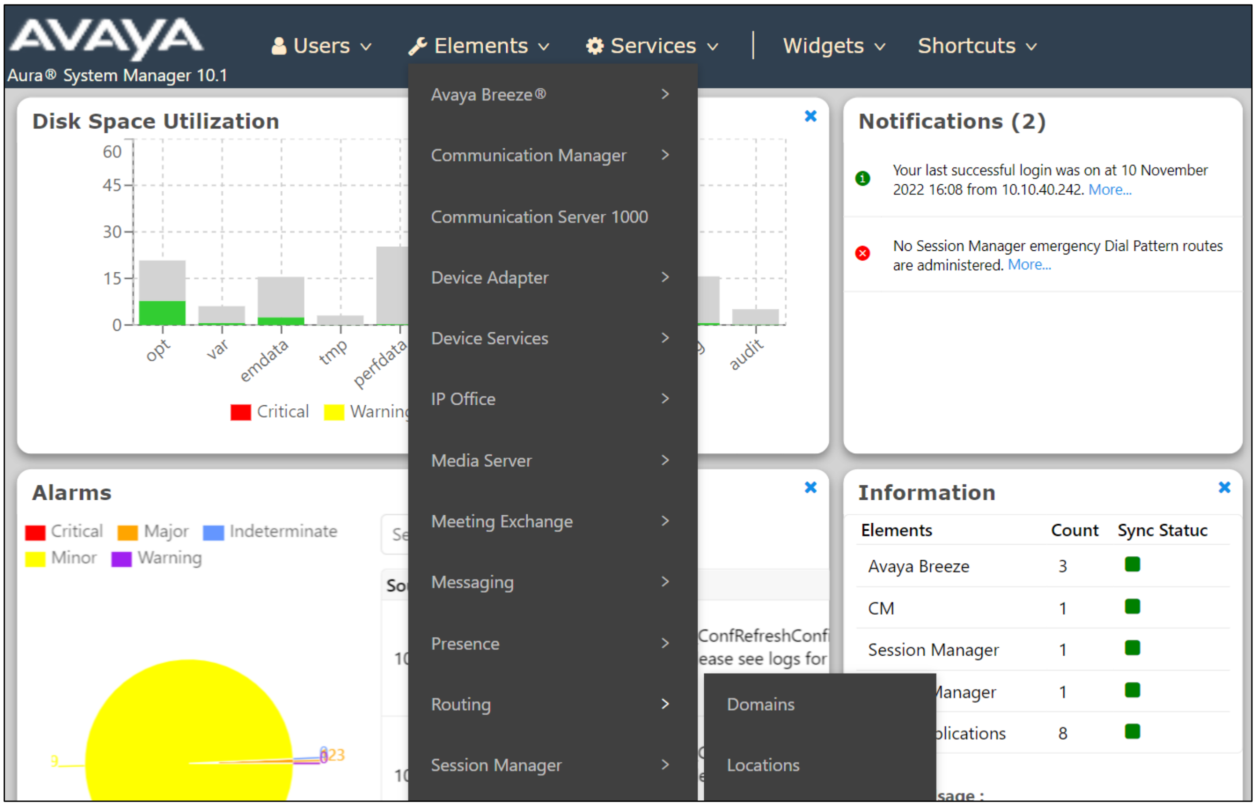
This section provides the procedures for configuring Session Manager to add SIP Entities, Application Sequence, Implicit User and Call Routing to allow VDN calls to be recorded. Configuration is required to route calls to Session Border Controller for Enterprise using Implicit User, looping back into Session Manager, and then routing back to Communication Manager. This looping of the call into the SBCE allows the call to be recorded using SIP Recording on the SBCE. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure Routing to ASBCE
- Configure Routing to Communication Manager
- Configure Remote Workers

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to https://<System Manager FQDN>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing**, as shown below.

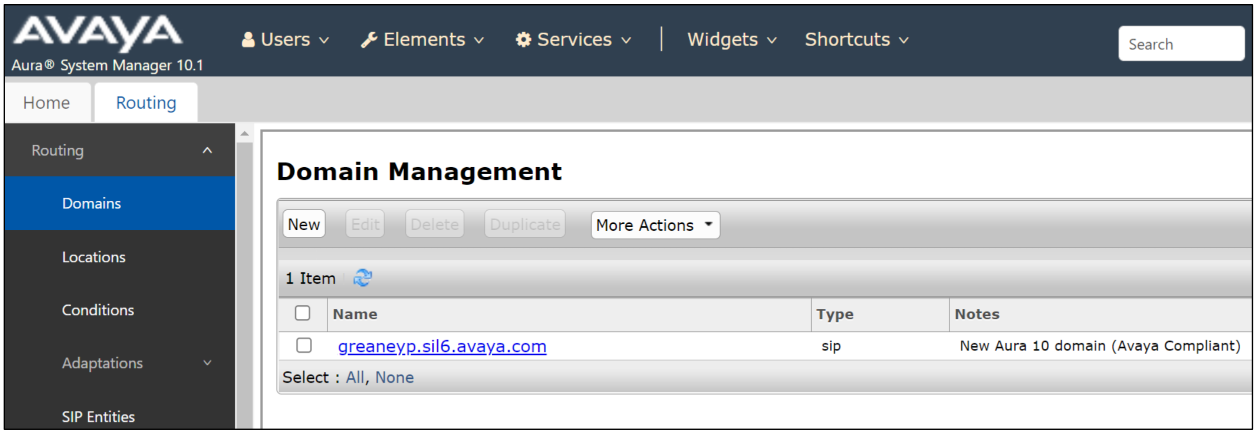


6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

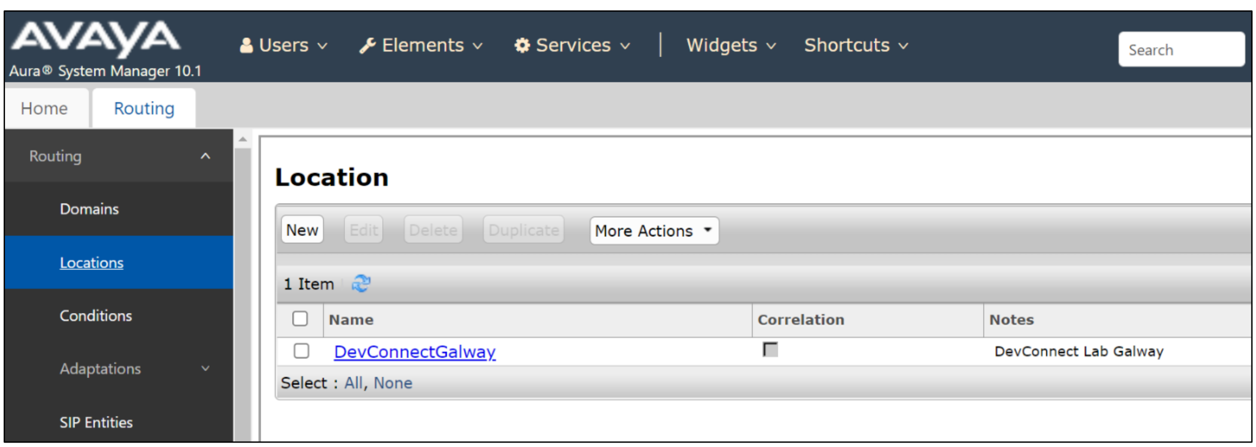
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greeneyp.sil6.avaya.com** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectGalway** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.

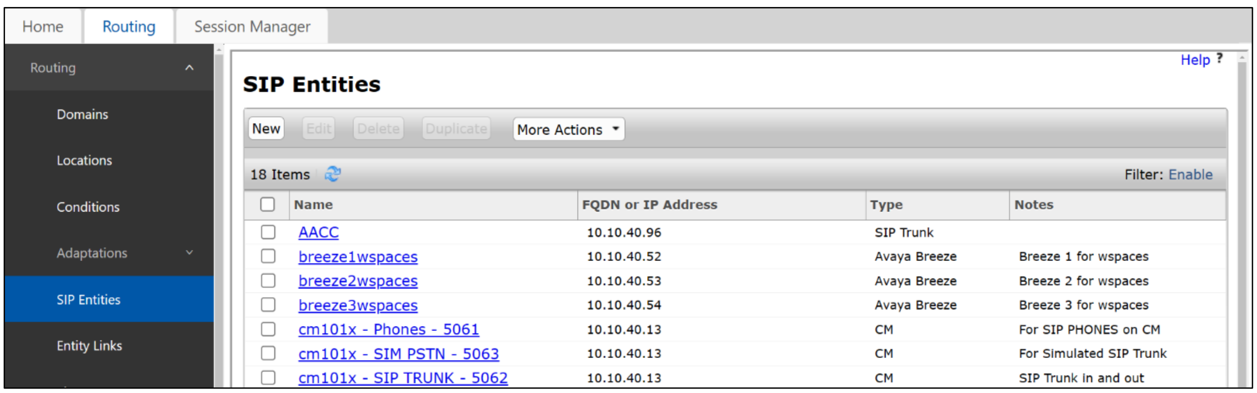


6.2. Configure Routing to Avaya Session Border Controller for Enterprise

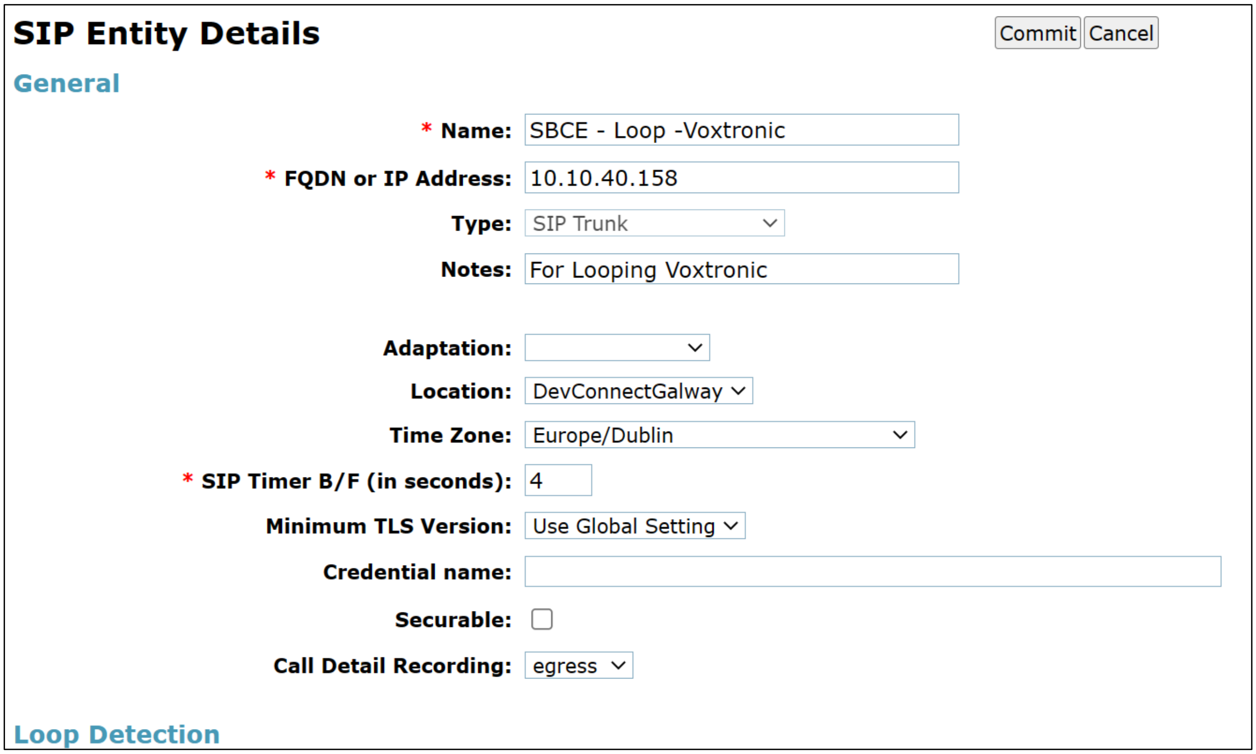
Calls must be routed to the SBCE to allow them to be recorded. Calls made to and from Remote Worker's phones are recorded by the SBCE without the need for any extra setup on Session Manager. However, calls to VDN's that involve announcements and options before the call lands on the Remote Workers phones will not be recorded by default as the call is not yet routed through the SBCE. In order to record such calls, the call will need to loop in the SBCE, which involves the call being routed from Communication Manager to the SBCE and back again into Communication Manager, thus creating a loop. The various setups illustrated in the sections following may refer to this as the "Voxtronic Loop".

6.2.1. Configure SIP Entity for Avaya Session Border Controller for Enterprise

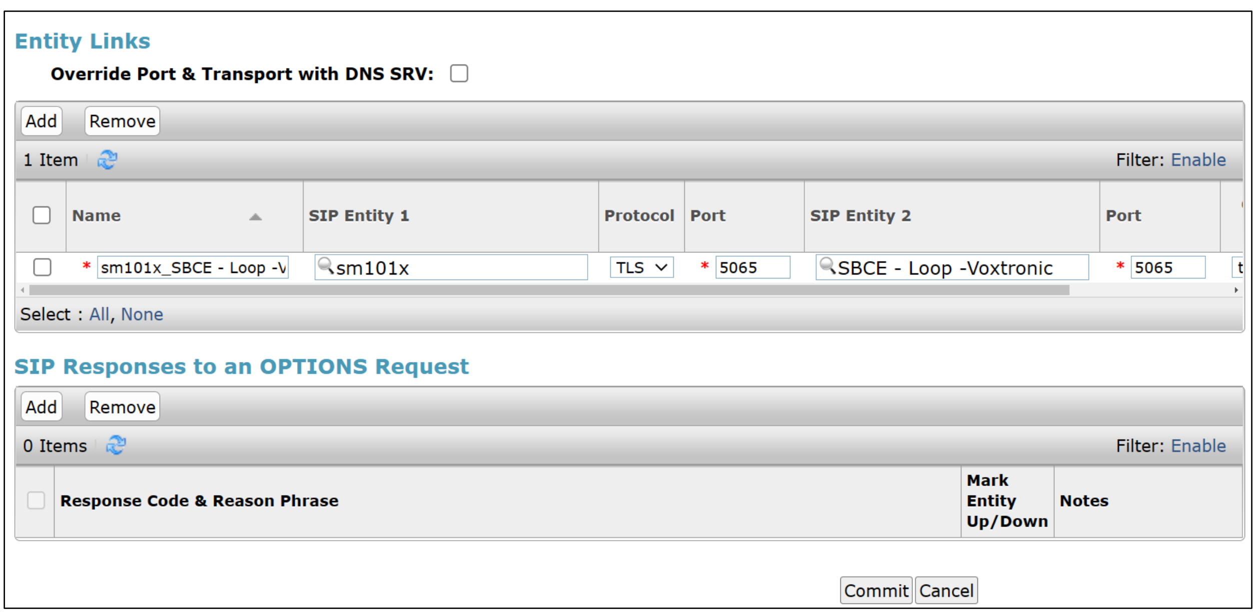
Navigate to **SIP Entities** in the left window and click on **New** in the main window. This will add a new SIP Entity for the SBCE to allow calls to be routed to it.



The inside address for the SBCE is used. This can be obtained from **Section 7.4.** Once the information below is filled in, scroll down to add the Entity Link.

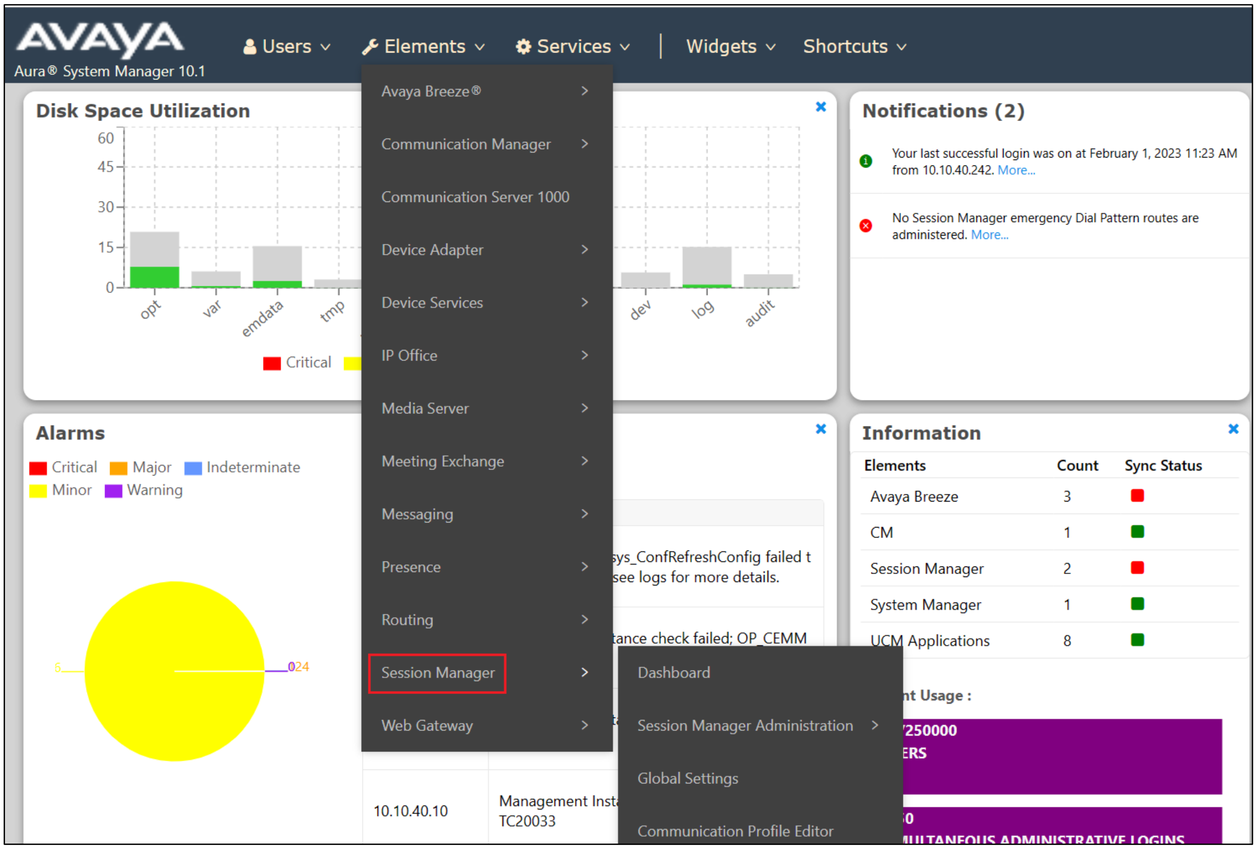


The following Entity link was added for the connection between the SBCE and Session Manager, note that **Port 5065** was used, and this will correspond to that same port in **Section 7.4**.

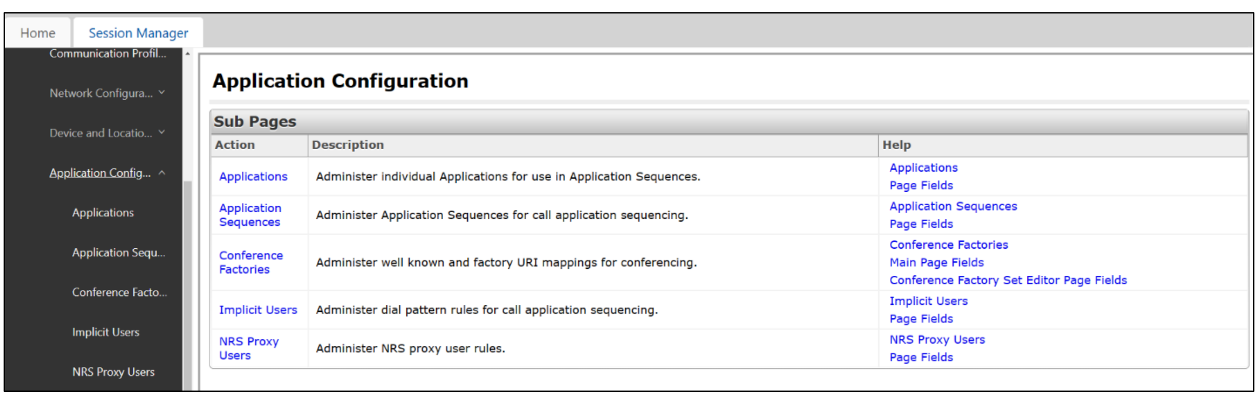


6.2.2. Configure Application Sequence

Navigate to **Elements → Session Manager**.

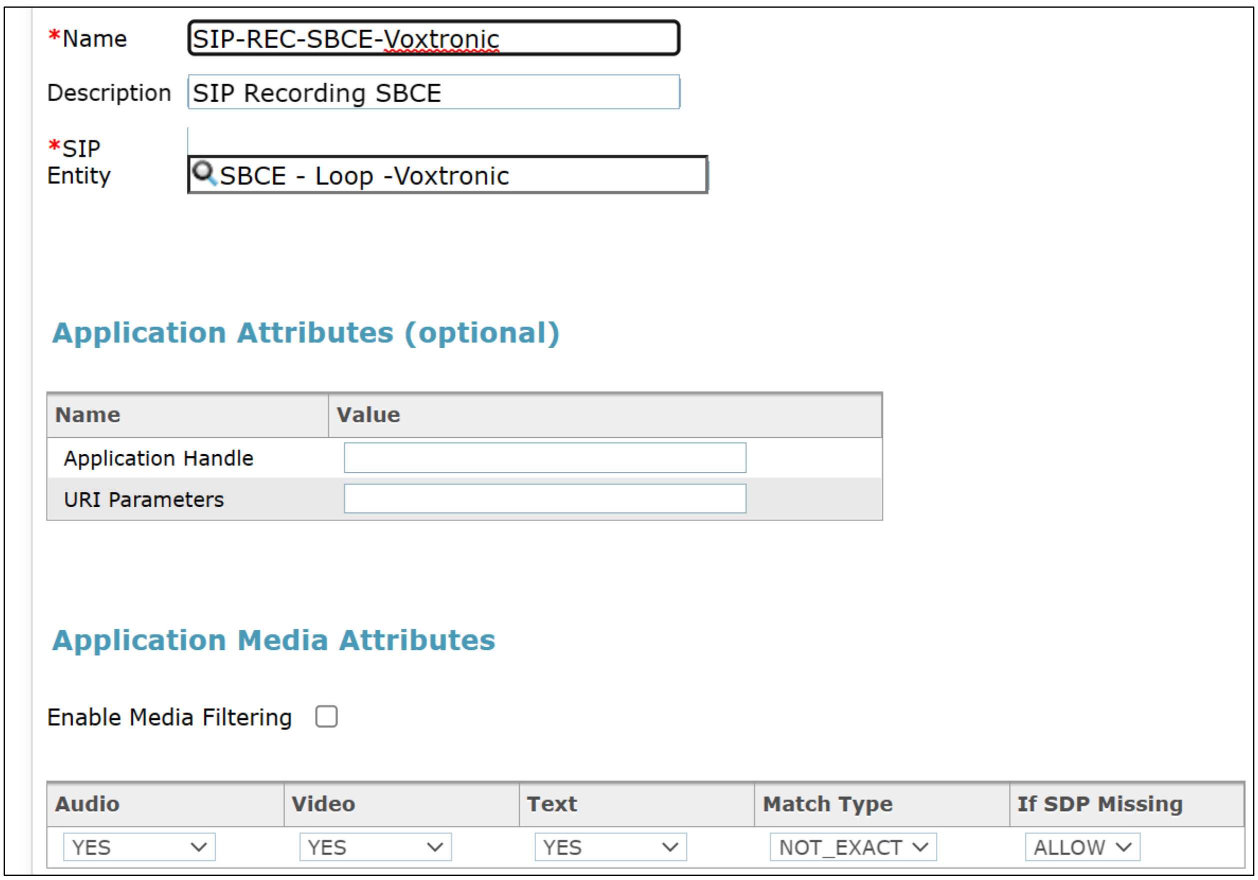


Navigate to **Application Configuration** where the **Applications** and **Application Sequences** can be configured as well as **Implicit Users**. An Application is first configured and then assigned to the Application Sequence.

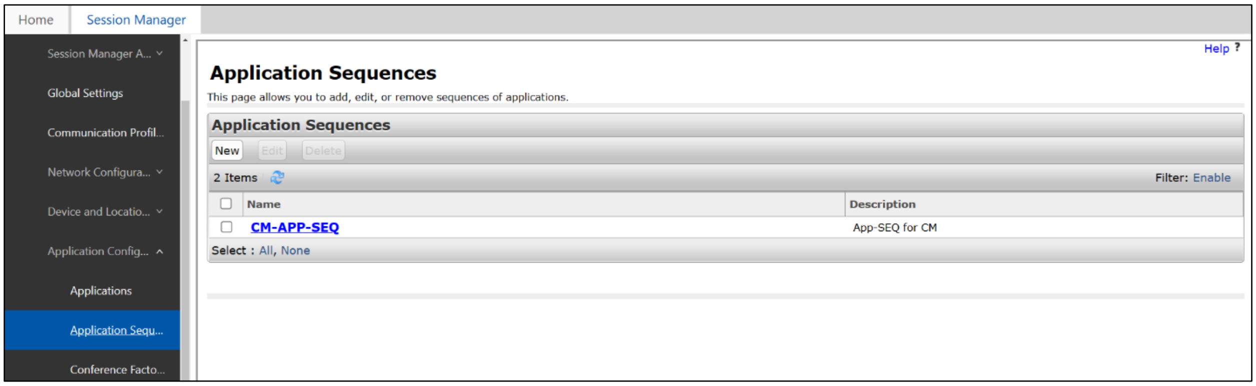


Click on **Applications** in the left window and then **New** in the main window.

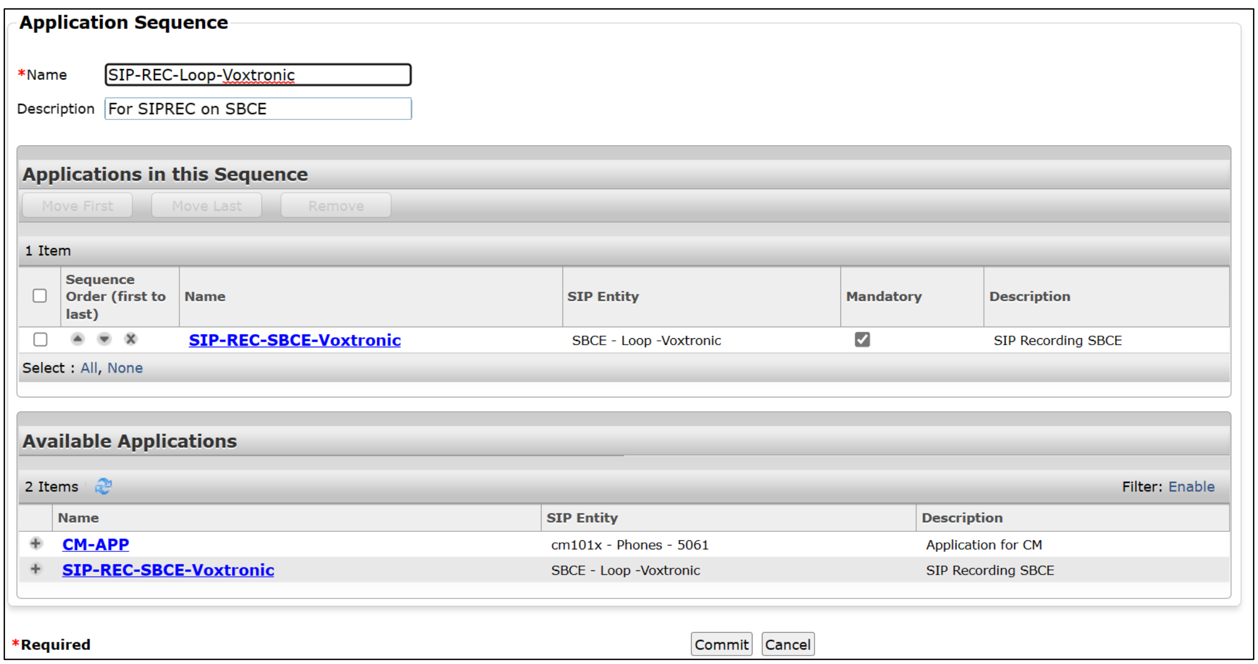
An Application for the Session Border Controller is added as shown below. Note the **SIP Entity** created in **Section 6.2.1** was used.



Navigate to **Application Sequences** in the left window and click in **New** in the main window.

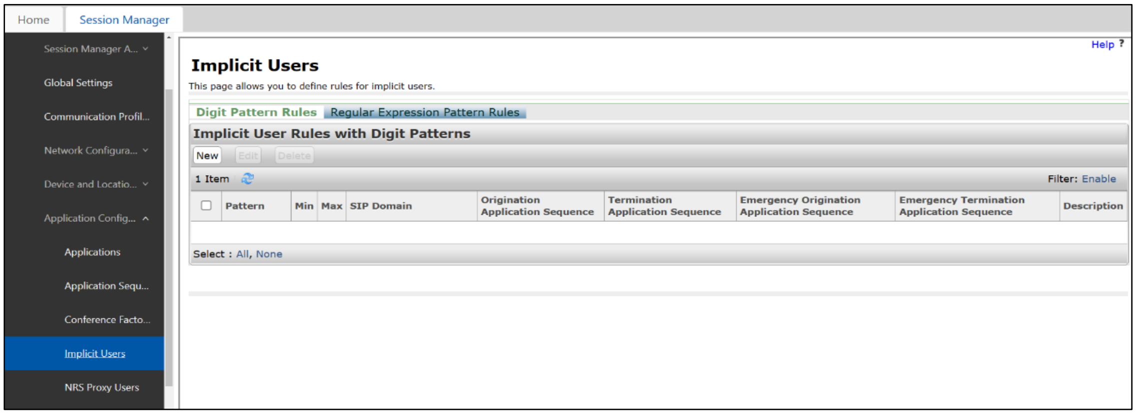


Under the section **Available Applications**, click on the + beside the Application created above, the new Application will then be associated with the Application Sequence being configured here. Click on **Commit** at the bottom of the screen once this is complete.

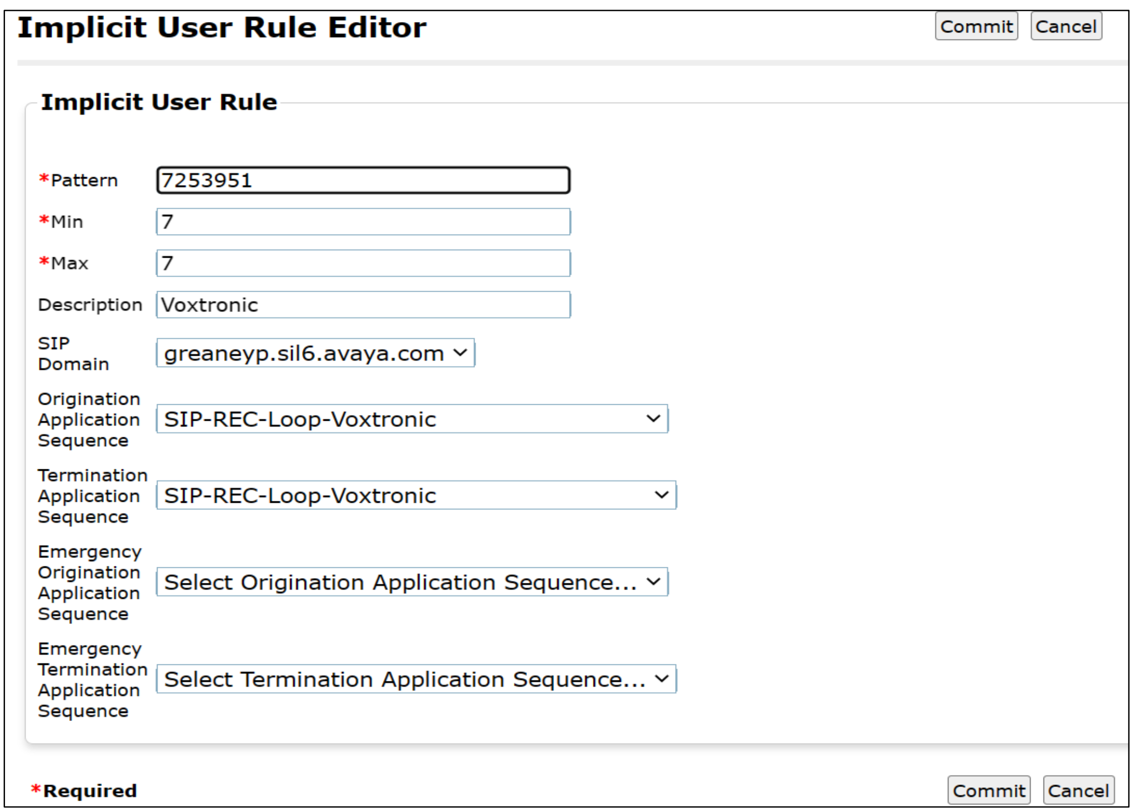


6.2.3. Configure Implicit User

With the Application Sequence in place, the Implicit User can be created. The Implicit user will have the same number as that number configured in **Section 5.5,** that was routed from Communication Manager to Session Manager. Click on **Implicit Users** in the left window and **New** in the main window.



Enter the appropriate **Pattern**, this will be the same as the routed number from **Section 5.5.** Note the **SIP Domain** from **Section 6.1.1** was chosen as well as the **Application Sequence** from **Section 6.2.2**. Click on **Commit** once the **Implicit User Rule** has been configured as shown below.

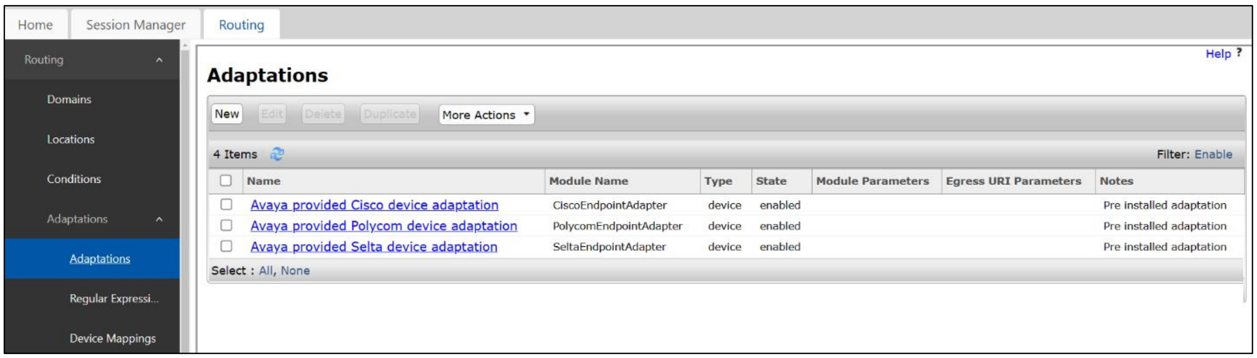


6.3. Configure Routing to Communication Manager

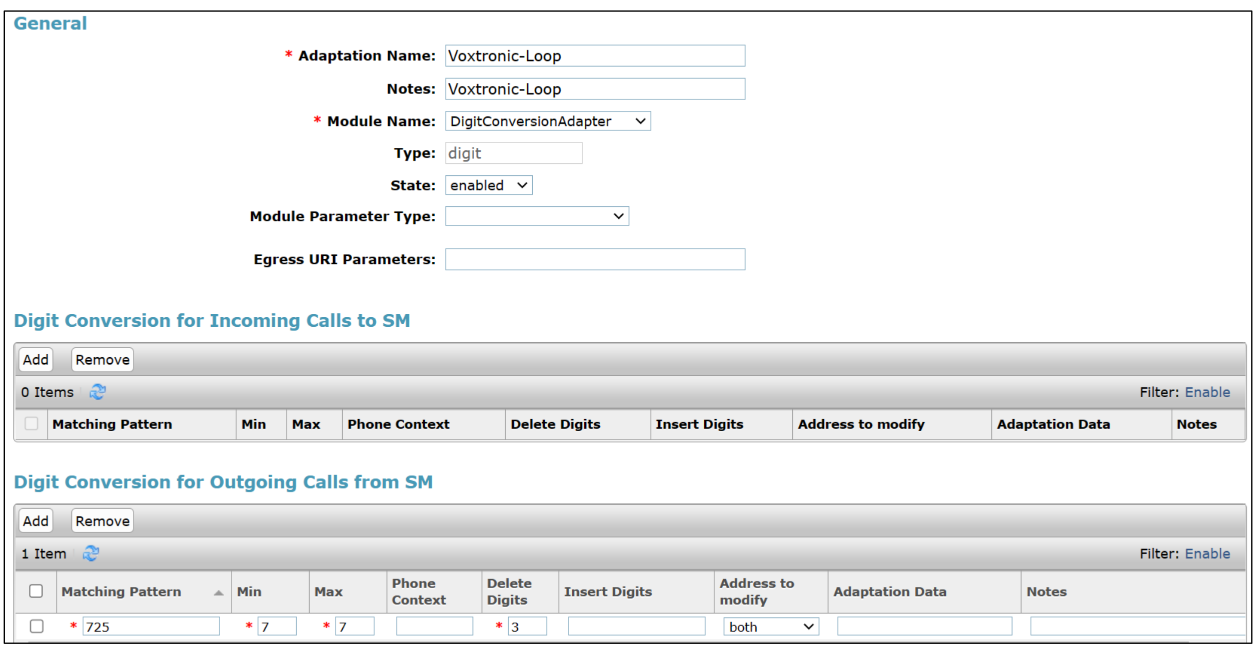
Routing to SBCE is part one of creating the loop, part two is routing the call back to Communication Manager again and back into the VDN to allow the call to proceed and the announcements to be played.

6.3.1. Configure Adaptation for Voxtronic

An Adaptation is first configured, this will strip some digits from the number associated with the Implicit User and then use that number to route the call to Communication Manager. Navigate to **Routing → Adaptations**. Click on **New** in the main window.

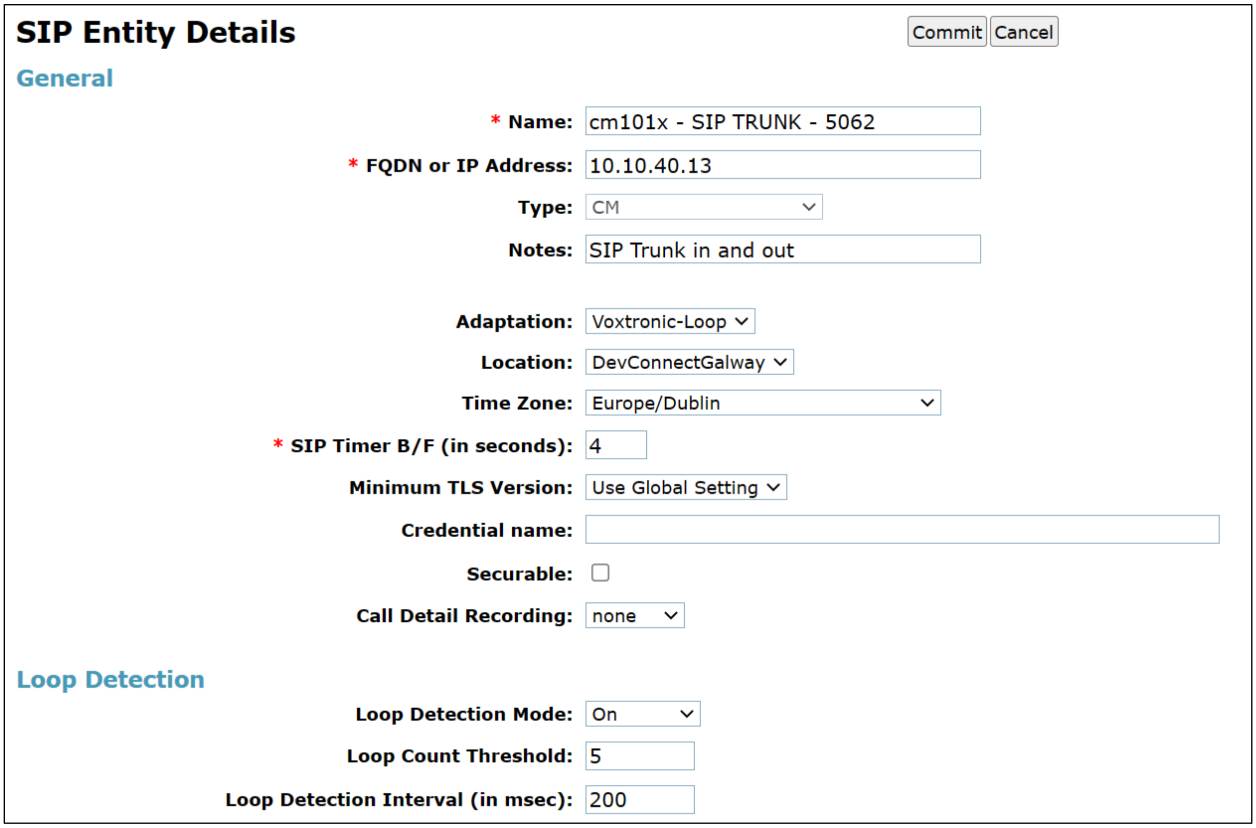


The **Module Name** must be set to **DigitConversionAdapter**. The section **Digit Conversion for Outgoing Calls from SM** is used, as the calls that are being passed from Session Manager to Communication Manager are altered. In this case, there are three digits deleted from 7253951, these being **725** leaving 3951which corresponds to the VDN in **Section 5.5.1**. When 7253951 is routed to Communication Manager the call presents to Communication Manager as 3951. Click on **Commit** (not shown) when the Adaptation is complete.



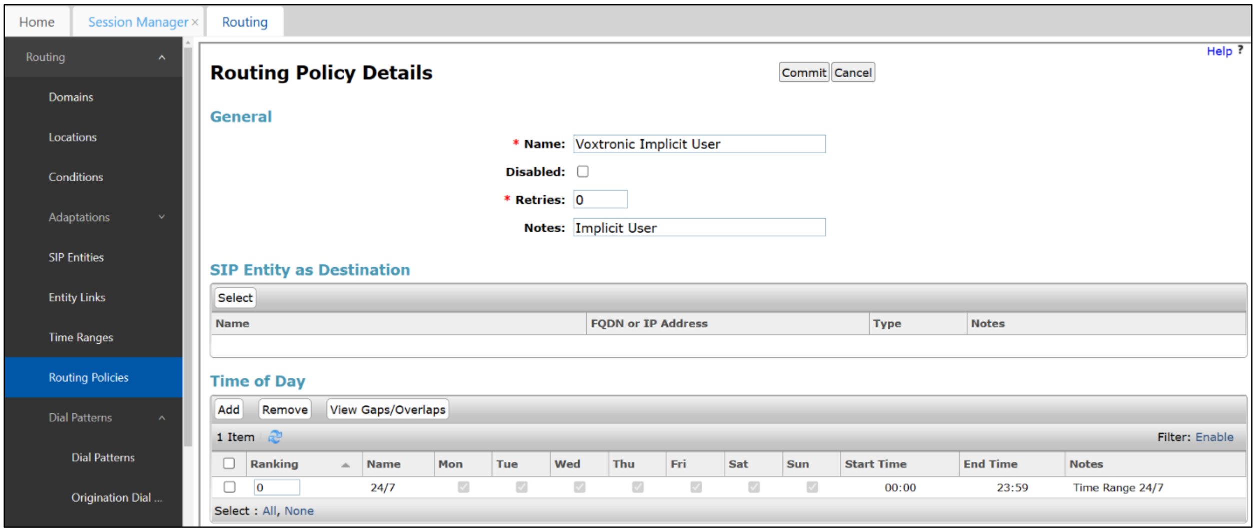
6.3.2. Configure SIP Entity with Adaptation

There was an existing **SIP Entity** already in use to route calls to Communication Manager, however a new SIP Entity can be created as per **Section 6.2.1.** This SIP Entity is then associated with the **Adaptation** created in **Section 6.3.1**. When calls are passed to this SIP Entity, they will follow the rules as per the SIP Entity in deleting 725 from 7253951.

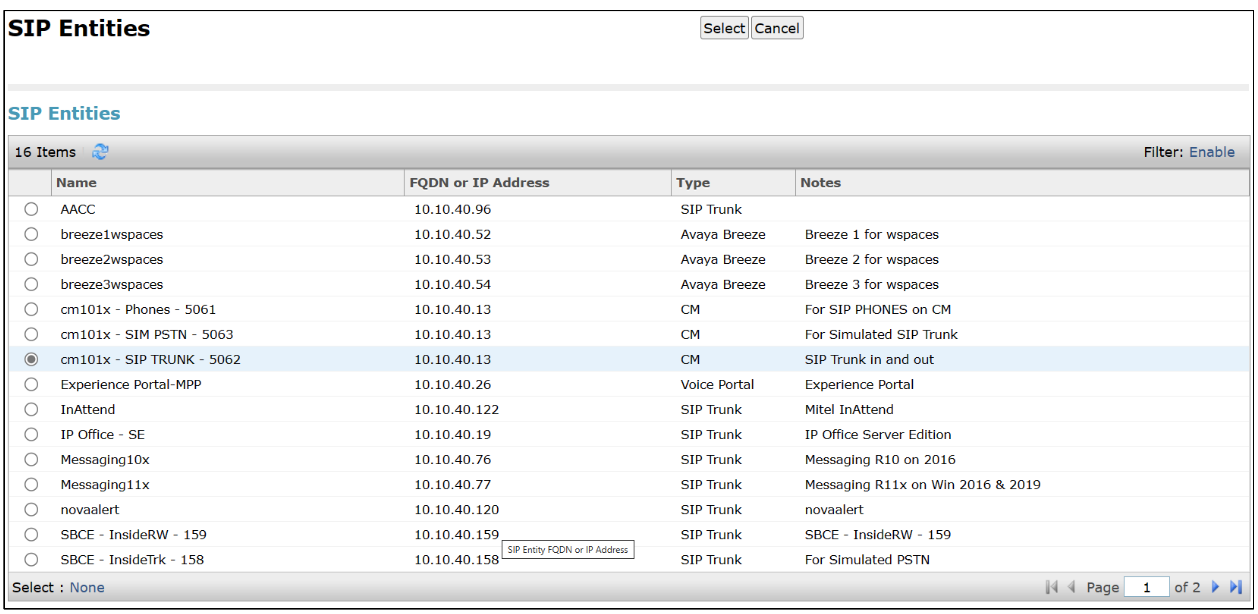


6.3.3. Configure Routing Policy

A **Routing Policy** is also created to allow calls to be routed to Communication Manager. This is configured as shown below. Navigate to **Routing Policies** in the left window and click on **New** in the main window (not shown). A suitable **Name** is chosen, and the **SIP Entity as Destination** is selected.

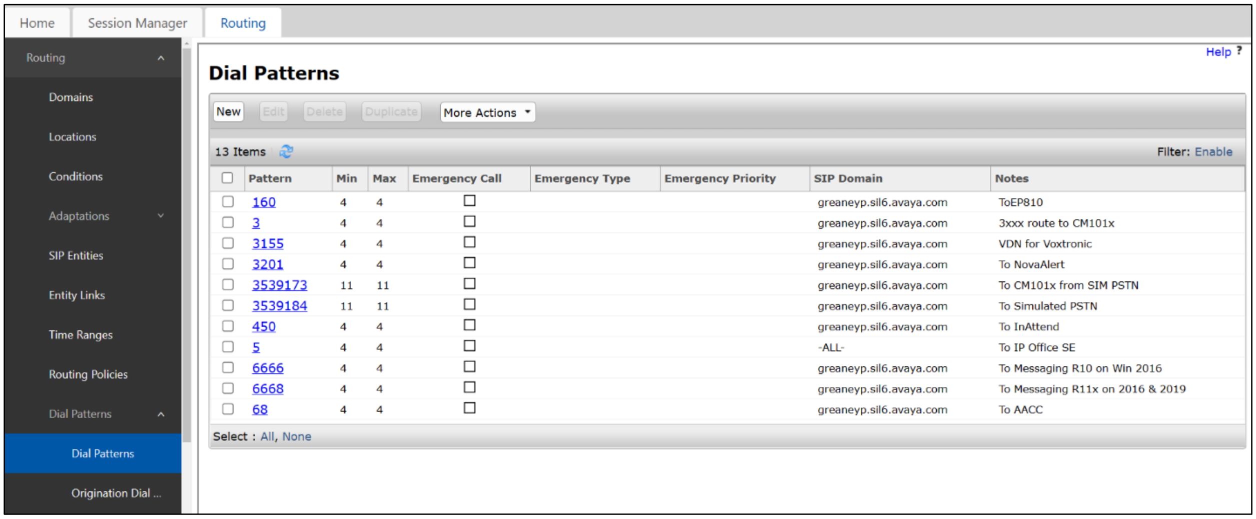


The SIP Entity shown in **Section 6.3.2** is selected to ensure that the correct Adaptation is used. Click on **Select**.

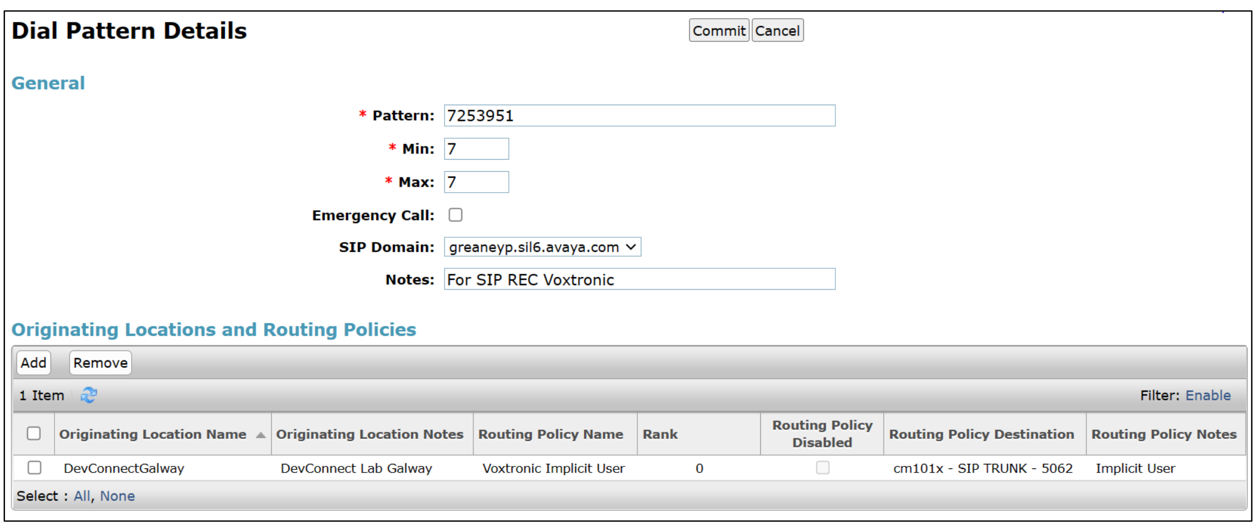


6.3.4. Configure Dial Pattern

Navigate to **Dial Patterns** in the left window and click on **New** in the main window. This creates a new Dial Pattern to route the call to Communication Manager.



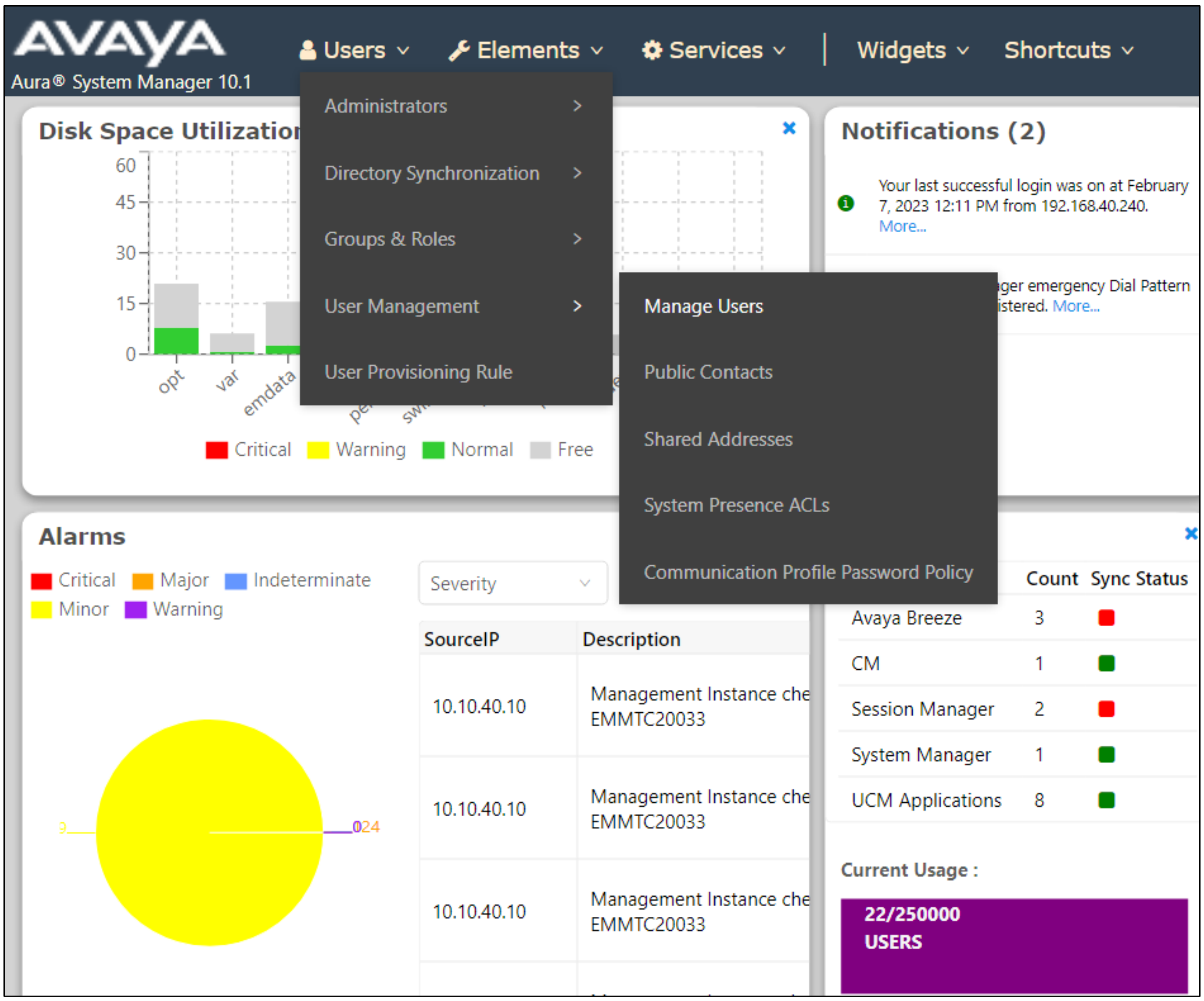
The **Pattern** is the same as the Implicit User. The Implicit User is used first and then the Dial pattern follows. This Dial Pattern chooses the **Routing Policy** created above in **Section 6.3.3** which uses the **Adaptation** created in **Section 6.3.1** to route calls to the Communication Manager **SIP Entity** as per **Section 6.3.2**. Once the Dial Pattern details are filled out correctly as per the configuration shown below, click on **Commit** to complete the routing to Communication Manager.



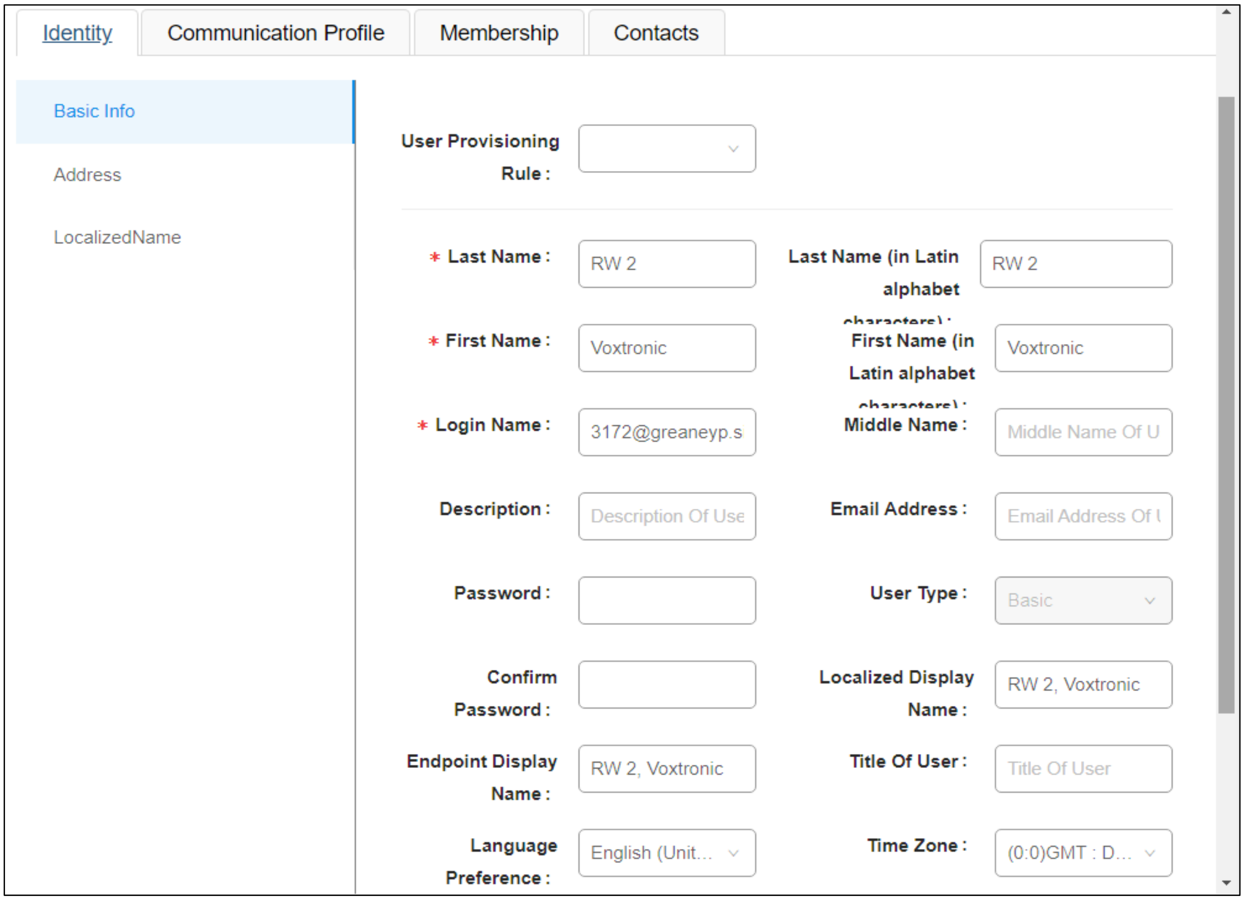
6.4. Configure Remote Workers

The following section shows the configuration for the Remote Workers that were used for compliance testing. Please note this may vary depending on the customer site.

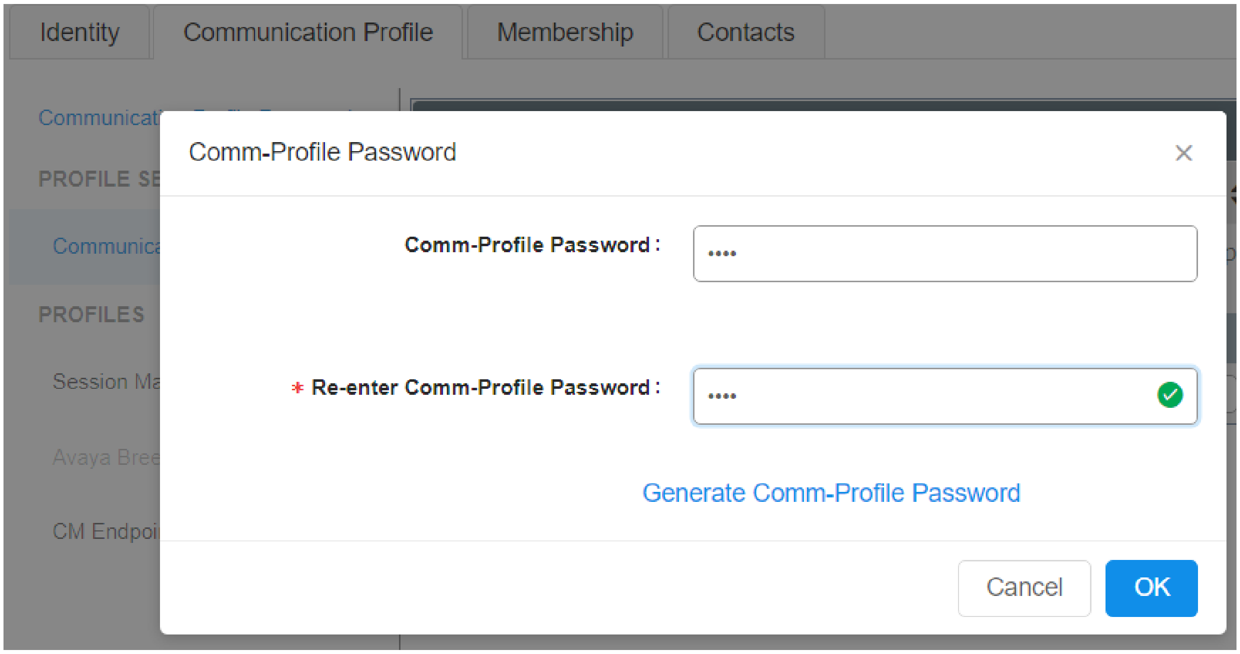
All Remote Worker phones are registered as SIP endpoints through the Session Border Controller for Enterprise, but they are configured as any SIP endpoint would be configured. All SIP endpoints are configured using System Manager by navigating to **Users → User Management → Manager Users**.



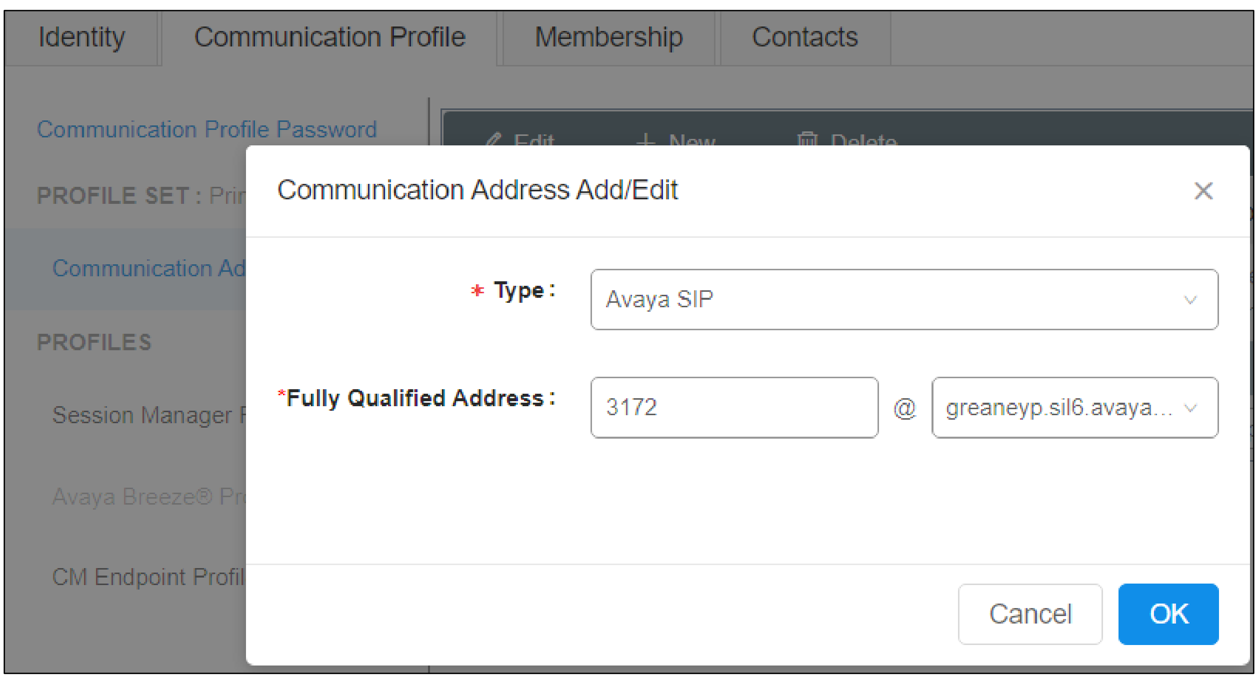
Click on the **Identity** tab to ensure the **Name**, **Description**, **Title**, and **Time Zone**.



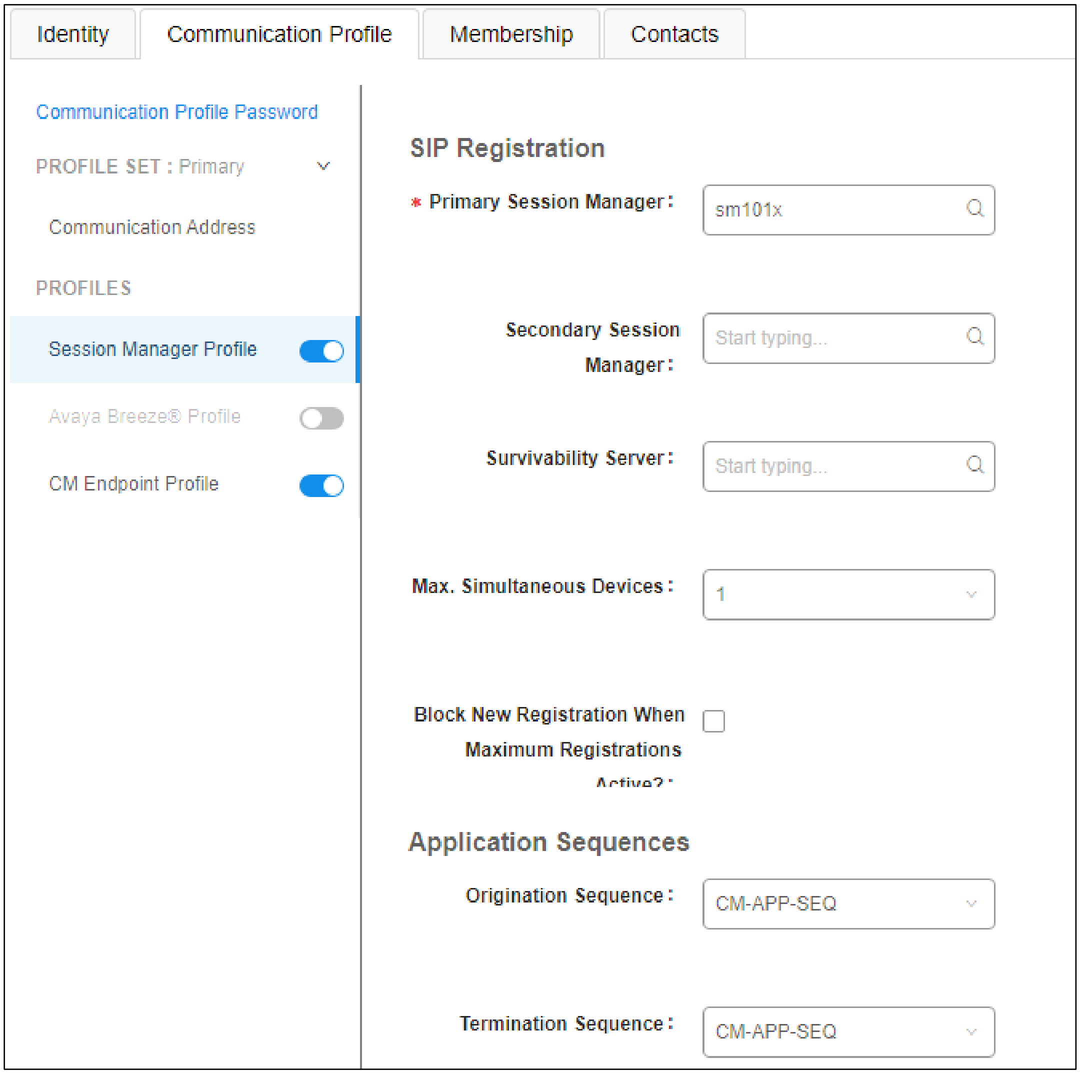
Click on the **Communication Profile** tab and **Communication Profile Password** in the left window. Enter a suitable password for the SIP user/phone.



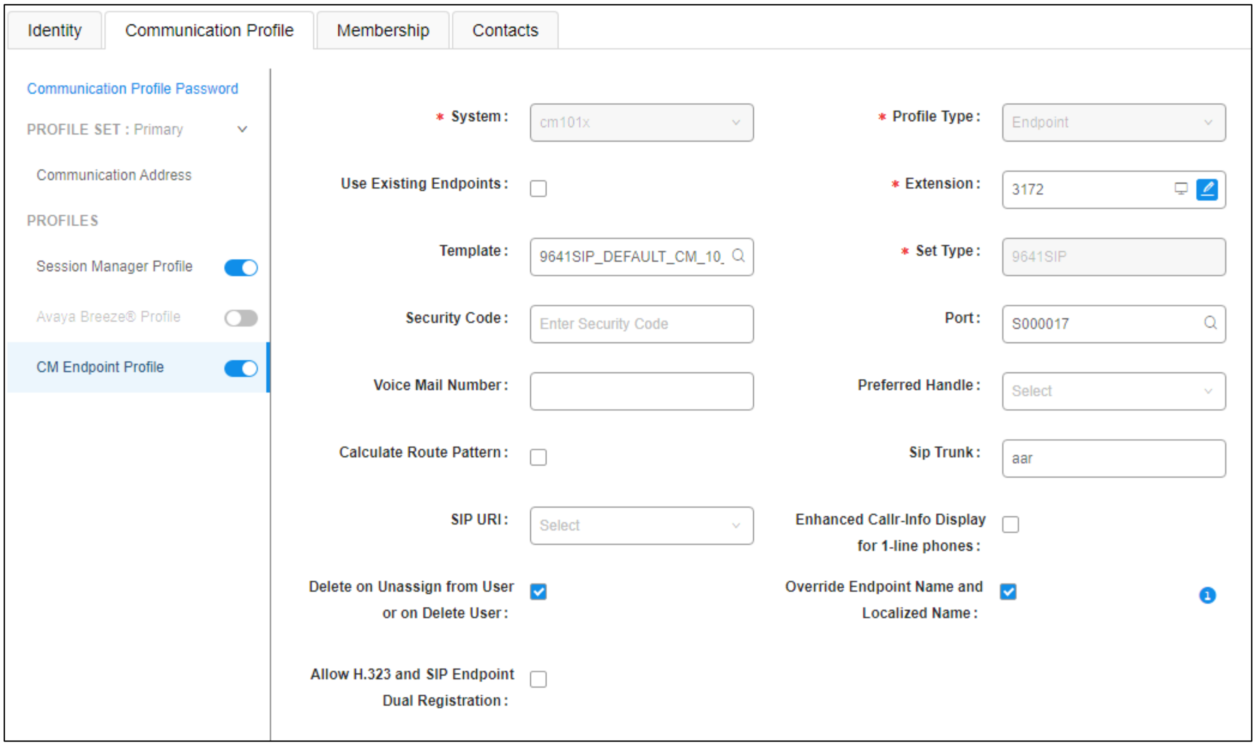
Click on **Communication Address** in the left window. The **Type** should be set to **Avaya SIP** as shown, with the **Fully Qualified Address** in the form of ext@domain.



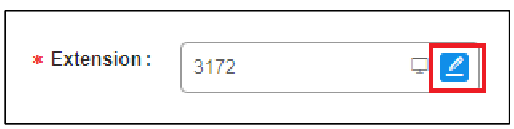
Click on **Session Manager Profile** in the left window. Ensure the correct **Session Manager** is chosen as well as the appropriate **Originating Sequence** and **Terminating Sequence**.



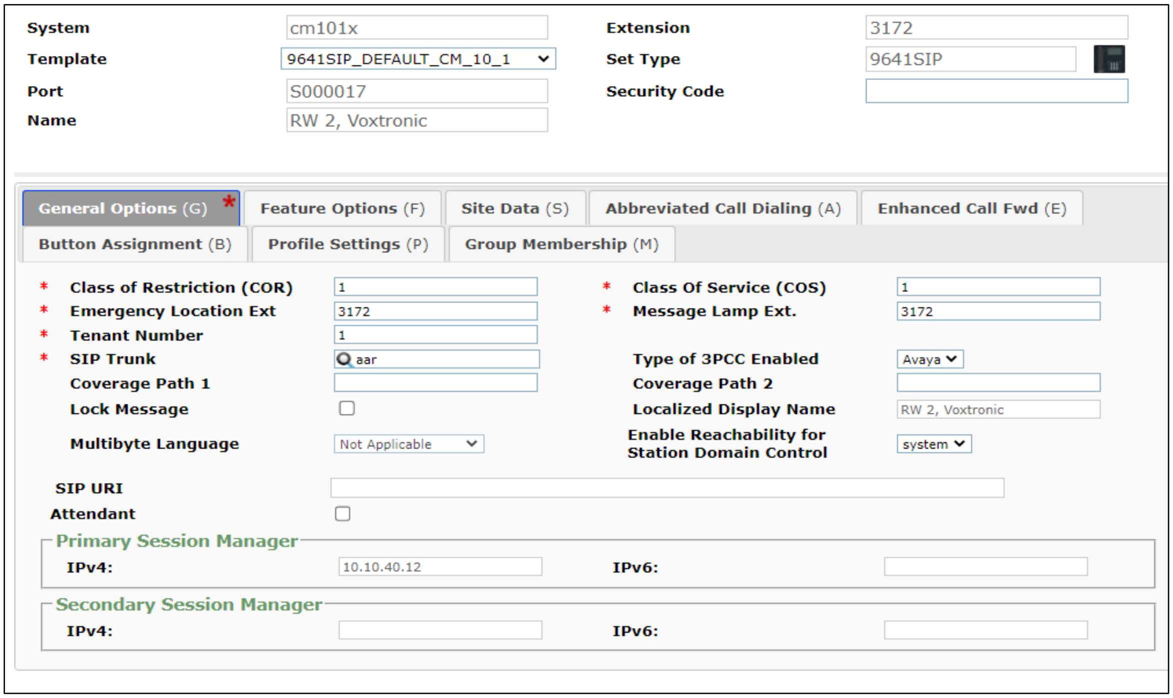
Click on **CM Endpoint Profile** in the left window and ensure the appropriate **Template** is chosen as well as the correct **Extension** and **Sip Trunk**.



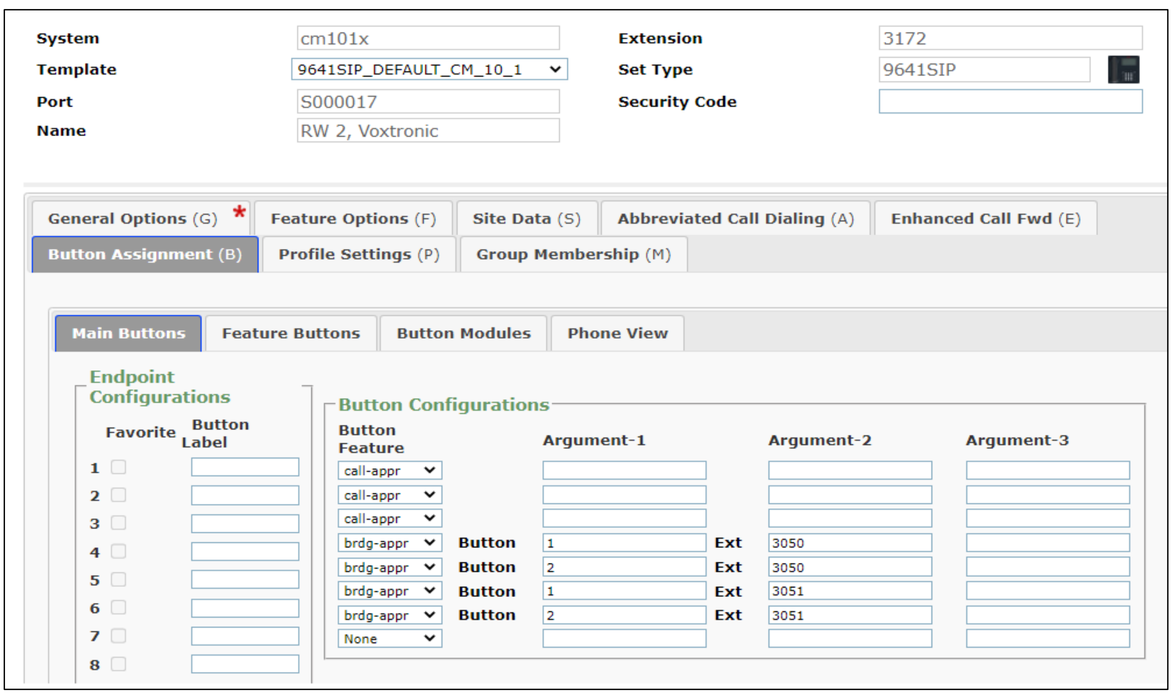
Click on the icon next to **Extension**. This will open the window shown on the next page.



These are the settings under the **General Options** tab that were used for compliance testing. Again, these may vary depending on the customer requirements.

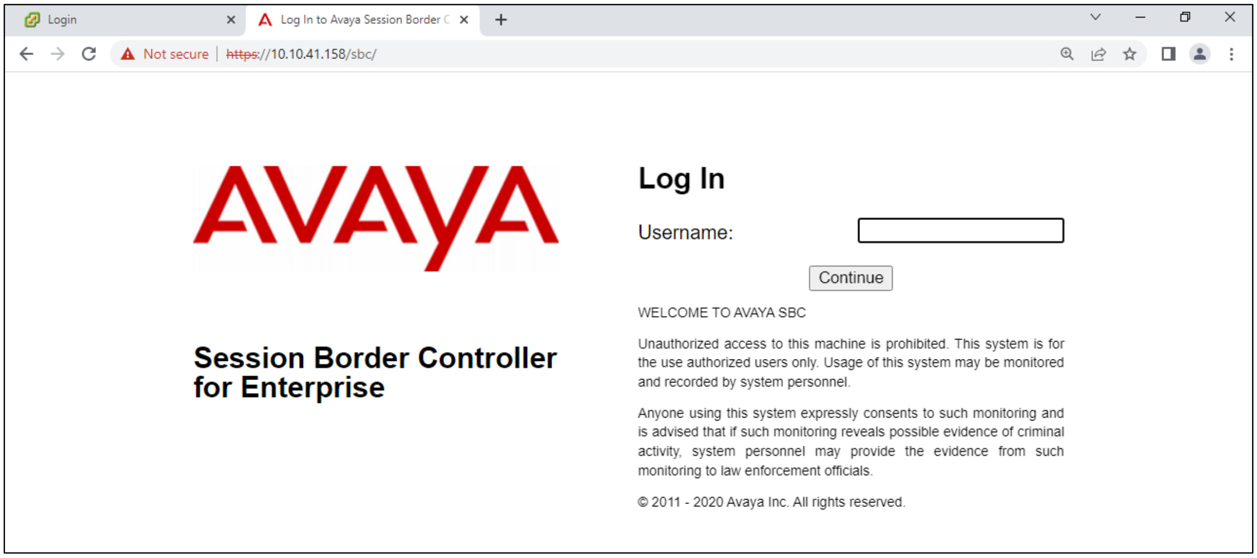


The **Button Assignment** tab shows the additional Bridged Appearance buttons (**brdg-appr**). Note that two buttons were added for each bridged appearance **3050** and **3051**. Click on **Done** (not shown) once all is correctly filled in and then **Commit** on the page that follows (not shown).

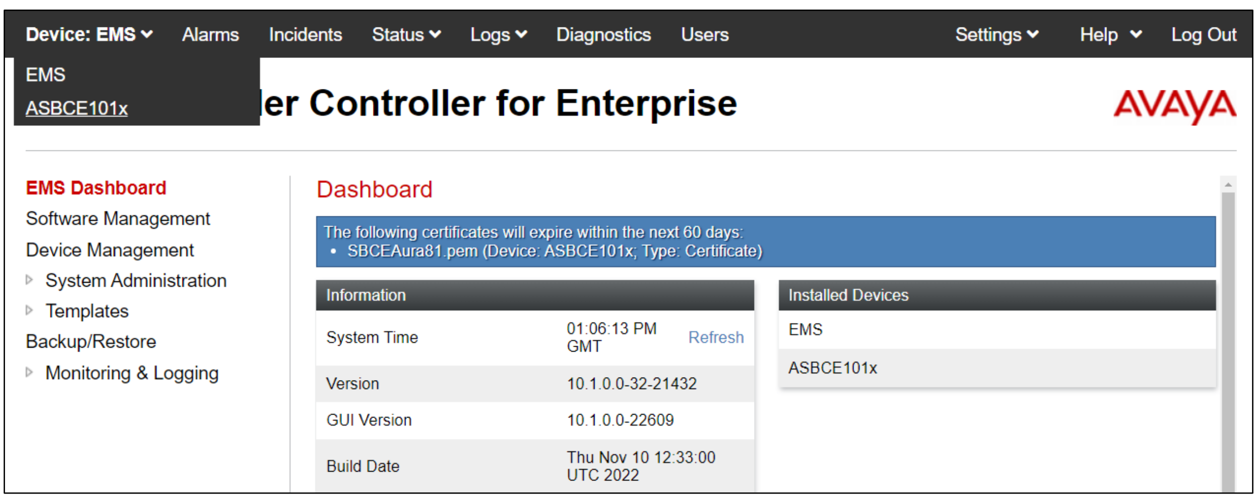


7. Configure Avaya Session Border Controller for Enterprise

Configuration for the Session Border Controller is performed by opening a web session to the Session Border Controllers management IP address. Open a URL to **https://<SBCManagementIP>/sbc** and log in using the appropriate credentials.



Once logged in ensure that the correct Device is chosen, as in the case below the EMS and the SBCE are coresident and therefore the SBCE must be selected.



Some of the configuration is dependent on having other parameters already set, however most of the configuration shown below will be in sequence. Note that the configuration illustrated in the section illustrates the connection to Voxtronic Conex only, for all other setups such as Remote Worker or SIP Trunk, please refer to **Section 12**. Some of the setup for the Remote Workers that were used for compliance testing can be found in **Appendix A** of these Application Notes.

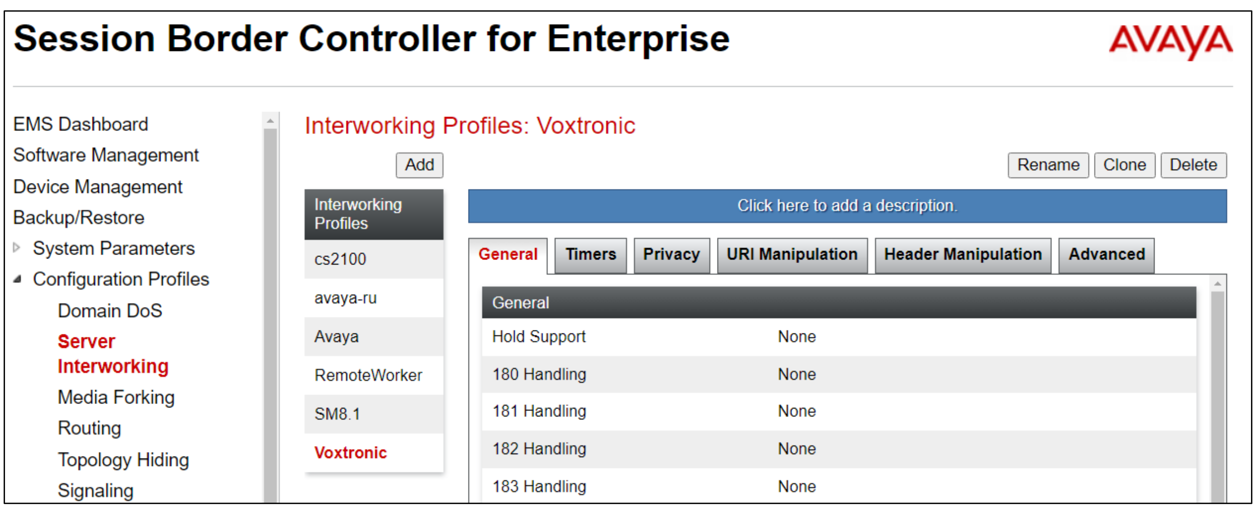
The various components can be configured by navigating the left window and adding or editing the existing Profiles/Policies/Rules. When adding a new component, a clone can be made of an existing component and then edited to suit. A new component can also be added by clicking on **Add**, rather than cloning an existing one.

Note:

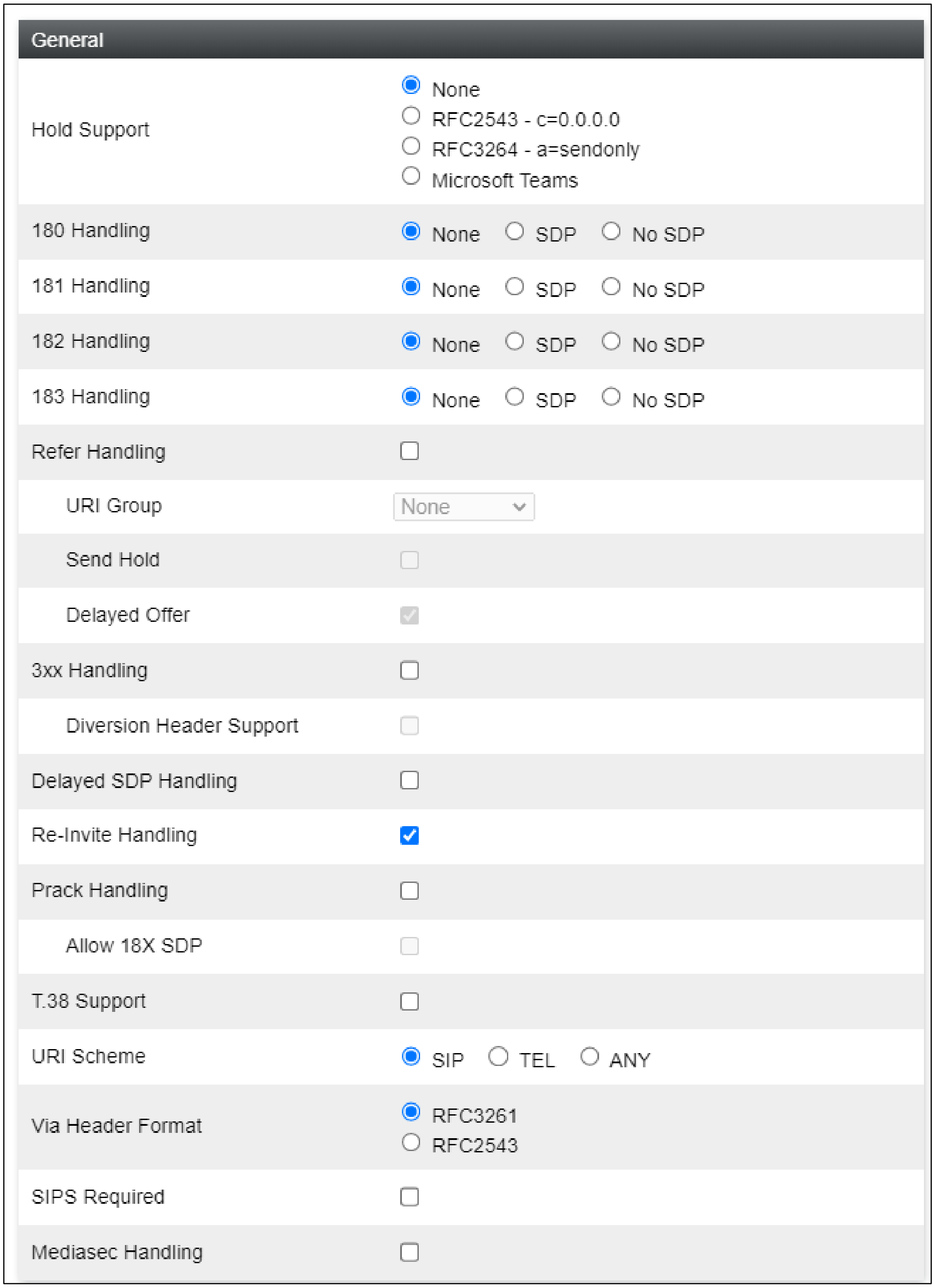
1. For the purpose of illustrating the setup of the various components outlined in this section, these components, which are already configured and in place, will show as edited rather than show as added or new.
2. The connection to the Voxtronic Conex recorder will be named as Voxtronic in the screen shots in this section.
3. The following sections show the setup that was used for compliance testing but some of these settings may need to be altered to suit each customer requirement.
4. For information on the configuration and setup of any of the SBCE that is not explained in this section, please refer to **Section 12** of these Application Notes.

7.1. Setup of Configuration Profiles

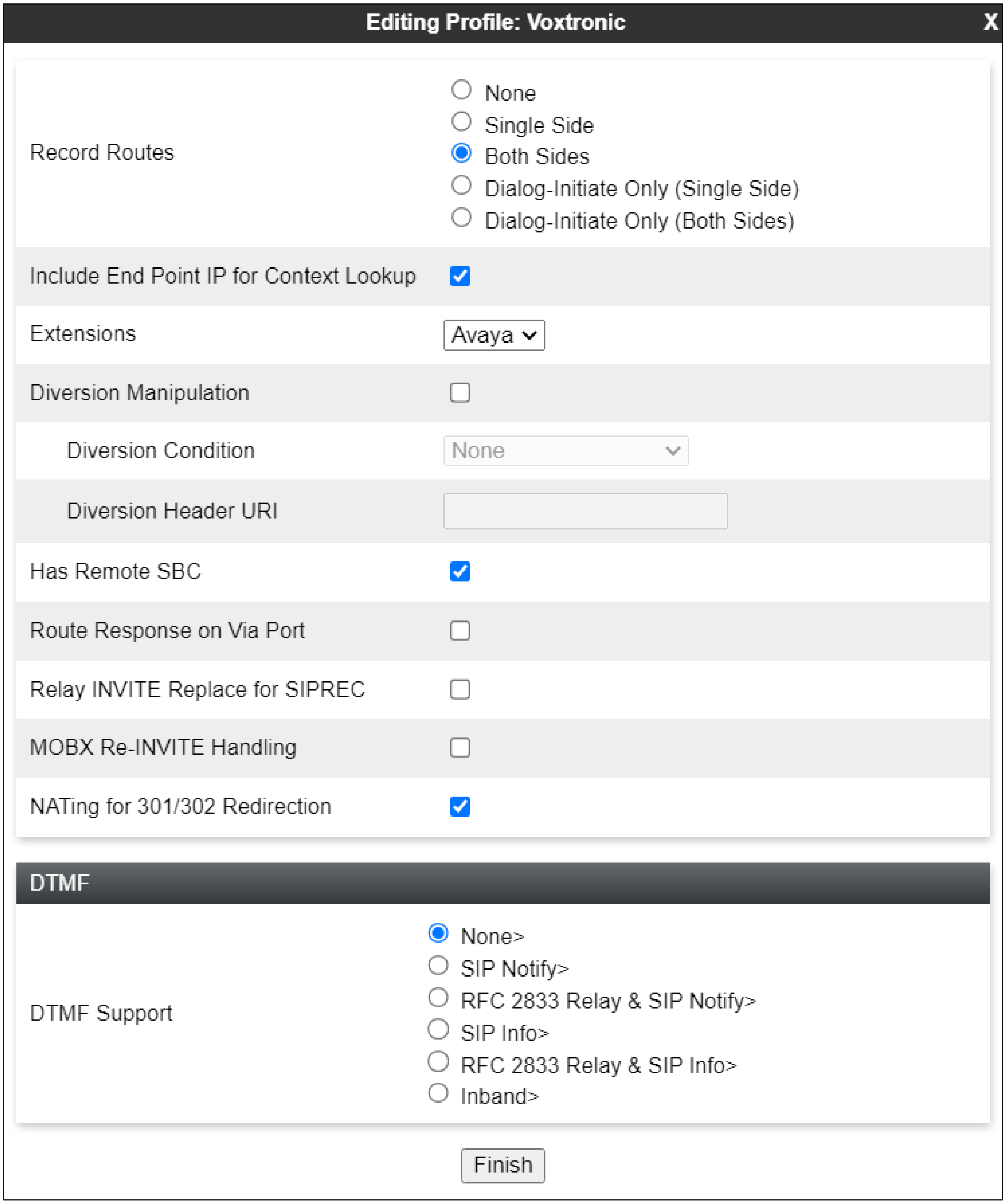
Navigate to **Configuration Profiles** in the left window and **Server Internetworking**. From the main window, click on Add to create a new profile, or select an existing profile and click on Clone to create a new profile in that image. This profile can then be changed or edited to suit the connection to Conex. A profile below called **Voxtronic** was created.



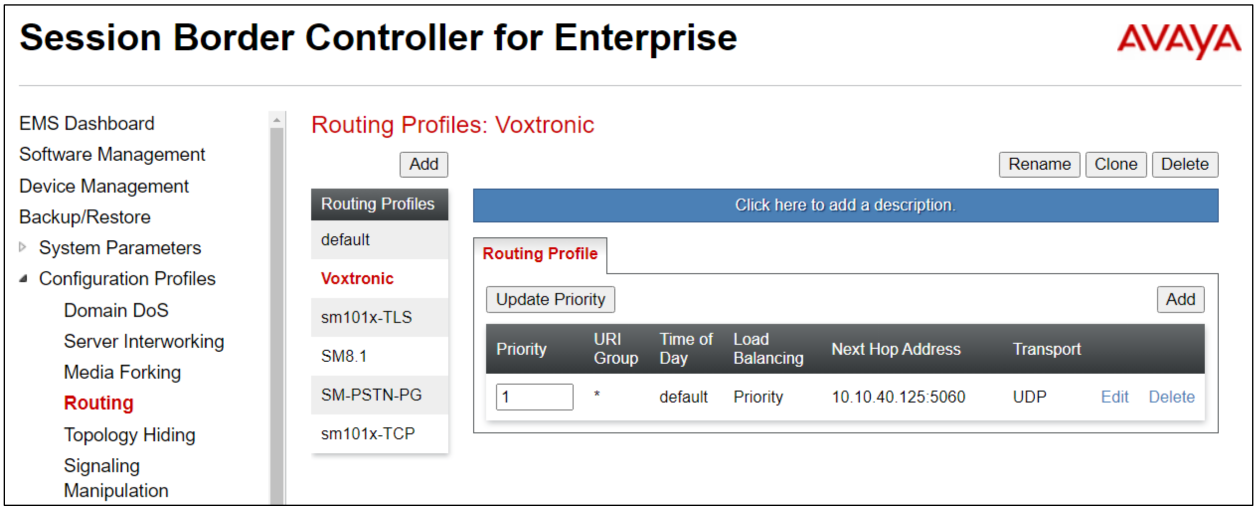
These are the settings under the **General** tab for the Internetworking Profile, Voxtronic. Note that **SIPS Required** was not ticked.



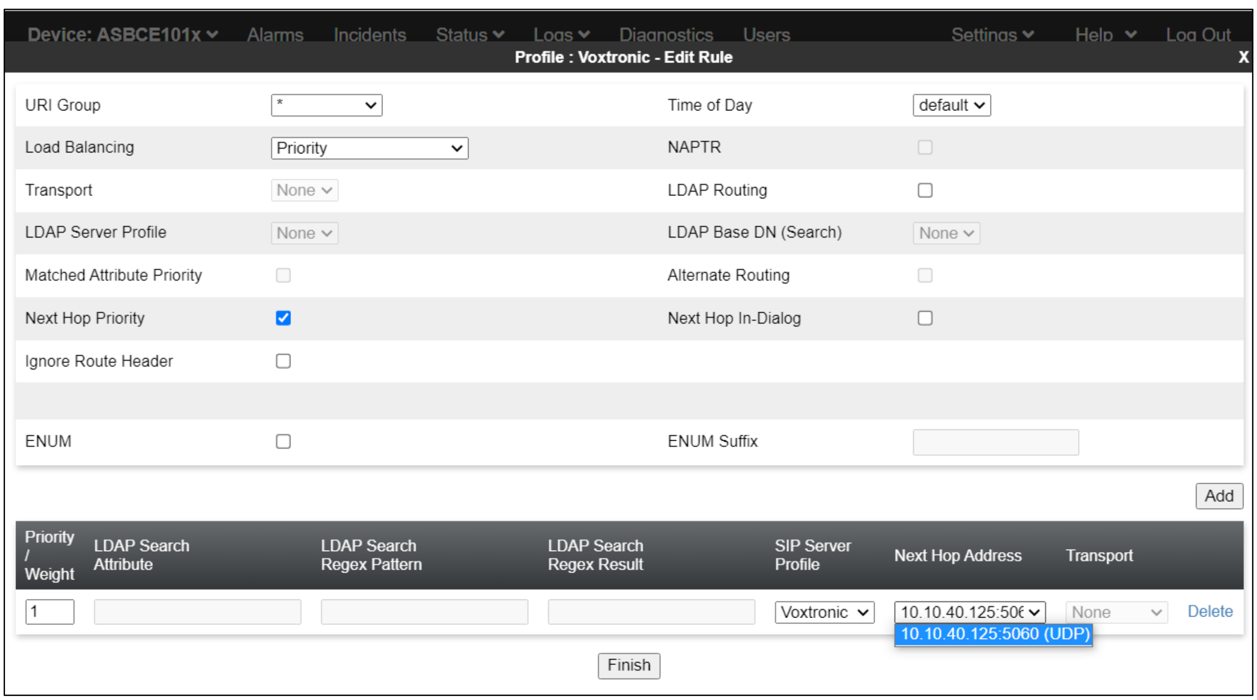
These are the settings for the same profile, under the **Advanced** tab. These settings can be site specific, and each customer may have other requirements to those set below.



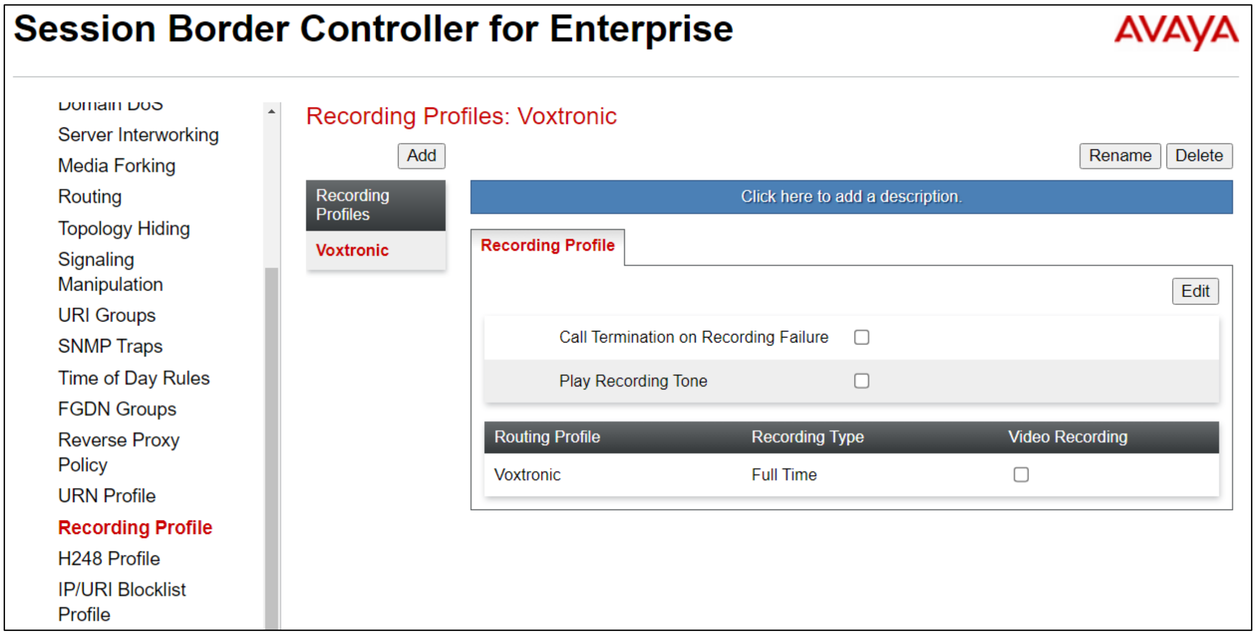
Navigate to **Routing** in the left window. A new **Routing Profile** can be added.



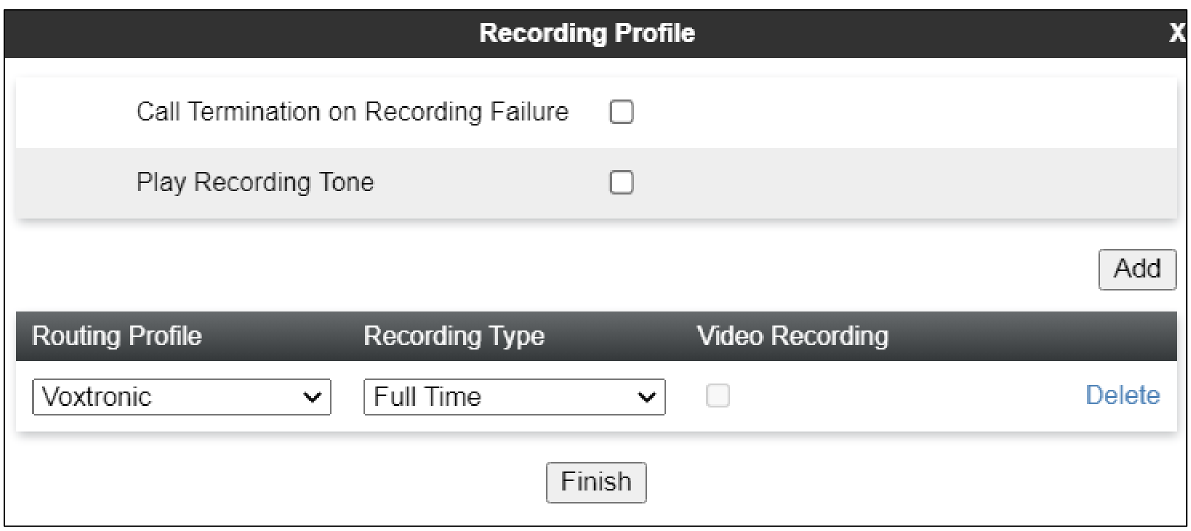
The following is the setup for the **Voxtronic** Profile. Note the **SIP Server Profile** had already been setup, this is configured in **Section 7.2**. The **Next Hop Address** takes its information from this SIP Server Profile.



Navigate to **Recording Profile** in the left window. A new profile for **Voxtronic** can be added.

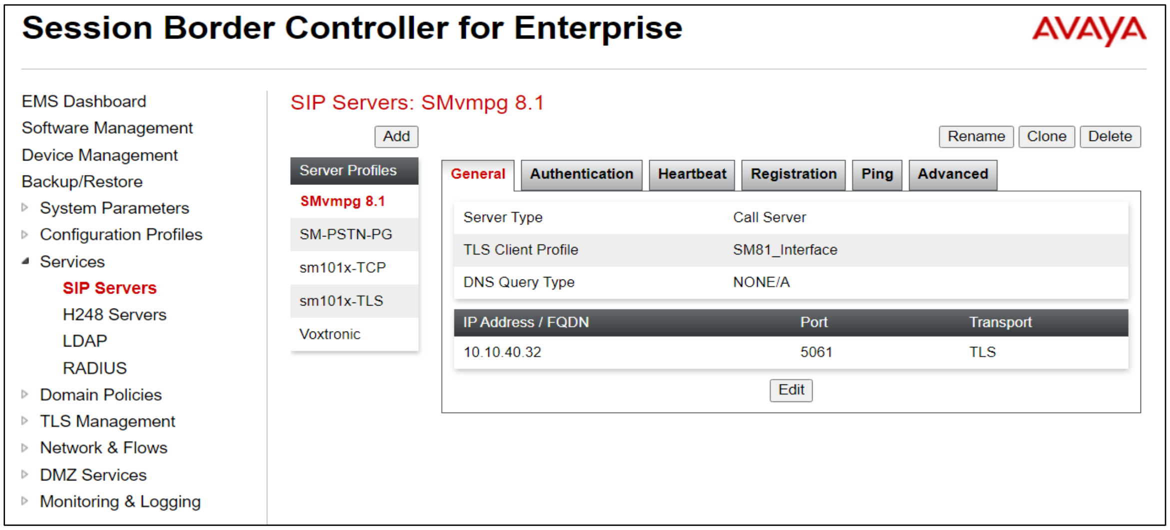


The **Routing Profile** created earlier is used, and the **Recording Type** is set to **Full Time**.

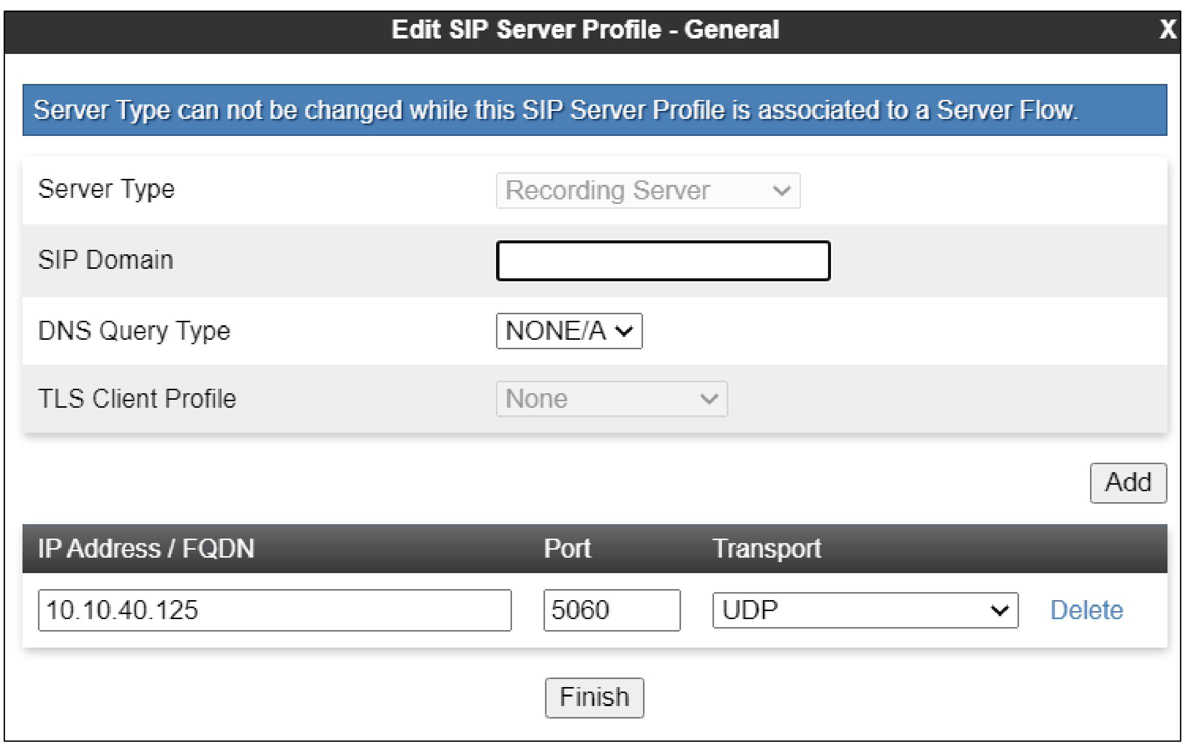


7.2. Configure Services

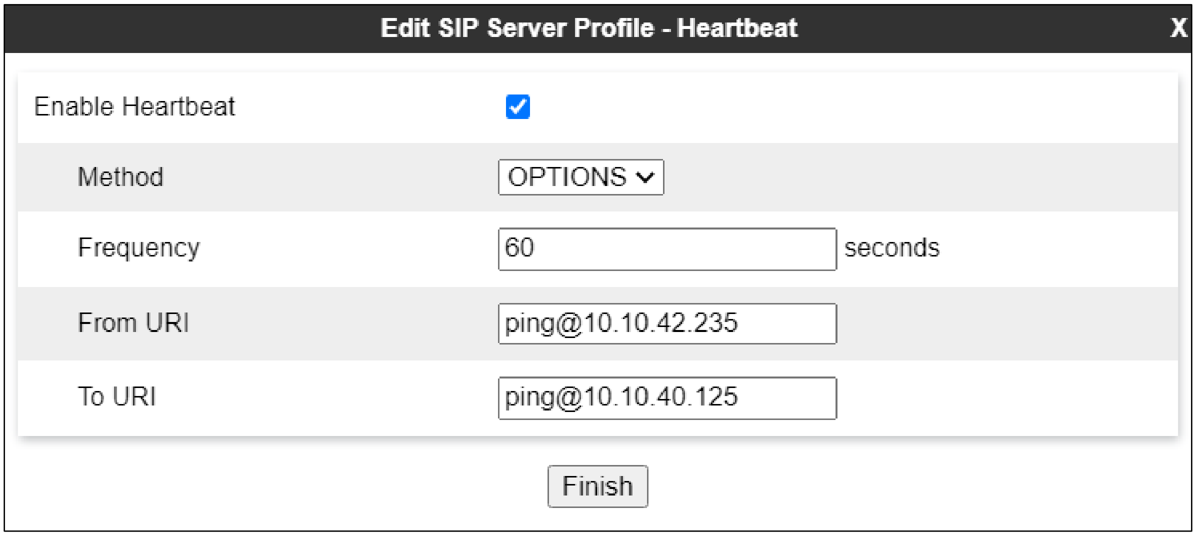
A new **SIP Server** must be created for the connection to the VoIP Recorder. This new profile can be created by either cloning the existing Session Manager profile or by clicking on **Add**. Navigate to **Services → SIP Servers** in the left window to add the SIP Server called **Voxtronic**.



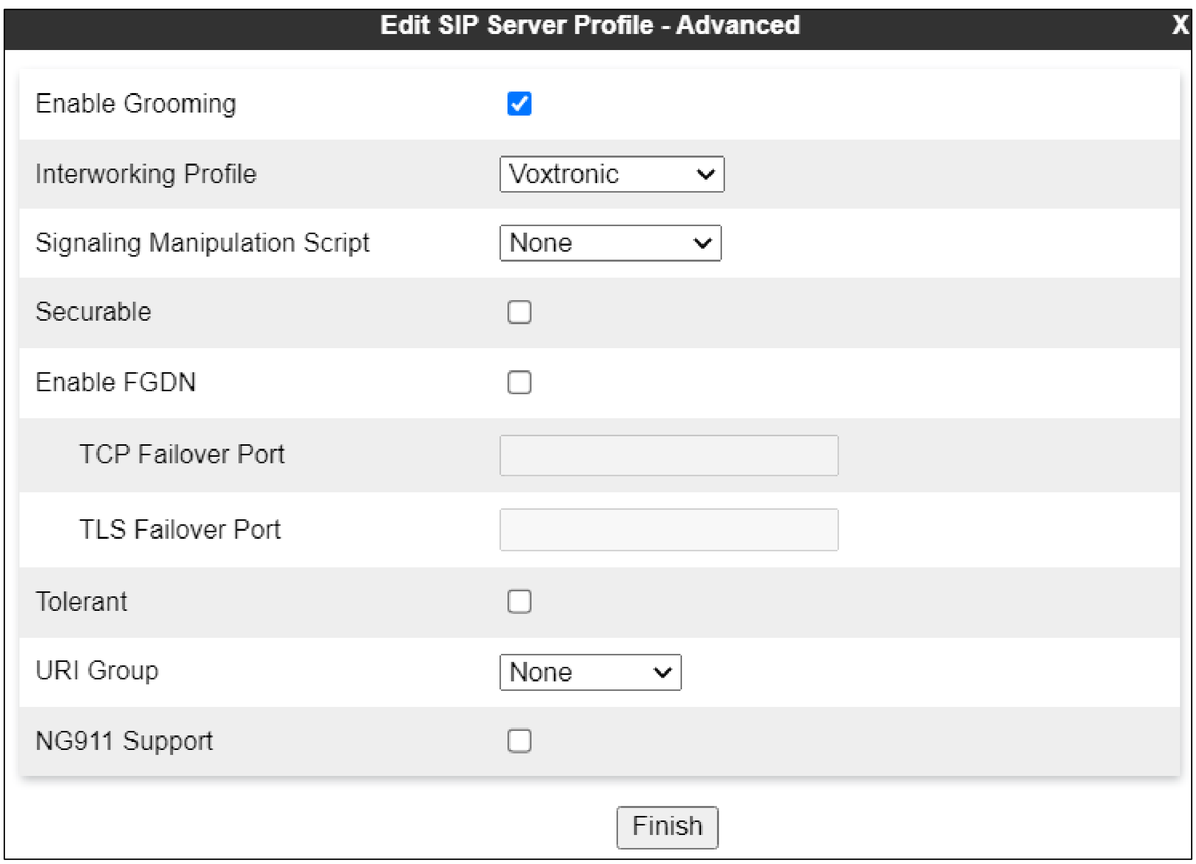
Under the **General** tab, the **Server Type** must be set to **Recording Server**. Seen as the connection is not using TLS there is no requirement for a **TLS Profile**. The **IP Address** of the VoIP Recorder is entered here along with the **Transport** Protocol and the **Port** that is being used.



Under the Heartbeat tab, **OPTIONS** can be sent to the recorder as a keepalive or to ensure the link is setup. This is done as shown below.

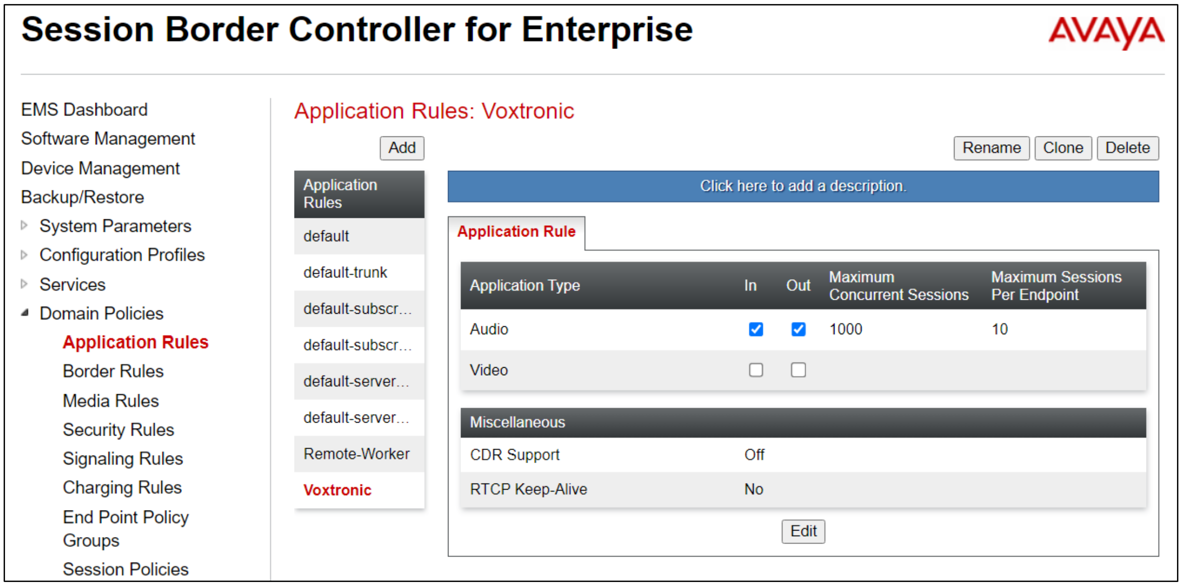


Under the **Advanced** tab, the following was set for compliance testing. Note, the Server **Internetworking Profile** setup in **Section 7.1** was used here.

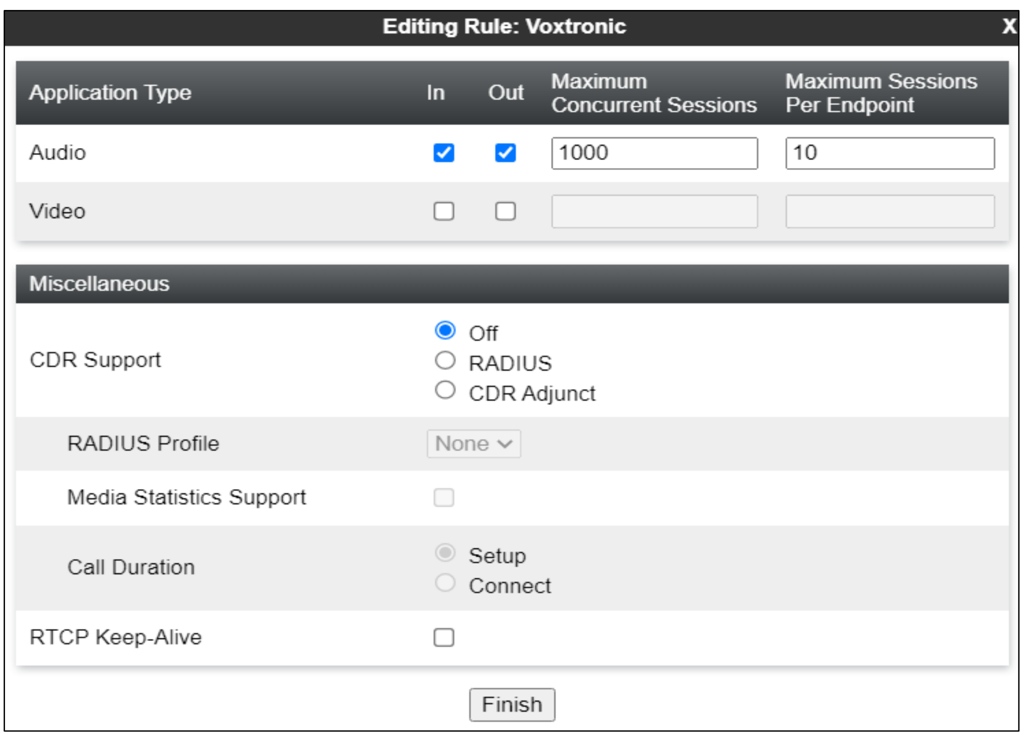


7.3. Configure Domain Policies

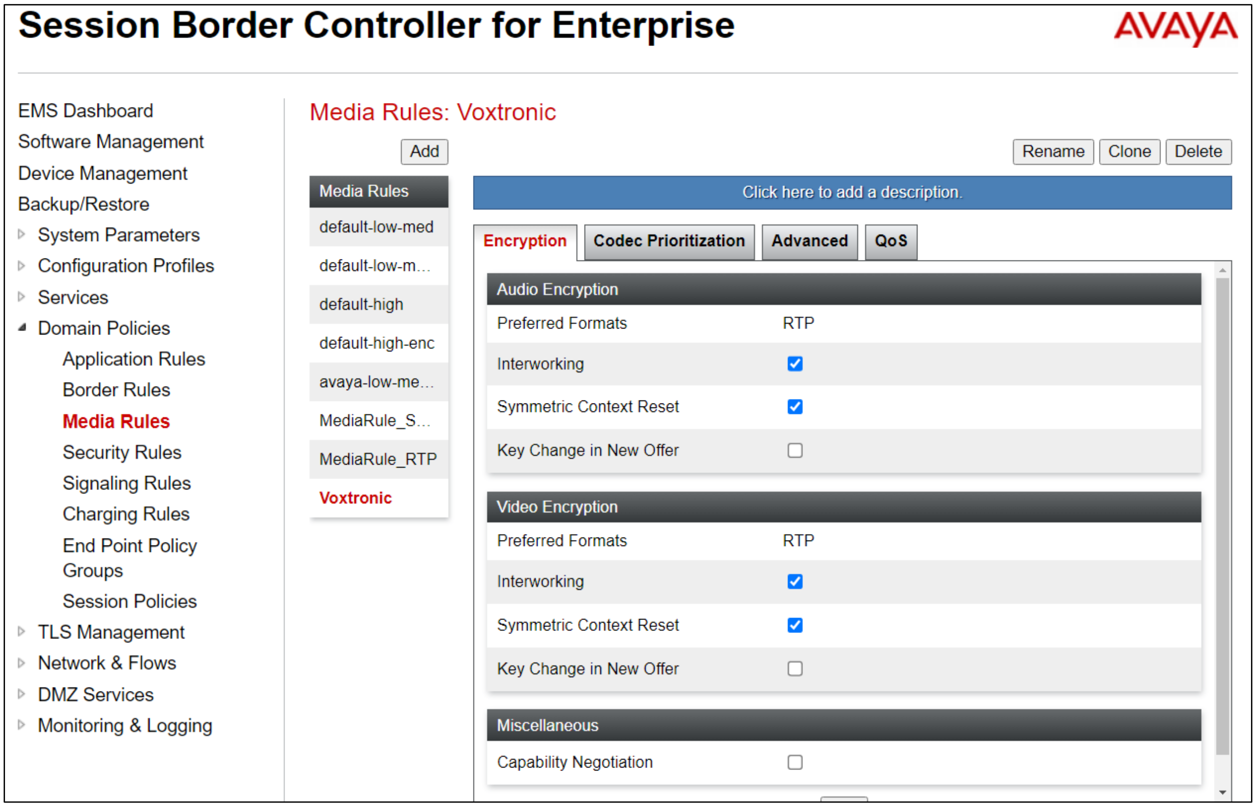
An End Point Policy Group for Voxtronic is the aim within Domain Policies, and in order to create this policy group certain rules must be created first, beginning with **Application Rules**. Like with almost all rules and policies, a new one can be either cloned from an existing one or created fresh by clicking on **Add**.



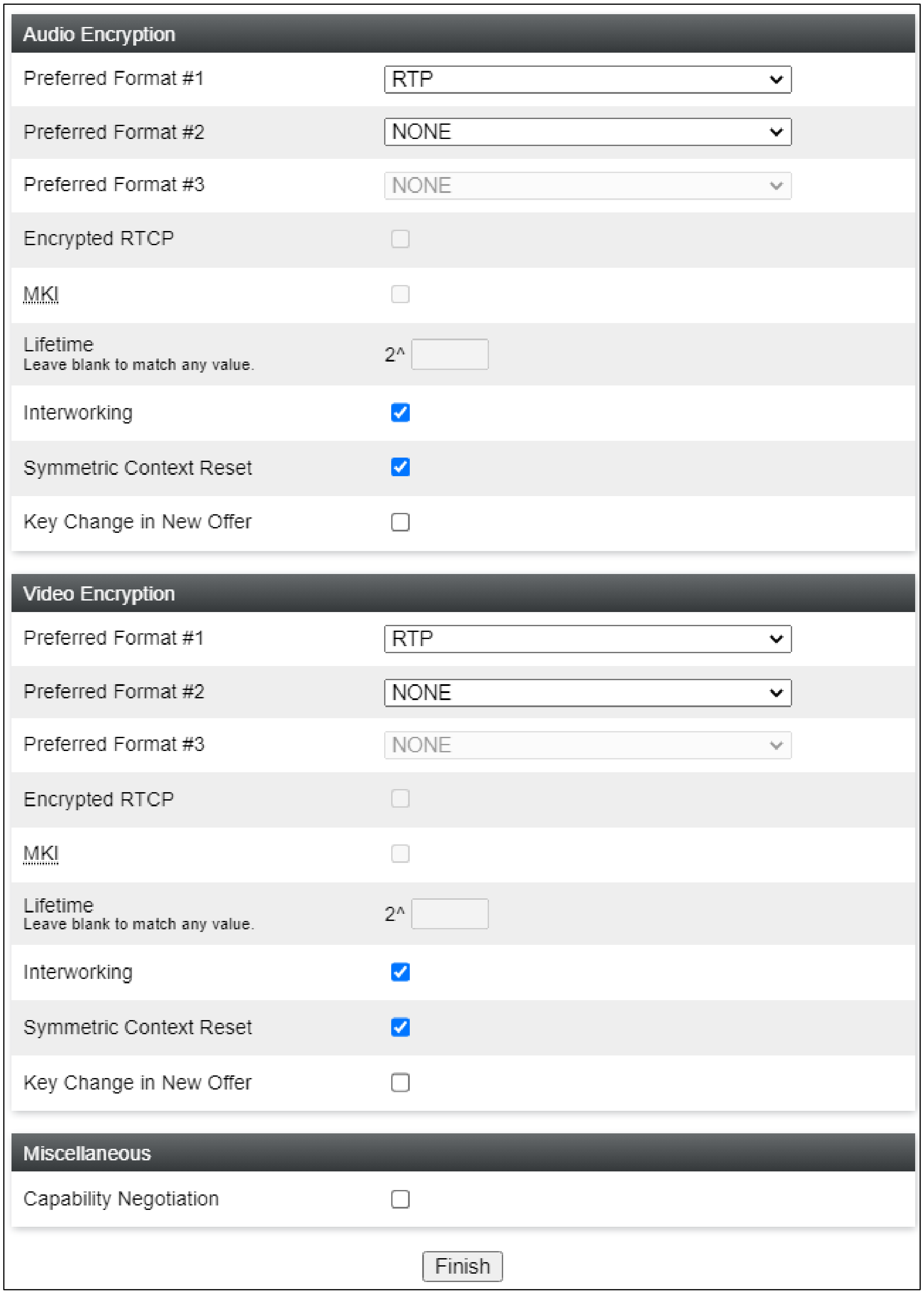
The information contained in the **Application Rule** below was used for compliance testing.



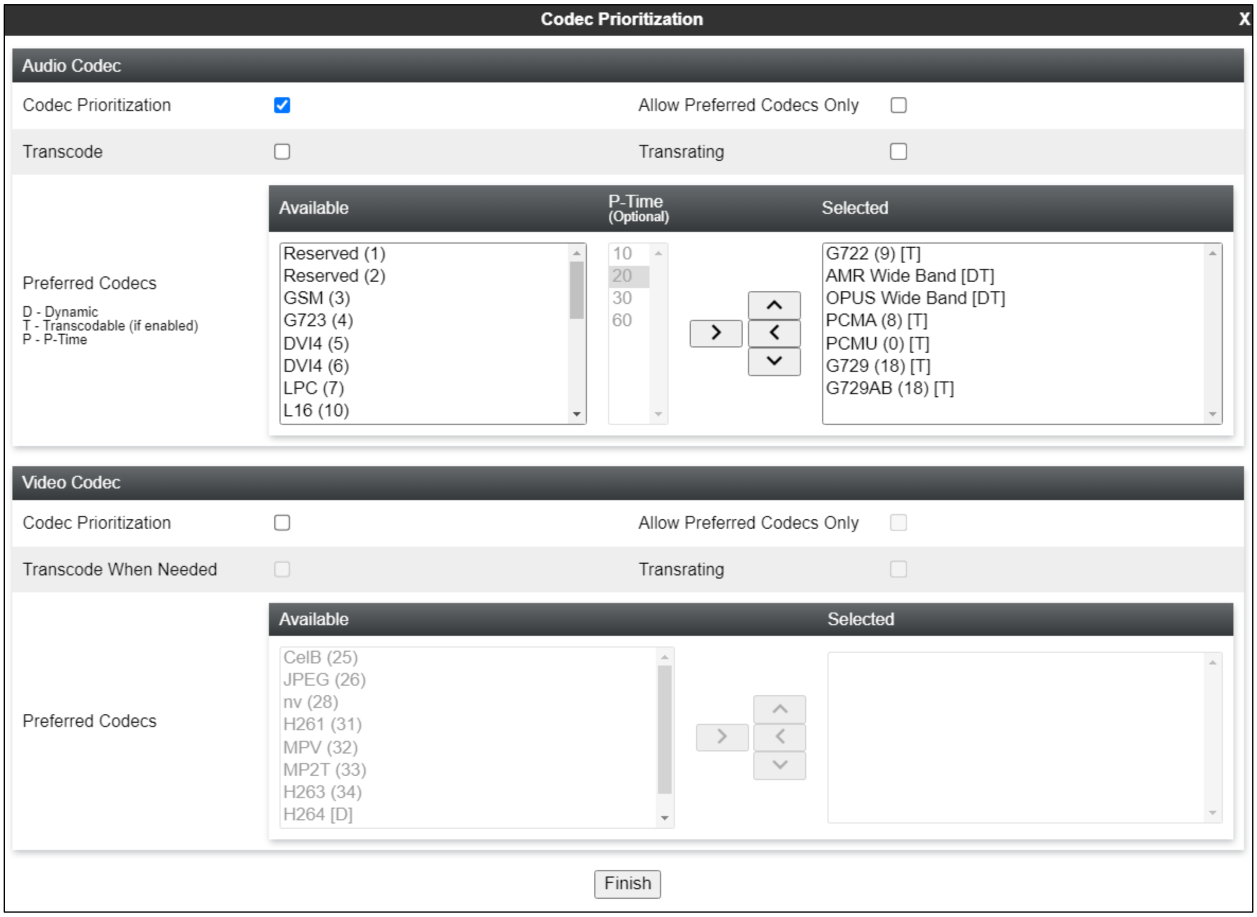
A new Media Rule was also created, click in **Media Rules** in the left window, and either clone one or add a new Media Rule.



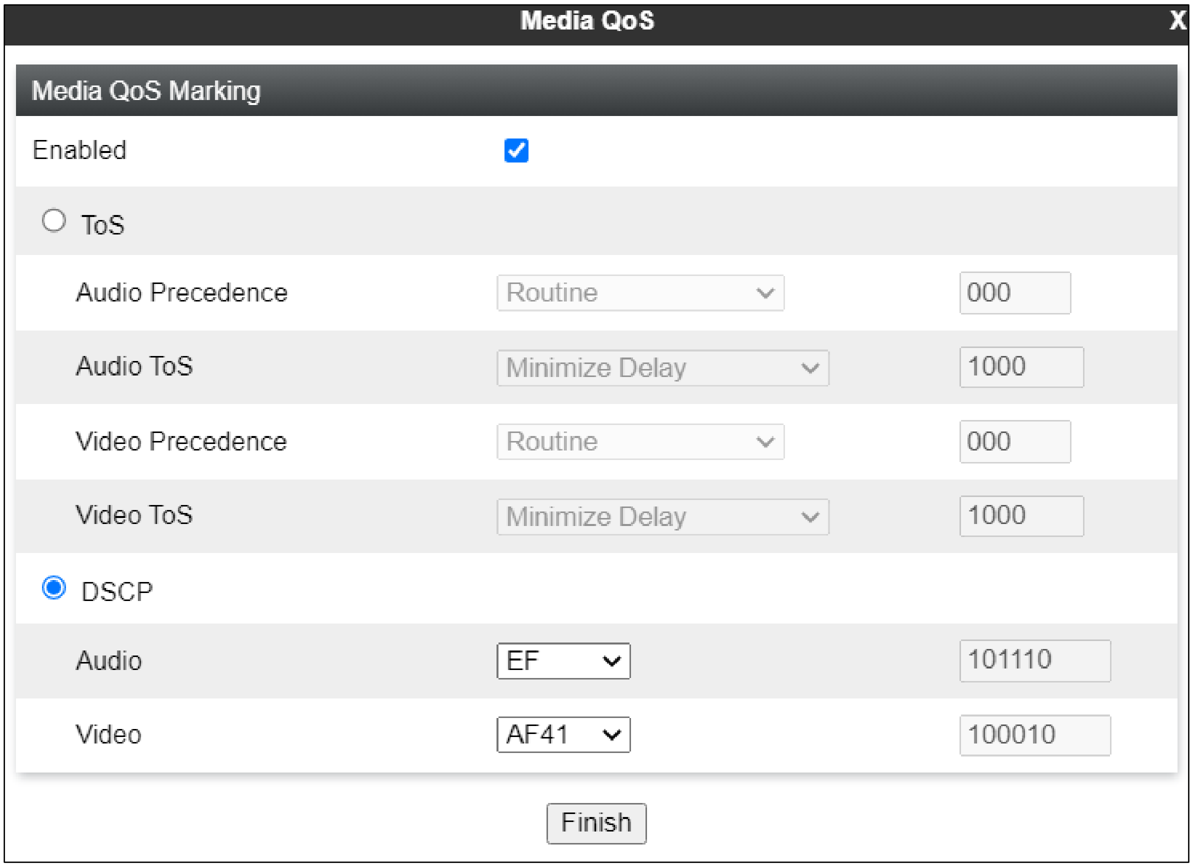
Looking at the **Encryption** tab. The connection to Conex did not avail of any security as per the wishes of Voxtronic, and so **RTP** is the preferred **Audio** and **Video Encryption**.



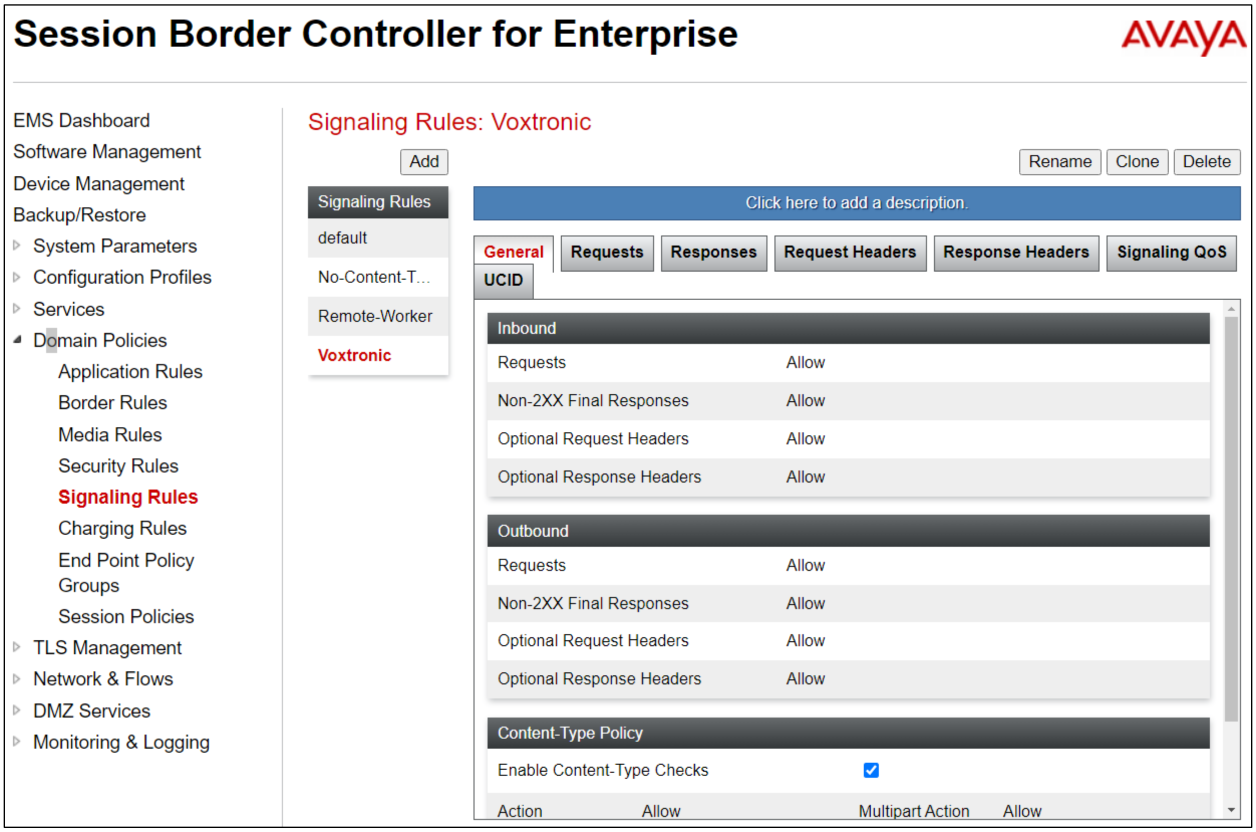
Looking at the **Codec Prioritization** tab. **Codec Prioritization** can be left unticked as default. Below serves to show how each Codec can be chosen and prioritized, should that need arise.



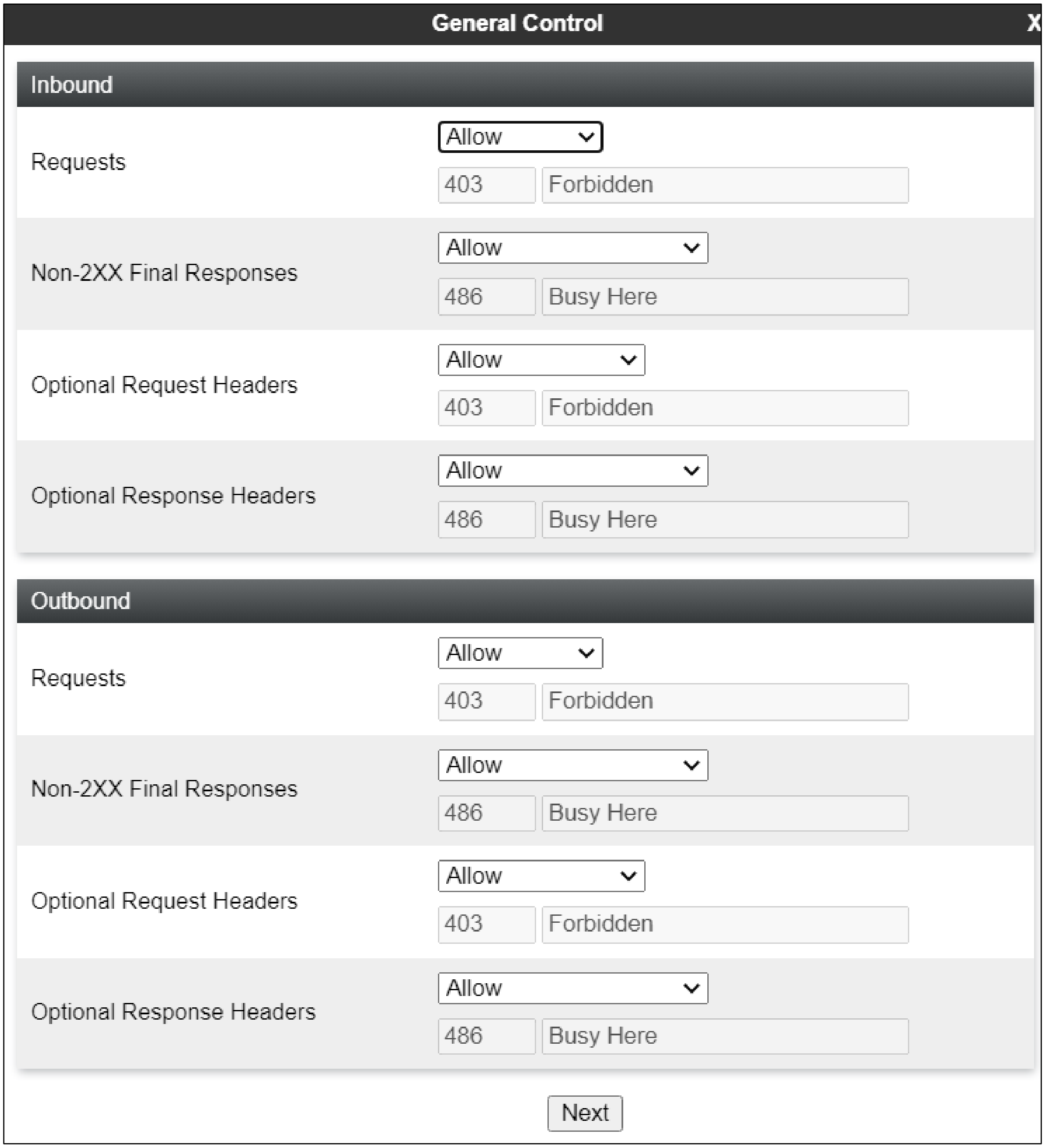
Looking at the **QoS** tab, this was enabled and set as shown below.



Click on **Signalling Rules** in the left windows to add or clone one for Voxtronic.

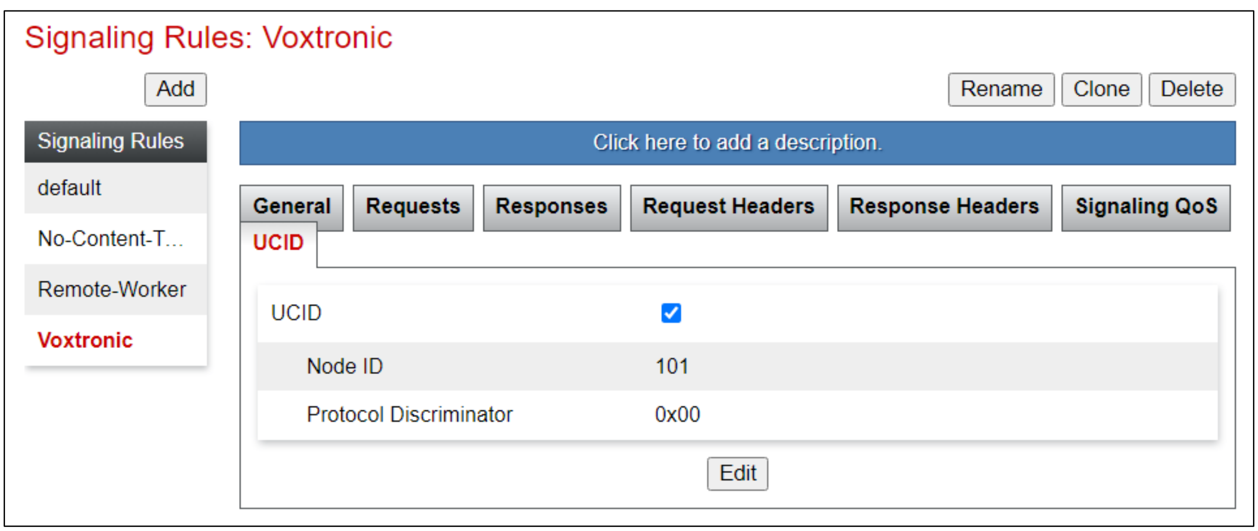


Clicking on the **General Tab** (from the previous page), shows the default settings below which were not changed.

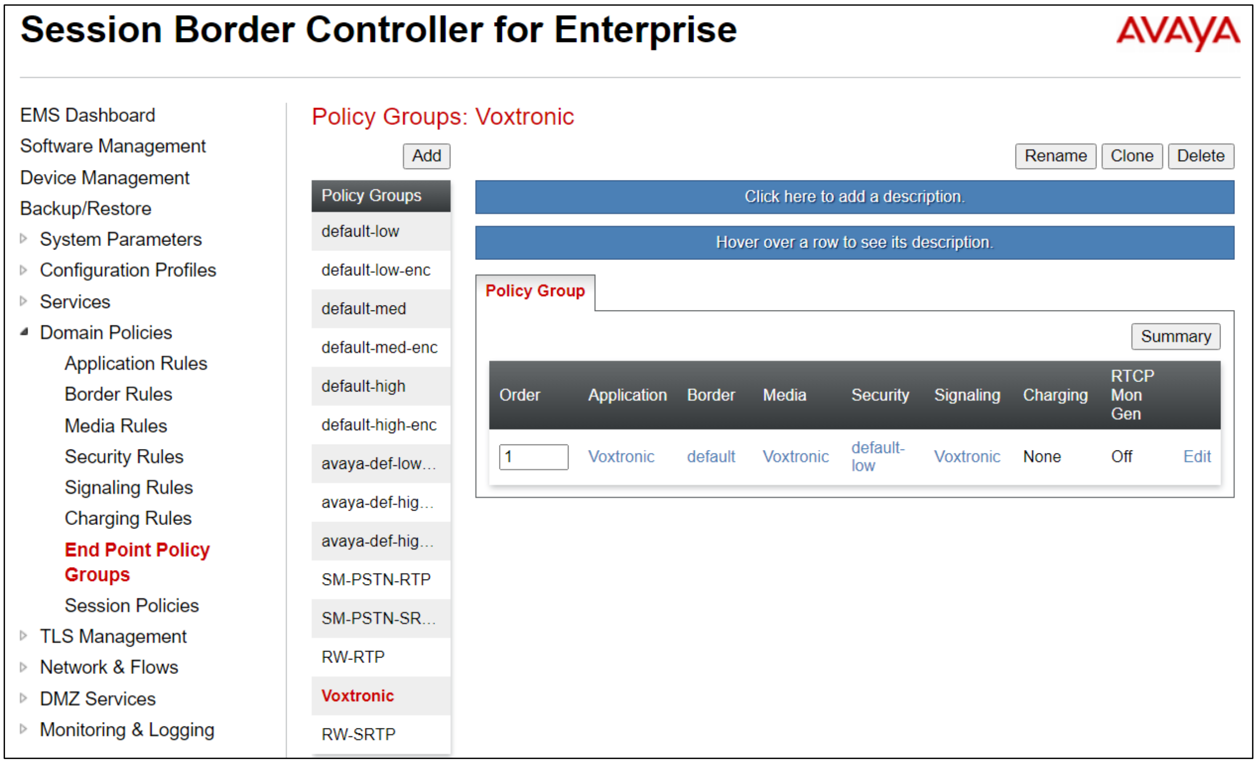


All other tabs for the Signalling Rule were left as default, and the **Signalling QoS** tab was set as shown below.

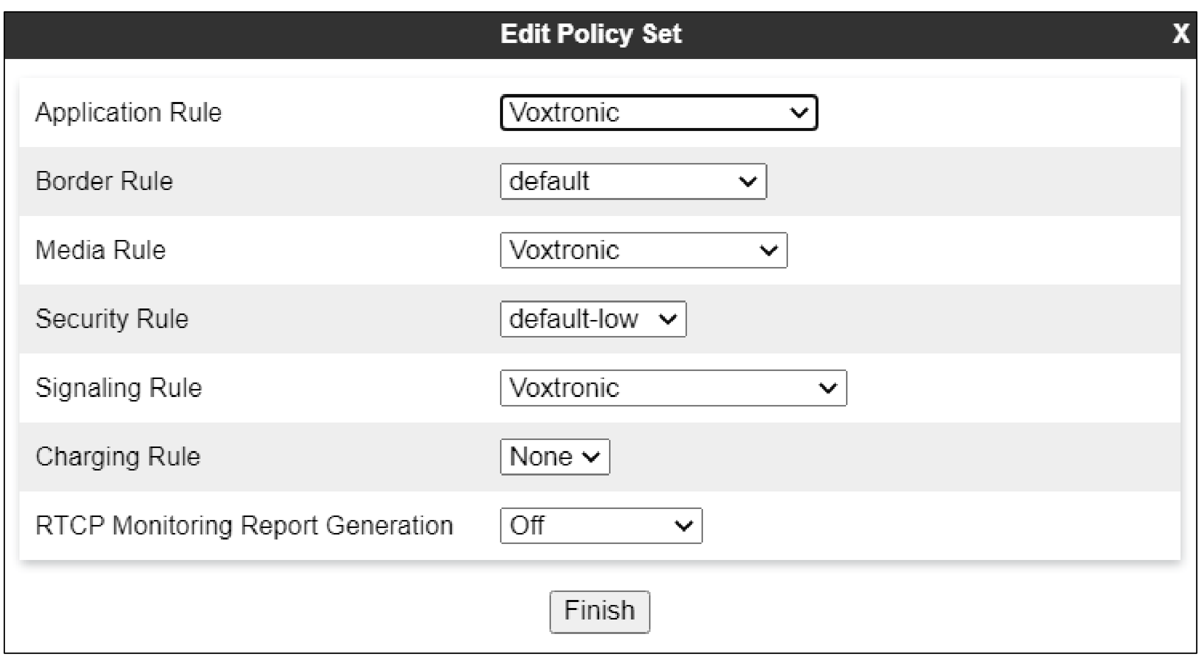
The **UCID** tab must be set, by ticking the **UCID** box as shown below, with a unique **Node ID** set.



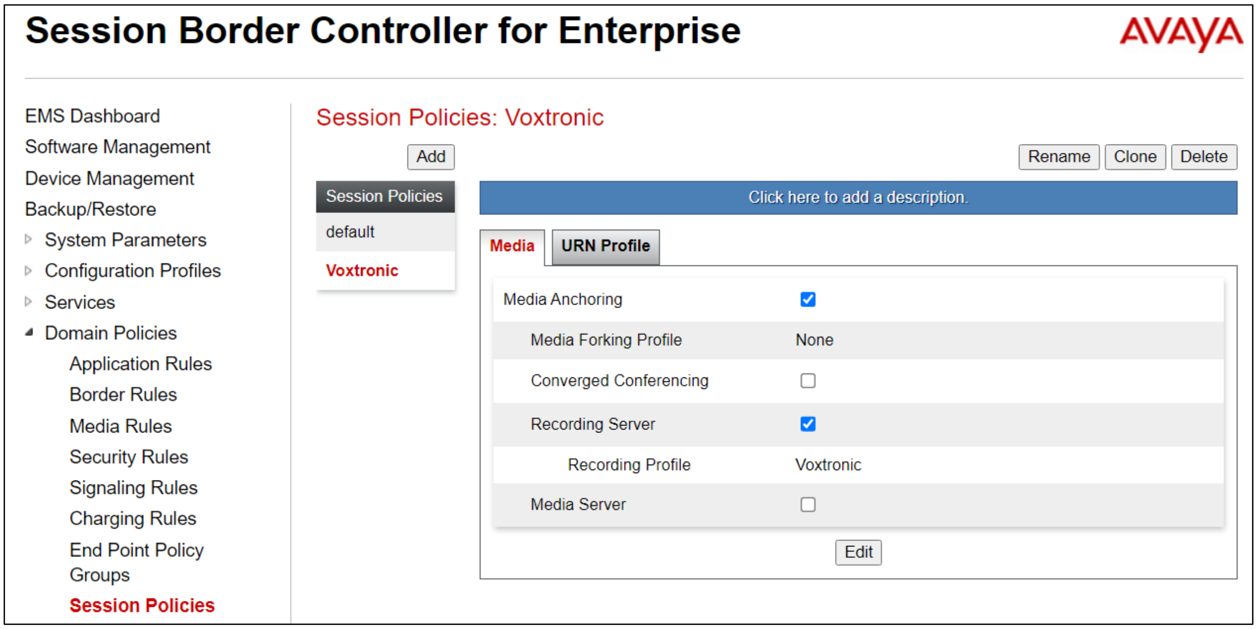
Finally, the **End Point Policy Group** can be created using some of the previous set rules. Again, this End Point Policy Group can be added as new or cloned from an existing group and then altered to suit the Voxtronic connection to the SBCE.



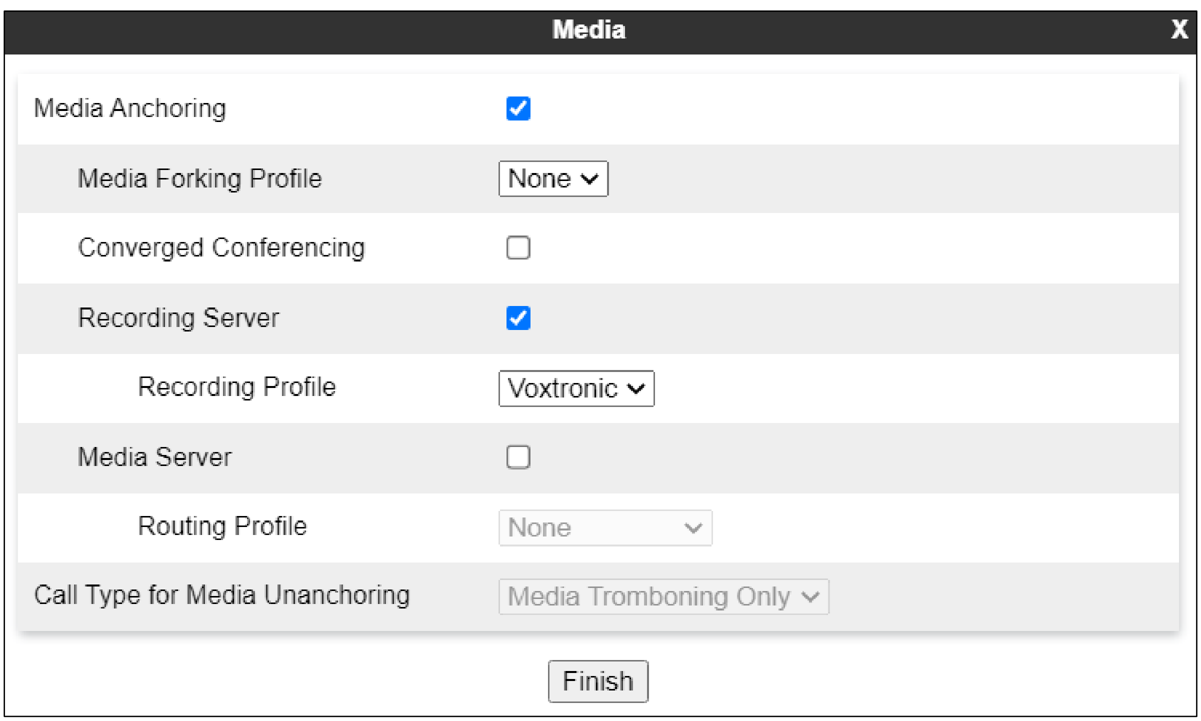
Below shows the various **Rules**, amply named **Voxtronic**, being used for this Policy Group.



The final policy within **Domain Policies** set for Voxtronic was **Session Policies**.



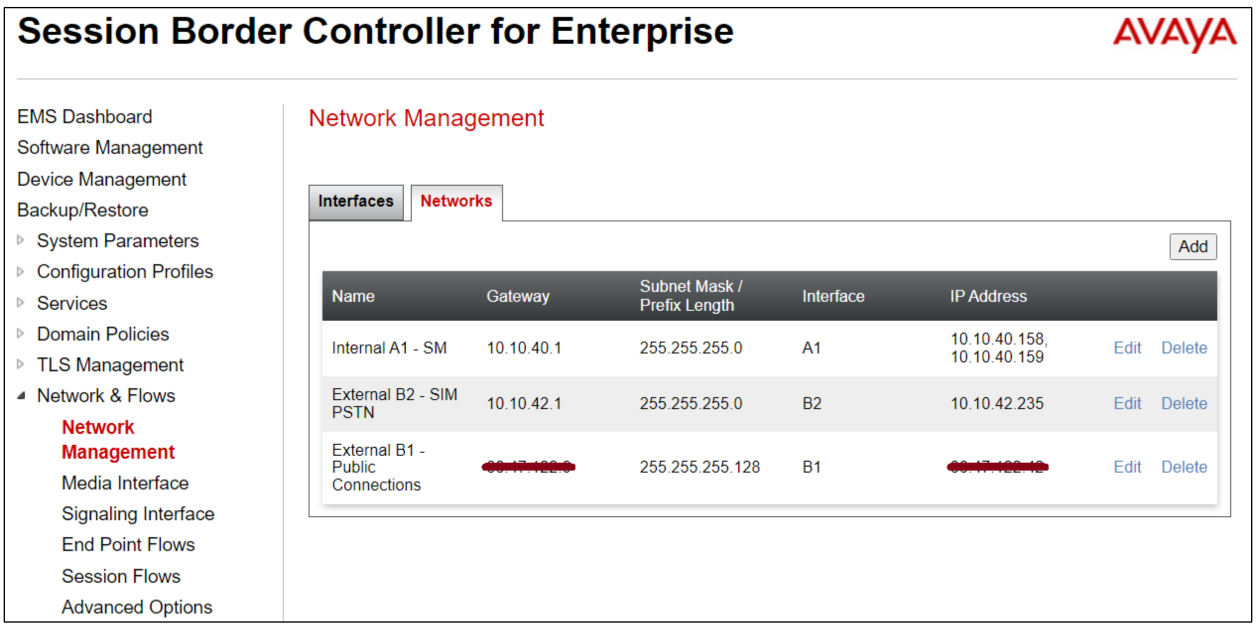
Below shows the Session Policy details, note that both **Media Anchoring** and **Recording Server** are both ticked, and the **Recording Profile** created in **Section 7.1** was used.



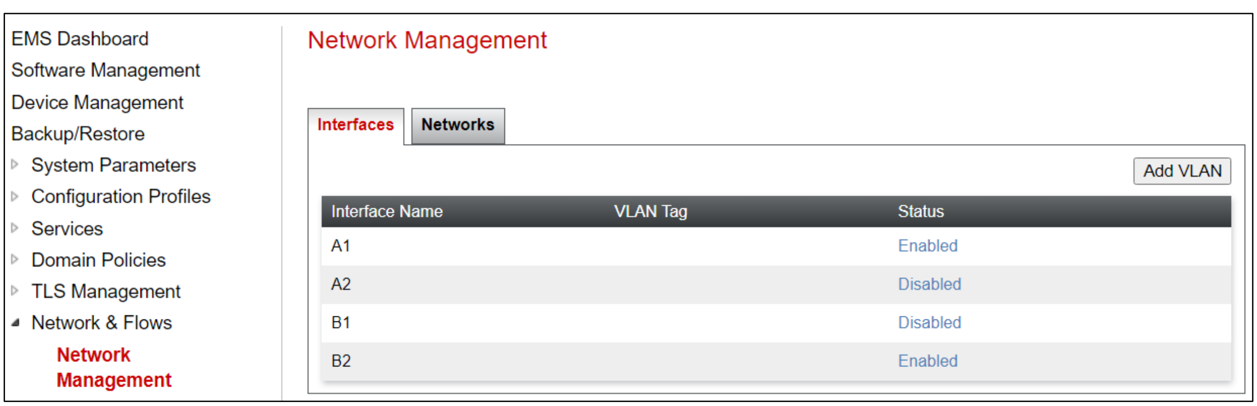
7.4. Configure Network & Flows

This is the core setup for the routing of SIP messages to Conex. Most of the settings described in the previous sections are geared towards providing a suitable server flow. When calls are made to or from Remote Workers, this must trigger the appropriate server flow and send the SIP INVITE to Conex. The “SBCE Loop” which was setup to record all VDN calls is also configured here to ensure that when the Implicit User is called and the Application Sequence is used, that the same INVITE is again triggered to Conex. The screens below will show a number of Server Flows as there are many required to route SIP messages through the SBCE, however this section focuses on those created specifically for Voxtronic.

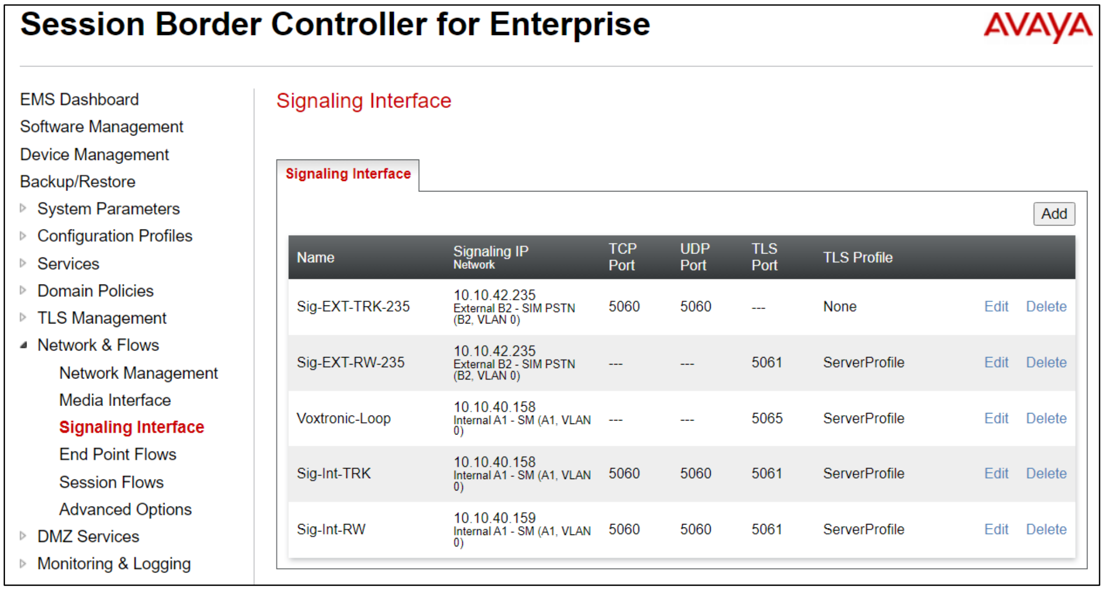
Clicking on **Network Management** in the left window, shows the **Networks** and **IP Address**es involved. For compliance testing and the setup to Conex, both the **A1** and **B2** interfaces are involved.



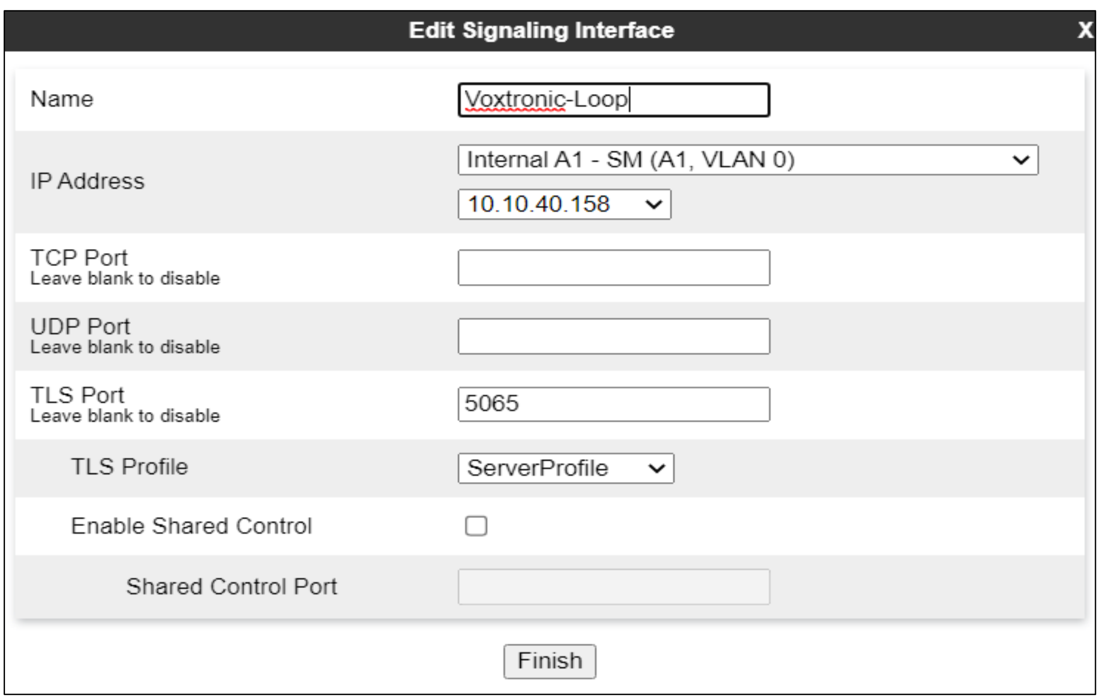
Clicking on the **Interfaces** tab, shows the **A1** and **B2** interfaces are the only ones **Enabled**.



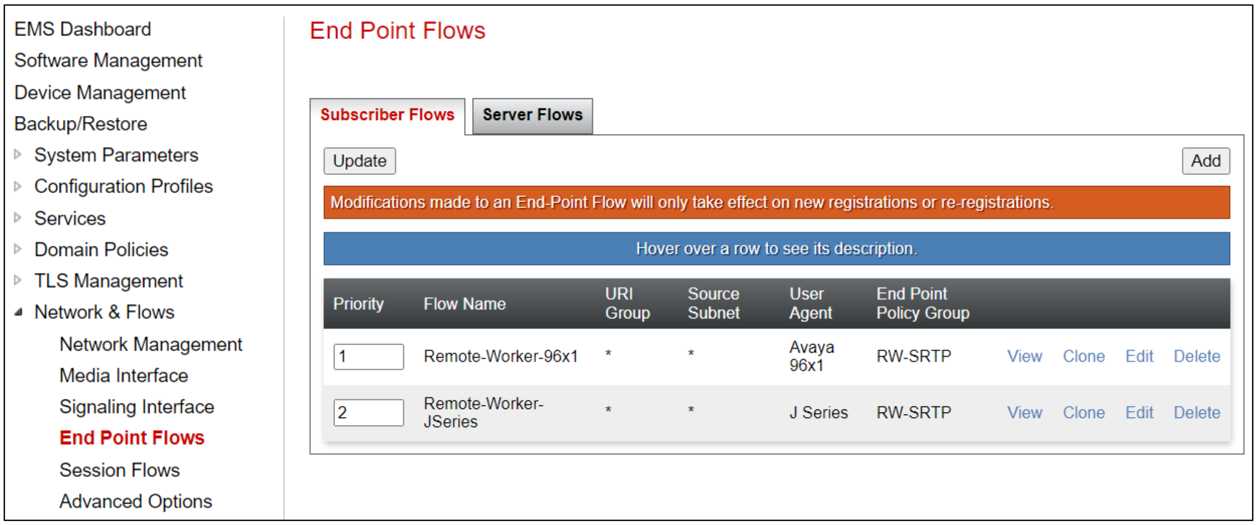
Clicking on the **Signalling Interface** in the left window, shows all the interfaces that are currently setup. A new Signalling Interface for the "Voxtronic-Loop" was created to allow the VDN calls to be recorded along with any and all announcements.



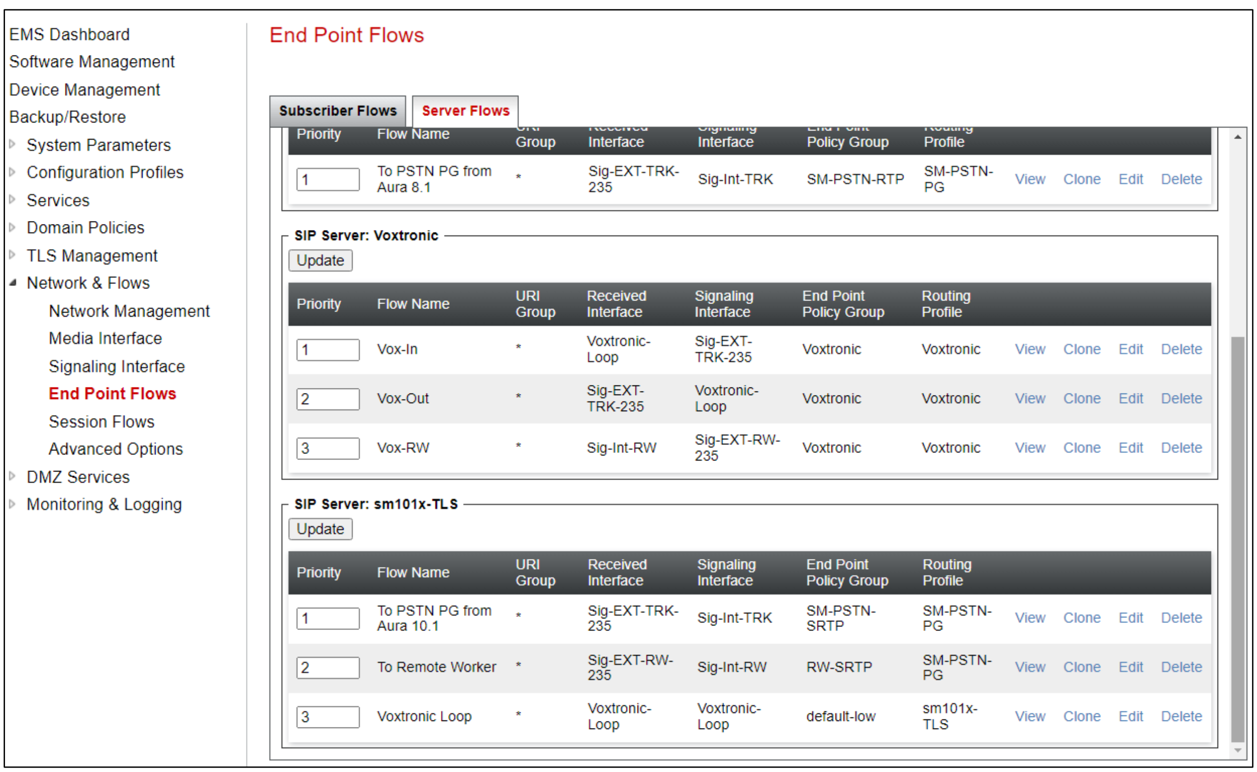
For this to work, the Inside IP address of the SBCE was used, and the port to Session Manager was specifically set to match that in **Section 6.2.1**. This uses TLS as this is a connection between the two Avaya components, that being the SBCE and Session Manager. This is used however for the recording of calls but is not connected to the VoIP Recorder.



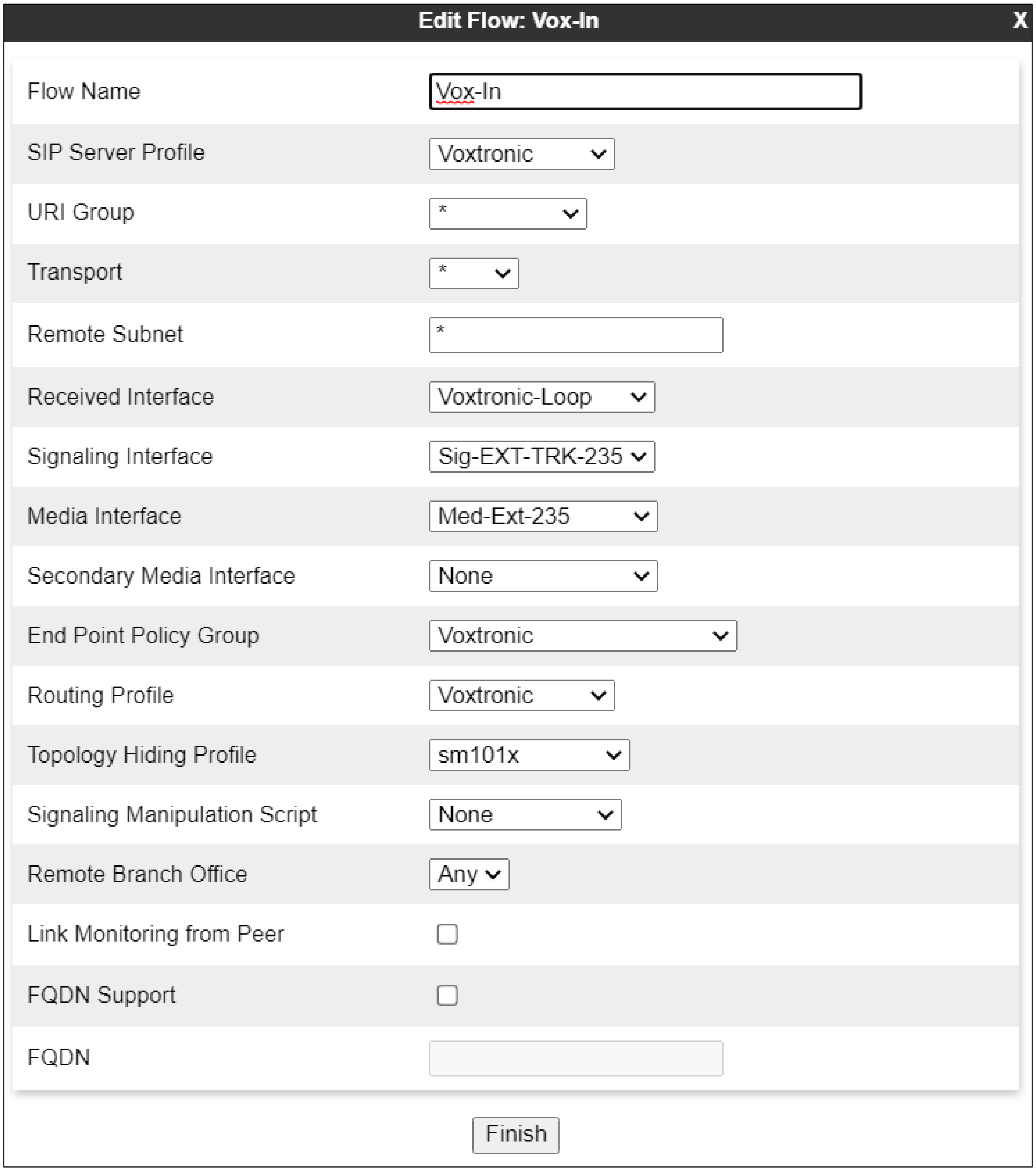
Clicking on **End Point Flows** in the left window shows the **Subscriber Flows** and the **Server Flows**. The Subscriber Flows are setup for Remote Workers and are outside the scope of these Application Notes. However, most of the setup for Remote Workers is shown in **Appendix A**.



Clicking on the **Server Flows** tab shows all the Server Flows in operation. There are three flows created that use the **Voxtronic SIP Server**, these are **Vox-In**, **Vox-Out** and **Vox-RW**. Another flow is created for the **Voxtronic Loop** for recording the VDN calls, and this uses the Session Manager **SIP Server**.



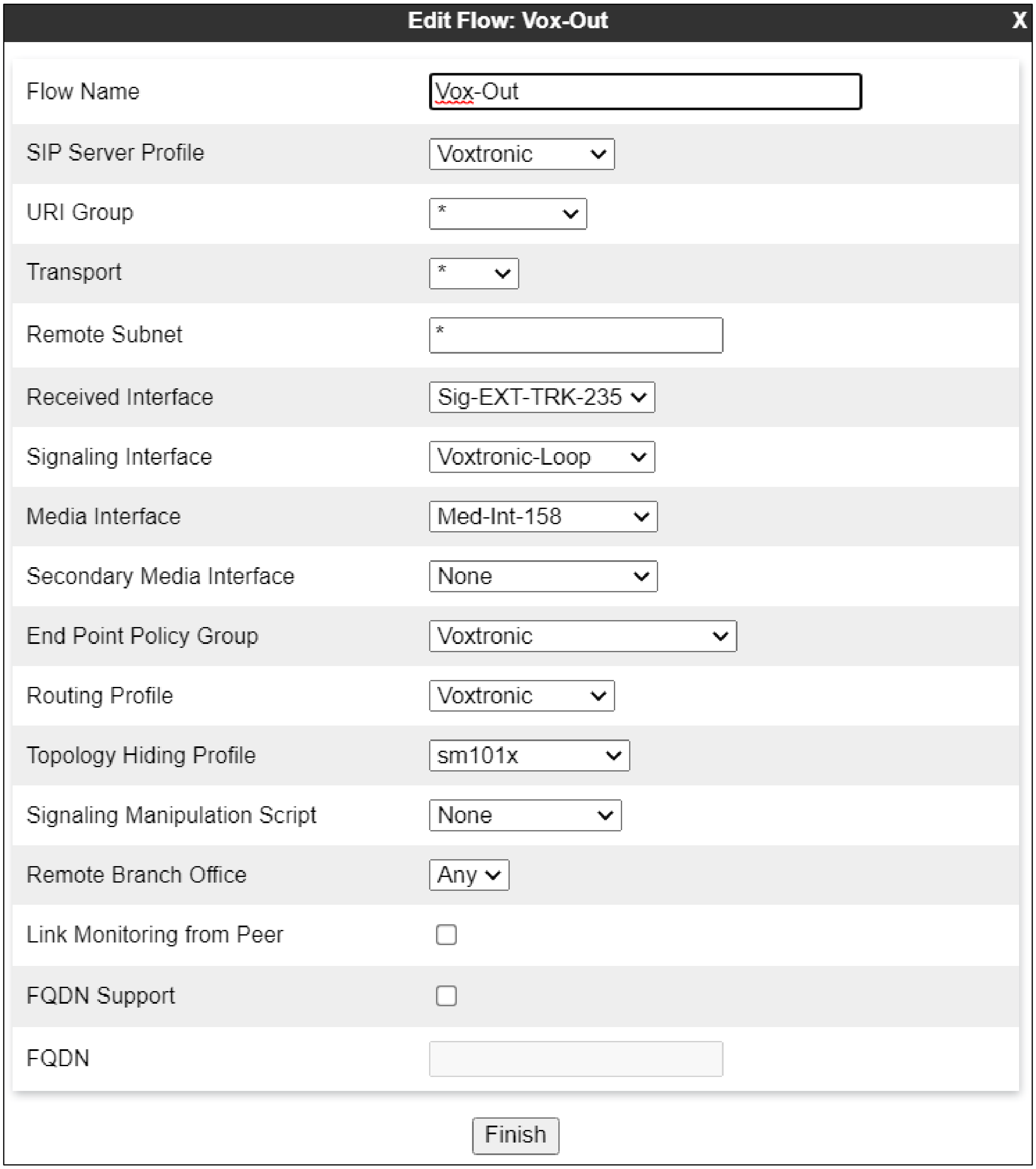
Below are the details for the **Vox-In** Server Flow.


Edit Flow: Vox-In

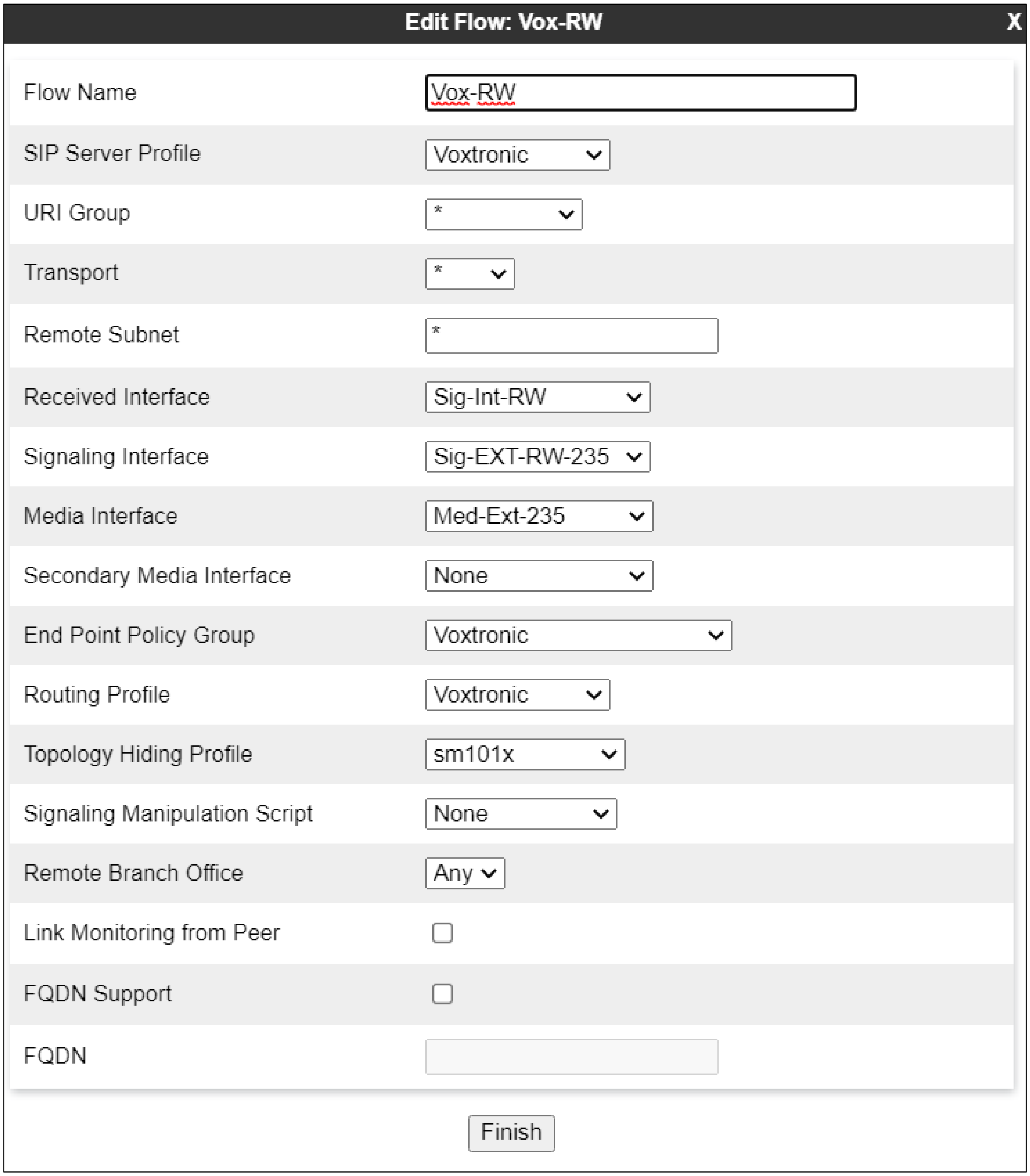
Flow Name	Vox-In
SIP Server Profile	Voxtronic
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Voxtronic-Loop
Signaling Interface	Sig-EXT-TRK-235
Media Interface	Med-Ext-235
Secondary Media Interface	None
End Point Policy Group	Voxtronic
Routing Profile	Voxtronic
Topology Hiding Profile	sm101x
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	
FQDN Support	
FQDN	

Finish

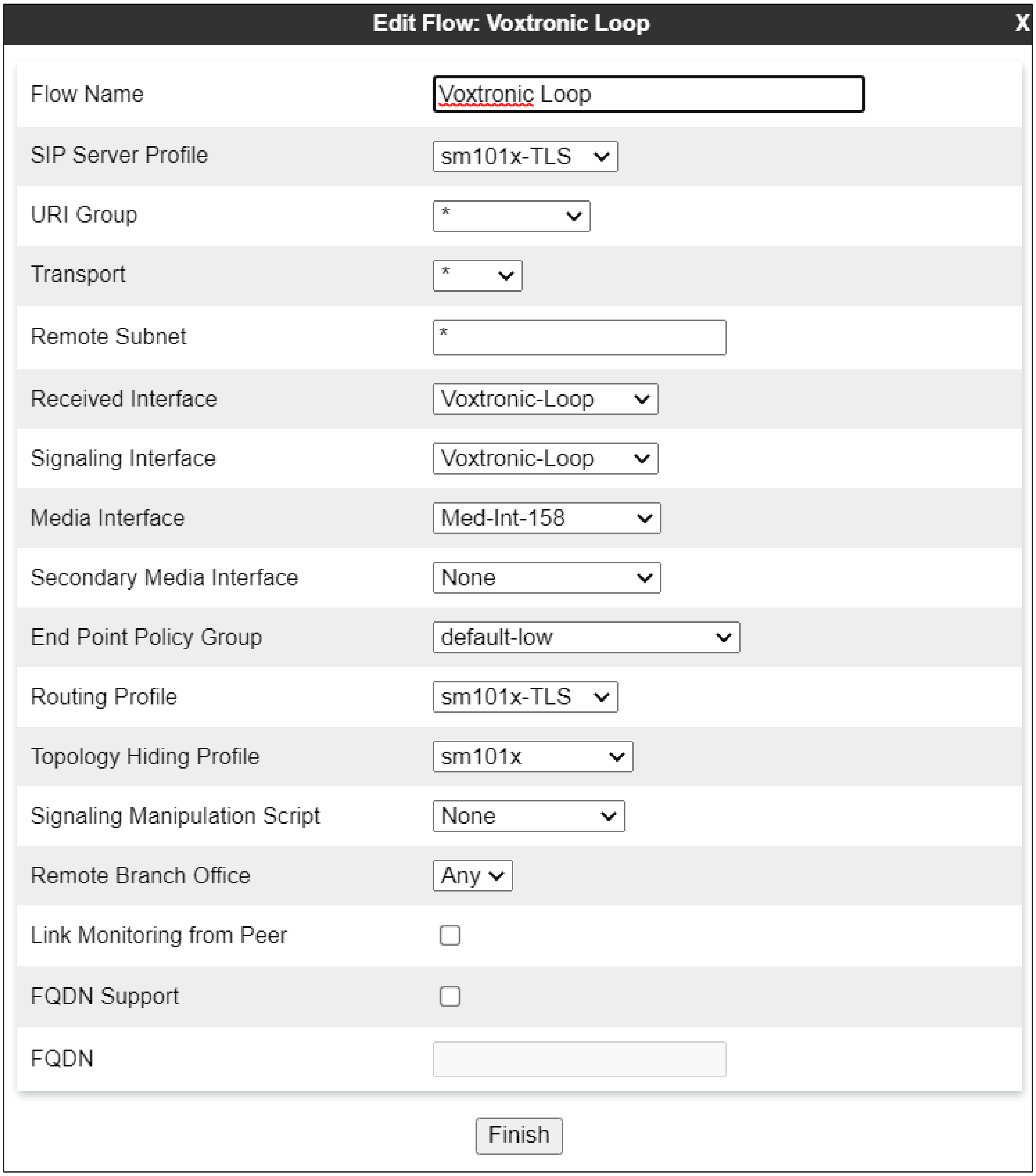
Below are the details for the **Vox-Out** Server Flow.



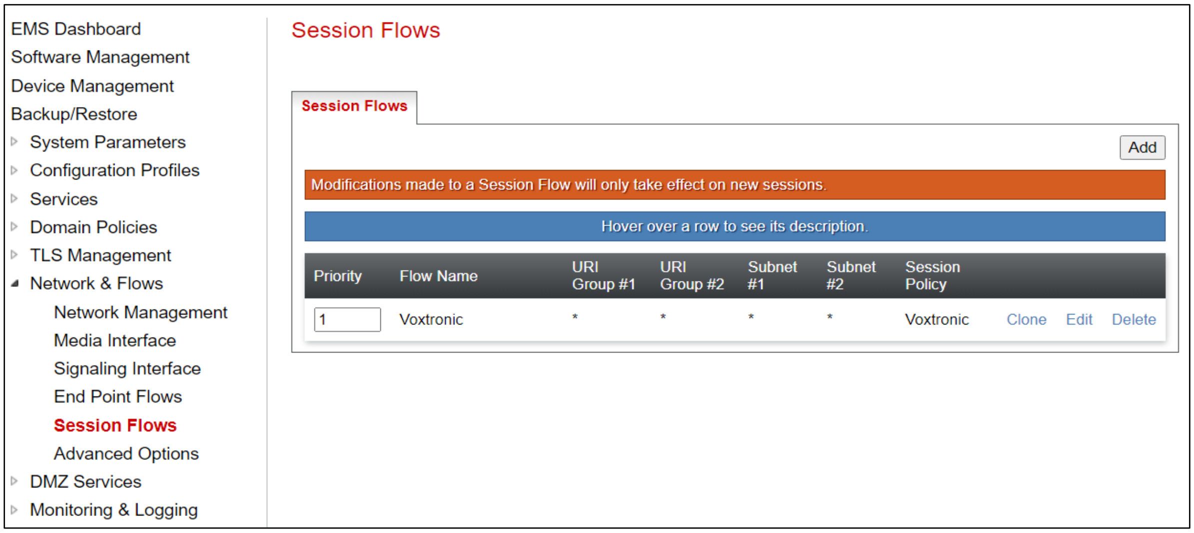
Below are the details for the **Vox-RW** Server Flow.



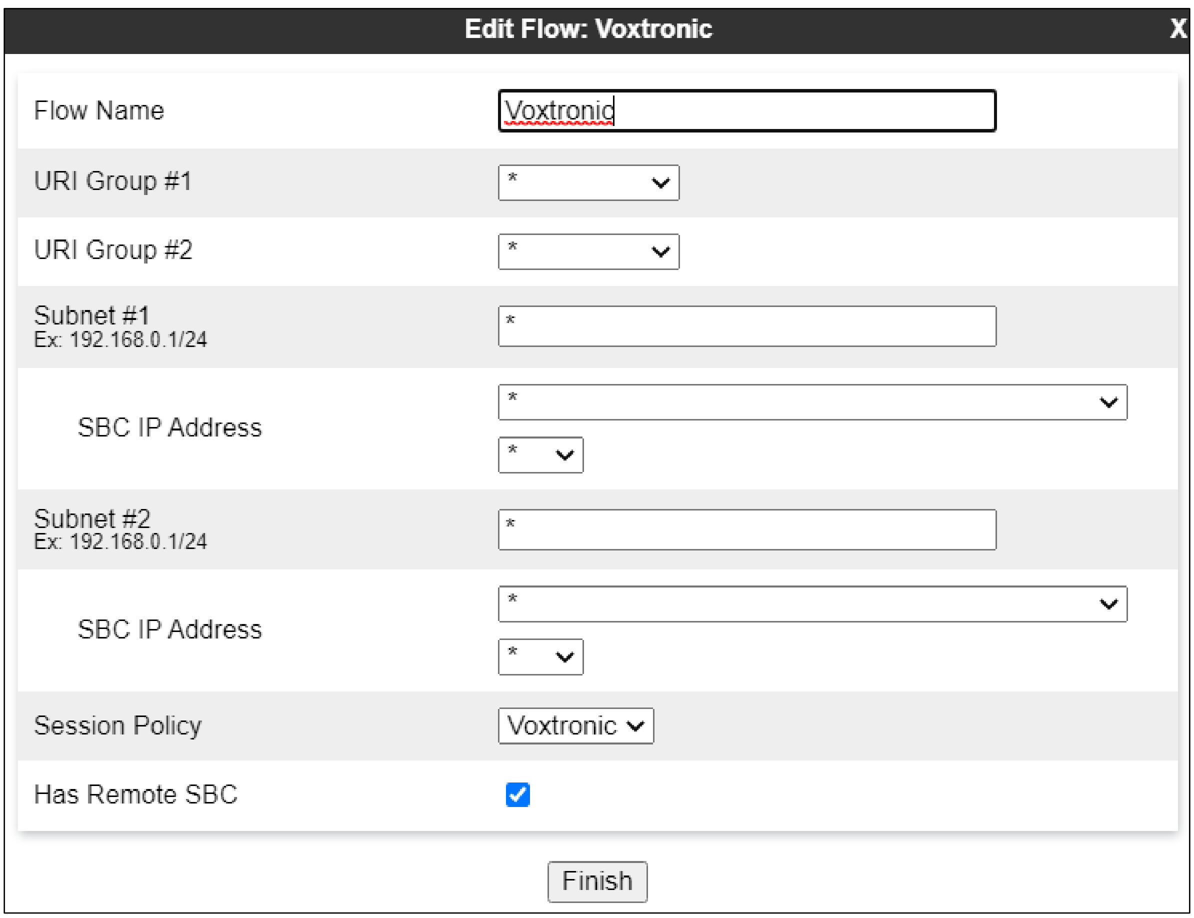
Below are the details for the **Voxtronic Loop** Server Flow.



Finally, within **Network & Flows**, the Session Flow for Voxtronic is added. Click in Session Flows in the left window and click on **Add** to add a new flow.



Below are the details for the **Voxtronic** Session Flow.



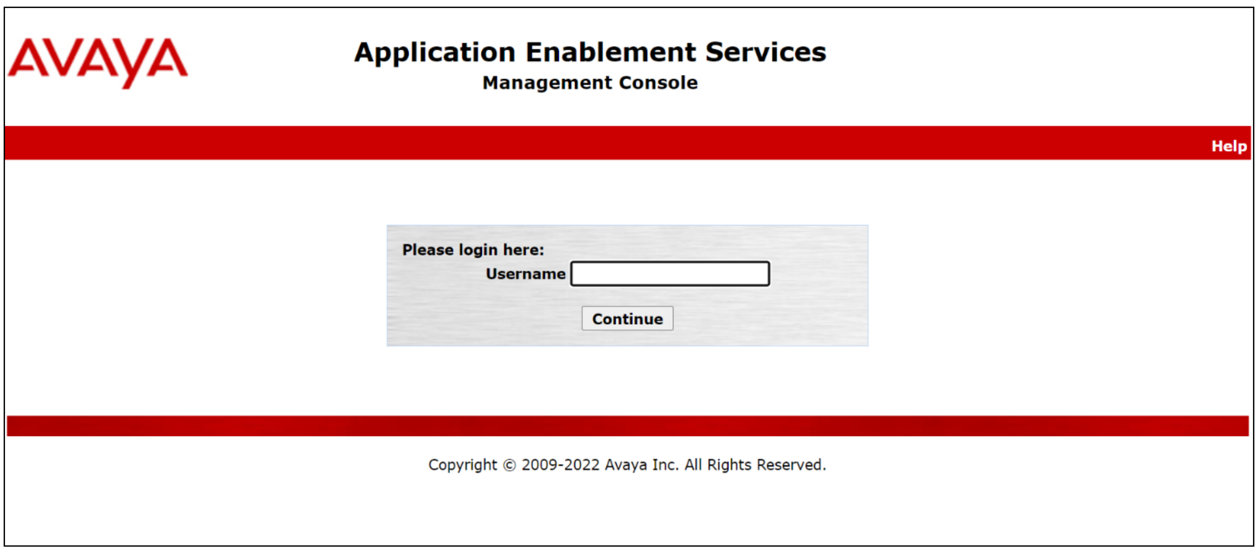
8. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring AES. The procedures fall into the following areas:

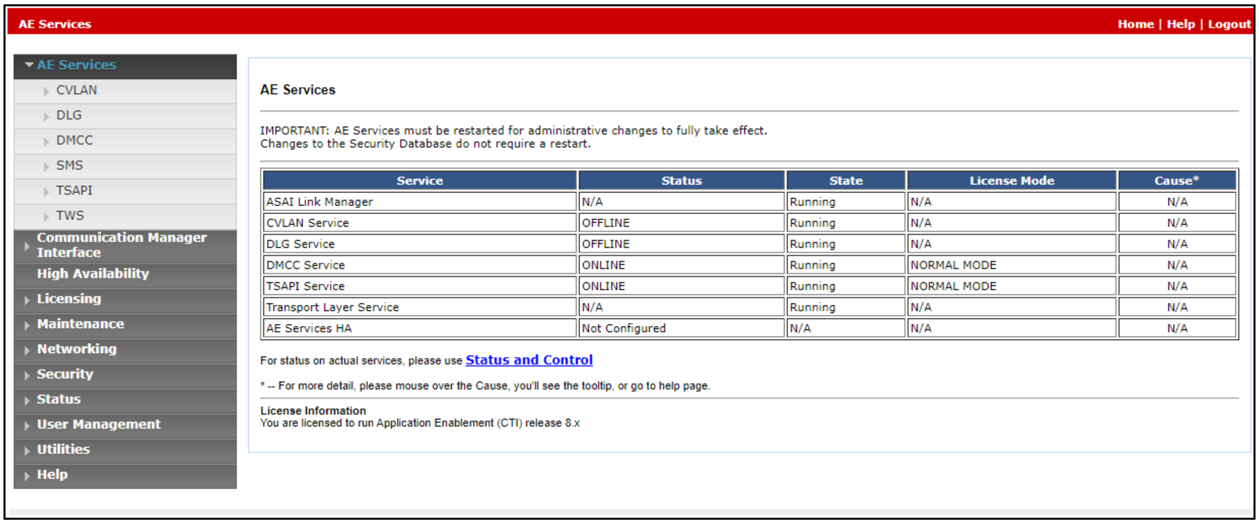
- Verify Licensing
- Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Configure Security
- Restart AE Server

8.1. Verify Licensing

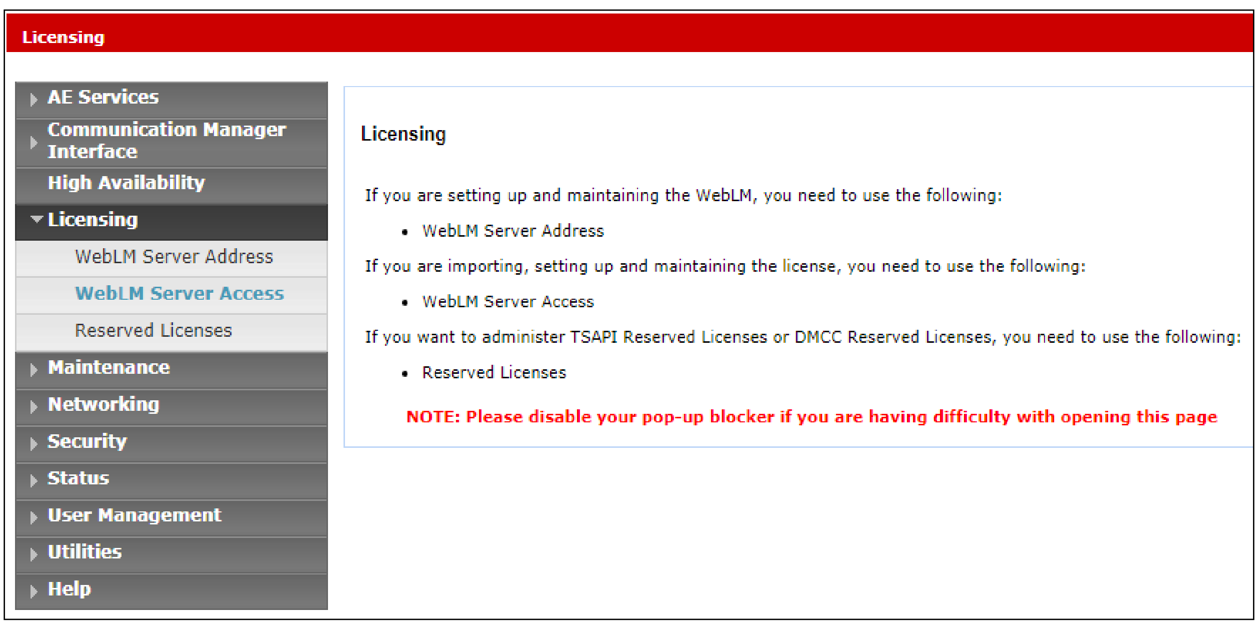
To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



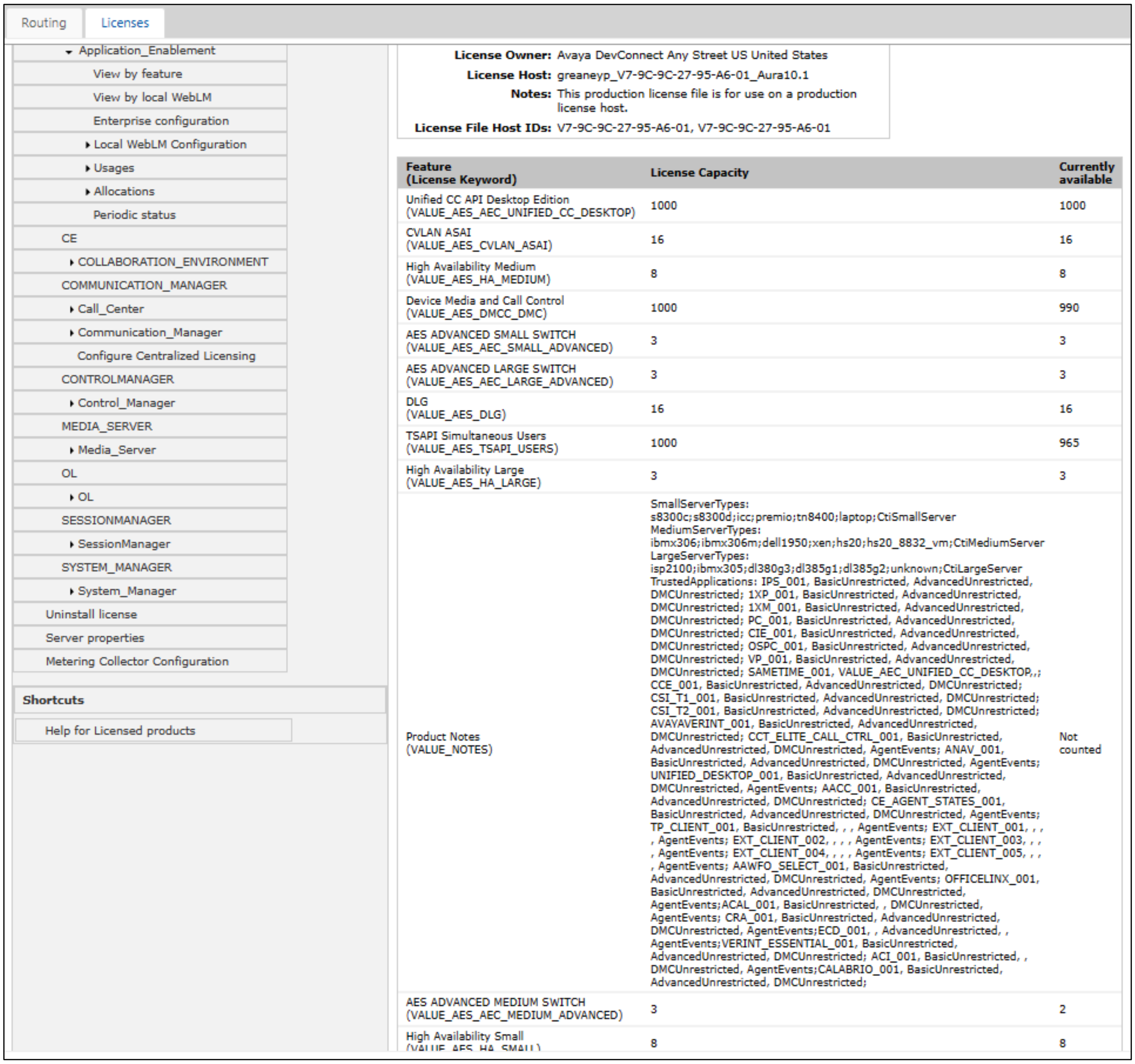
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Services are licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the appropriate license.



The TSAPI licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

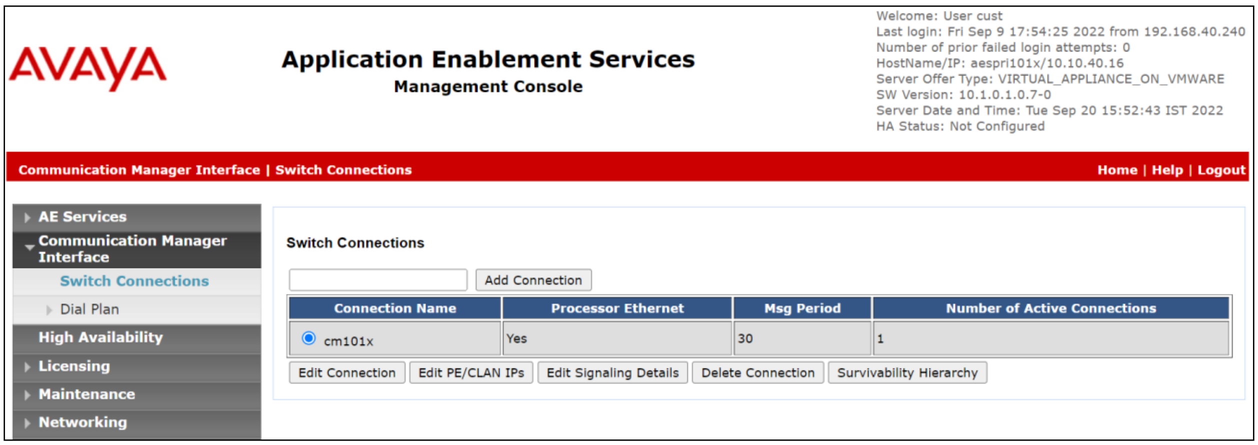


The following screen shows the available licenses for **TSAPI** users.

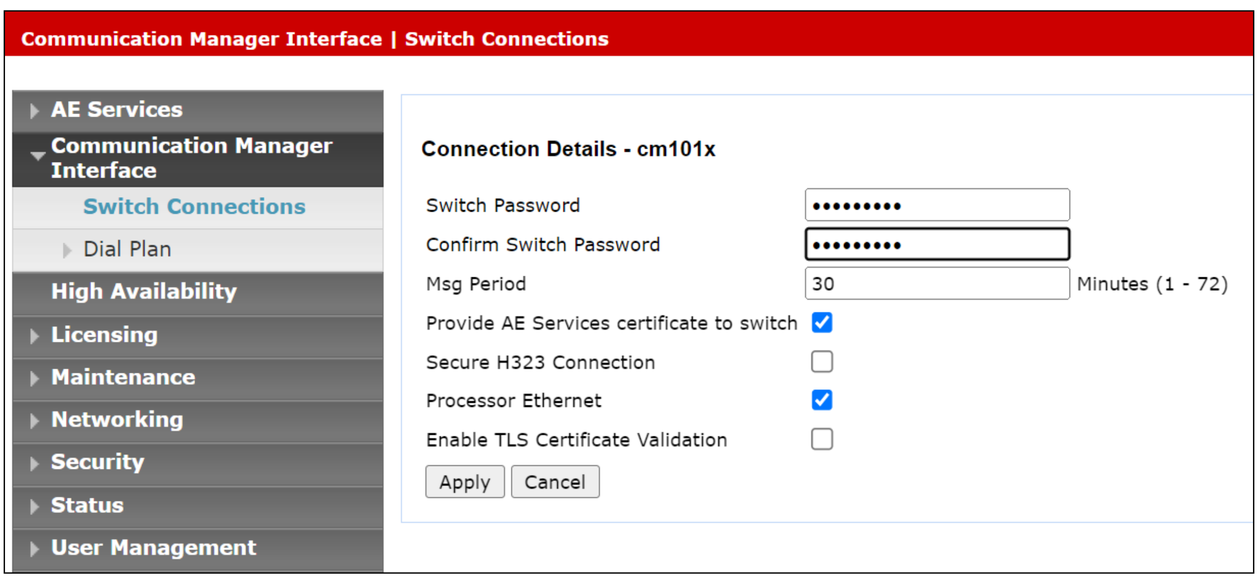


8.2. Create Switch Connection

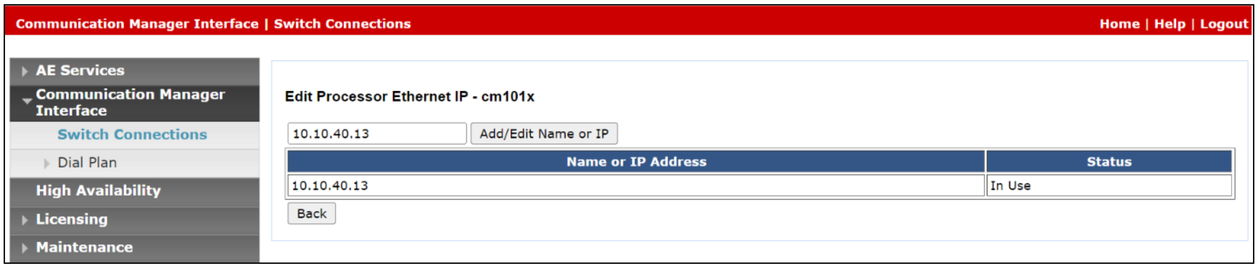
Typically, the connection between the AES and Communication Manager is setup as part of the initial installation and would not usually be outlined in these Application Notes. Due to the nature of this particular setup with two connections from Communication Manager to two separate AES's the switch connection will be displayed on this section. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.



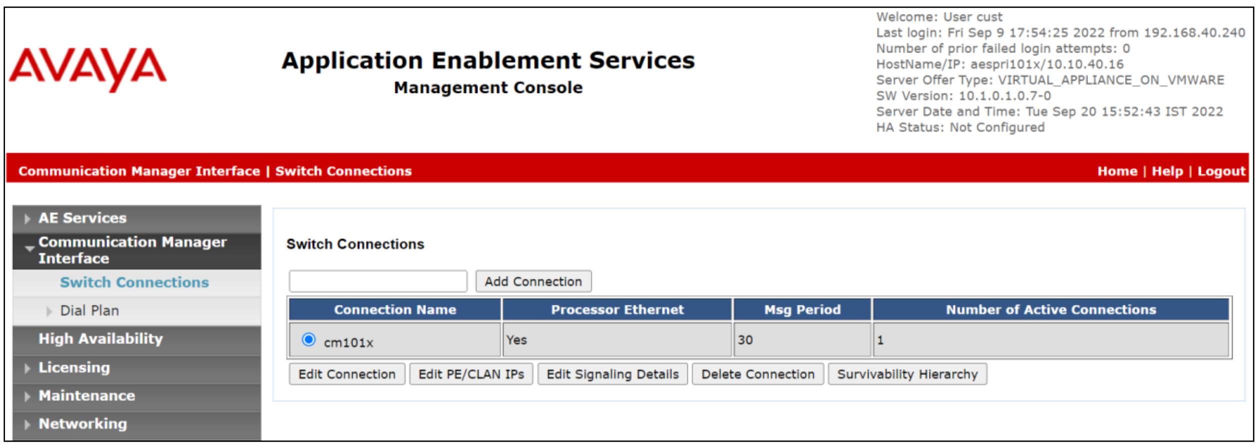
In the resulting screen, enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4.2**. **Secure H323 Connection** was left unticked, as shown below. Click **Apply** to save changes.



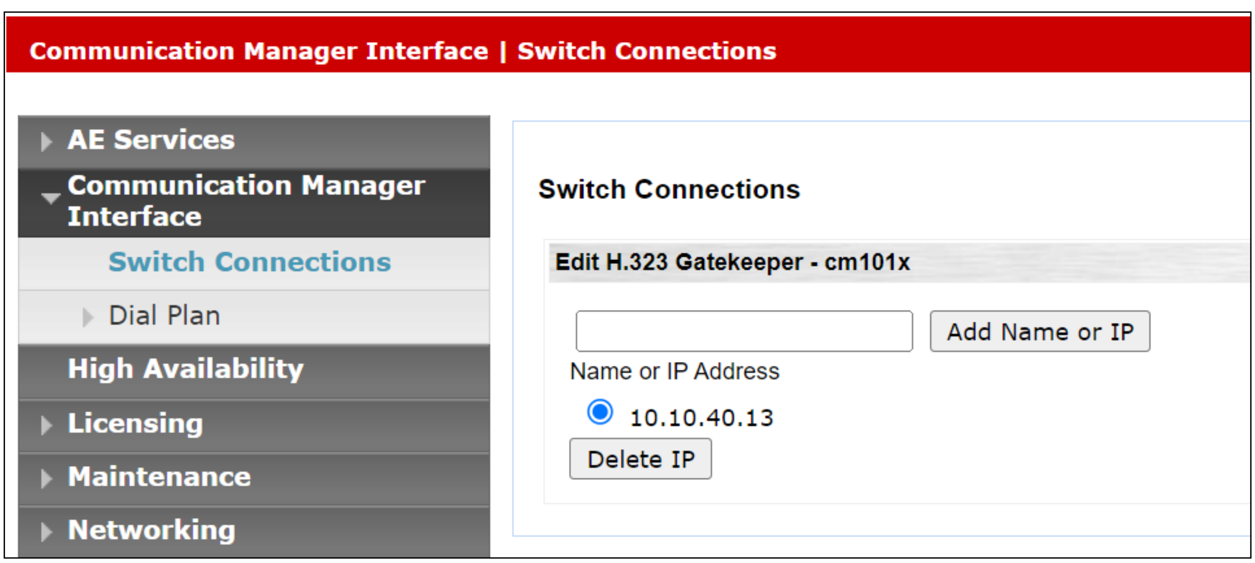
From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown), see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section 5.4.1** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.

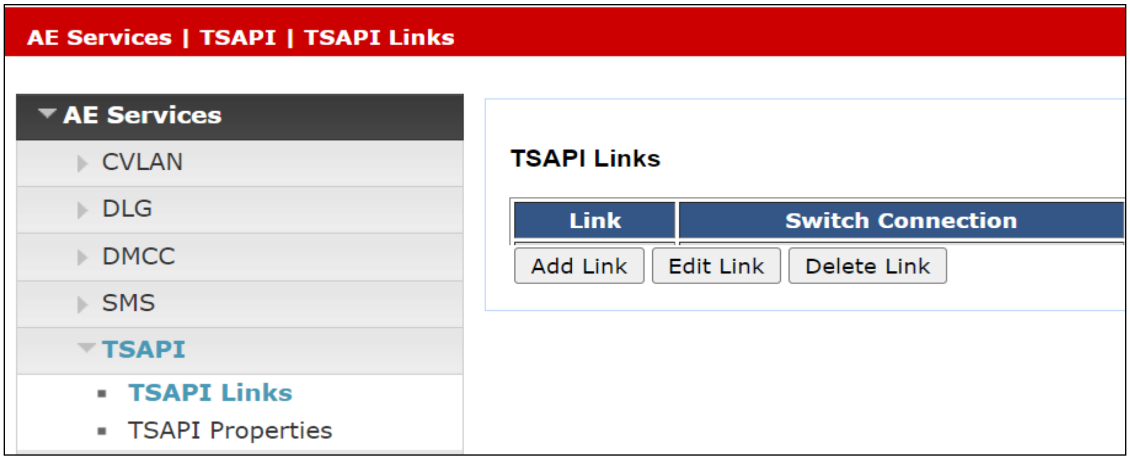


The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.



8.3. Administer TSAPI link

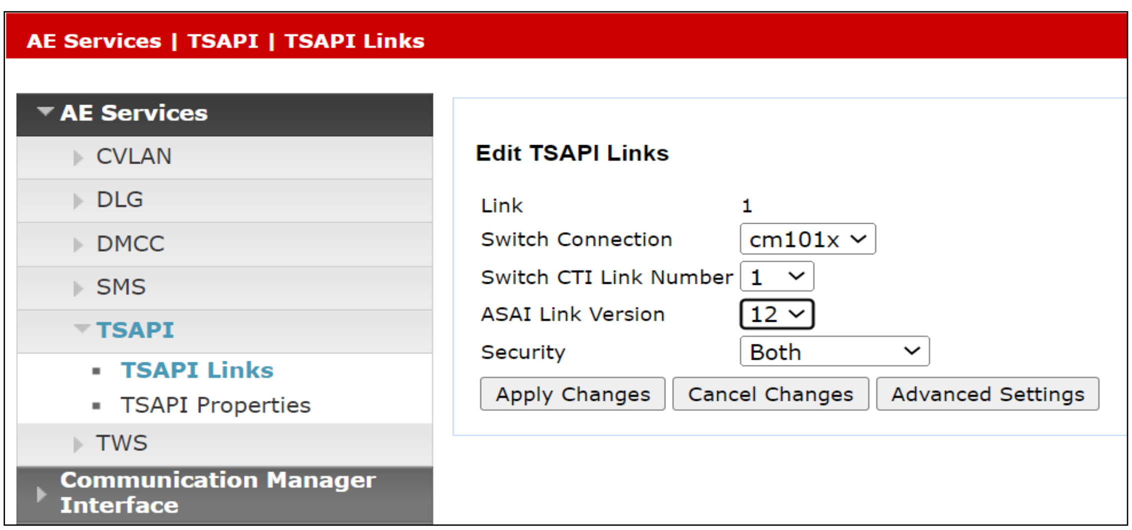
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



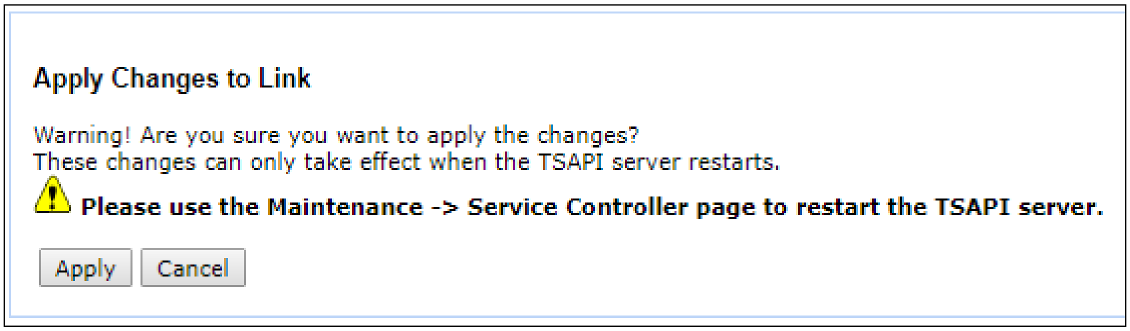
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, which has already been configured in **Section 8.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4.3** which is **1**.
- **ASAI Link Version:** This should correspond with the Communication Manager version (the latest version available should be chosen).
- **Security:** This can be left at the default value of **both**.

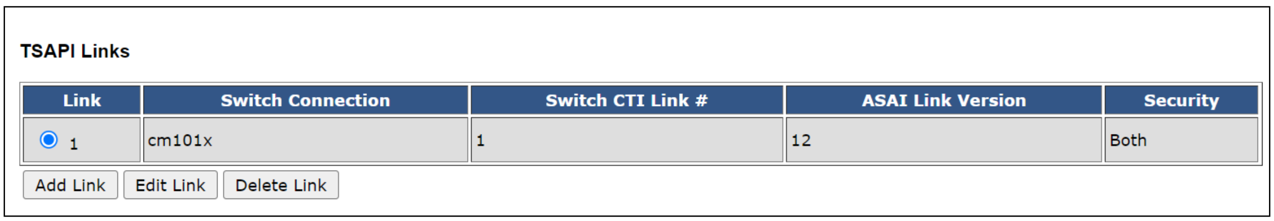
Once completed, select **Apply Changes**.



Another screen appears for confirmation of the changes made. Choose **Apply**.



When the TSAPI Link is completed, it should resemble the screen below.



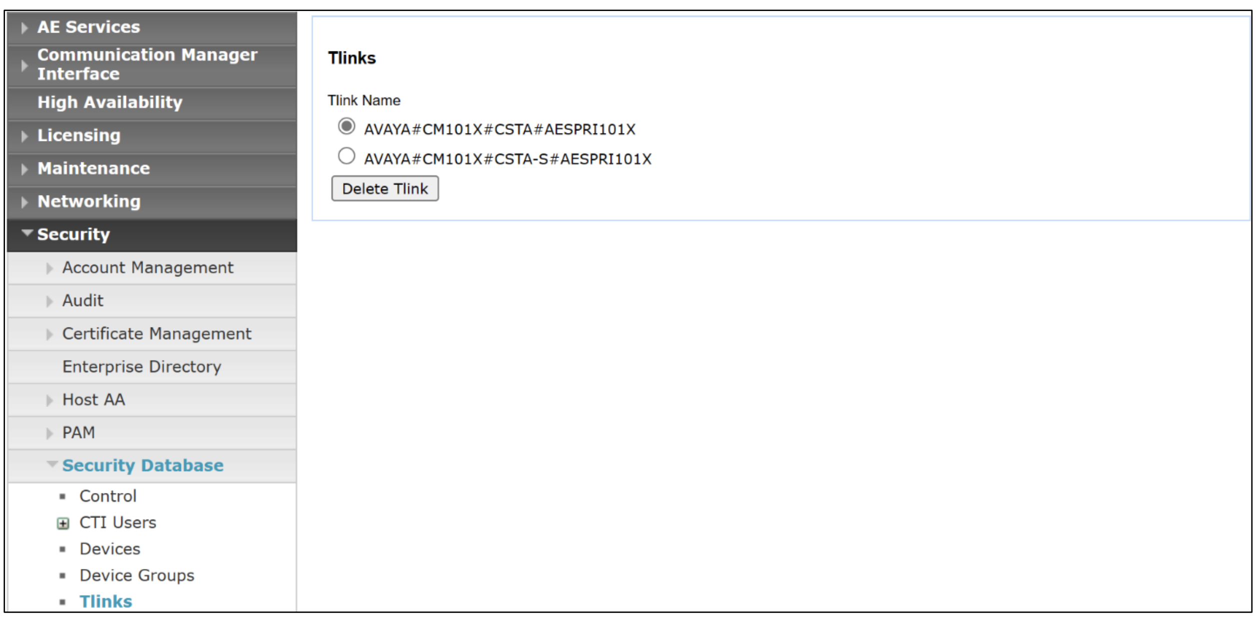
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm101x	1	12	Both

Add Link | Edit Link | Delete Link

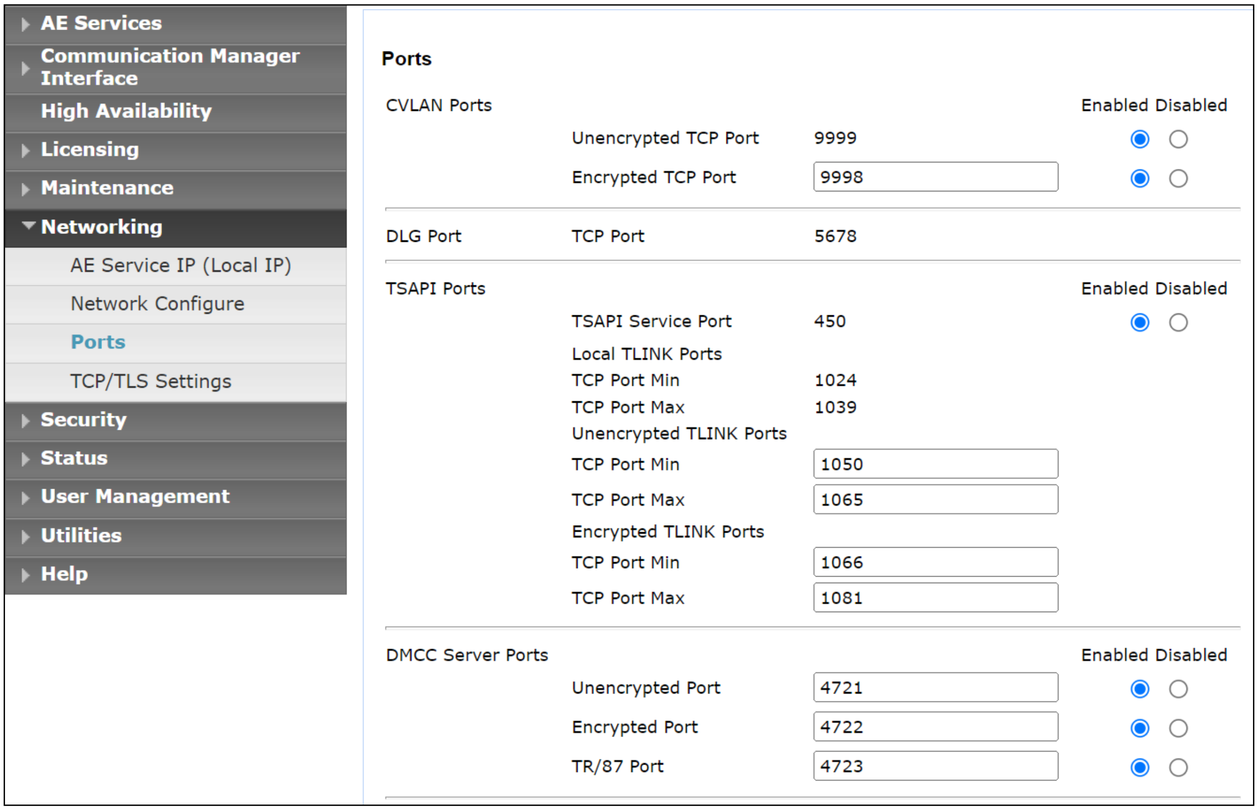
8.4. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**.



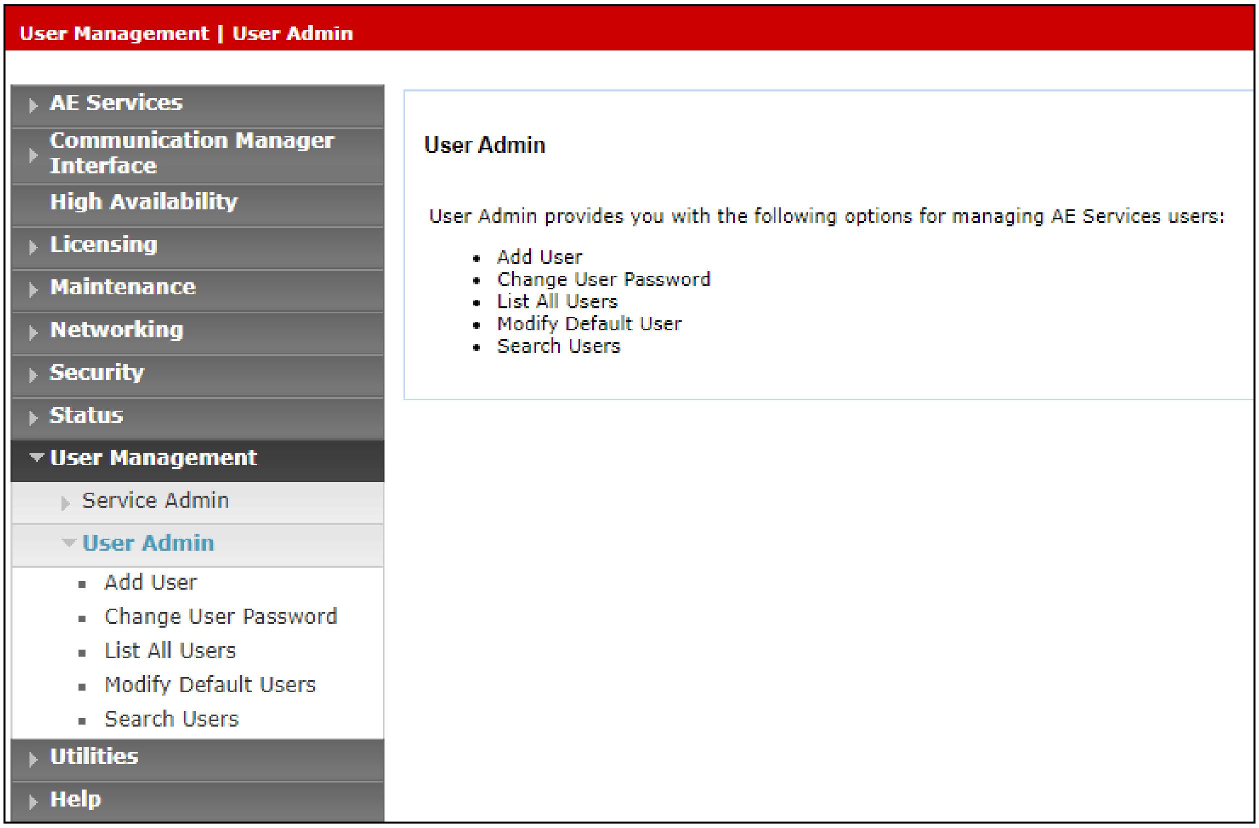
8.5. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Also, note the port numbers required to make a successful connection.



8.6. Create Avaya CTI User

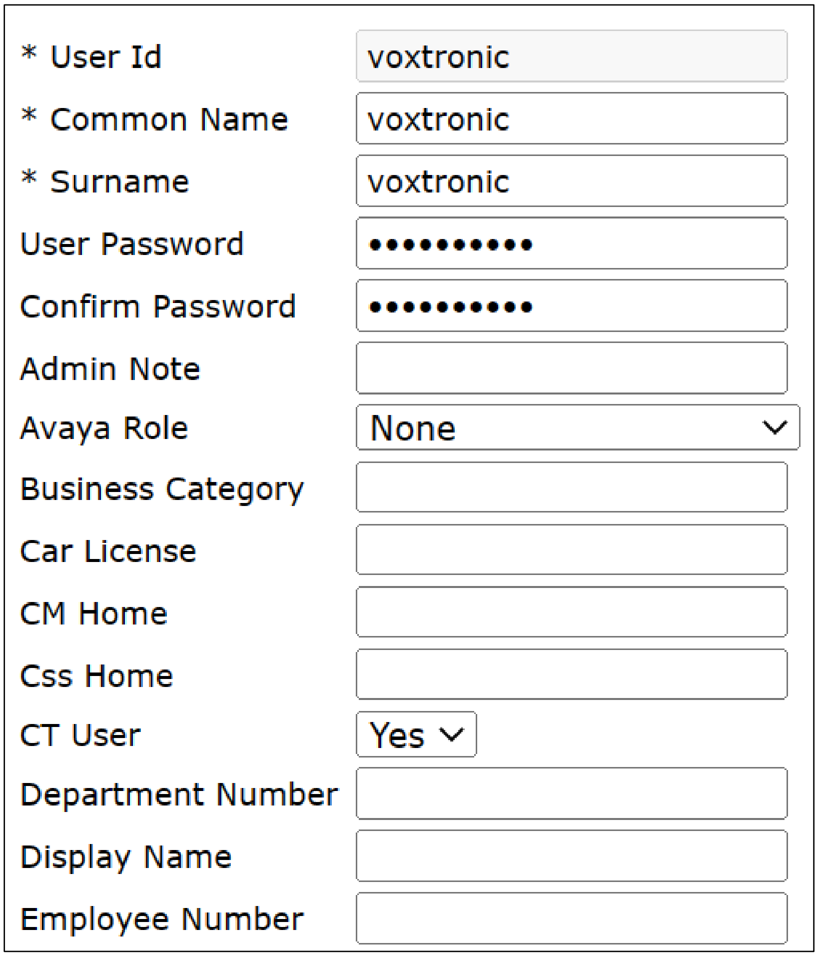
A User ID and password needs to be configured for Conex to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by the VoIP Recorder.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used by the VoIP Recorder.
- **CT User -** Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).



The next screen will show a message indicating that the user was created successfully (not shown).

8.7. Configure Security

The CTI user and the database security are set here under **Security Database**.

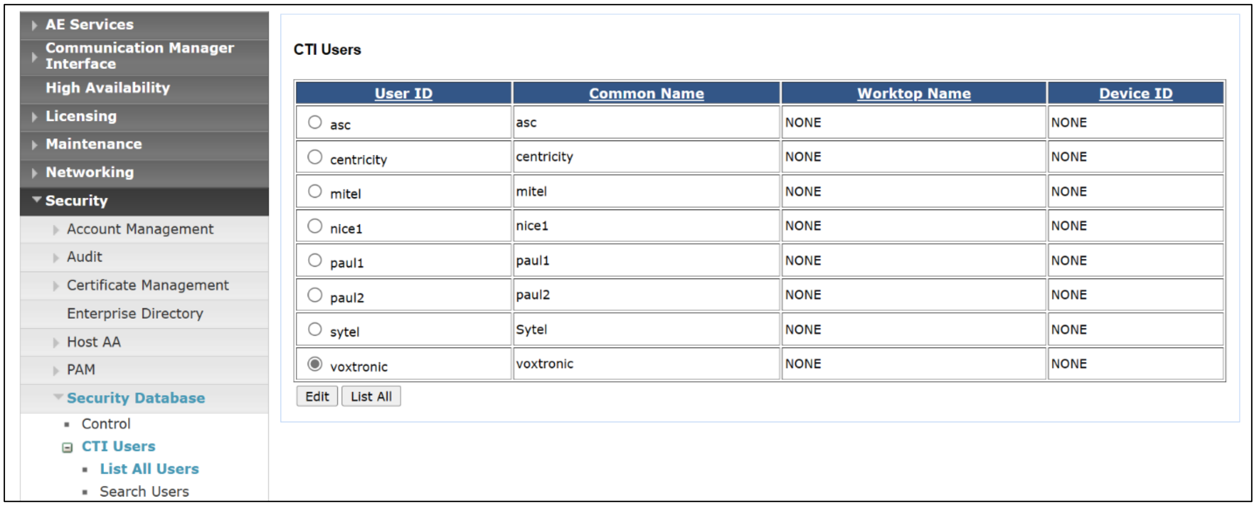
8.7.1. Configure Database Control

Open **Control** and ensure that the **SDB Control** is set as shown below.

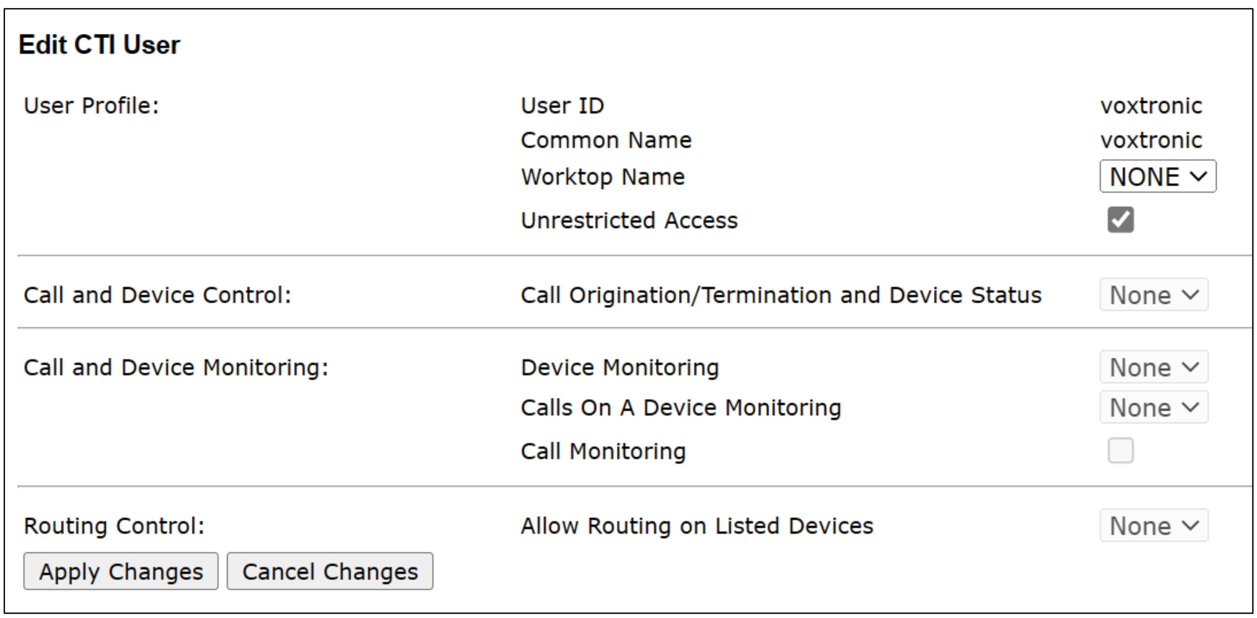
Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section 12** for more information on this.

8.7.2. Associate Devices with CTI User

Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 8.6** and click on **Edit Users**.

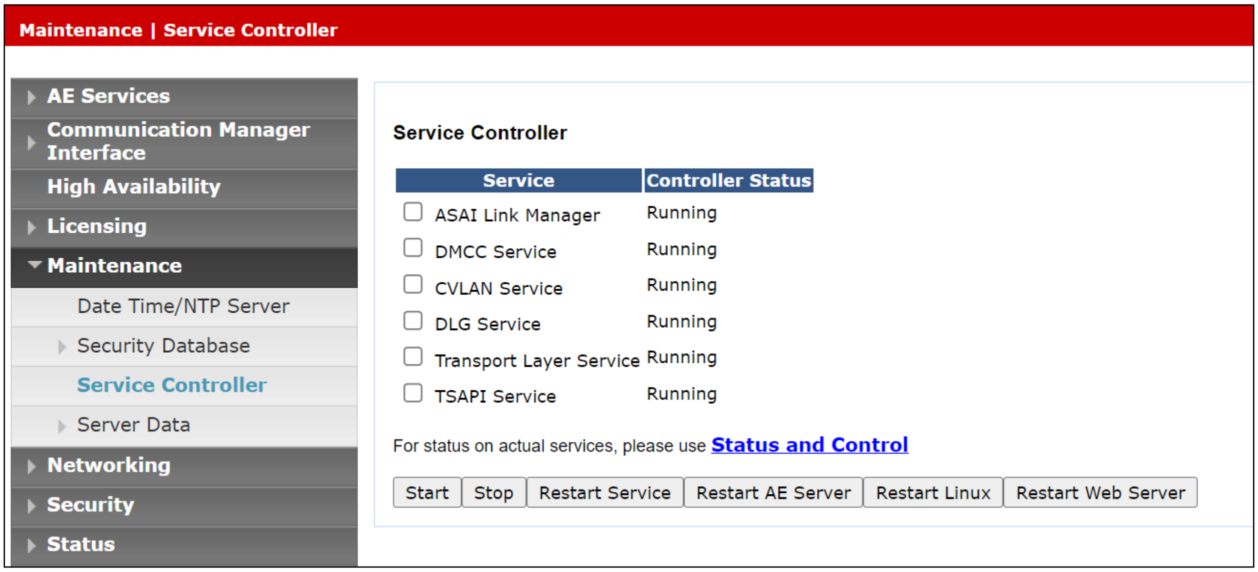


In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

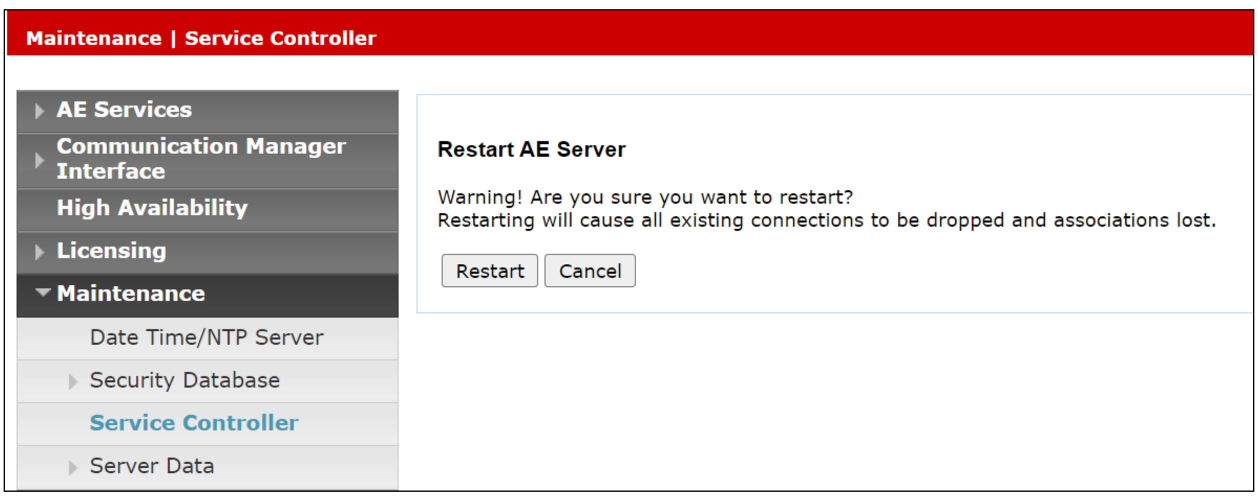


8.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.



A message confirming the restart will appear, click on **Restart** to proceed.

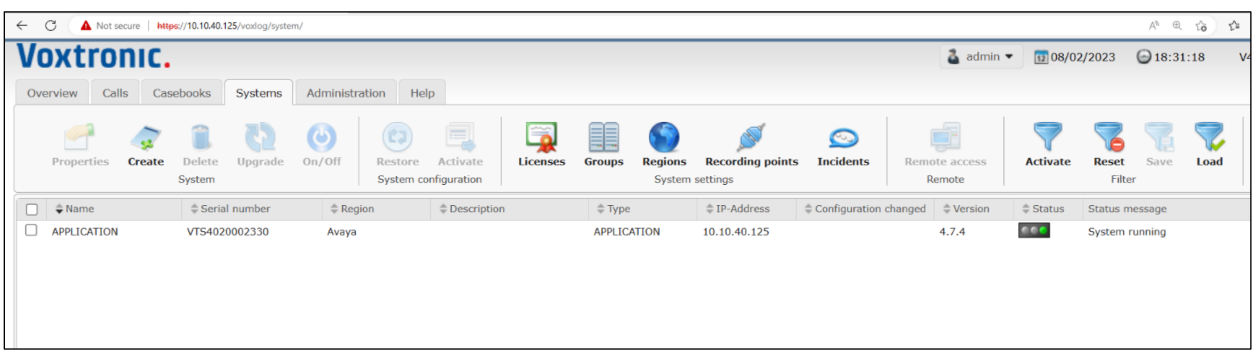


9. Configure Voxtronic Conex

The configuration of Conex can be carried out by opening a web GUI that can be used to configure the connection to AES and change the SIP settings accordingly.

Open a Web browser to **https://<ServerIP>/voxlog/login** and enter the appropriate credentials.

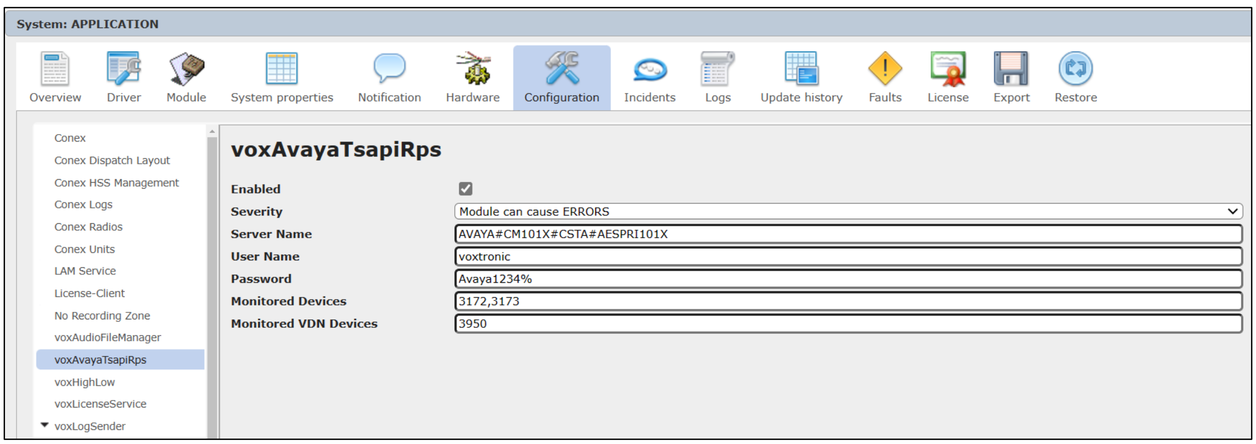
Navigate to the **Systems** Tab. In the main window, there should already be a system displayed that was setup during the initial installation and configuration. Double-click on this system or mark this system and click the action Properties to change the configuration of this system.



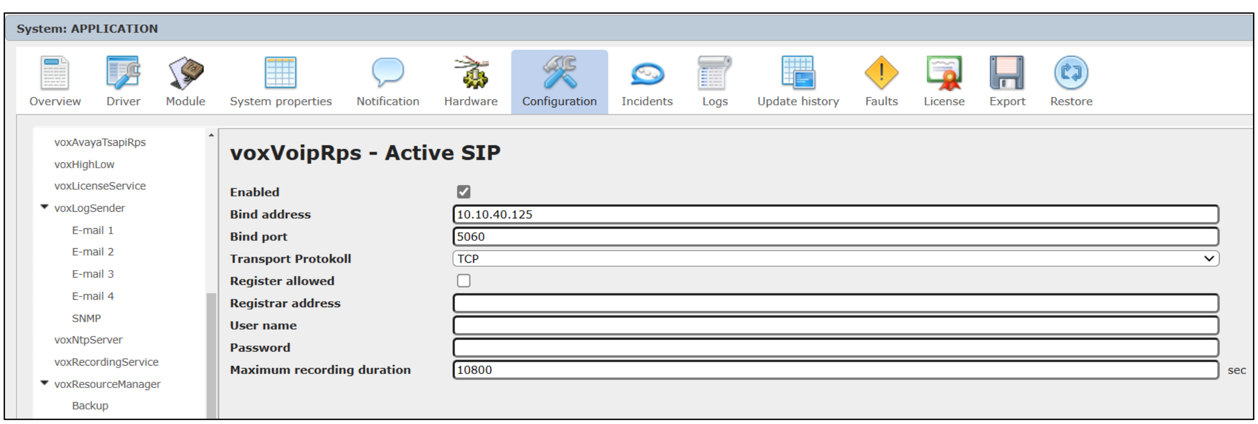
Click Configuration on the upper menu to see and change the configuration for this system. The menu on the left side shows all installed modules.

Note: An Avaya TSAPI client must be installed on the Conex server. This client contains the IP address of the AES and the port to connect. This TSAPI client was installed during the initial setup and installation of the Conex server and is outside the scope of these Application Notes.

The connection to AES is configured by selecting the module **voxAvayaTsapiRps** in the left window. This module provides all metadata like call states, numbers for recorded calls. Configure the interface to the Avaya TSAPI server using the settings **Server Name**, **User Name** and **Password**. These settings must match the configuration from Application Enablement Services. Configure the endpoints to be recorded using the setting **Monitored Devices**. Several devices can be added using a **,** as separator. For more details, hover the mouse over this setting. Configure the VDN numbers to be recorded using the setting **Monitored VDN Devices**. Several devices can be added using a **,** as separator. For more details, hover the mouse over this setting.



The connection to RTP is configured by selecting the module **voxVoipRps** in the left window. This module provides all audio for recorded calls. Configure the IP address and the port which should be listened and recorded using the settings **Bind address** and **Bind port**.



10. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Voxtronic solution.

10.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established.**

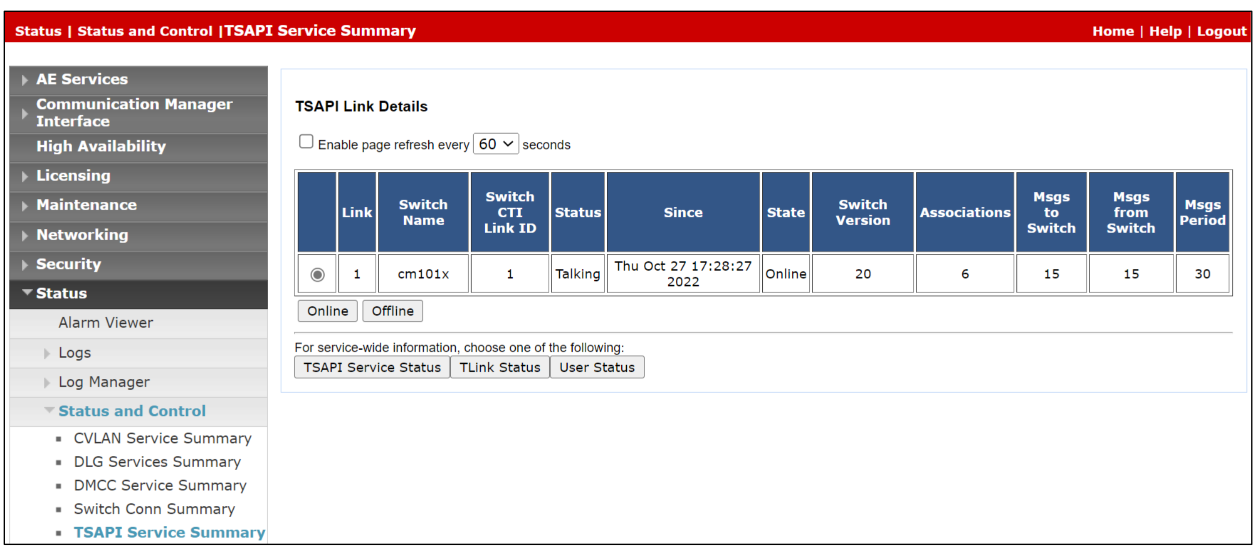
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version     Mnt   AE Services           Service      Msgs     Msgs
Link              Busy     Server             State        Sent     Rcvd

1        12       no       aespri101x         established  865      865
```

10.2. Verify TSAPI Link

This section will verify the TSAPI link between AES and Communication Manager and from Conex to AES.

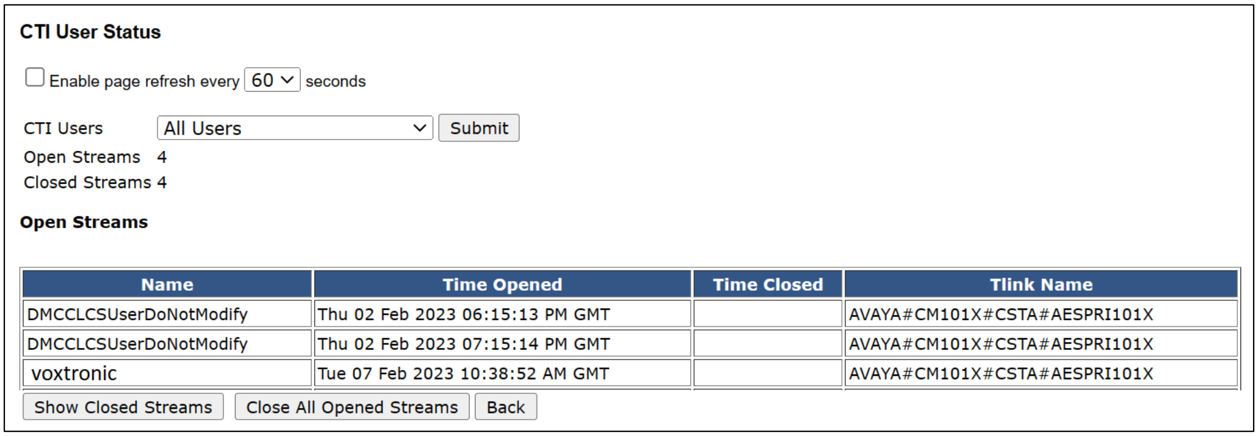
10.2.1. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



10.2.2. Verify TSAPI User

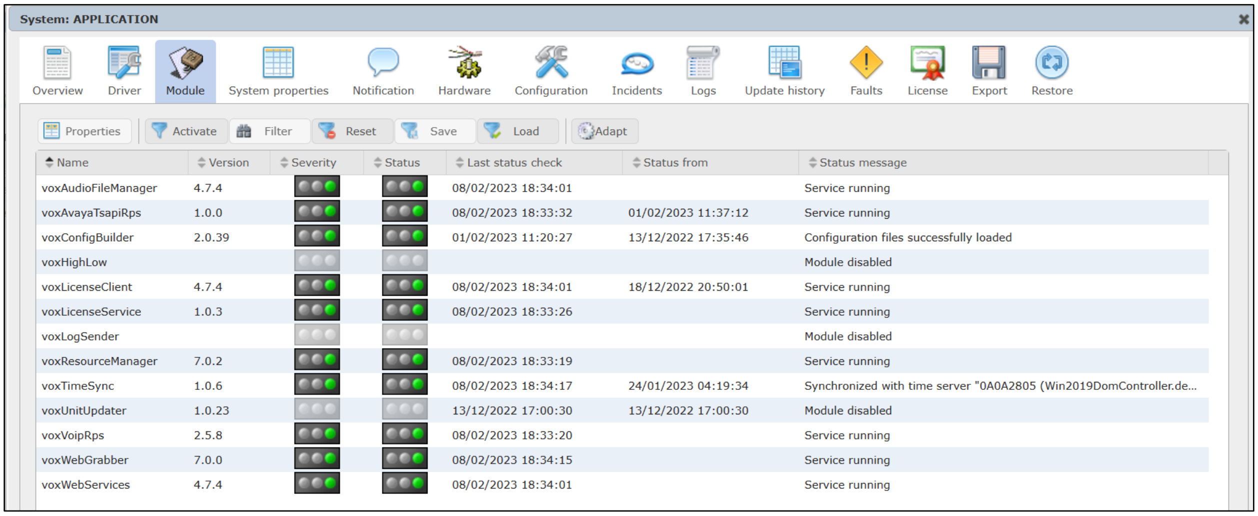
The following steps are carried out on AES to validate the communication between the TSAPI client and the AES by checking the user status. From the screen on the previous page, click on **User Status**. Verify the user setup in **Section 8.6** is connected as shown below.



10.3. Verify Conex services are running

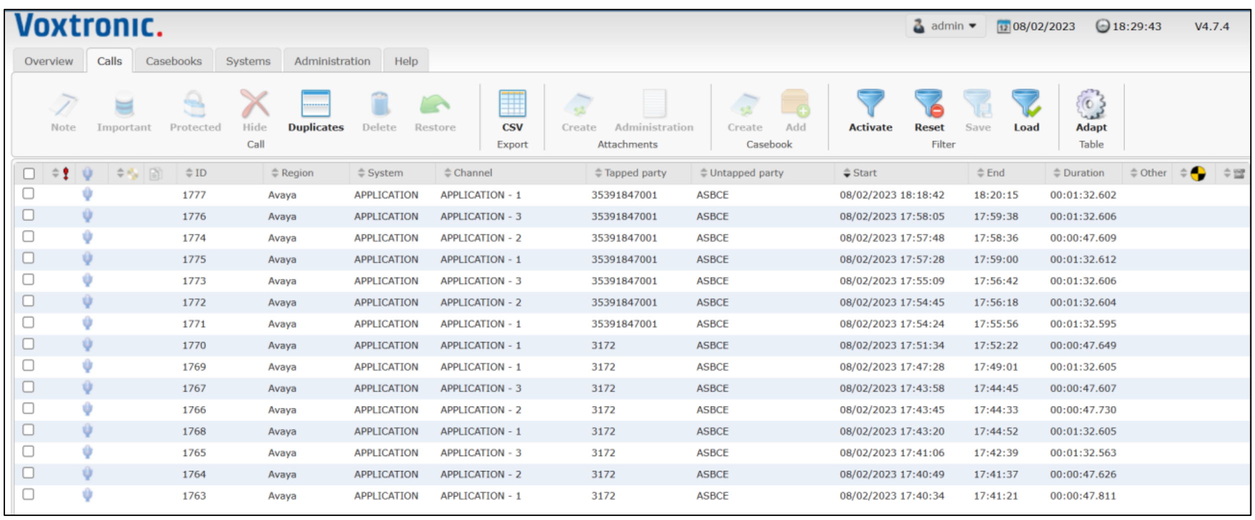
Log into Conex as shown below.

Navigate to the **Systems** tab, select the configured system, navigate to **Module**. This will show all the various modules running and information on how they are operating.

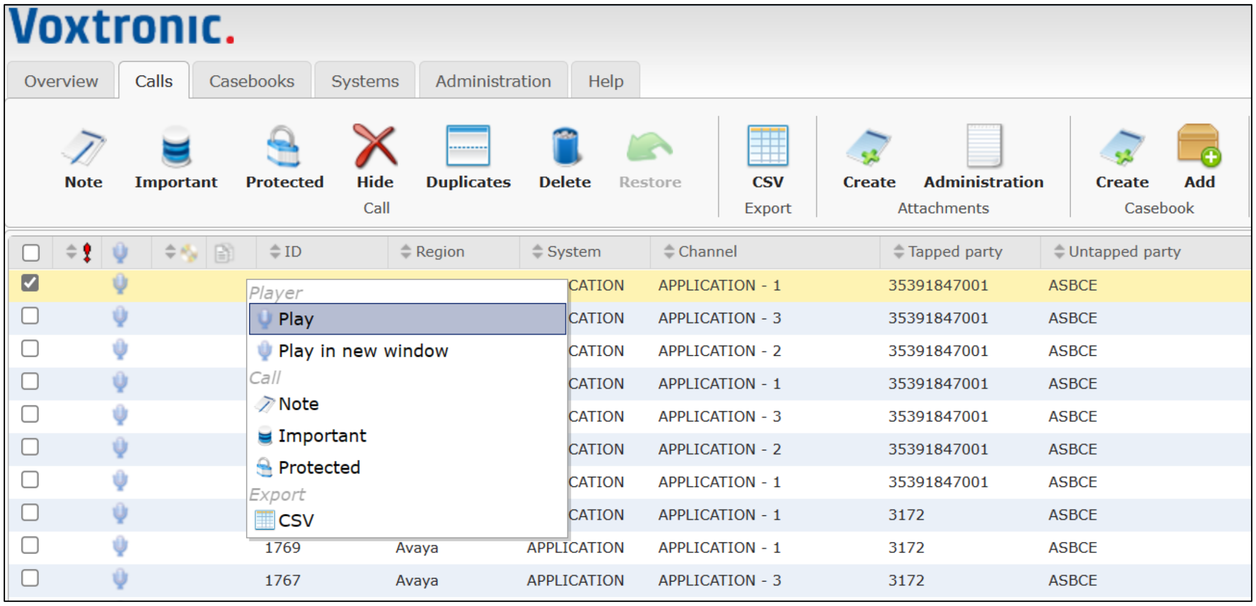


10.4. Verify Conex Capture and Playback

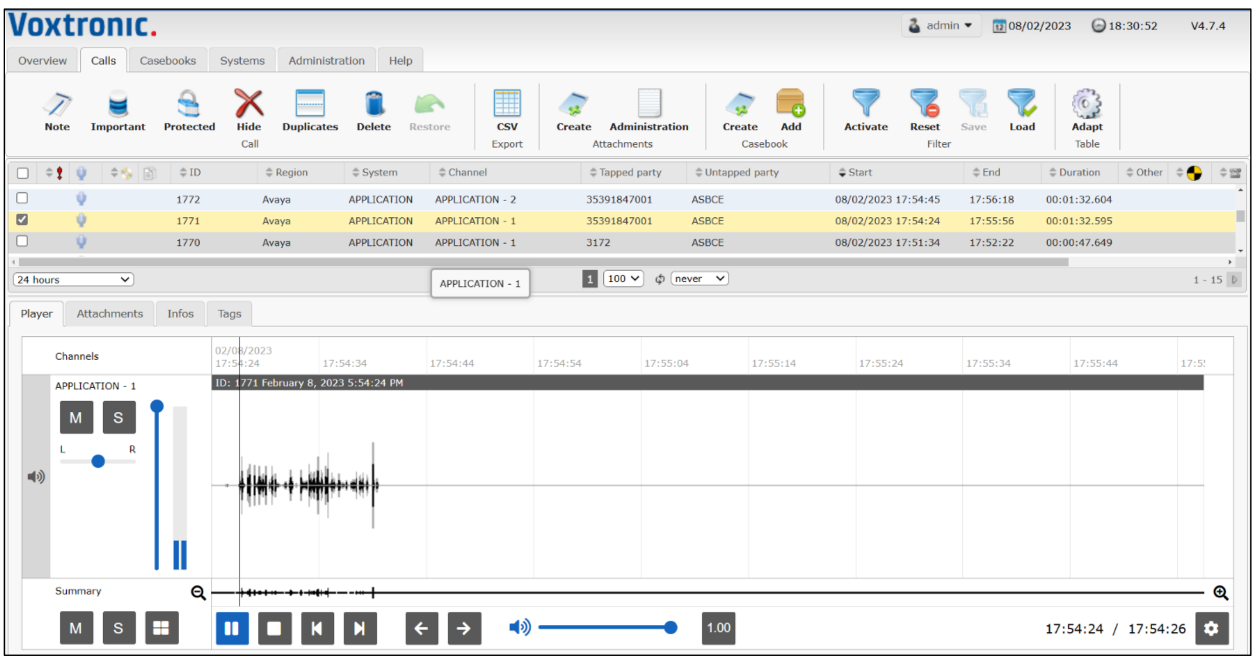
Navigate to the **Calls** tab. All the calls that were previously recorded should appear, something like that shown below.



Right-click on a call and select **Play**, as shown below. Or double-click on a call to play it back also.



The call should then appear and get played back as shown below.



11. Conclusion

These Application Notes describe the configuration steps required for Conex Release 4.9.0 from Voxtronic to successfully interoperate with Avaya Session Border Controller for Enterprise R10.1 using Avaya Aura® Application Enablement Services R10.1. All feature functionality and serviceability test cases were completed successfully, with any observations shown in **Section 2.2**.

12. Additional References

This section references the Avaya and Voxtronic product documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Session Border Controller for Enterprise.* Release 10.1, Issue 1.

[2] *Administering Avaya Aura® Communication Manager.* Release 10.1, Issue 1, December 2021.

[3] *Avaya Aura® Communication Manager Feature Description and Implementation*. Release 10.1, Issue 1

[4] *Administering Avaya Aura® Application Enablement Services.* Release 10.1.x, Issue 4, April 2022.

[5] *Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform.*

[6] *Application Notes for configuring Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 with MiaRec.*

Product documentation for Conex can be obtained from Voxtronic as follows:

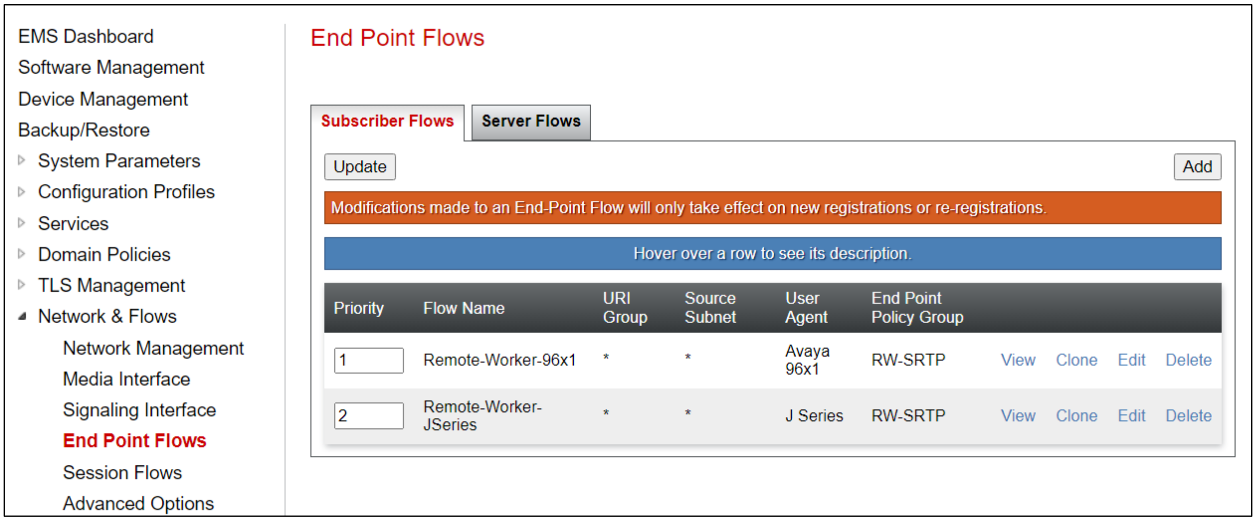
- Email: sales@voxtronic.com
- Website: http://www.voxtronic.com
- Phone: +43 1 8174846 0

Appendix A

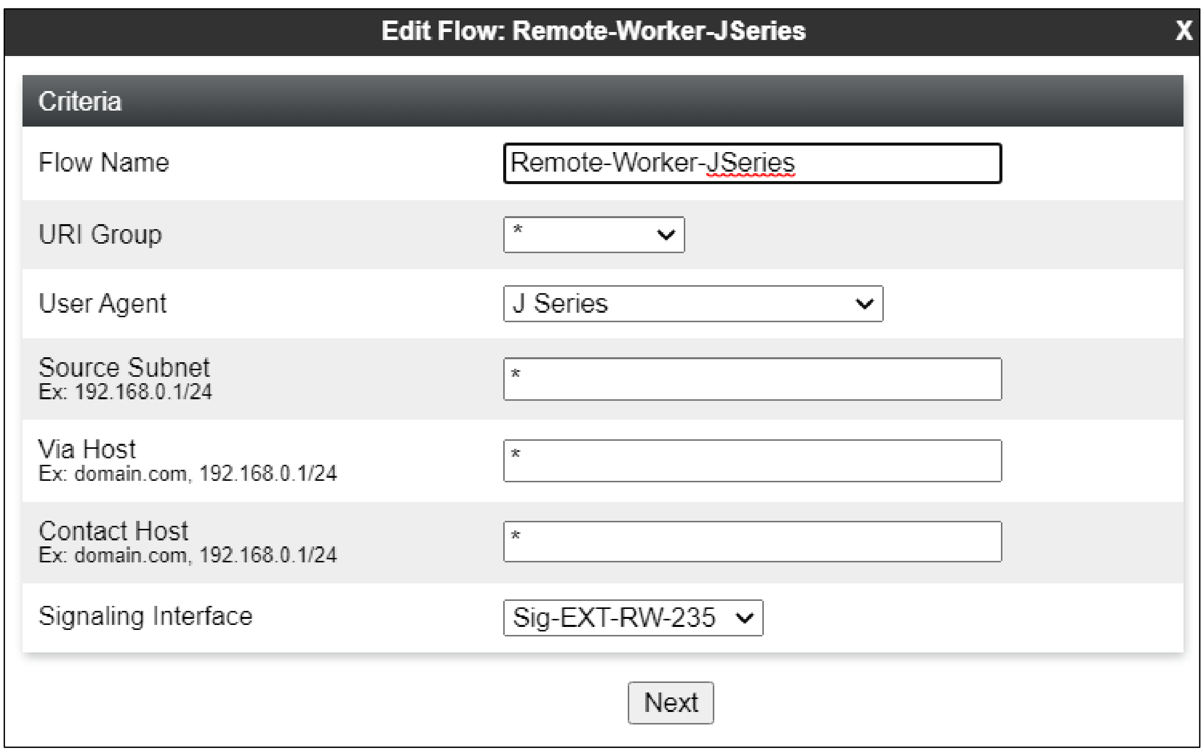
The following shows the setup of the Remote Workers on SBCE. User Agents are created for the various phone types that are used as Remote Workers.

The example below shows the J100 Series Phone.

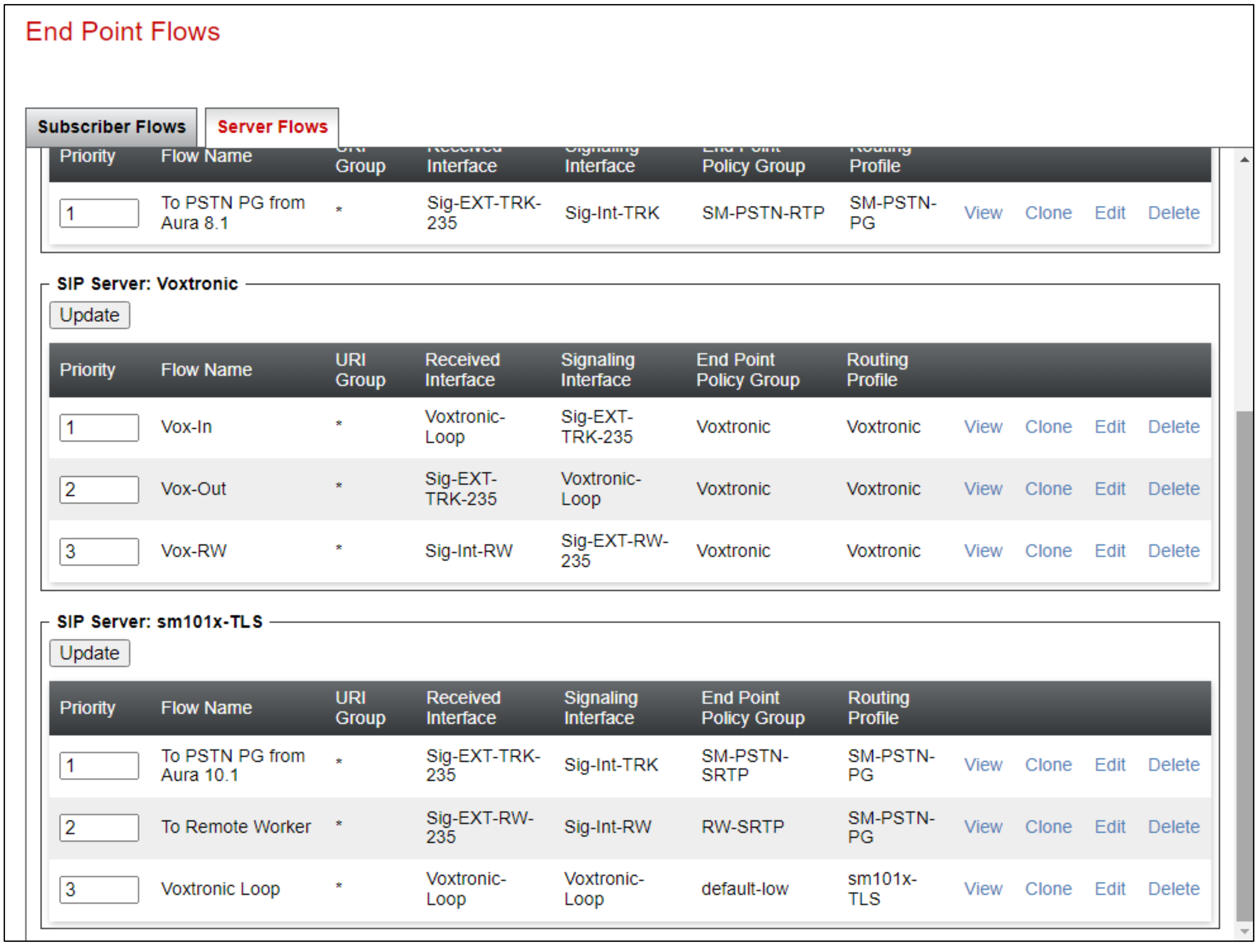
Subscriber Flows must be created for Remote Workers, these are created using the User Agent details configured on the previous page.



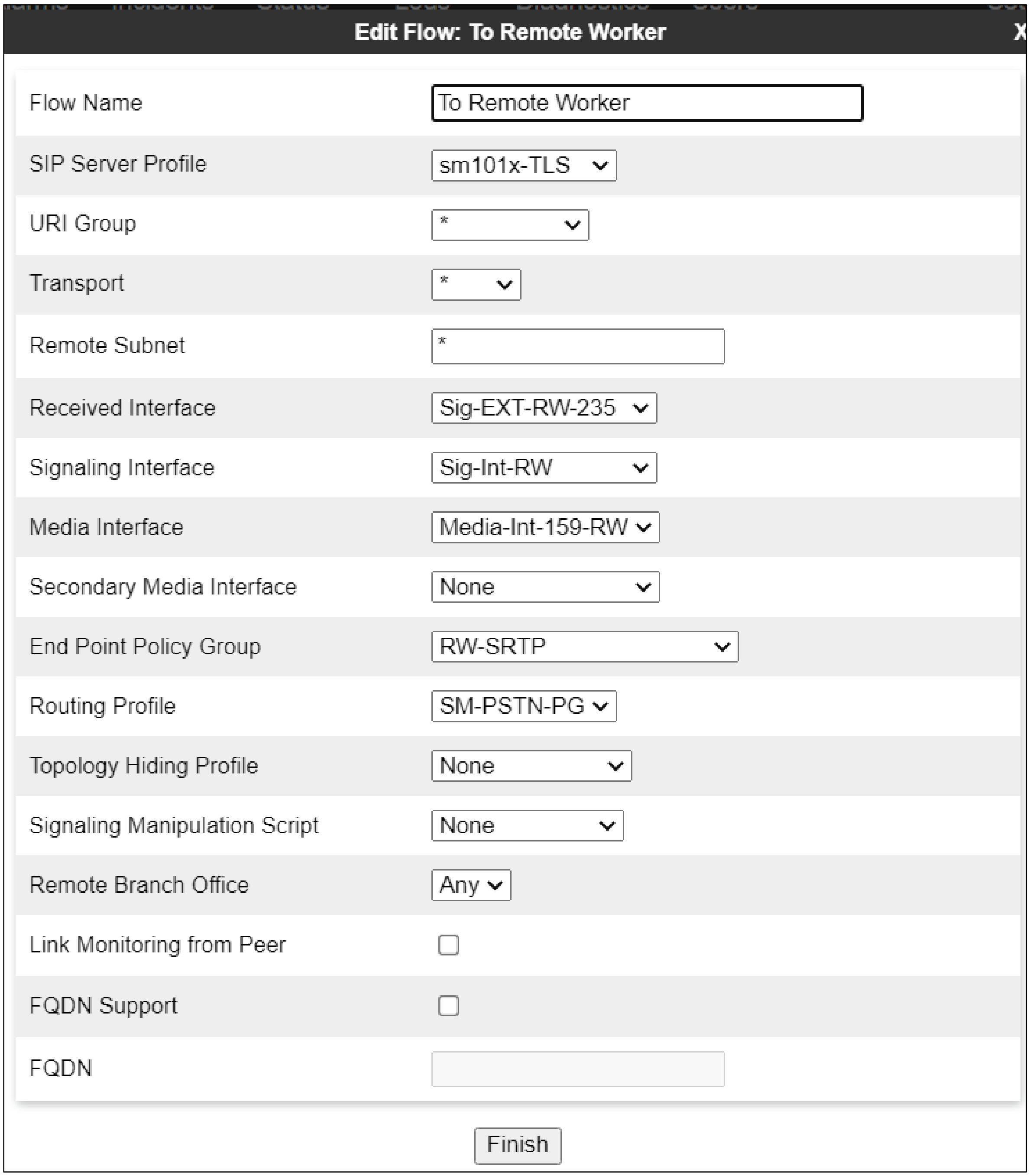
Below shows the J100 Series phone configured for the Subscriber Flow, note the **User Agent** and **Signaling Interfaces** are chosen based on what should be configured for this phone type.



A **Server Flow** must also be created for Remote Workers. The Flow called **To Remote Worker** was added prior to compliance testing to allow Remote Workers to register correctly.



Below shows the Server Flow for the Remote Workers. Note, the **SIP Server Profile** as well as the Interfaces that were previously configured are chosen. **SRTP** and **TLS** are used for the Remote Workers as per Avaya guidelines.



Edit Flow: To Remote Worker

Flow Name	To Remote Worker
SIP Server Profile	sm101x-TLS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-EXT-RW-235
Signaling Interface	Sig-Int-RW
Media Interface	Media-Int-159-RW
Secondary Media Interface	None
End Point Policy Group	RW-SRTP
Routing Profile	SM-PSTN-PG
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

Finish

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.