Avaya Solution & Interoperability Test Lab

Application Notes for FROX AG talkbase 22.02 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1– Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate FROX AG talkbase with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. FROX AG talkbase is an IP Attendant that integrates with Avaya Aura® Session Manager using both a SIP trunk connection and a SIP user connection.

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

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

1. Introduction

These Application Notes describe the configuration steps required to integrate FROX AG talkbase with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. FROX AG talkbase is an IP Attendant that integrates with Avaya Aura® Session Manager using both a SIP trunk connection and a SIP user connection.

FROX AG talkbase has a web-based attendant console, talkbase Attendant, which works with a number of telephony platforms including Communication Manager and Session Manager. It interfaces with Active Directory, Presence and Exchange servers. Compliance testing focused on telephony functionality only and Presence or Exchange server functionality was not covered. Interoperability with Avaya H.323 endpoints in the Avaya environment is not supported or tested.

2. General Test Approach and Test Results

The general test approach evaluated the ability of talkbase Attendant to place calls and to receive calls placed to the main number routed to an available attendant.

talkbase must reside on a domain with an Active Directory controller and it requires a separate server within that domain. talkbase relies on the user management of Active Directory. One user account is required per attendant, with one Avaya SIP user (assigned an extension and password). talkbase internally queues main number calls to attendants using WebRTC connections and attendant consoles answer these calls. talkbase will not call attendants directly so they will not receive calls made to their number.

Because talkbase creates a self-signed certificate and installs it, both the clients and the talkbase server must be on the same domain as the Active Directory controller otherwise there may be an issue with the trust of the certificates issued.

A SIP user was created for each talkbase Attendant user. talkbase server registers the user to Session Manager when talkbase Attendant logs in. Please note that Application Sequences must not be defined on these users. A dialplan was added to route calls to talkbase Attendant. This would typically be the “main number” of the company and calls to that number would be answered by one of the attendants.

Calls were placed to the “main number” which is configured on Communication Manager to route across the SIP trunk to the talkbase server. Any calls then made to the main number were routed to talkbase and were answered by talkbase Attendant. Calls cannot be made to that SIP user directly but only to the main number. The SIP user was configured without any Application Sequences.

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 talkbase did not include use of any specific encryption features to Session Manager as requested by FROX AG. The SIP trunk between talkbase Server and Session Manager was configured using TCP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The testing for talkbase Attendant focused on the following functionality:

- login/logout attendants.
- make/receive basic calls.
- make/receive PSTN calls.
- hold/transfer/forward calls.

The serviceability testing focused on verifying the ability of the talkbase solution to recover from network outage of the talkbase server, talkbase Attendant, and Session Manager. Recovery from talkbase server reboot was also verified.

2.2. Test Results

All test cases were executed and verified. All test cases passed successfully. The following observations were noted during interoperability testing.

- G.711MU and G.711A codecs were verified during testing. Other codecs can be configured through talkbase and their dialogic licensing, but were not tested.
- Environments using H.323 endpoints are not supported due to issues with one way audio during calls with talkbase Attendant. Interoperability with H.323 endpoints in the Avaya environment are not supported by talkbase.
- Setting call forwarding from talkbase Attendant is not supported.
- The caller display of an incoming PSTN call made to an Avaya SIP endpoint that was blind transferred to talkbase Attendant did not show the PSTN number but the (transferring) Avaya SIP endpoint number. This is a known problem with talkbase and may be fixed in a future release.
- Since SIP users are administered without application sequences, features requiring feature access codes activation are not supported.

2.3. Support

Technical support for Frox AG talkbase can be found as follows.

- **Phone:** +41 55 254 12 54/89
- **Email:** info@talkbase.com
- **Web:** https://talkbase.com/en/

3. Reference Configuration

Figure 1 shows the configuration used during compliance testing. The talkbase server is placed on the Avaya telephony LAN. Session Manager provides the talkbase SIP connection to Communication Manager. talkbase Attendant is capable of logging into an Avaya SIP endpoint and receiving calls via a web page on a client PC.

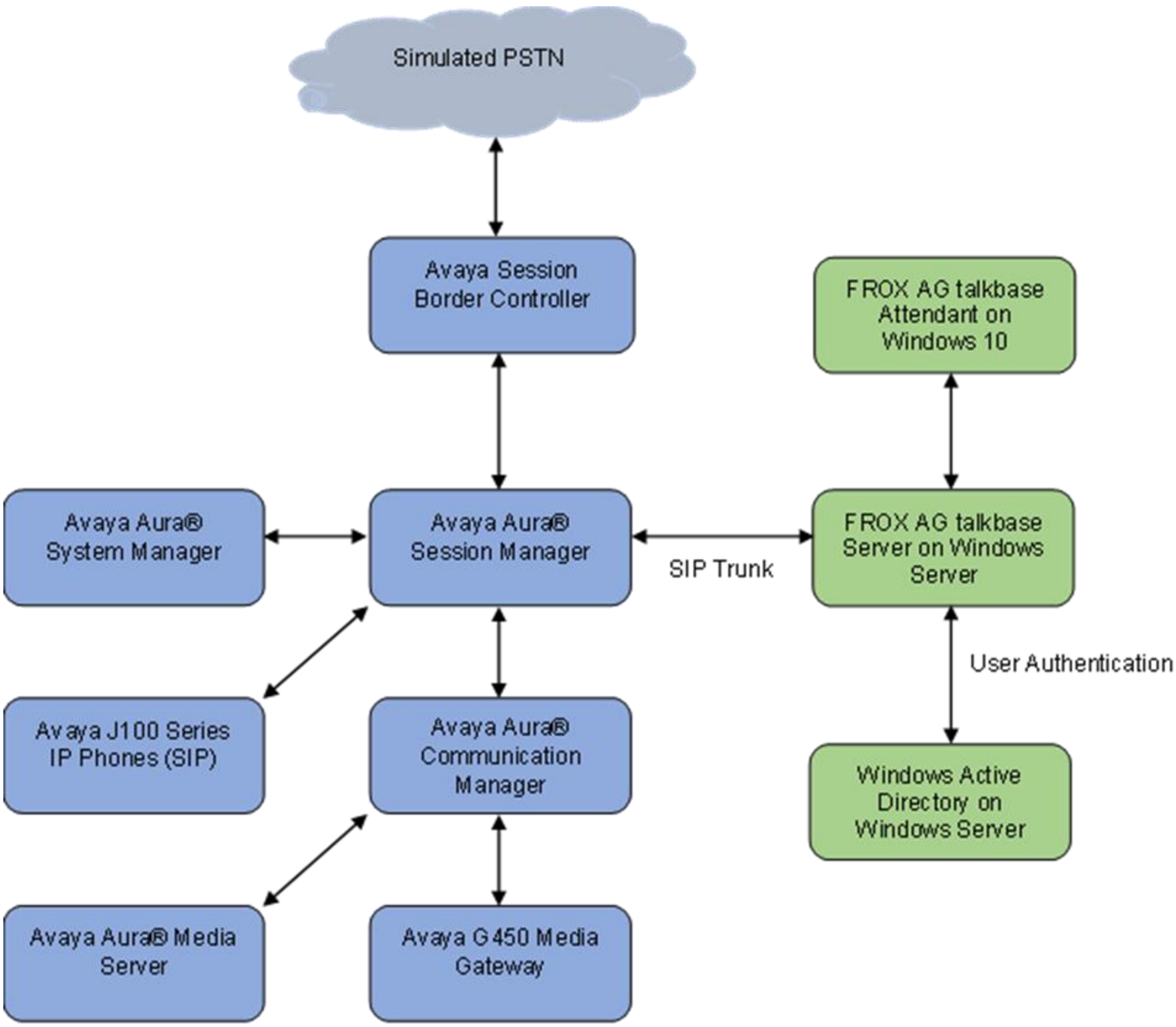


Figure 1: Network Solution of FROX AG talkbase and Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

The following equipment and software versions are used for the sample configuration:

Equipment / Software	Release / Version
Avaya Aura® System Manager running on Virtual Machine	10.1.0.2 Service Pack 2 10.1.0.2.0715160
Avaya Aura® Session Manager running on Virtual Machine	10.1.0.2 Service Pack 10.1.0.02.1010215
Avaya Aura® Communication Manager running on Virtual Machine	10.1.0.2-SP2 01.0.974.0-27607
Avaya Session Border Controller for Enterprise running on Virtual Machine	10.1.1.0-35-21872
Avaya Aura® Media Server running on Virtual Machine	10.1.0.101
Avaya J139/J179/J189 SIP Deskphone	4.0.13.0.6
Avaya G450 Media Gateway	42.7.0
FROX AG talkbase server running on Windows Server 2019	22.02-4
talkbase Attendant on Windows 10 PC	22.02-4 on Chrome 106.0.5249.119 (Official Build) (64-bit)

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are 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 10**. The procedures include the following areas:

- Verify System Parameters Customer Options
- Verify System Features
- Configure SIP Trunk
- Administer Call Routing

Note: The configuration of the simulated PSTN is outside the scope of these Application Notes.

5.1. 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 the **Maximum Administered SIP Trunks** have sufficient capacity. Each call uses a minimum of one SIP trunk.

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

IP PORT CAPACITIES                                            USED
                 Maximum Administered H.323 Trunks: 12000      0
       Maximum Concurrently Registered IP Stations:  2400      4
         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:    150    21
                   Maximum Administered SIP Trunks: 12000     20
  Max Administered Ad-hoc Video Conferencing Ports: 12000      0
   Max Number of DS1 Boards with Echo Cancellation: 688    0
```

5.2. Verify System Features

For compliance testing, **Trunk-to Trunk Transfer** is 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 10** 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): 8
                       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: attendant
    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
```

5.3. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of Communication Manager (**procr)** and Session Manager (**sm10**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to see node names.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
aes10               10.64.110.247
aes811              10.64.110.209
ams10               10.64.110.214
aura_cms18          10.64.110.20
cms19               10.64.110.225
default             0.0.0.0
procr               10.64.110.213
procr6              ::
remotecms191        10.64.110.226
sm10                10.64.110.212




( 10 of 10   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

In the **IP Network Region** form, the **Authoritative Domain** field is that configured on Session Manager. In this configuration, the domain name is **avaya.com**. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the G450 Media Gateway or Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set is 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       NR Group: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main                  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? 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 to talkbase. **IP codec set 1** is specified in **IP Network Region 1** previously discussed. Multiple codecs may be specified in the **IP Codec Set** form in order of preference. The example below includes **G.711A** (a-law) and **G.711MU** (mu-law) which are both supported by talkbase.

Media Encryption is used on the Avaya sets where possible. **None** is also present to facilitate any extension not capable of handling encryption. Calls to talkbase Attendant did not use Media Encryption.

```
display ip-codec-set 1                                          Page   1 of   2
                          IP MEDIA PARAMETERS
    Codec Set: 1

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

     Media Encryption                    Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 10-srtp-aescm256-hmac80
 3: none
 4:
 5:
```

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

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method. **tls** (Transport Layer Security) should be used for DevConnect testing.
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- 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 (**sm10**).
- Ensure that the TLS port value of **5070** 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 (e.g., **1**) configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field is set to the domain name specified in the IP Network Region (e.g., **avaya.com**).
- 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 also set to **y** to allow the RTP to setup directly between talkbase and the caller.
- The default values for the other fields may be used.

Note: These are settings for compliance testing, however, this trunk may be setup differently on each customer site depending on the customer's requirements for SIP routing.

```
change signaling-group 12                                       Page   1 of   3
                                SIGNALING GROUP

Group Number: 12             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sm10
 Near-end Listen Port: 5070                Far-end Listen Port: 5070
                                        Far-end Network Region: 1

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

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from talkbase. 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 12                                             Page   1 of  5
                               TRUNK GROUP

Group Number: 12                  Group Type: sip           CDR Reports: y
  Group Name: talkbase                   COR: 1        TN: 1        TAC: 112
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 12
                                                    Number of Members: 10
```

On **Page 3** of the trunk-group form the **Numbering Format** is set to **private**. The rest of the fields are set as shown.

```
change trunk-group 12                                           Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



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


                                Modify Tandem Calling Number: no
               Send UCID? n



 Show ANSWERED BY on Display? y

 DSN Term? n
```

Settings on **Page 5** are as follows.

```
change trunk-group 12                                           Page   5 of   5
                              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
     Resend Display UPDATE Once on Receipt of 481 Response? 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
```

5.4. Administer Call Routing

A range of numbers is assigned to the Attendant as main numbers where Communication Manager users can dial to or the PSTN can call. For compliance testing, the range of numbers made available is 70110 to 70119. 70115 and 70116 are used for talkbase main numbers during testing. The configuration must route calls 7011x to the SIP trunk created in **Section 5.3** and to do that a route pattern must be created before the routing can be set. This route pattern references the SIP trunk and the routing then references the route pattern.

5.4.1. Configure Route Pattern

Use the **change route-pattern *12*** command to add the SIP trunk group to the route pattern that Automatic Alternate Routing configured in **Section 5.4.3** selects. In this configuration, Route Pattern Number **12** is used to route calls to trunk group **12** configured in **Section 5.3**. The **Numbering Format** is set to **lev0-pvt**.

```
change route-pattern 12                                           Page   1 of   3
                    Pattern Number: 12     Pattern Name: Talkbase
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 12   0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               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
```

5.4.2. Configure Uniform Dialplan

For compliance testing, all calls to talkbase Attendant are calls that began with **7011** and these are to be sent across the SIP trunk to Session Manager and then to talkbase. To achieve this routing, Automatic Alternate Routing (AAR) is used to route the calls. The dial plan and aar routing analysis configuration will allow this routing.

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below, calls to **7011x** will use Automatic Alternate Routing (AAR). No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

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

  Matching                          Insert                Node
  Pattern             Len Del       Digits        Net Conv Num
 7011                 5    0                      aar n
 7204                 5    0                      aar n
 7205                 5    0                      aar n
 76                   5    0                      aar n
                                                      n
                                                      n
                                                      n
```

5.4.3. Configure Automatic Alternate Routing

Use the **change aar analysis** command to further configure the routing. Calls to the Attendant are achieved by dialing **70115** or **70116** and are matched with the **Dialed String** entry shown below. Calls are sent to **Route Pattern 12**, configured in **Section 5.4.1**.

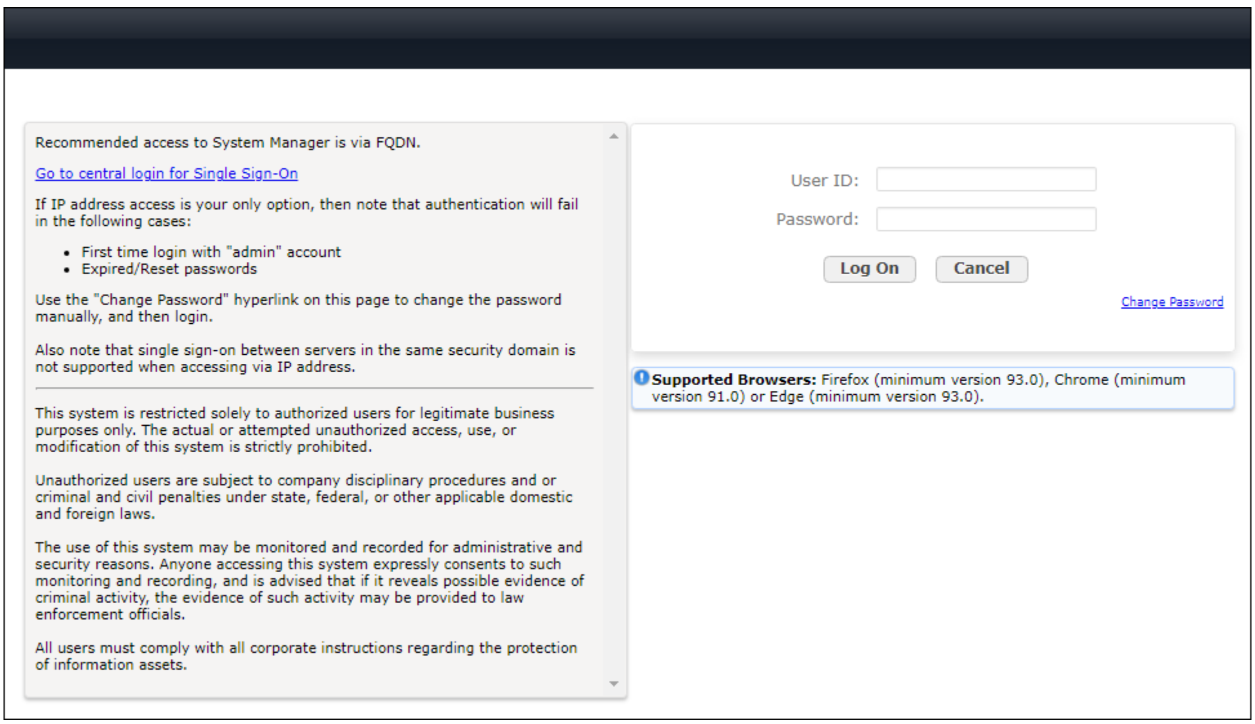
```
change aar analysis 7                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 0
    Dialed                  Total     Route     Call   Node  ANI
    String                 Min  Max  Pattern    Type   Num   Reqd
    70                      5    5      1        lev0          n
    7011                    5    5      12       lev0          n
    71                      5    5      1        aar           n
                                                               n
                                                               n
                                                               n
                                                               n
                                                               n
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure Communication Manager SIP Entity
- Configure Communication Manager Entity Link
- Configure talkbase SIP Entity
- Configure talkbase Entity Link
- Configure Routing Policy for talkbase
- Configure Dial Patterns
- Configure talkbase SIP User

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



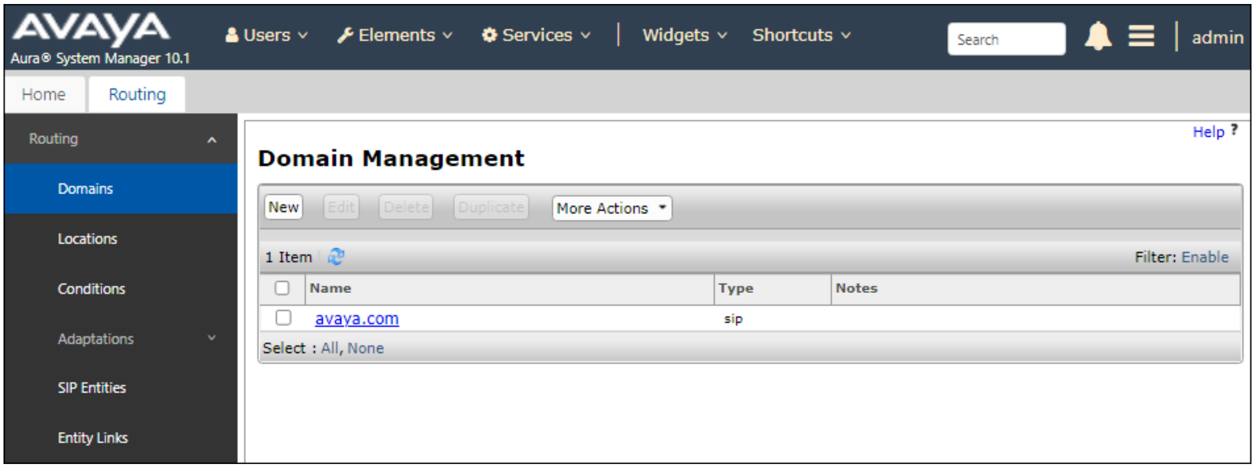
Once logged in navigate to **Elements** and click on **Routing** (not shown).

6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured. An overview of the domain and location that used in compliance testing is provided.

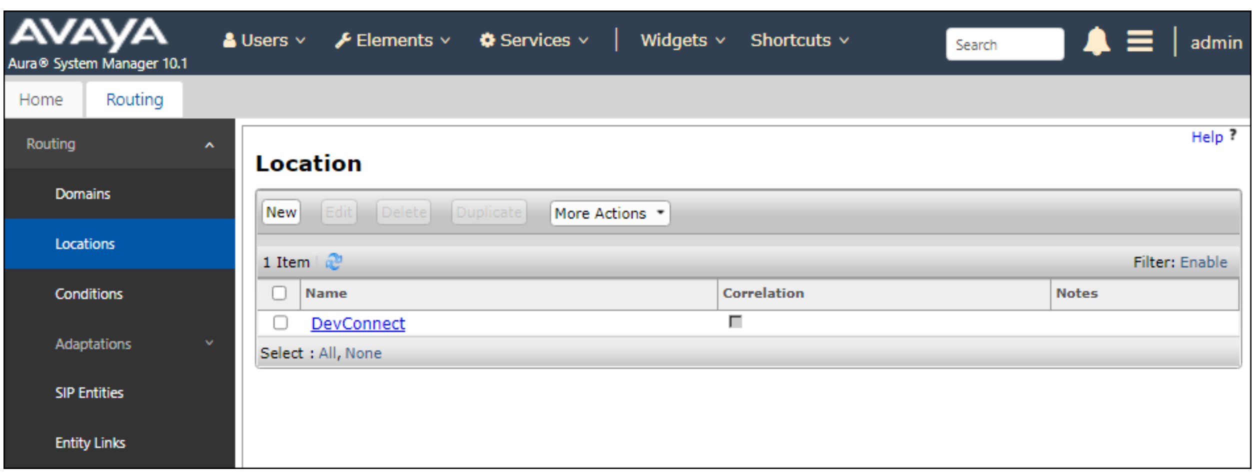
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain is **avaya.com** as shown below. If a domain is not already in place, click New to add a new domain.



6.1.2. Display the Location

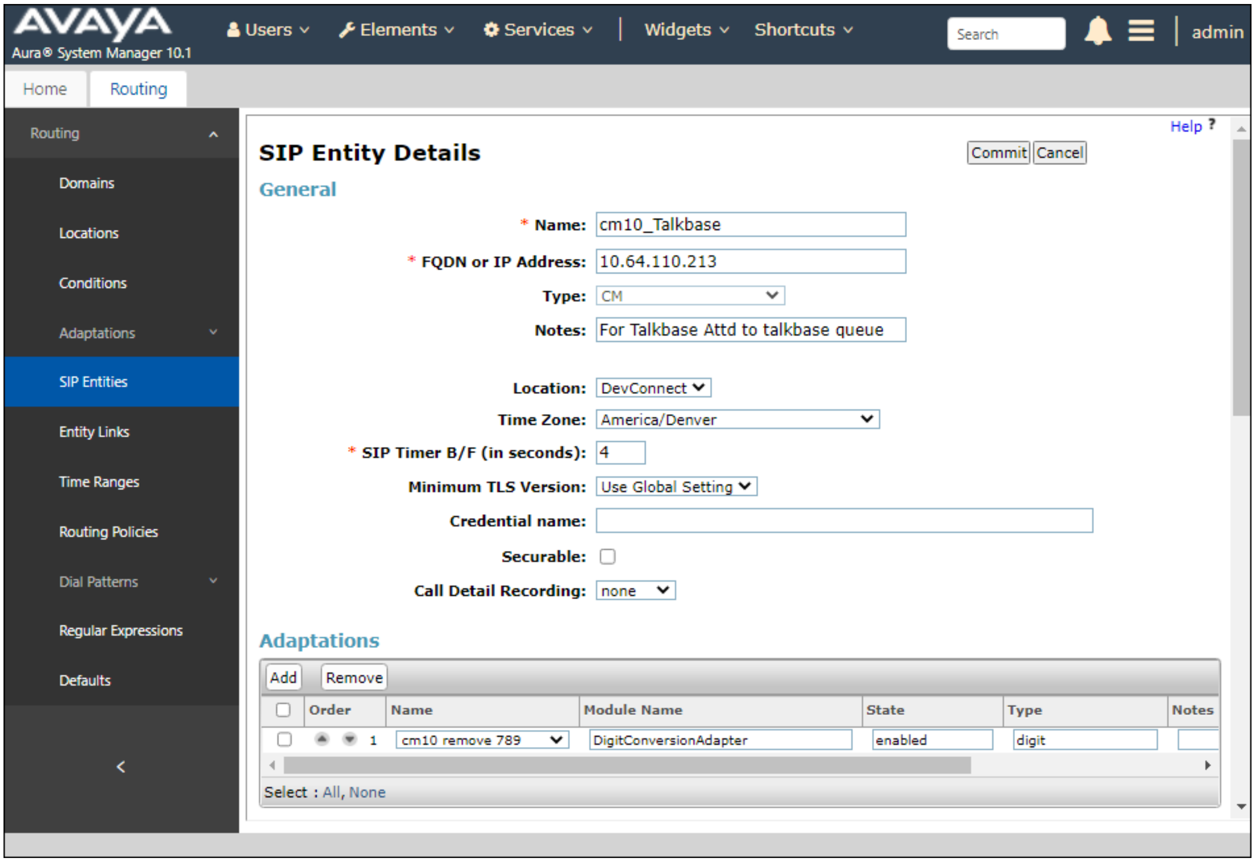
Select **Locations** from the left window. this will display the location configured on Session Manager. For compliance testing, this location is **DevConnect** as shown below. If a location is not already in place, click **New** to add a new location.



6.2. Configure Communication Manager SIP Entity

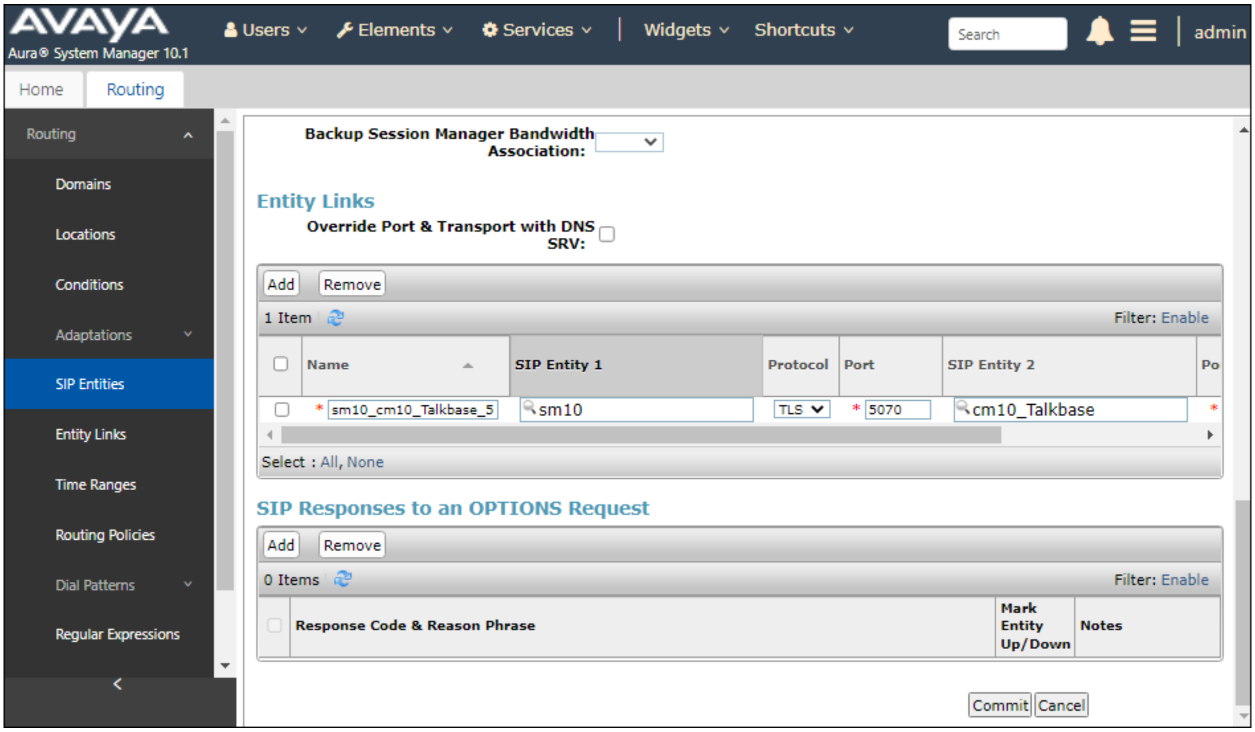
A SIP entity for Communication Manager should already be configured in the Avaya environment. SIP entity creation for Communication Manager is shown here for reference.

Click on **SIP Entities** in the left column and select **New** in the right window (not shown). Enter a suitable **Name** for the Communication Manager SIP Entity and the **IP Address** of Communication Manager. Select **CM** for **Type**. Enter the correct **Time Zone.** An adaptation may be used if attendants are required to forward calls to their assigned main number. Reference **[6]** for details. If needed, click the **Add** button and select the Adaptation created for talkbase from **Section 6.9.2**. In this case, the adaptation **cm10 remove 789** is used. Accept the default values for the remaining fields. Click **Commit**.



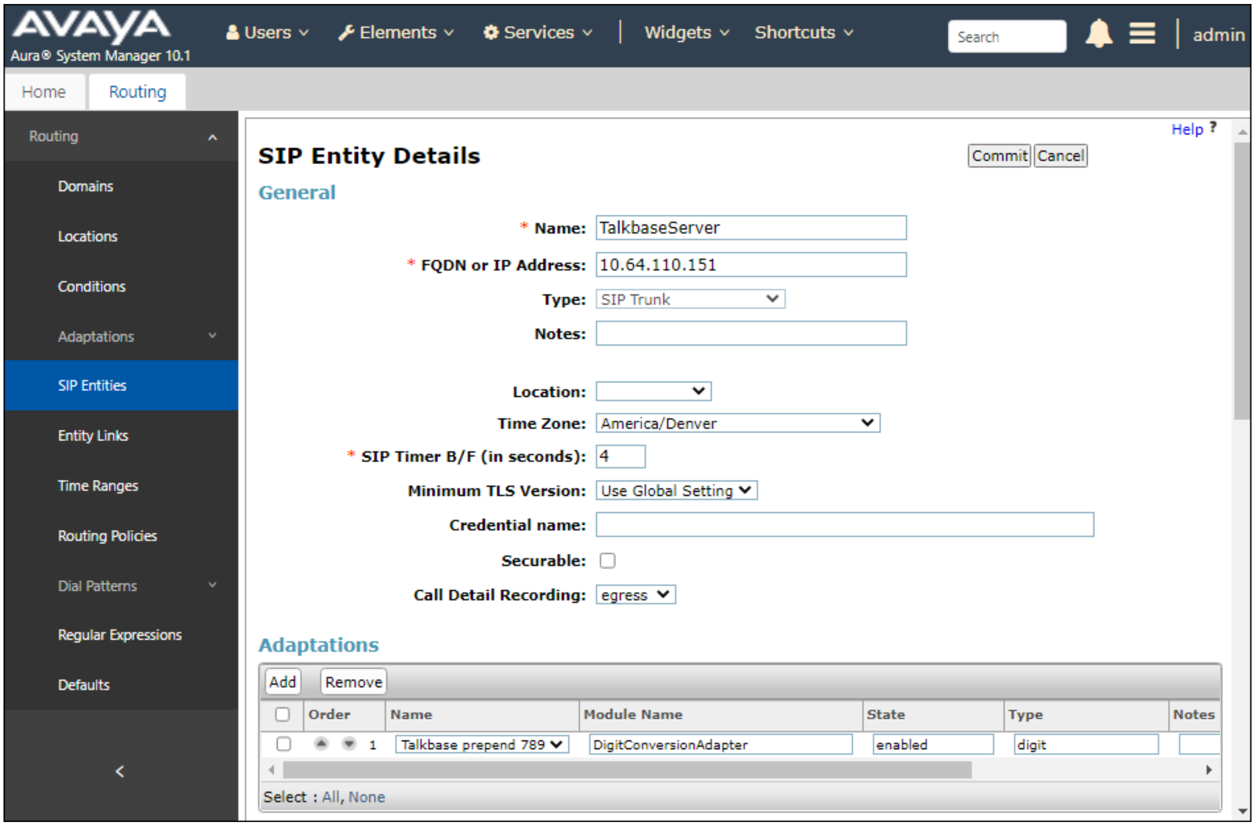
6.3. Configure Communication Manager SIP Entity Link

The Entity Link can be added from the Communication Manager SIP Entity page from **Section 6.2**. Scroll down to expose the **Entity Links** Section. Click on the **Add** button. Select the **Session Manager** SIP Entity (e.g., **sm10**) for **SIP Entity 1** and the newly created Communication Manager SIP Entity (e.g., **cm10_Talkbase**) for **SIP Entity 2**. Ensure that **TLS** is selected for the **Protocol** and that **Port 5070** to match the port values used in **Section 5.3**. Ensure **Trusted** is selected for **Connection** Policy. Click on **Commit** to save the new Entity Link.



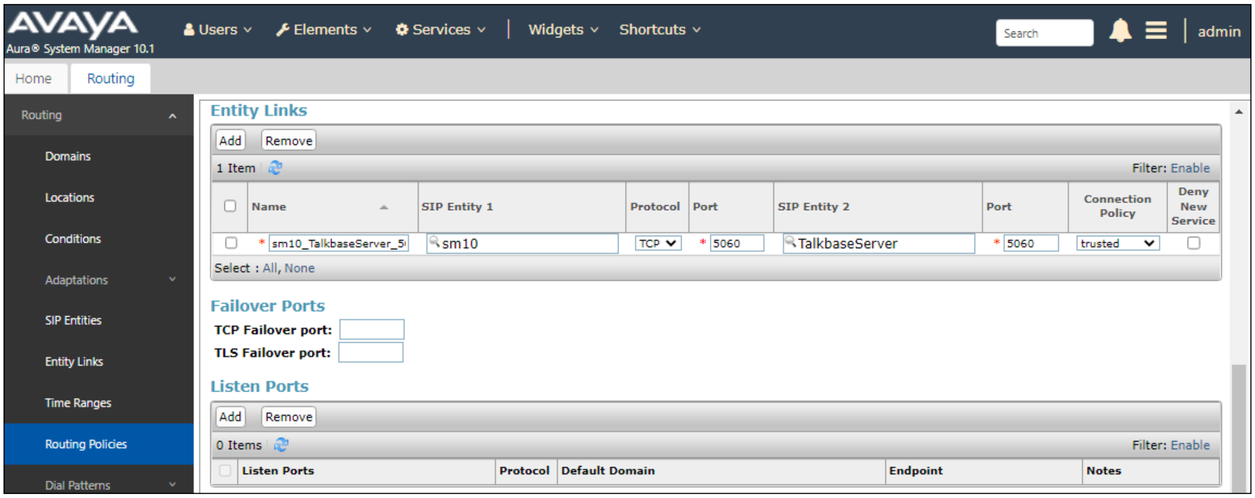
6.4. Configure talkbase SIP Entity

Click on **SIP Entities** in the left column and select **New** in the right window (not shown). Enter a suitable **Name** for the new talkbase SIP Entity and the **IP Address** of the talkbase server. Select **SIP Trunk** for **Type**. Enter the correct **Time Zone.** An adaptation can be used if attendants are required to forward calls to their assigned main number. Reference **[6]** for details. Click the **Add** button and select the Adaptation created for talkbase from **Section 6.9.1**. In this case, the adaptation **Talkbase prepend 789** is used. Accept the default values for the remaining fields. Click **Commit**.



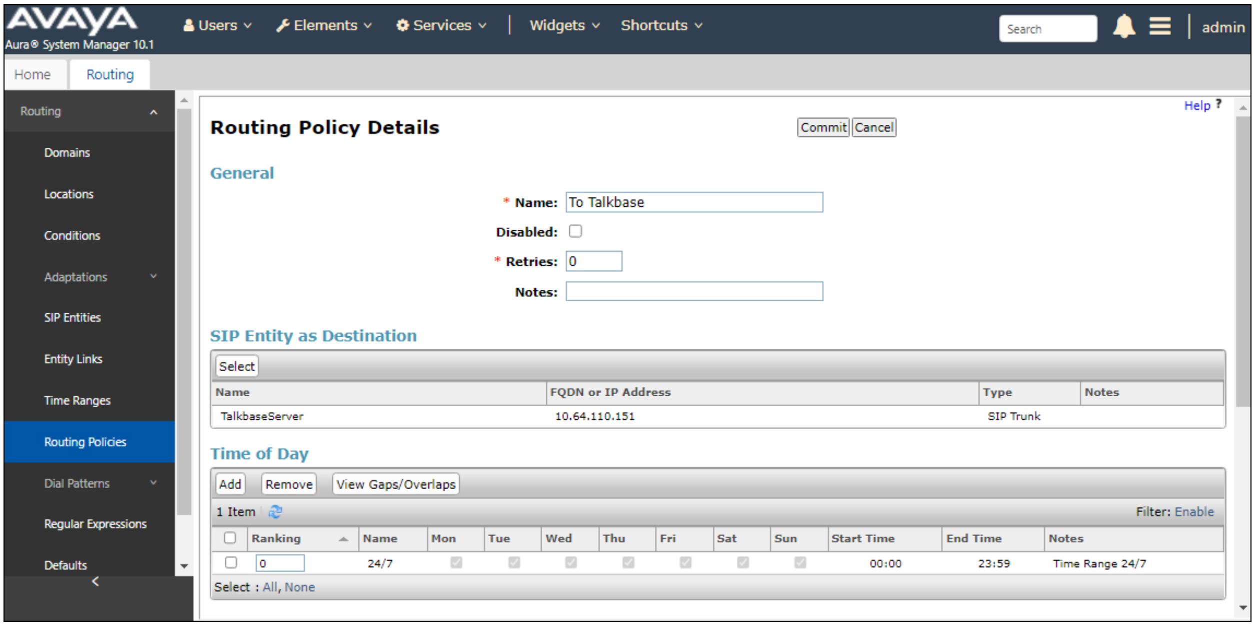
6.5. Configure talkbase SIP Entity Link

The Entity Link can be added from the talkbase SIP Entity page from **Section 6.4**. Scroll down to expose the **Entity Links** Section. Click on the **Add** button. Select the **Session Manager** SIP Entity (e.g., **sm10**) for **SIP Entity 1** and the newly created talkbase SIP Entity (e.g., **TalkbaseServer**) for **SIP Entity 2**. Ensure that **TCP** is selected for the **Protocol** and that **Port 5060** is used. Ensure **Trusted** is selected for **Connection** Policy. Click on **Commit** to save the new Entity Link.



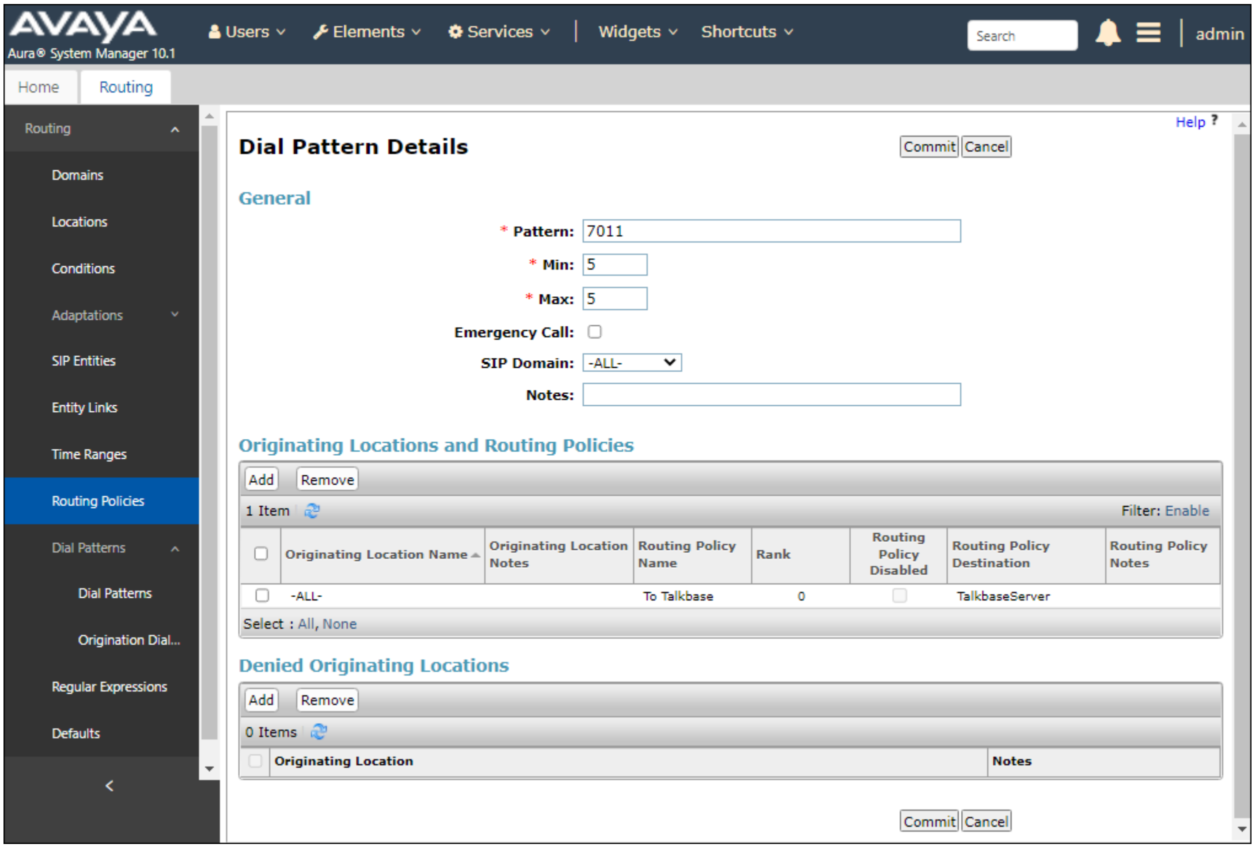
6.6. Configure Routing Policy for talkbase

Click on **Routing Policies** in the left window and select **New** in the main window.
Enter a suitable **Name** for the Routing Policy and click the **Select** button under **SIP Entity as Destination.** Select the SIP entity created in **Section 6.2** (e.g., **TalkbaseServer)** and click **Select**.
The selected destination is now shown. Click **Commit** to save the Routing Policy.



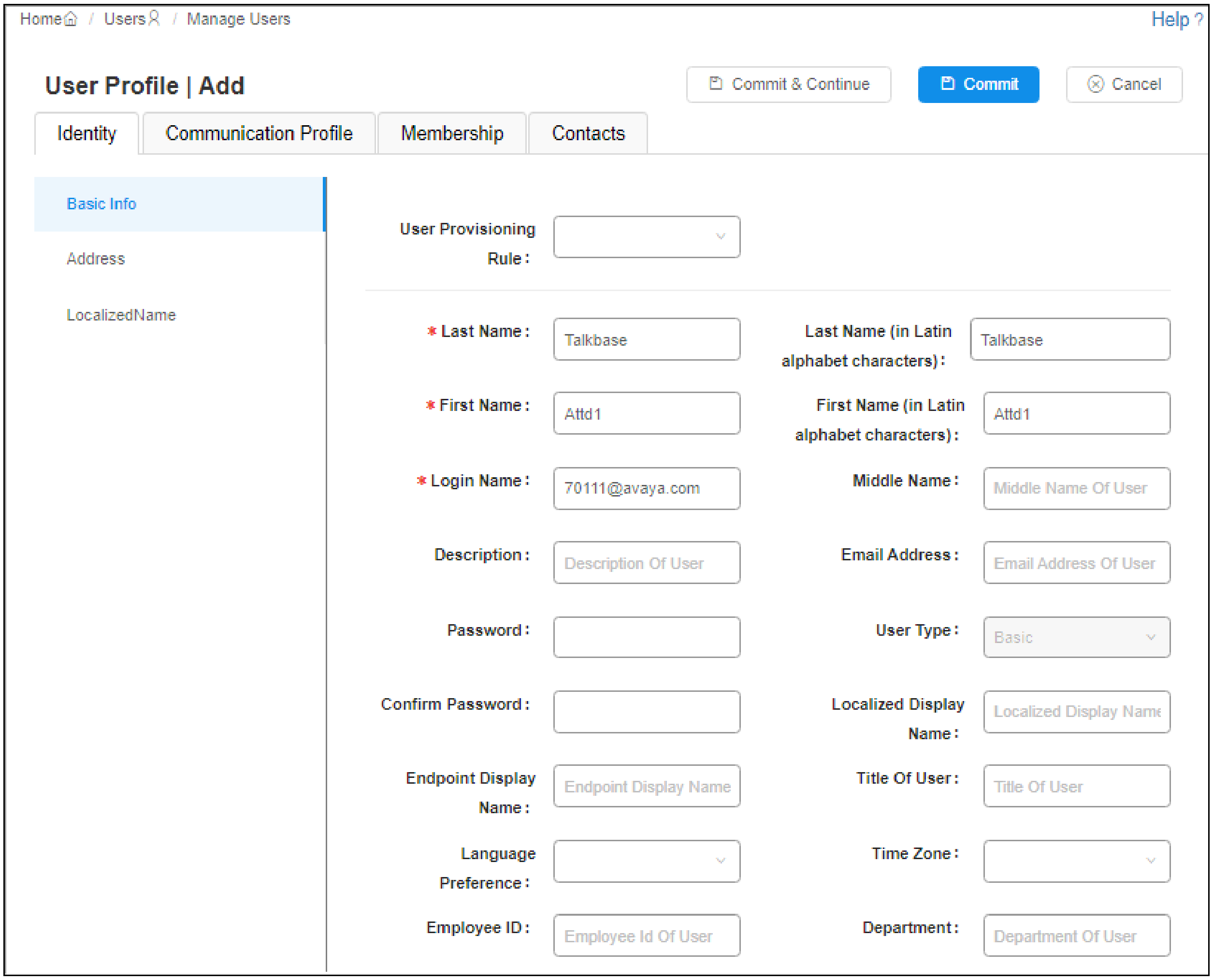
6.7. Configure talkbase Dial Patterns

A dial pattern must be created to route talkbase main numbers to the talkbase SIP entity. Select **Dial Patterns** in the left window and select **New** in the main window. Enter the required digits for **Pattern**, e.g., **7011**, and the appropriate **Min** and **Max** digits. Click on **Add** under **Originating Locations and Routing Policies** and select the appropriate **Originating Location Name** and the Routing Policy from **Section 6.6** (e.g., **To Talkbase**) for **Routing Policy Name**. Click the **Select** button. Click **Commit** to finish adding the Dial Pattern. The configuration below will route calls to extensions **7011x** to talkbase.

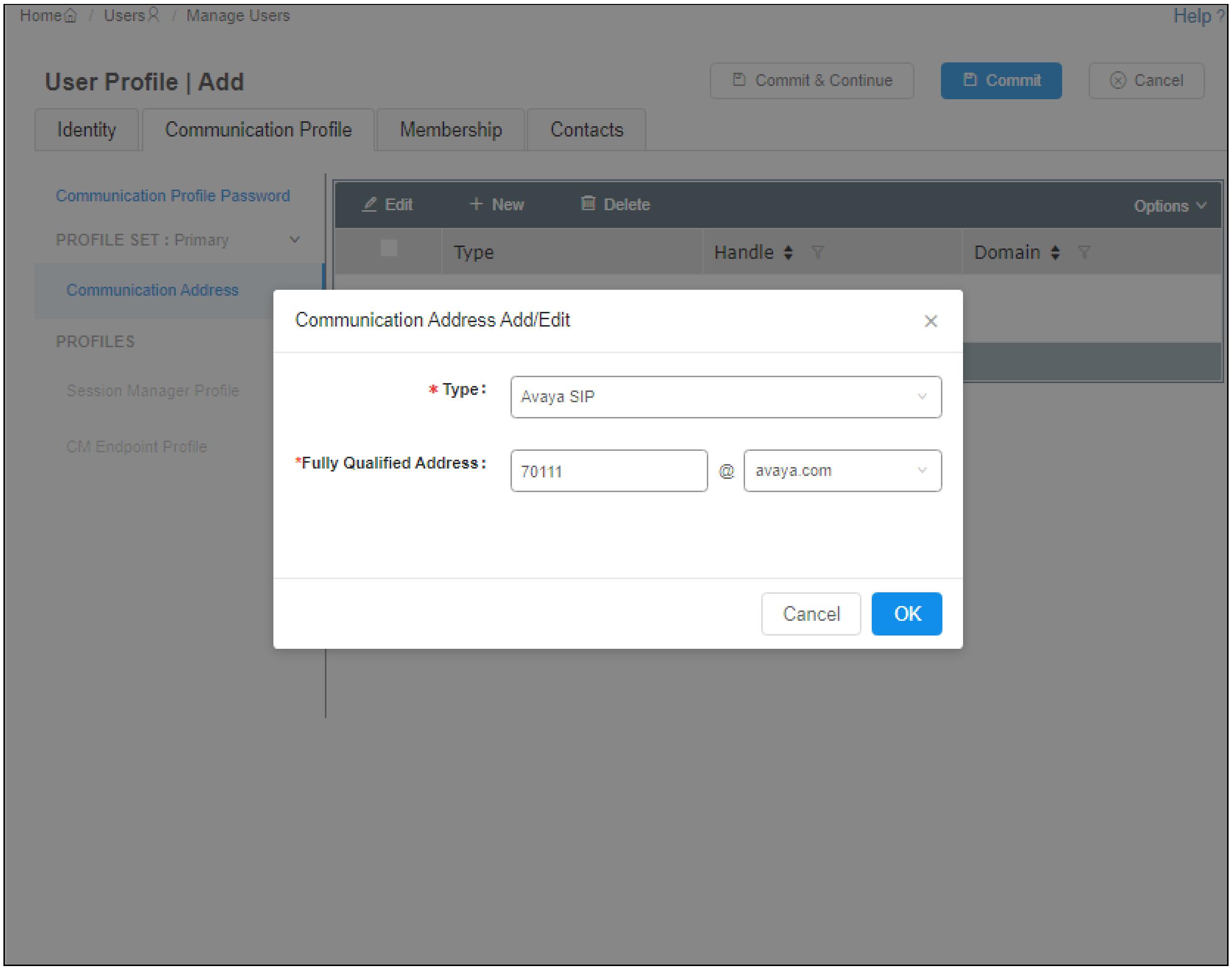


6.8. Configure talkbase SIP User

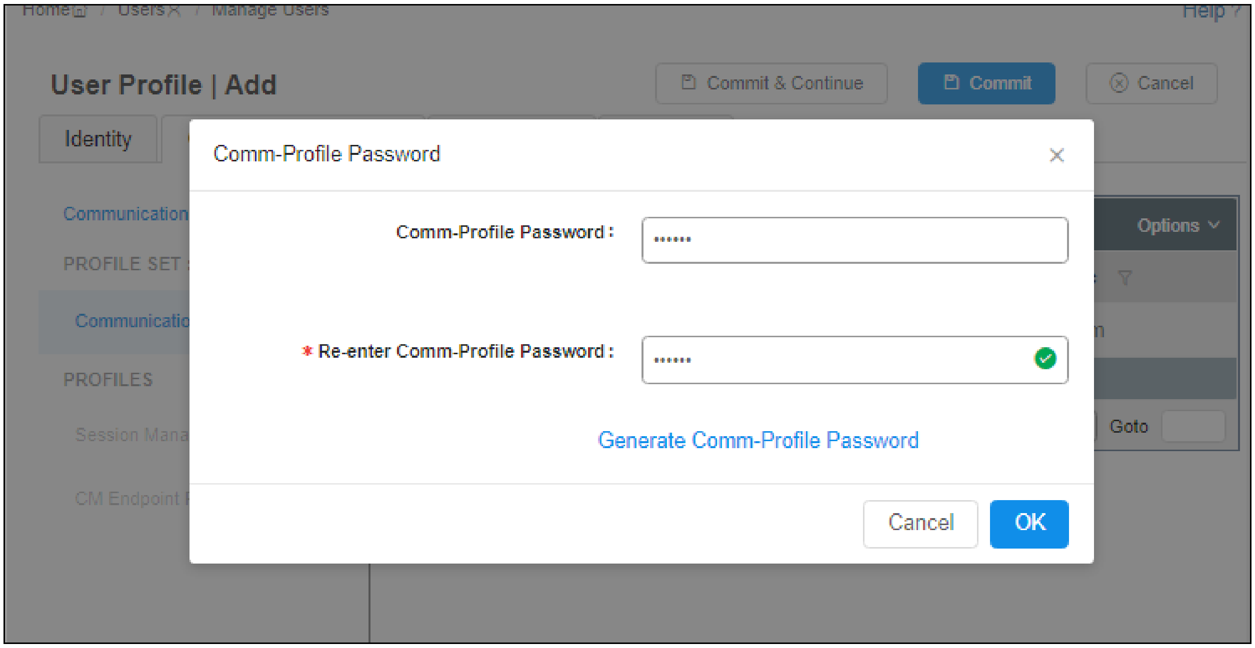
A SIP user must be configured for talkbase Attendant. In Session Manager, select **Users →User Management →Manage Users** to display the **User Management** screen (not shown). Click **+ New** to add a user. Under the **Identity** tab, enter an appropriate **Last Name** and **First Name**. Enter <extension>@<sip domain> of the user (e.g., **70111@avaya.com**).



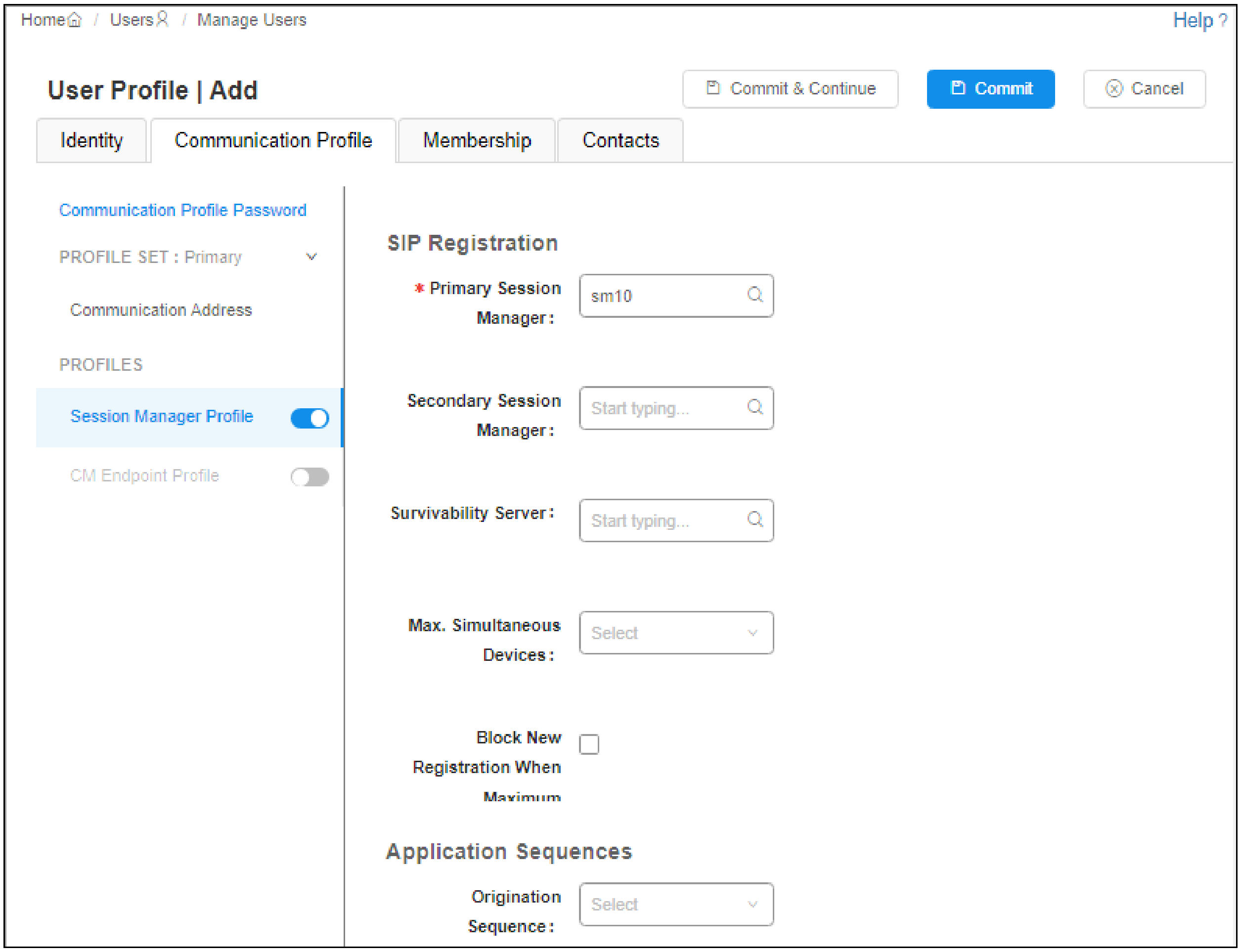
Select the **Communication Profile** tab. Select **Communication Address** in the left list and click **+ New**. Select **Avaya SIP** from the drop-down list for **Type**. Enter the extension number (e.g.,**70111**) for **Fully Qualified Address.** Enter the domain from **Section 6.1.1** (e.g., **avaya.com**). Click **OK**.



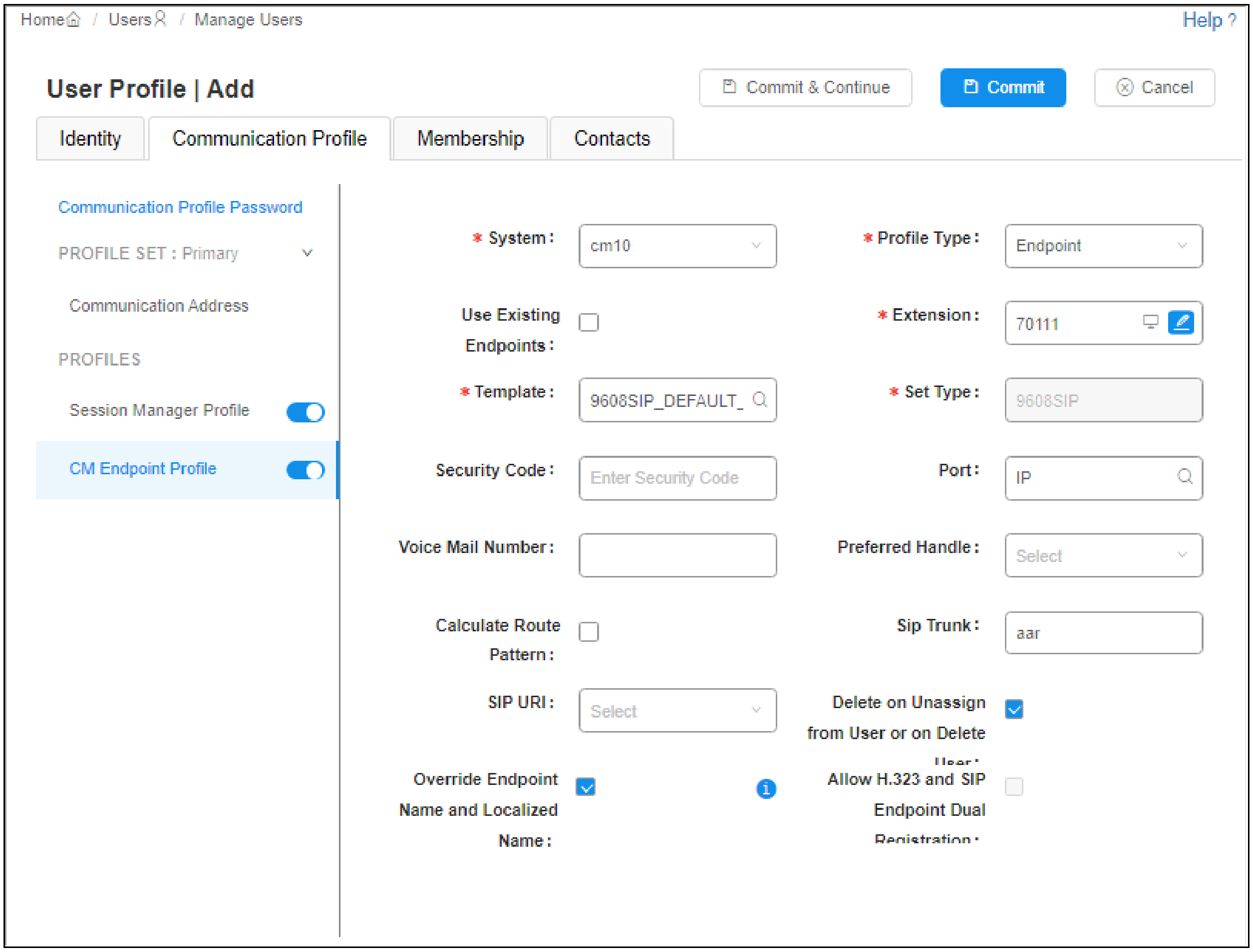
Select **Communication Profile Password** on the left and in the **Comm-Profile Password** and **Re-enter Comm-Profile Password** fields, enter a password. This will be used to register the device. Click **OK**.



Click on the **Session Manager Profile** slide button. For **Primary Session Manager**, select the values corresponding to the applicable Session Manager (e.g., **sm10**). Do not select any **Application Sequences**. Retain the default values in the remaining fields.



Click on the **CM Endpoint Profile**, slide button. Select the appropriate System (e.g., **cm10**), Endpoint for **Profile** Type, the Extension (e.g., **70111**). Click on **Commit** to save the new user.

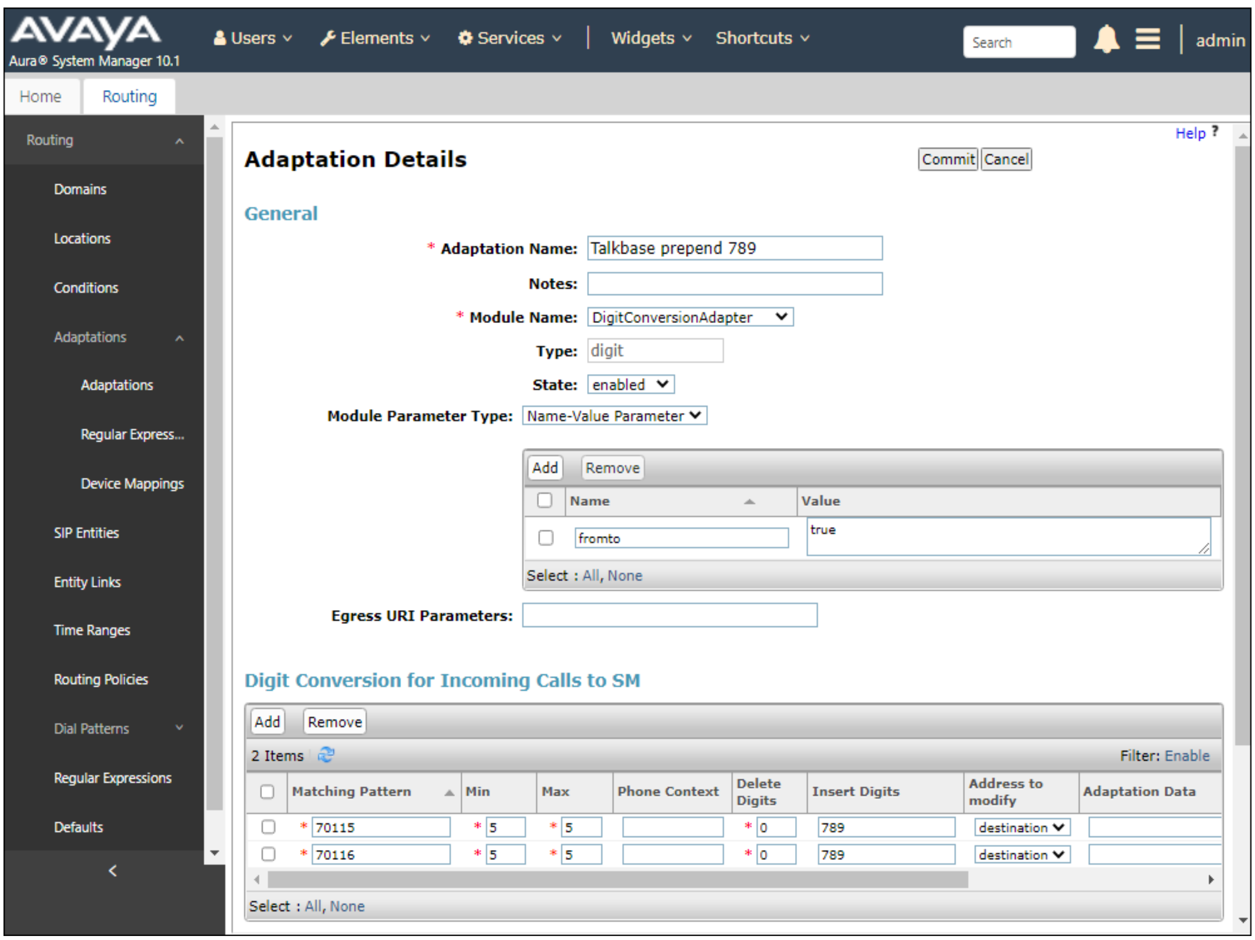


6.9. Configure for Attendant to Attendant Main Number Forwarding

This configuration is optional. In some situations, it may be desired for an attendant to forward a call back to their main number. Session Manager will route main number calls from attendants back to talkbase. talkbase cannot handle this case without additional configuration. In order to do this, call routing can be altered to have another call-id generated by routing these calls through Communication Manager. Refer to **[6]** for details. The below steps may be one such method to accomplish this.

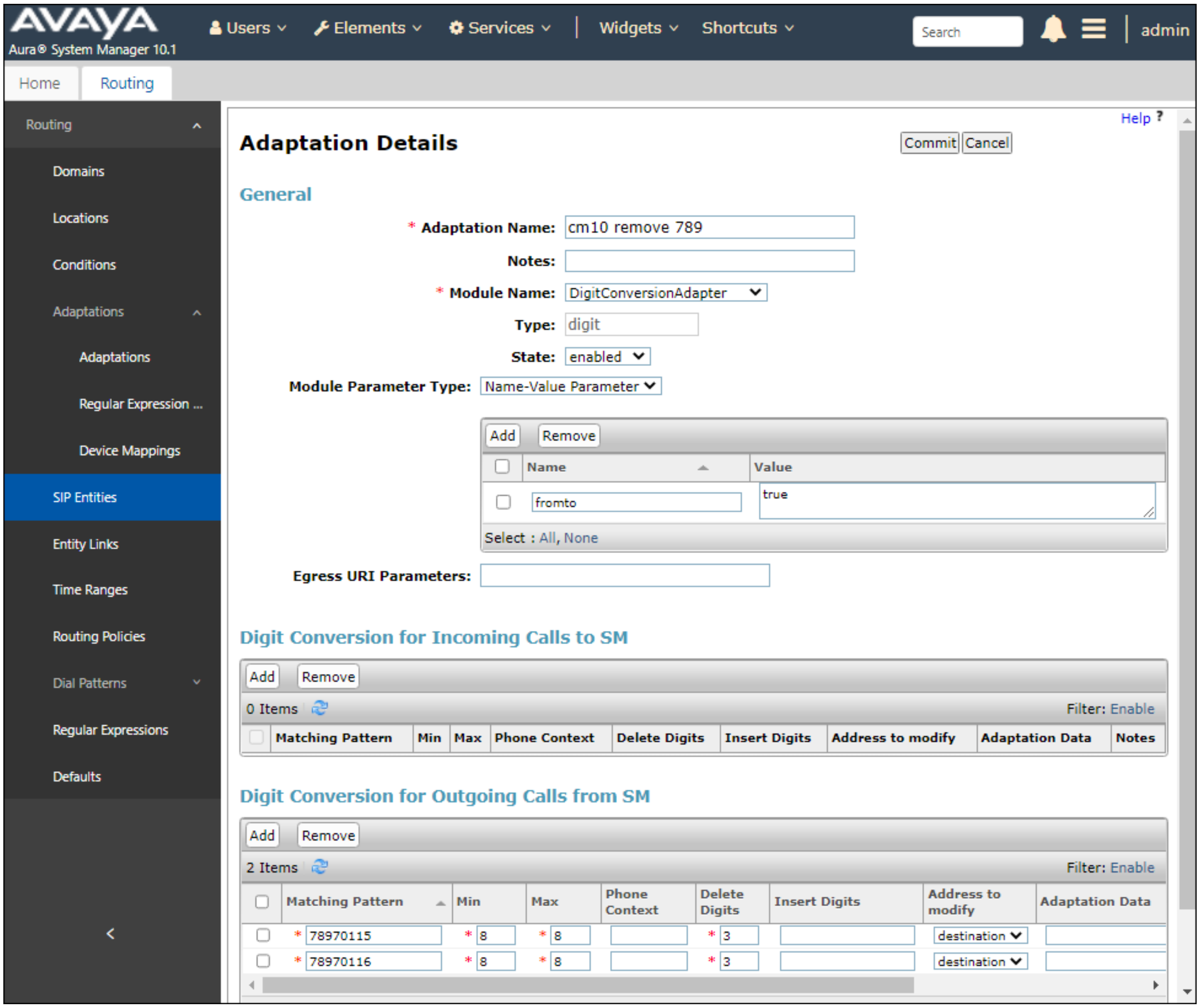
6.9.1. Talkbase SIP entity Adaptation

Create a SIP entity adaptation to modify incoming main number call digits coming from talkbase Attendant in order to route them to Communication Manager instead of talkbase. Such an adaptation prepends digits to the main number called which will ultimately route the call to Communication Manager. The Adaptation **Talkbase prepend 789** below adds the digits **789** to the main numbers **70115** or **70116** dialed by attendants and can be assigned to the talkbase SIP entity as per **Section 6.4.**



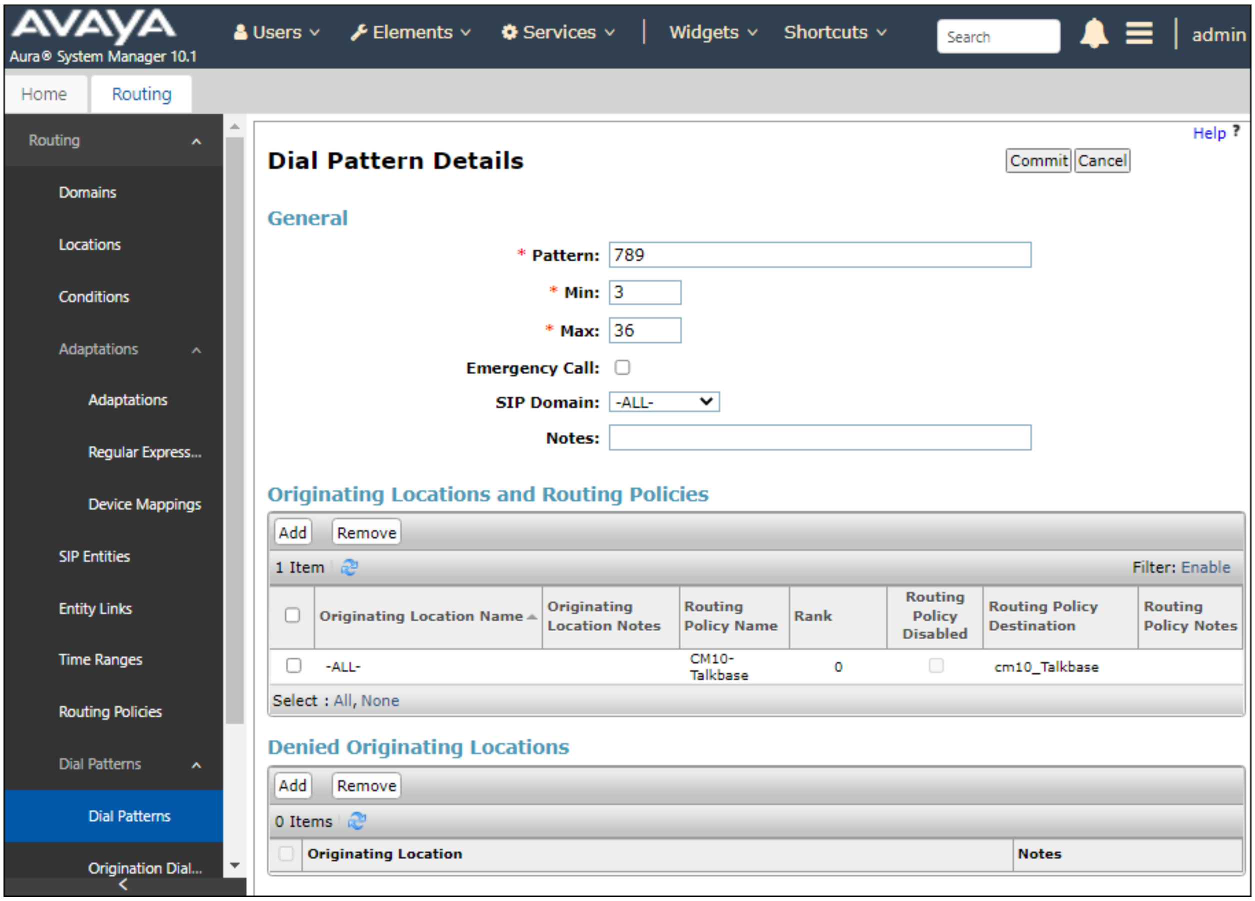
6.9.2. Communication Manager SIP Entity Adaptation

Create a SIP entity adaptation to modify incoming main number calls from talkbase Attendant with modified digits to route them back to talkbase by removing the prepended digits. The Adaptation **cm10 remove 789** below removes the digits **789** prepended to the main numbers **70115** or **70116** dialed by attendants and can be assigned to the Communication Manager SIP entity as per **Section 6.2.**



6.9.3. Dial Pattern Route to talkbase SIP Entity

A dial pattern may be needed to ensure the modified queue call's destination routes to Communication Manager. A pattern was created using the method shown in **Section 6.7** to route destinations prepended with the digits **789** used in the adaptations created in **Sections 6.9.1 and 6.9.2** to the Communication Manager SIP entity **cm10_Talkbase**.



7. Configure FROX AG talkbase

The configuration for talkbase to communicate with Session Manager is made on the talkbase server directly and a GUI using a web connection to the server. talkbase is dependent on having a Windows domain already in place with Windows Active Directory running. The talkbase server and talkbase Attendant client PC must be a part of this domain. talkbase users synchronize with Active Directory. The procedures include the following areas:

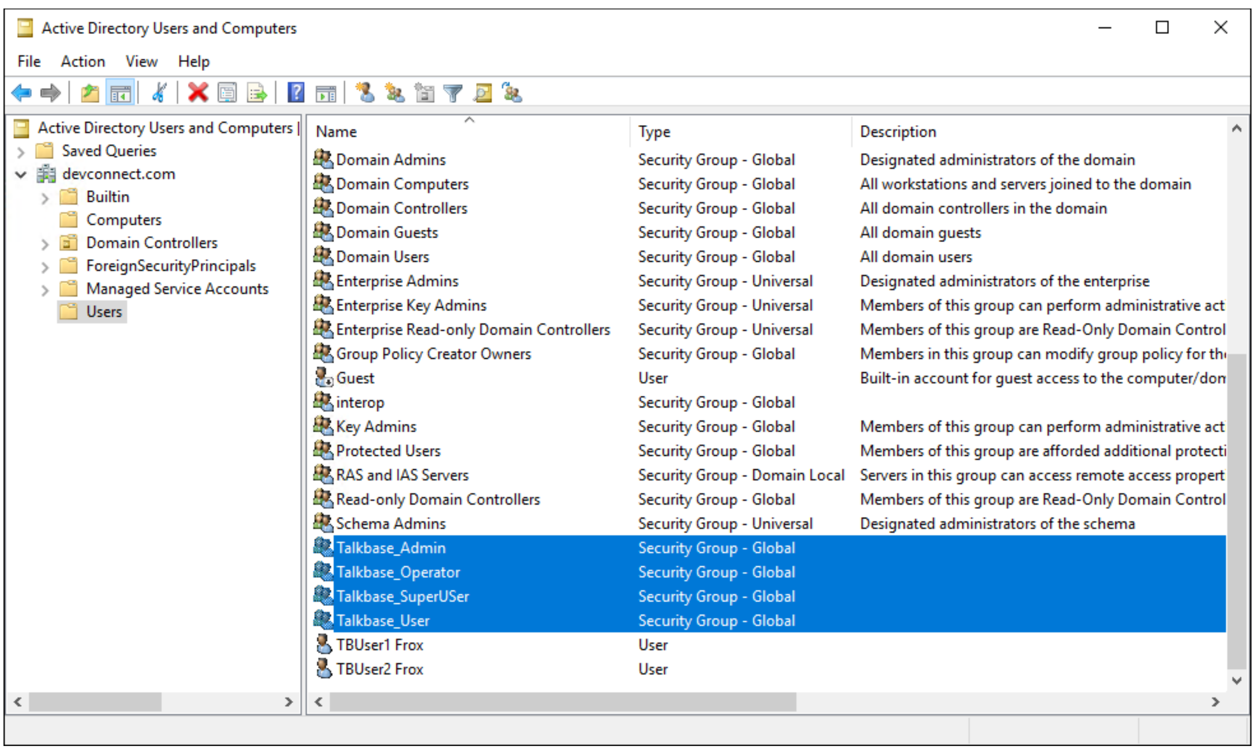
- Configure Active Directory for talkbase
- Configure the talkbase server
- Configure talkbase Attendant

7.1. Configure Active Directory for talkbase

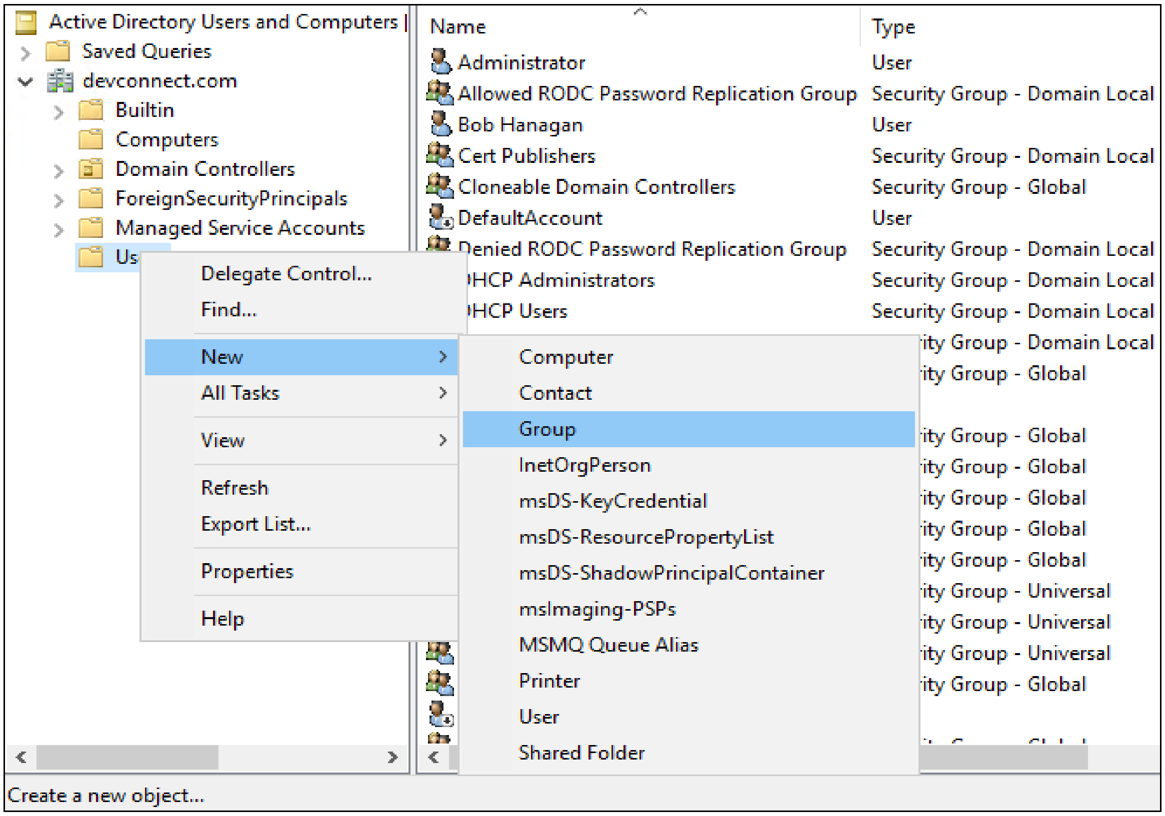
The Active Directory must be configured for the following groups.

- **Talkbase_Admin**
- **Talkbase_Operator**
- **Talkbase_SuperUser**
- **Talkbase_User**

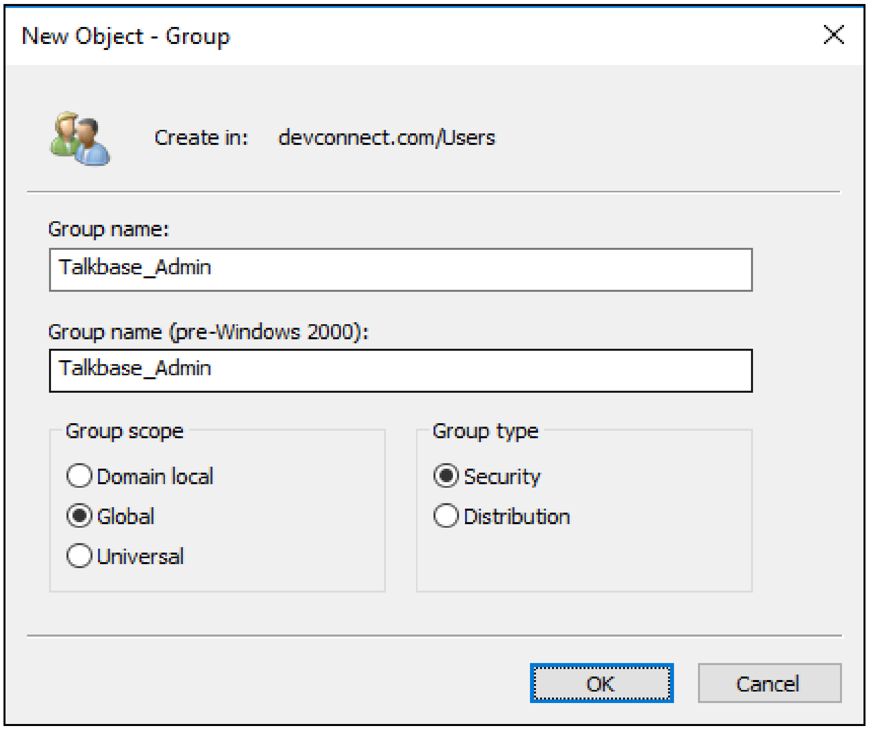
The various talkbase users that are added on Active Directory will be a part of one or more of these groups. The following shows these groups already configured.



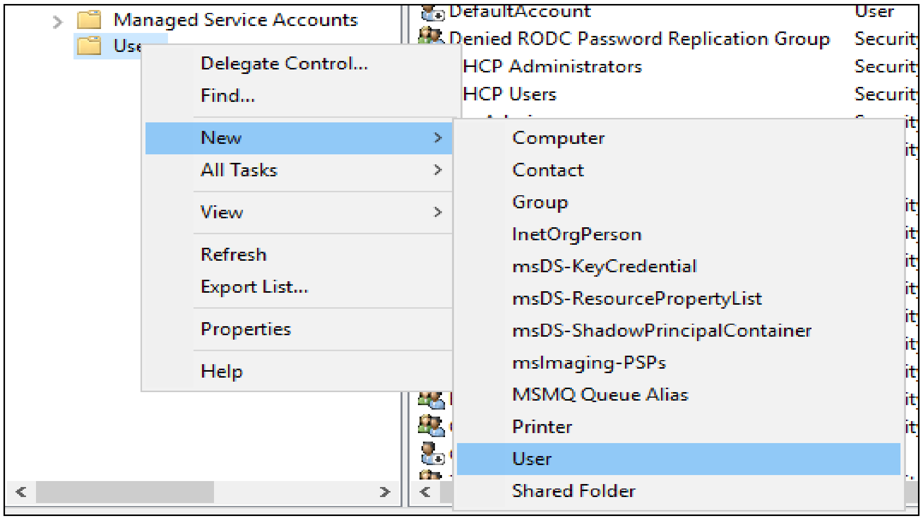
To add a new group, right-click on **Users** and select **New** and then **Group** as shown below.



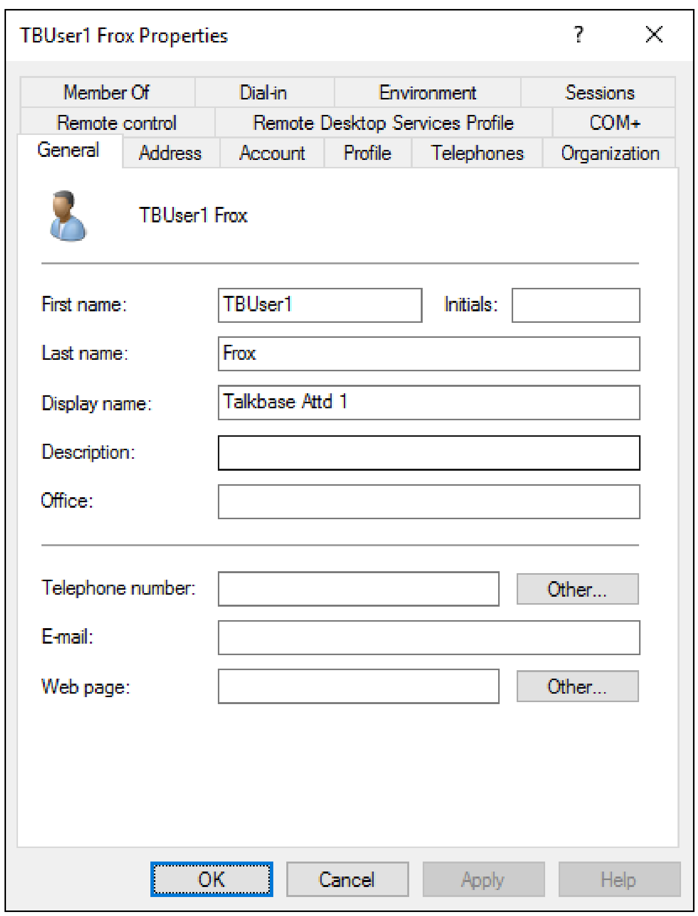
Enter the **Group name** and ensure the **Group scope** and **Group type** are selected as shown below.



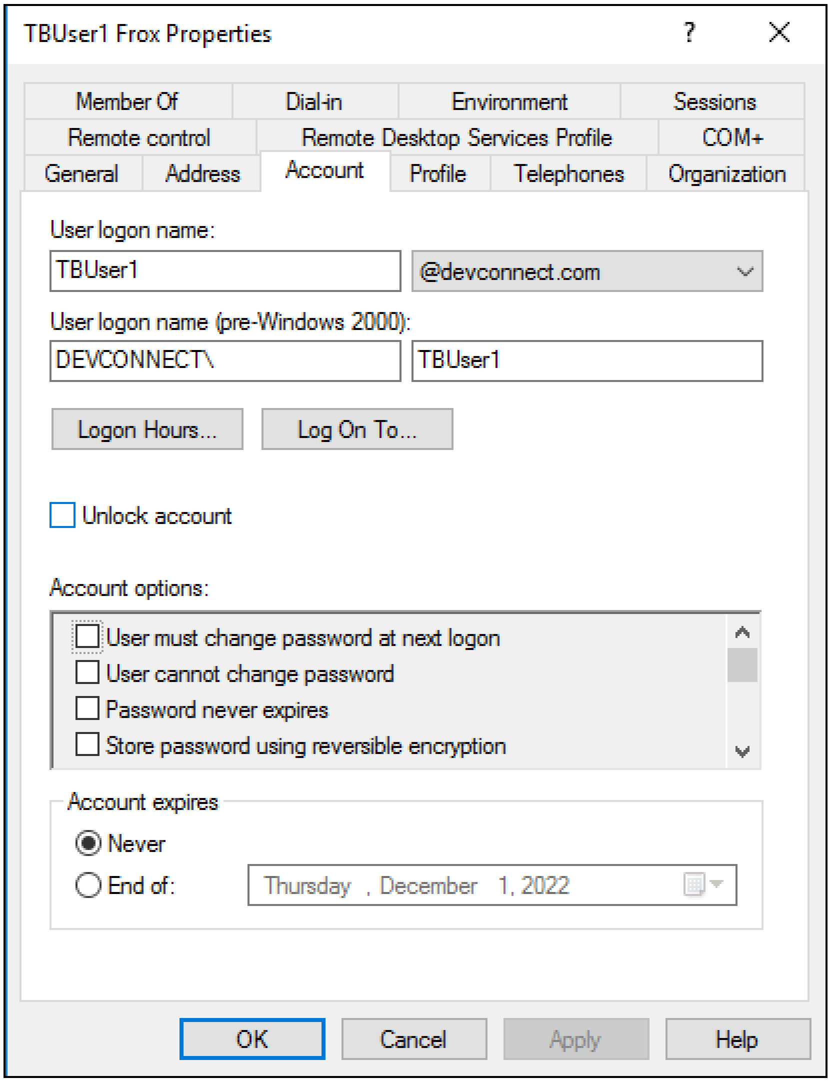
To add a new Active Directory user, right-click on **Users** and select **New** and then **User** as shown below.



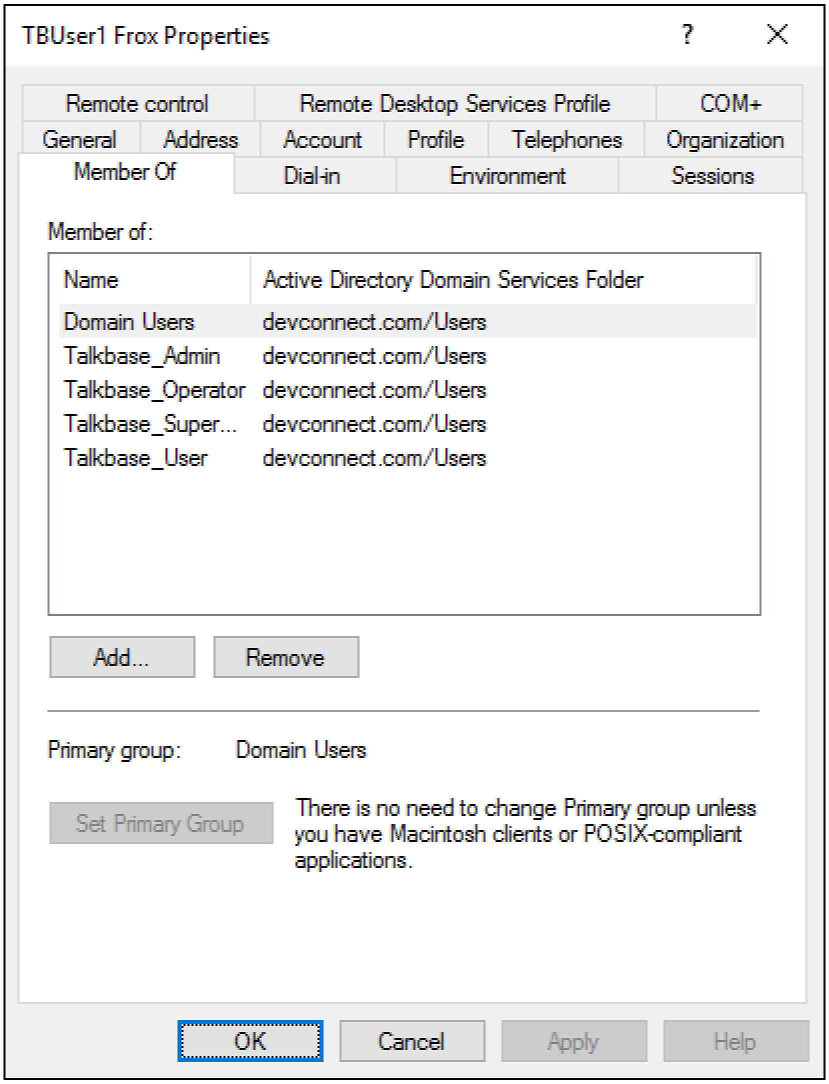
The following shows information on a user called **Talkbase Attd 1** set up and used for testing. These are the users name details under the **General** tab.



This is the account information under the **Account** tab.



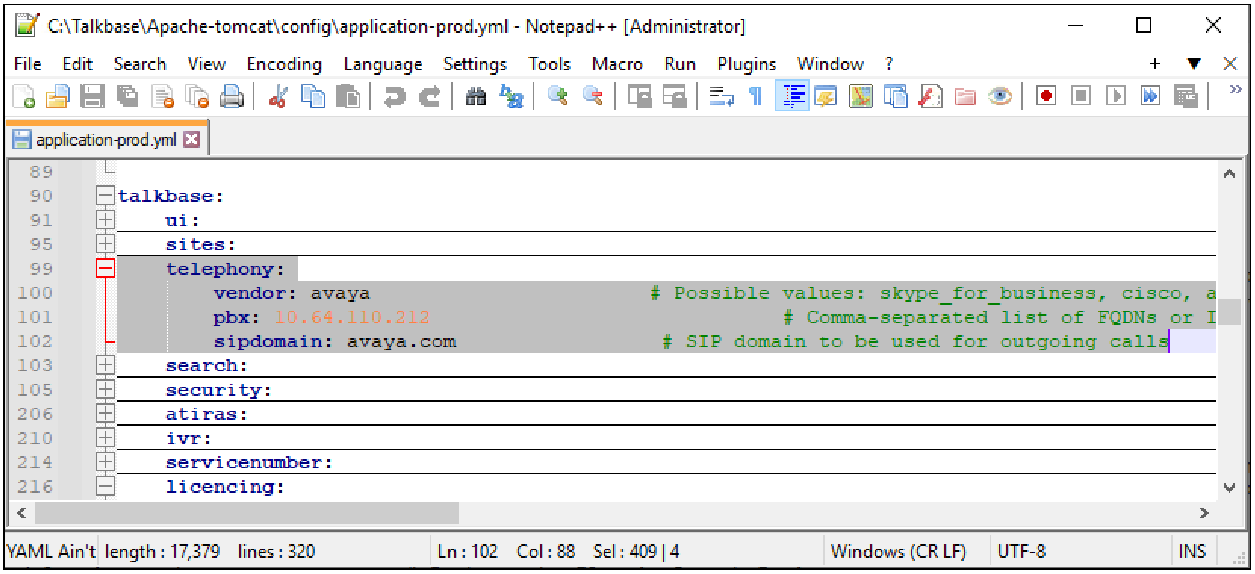
This particular user is set up to be a member of all four talkbase user groups, but this need not be the case on a customer site. Under the **Member Of** tab, the list of groups this user belongs to is displayed.



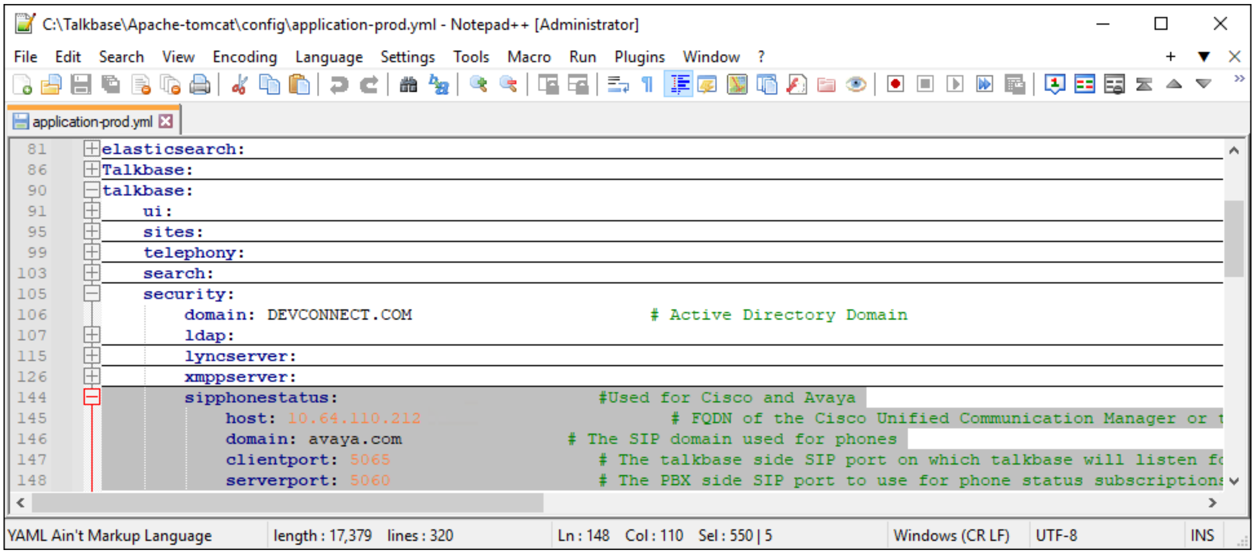
7.2. Configure the talkbase server

Configuration of the talkbase server is made by amending a file called **application-prod.yml**. The configuration file is created during the talkbase server installation and must be customized to specific installations. Essential modifications are detailed below. The file employed for compliance testing is included in **Appendix** 1 for reference.

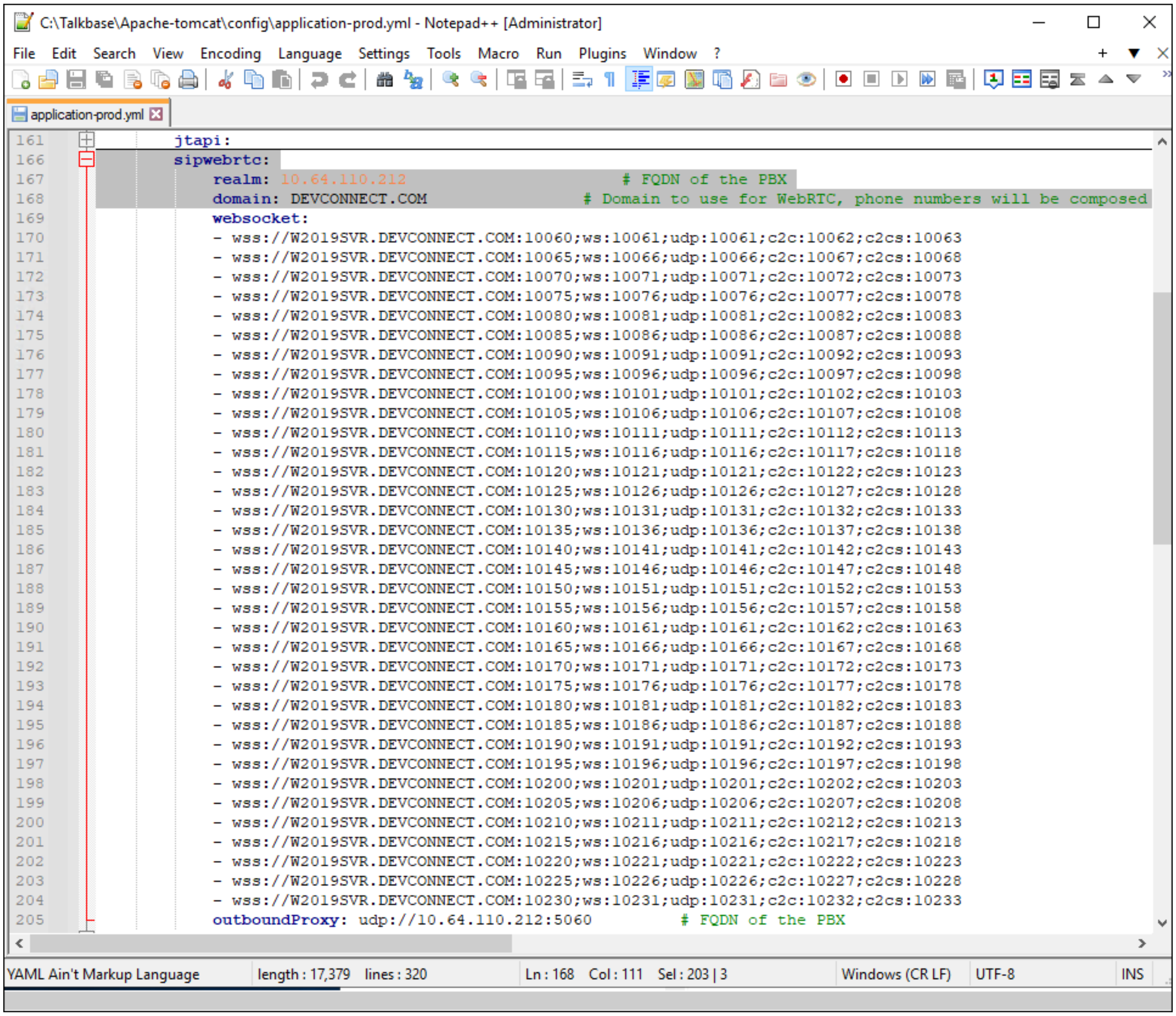
The talkbase server configuration file to modify is **C:\Talkbase\Apache-tomcat\config\application-prod.yml**. The file can be changed with a text editor. Under the **talkbase** block, verify the **Telephony** entries have the Session Manager IP Address (e.g., **10.64.110.212**) for **pbx** and the SIP Domain (e.g., **avaya.com**) for **sipdomain**.



Verify the **sipphonestatus** entries have the Session Manager IP Address (e.g., **10.64.110.212**) for **host,** the SIP Domain from **Section 6.1.1** (e.g., **avaya.com**) for **domain**, and the port number from **Section 6.3** (e.g., **5060**) for **serverport**.



Verify the **sipwebrtc** entries have the Session Manager IP Address (e.g., **10.64.110.212**) for **realm** and **outboundProxy,** and the Windows Active Directory domain (e.g., **DEVCONNECT.COM**) for **domain**.

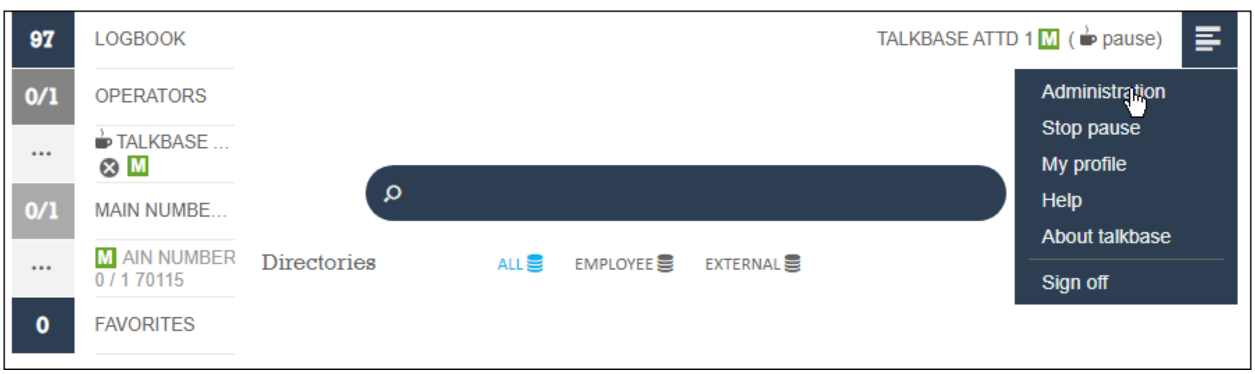


Websocket entries specify WebRTC ports configured for talkbase. Note the ports specified (e.g., ports**10060,10065,10070,10075,10080,10085,10090,10095,10100,10105,10110,10115,10120,10125,10130,10135,10140,10145,10150,10155,10160,10165,10170,10175,10180,10185,10190,10195,10200,10205,10210,10215,10220,10225,10230**). These ports are input to the **Site Detail** tab in **Section 7.3**.

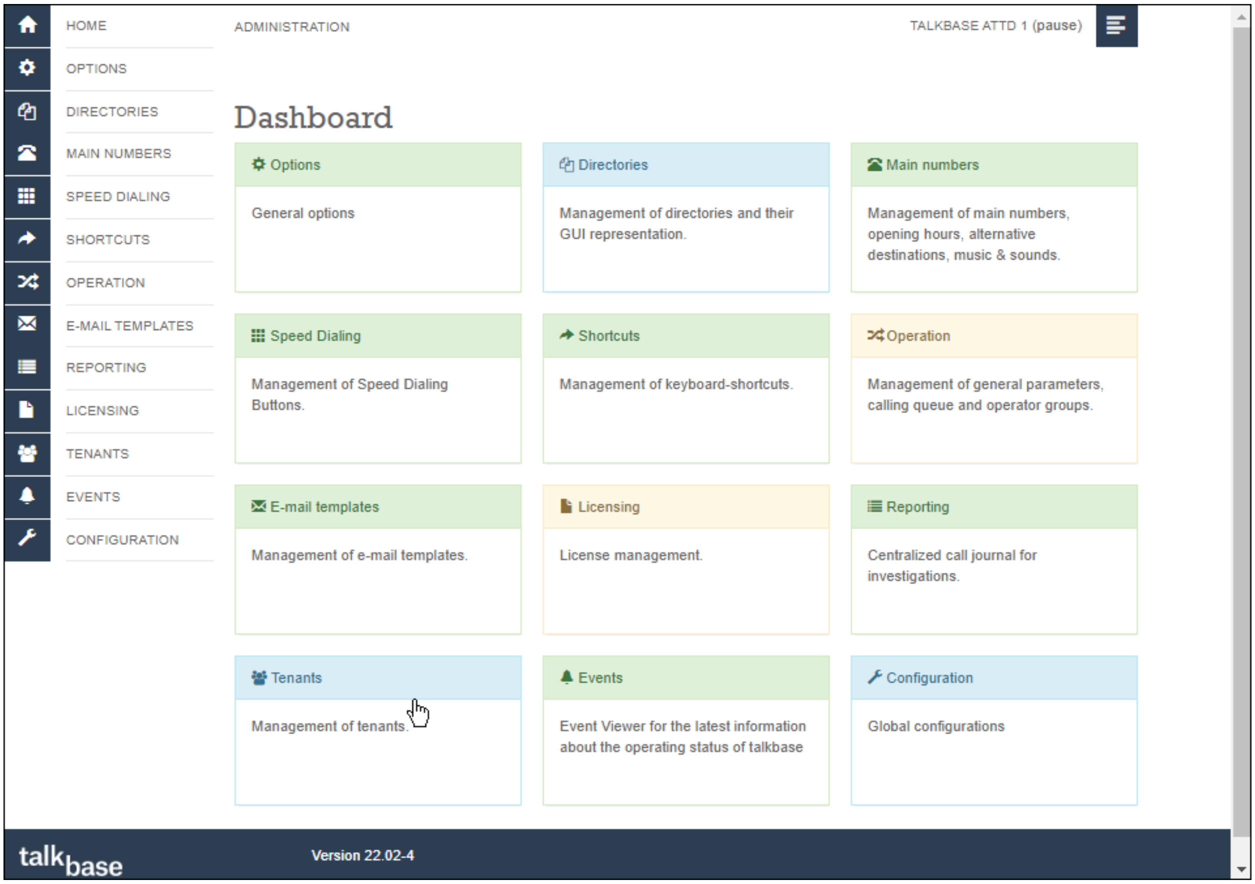
7.3. Configure talkbase Attendant

talkbase Attendant administration configures attendants, main numbers, and assigns attendants to answer calls from main numbers. Open a web browser (compliance testing employed Chrome browser) and navigate to talkbase Attendant using the URL **https://<FQDN of talkbase server>**. Enter the Active Directory user credentials of a user with **Talkbase_Admin** and **Talkbase_SuperUser** group memberships and click on **Sign in**.

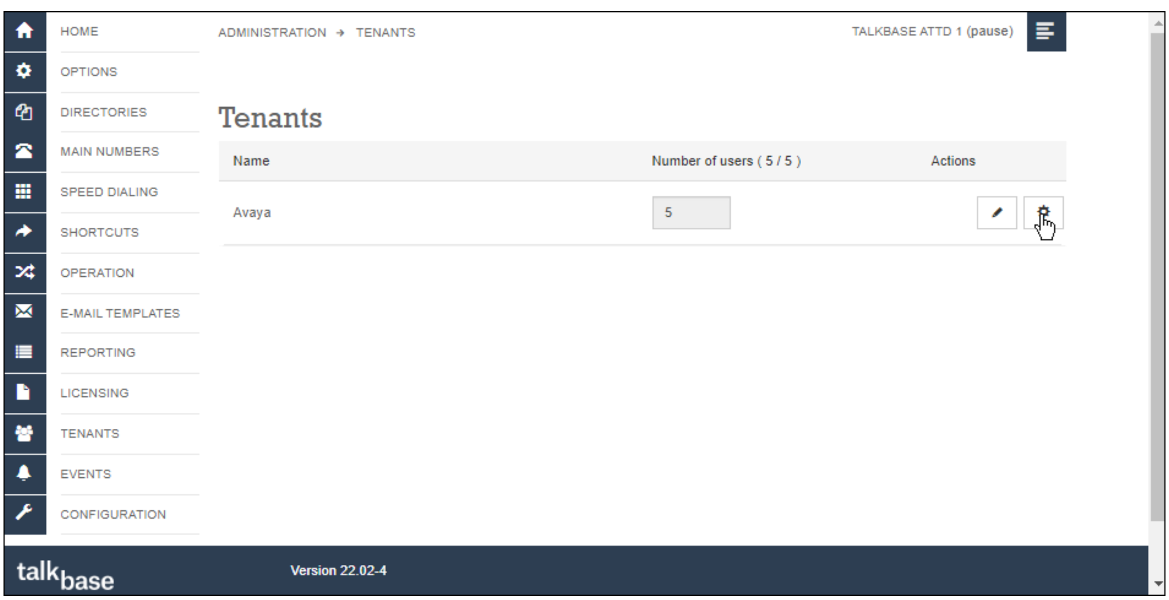
Click on the icon at the top right of the page and select **Administration** as shown below.



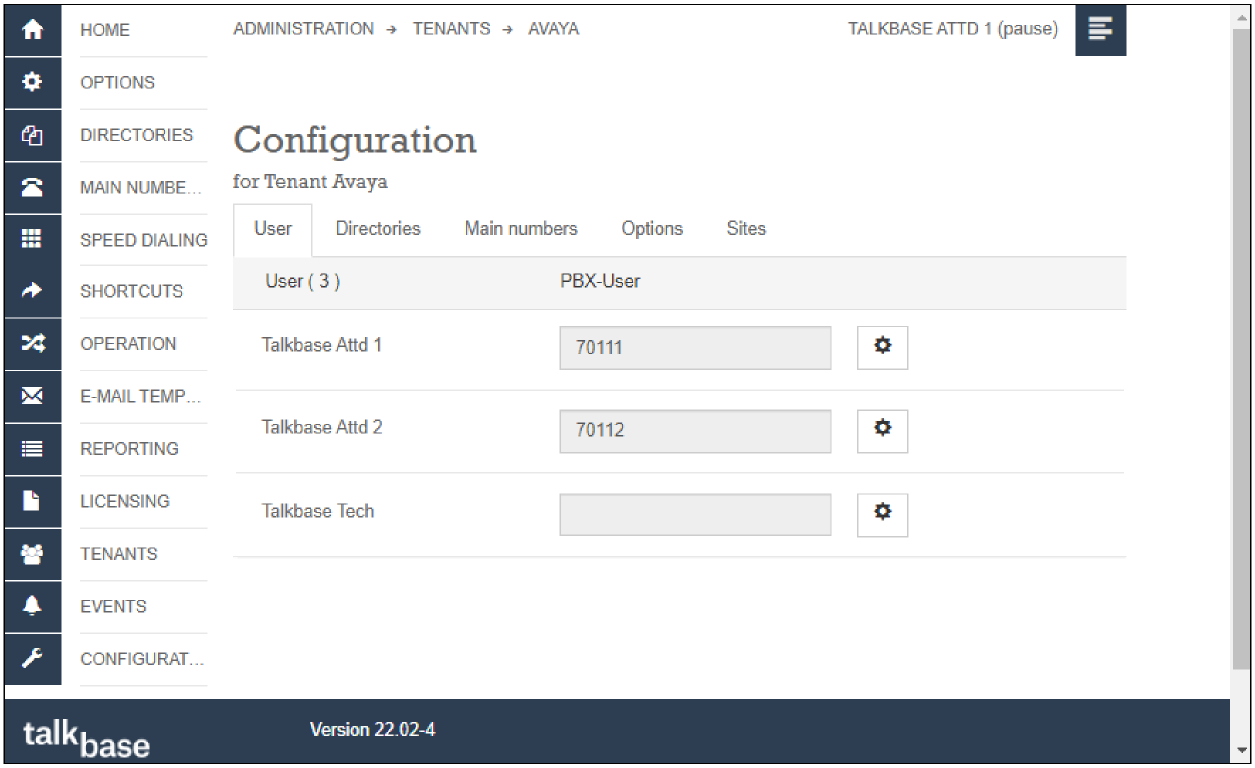
The screen displays the various modules. Click on **Tenants** at the bottom of the screen.



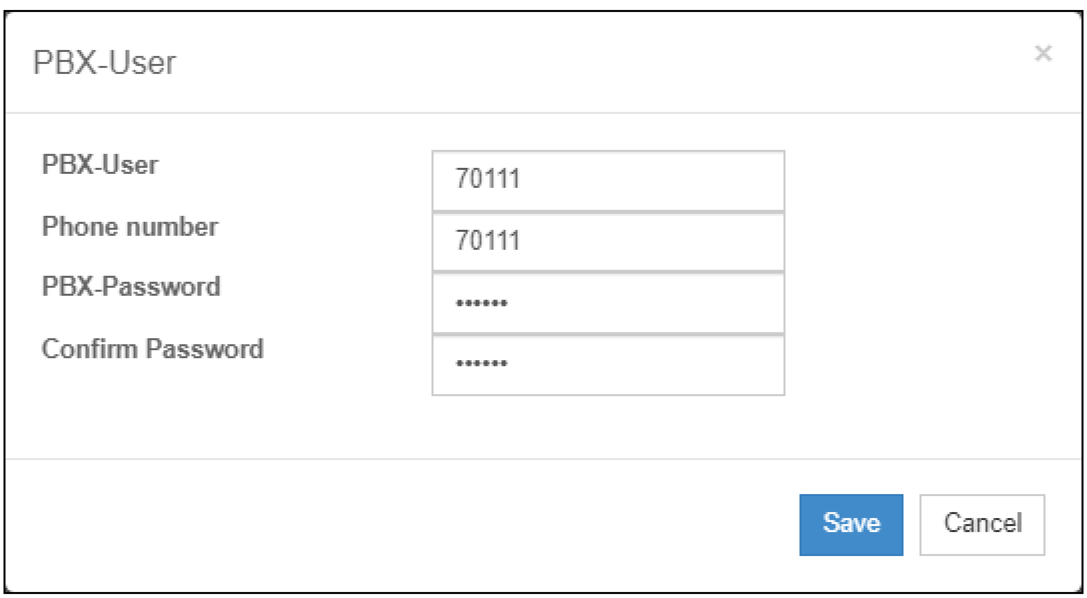
The **Tenant** called **Avaya** is set up by the FROX engineers as part of the original connection setup. Click on the detail (gear) icon to display the information on this tenant.



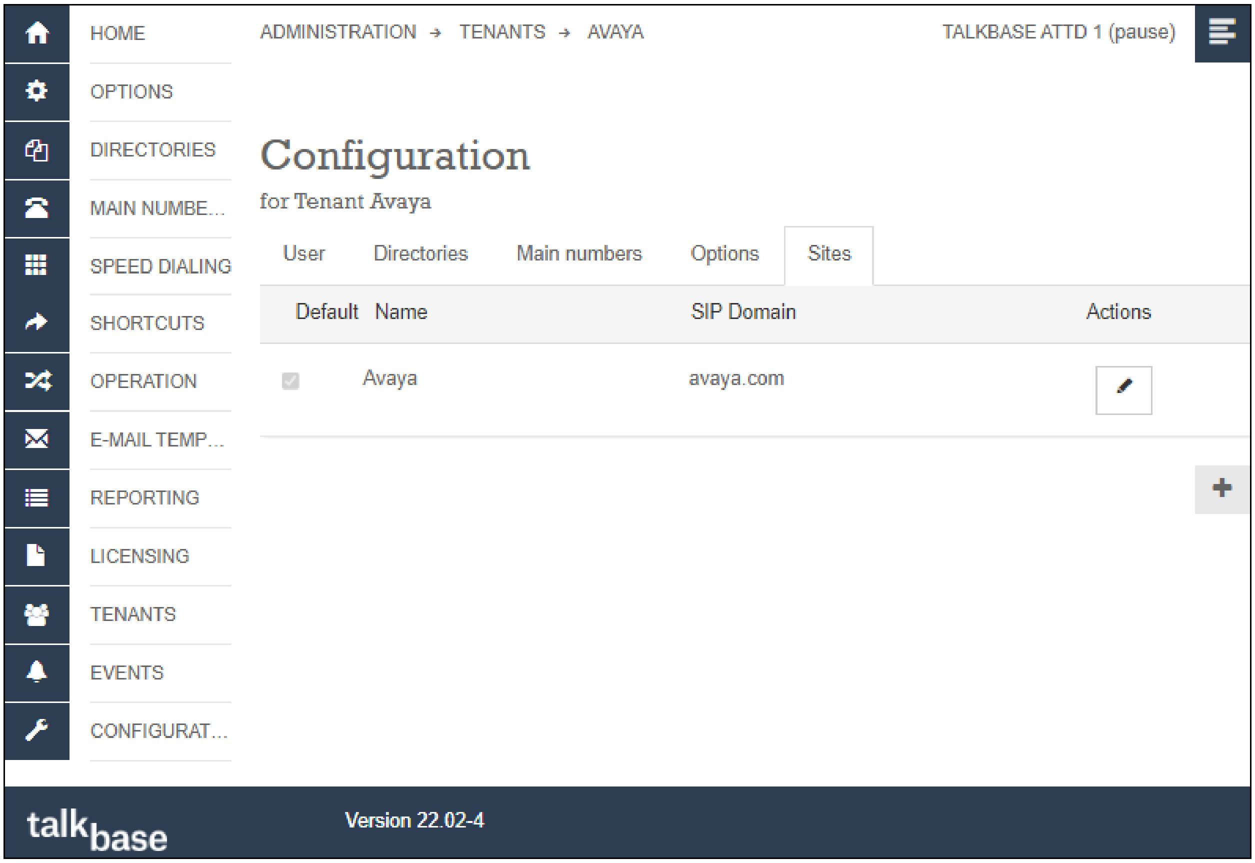
The users are automatically populated from the Active Directory of the domain that the talkbase server is a part of. **Talkbase Attd 1**, **Talkbase Attd2** and **Talkbase Tech** are all added as domain users as per **Section 7.1**. Talkbase Attendant users are shown with **PBX-Users** assigned. To assign **PBX-User**, click on the **Interface Configuration** (gear) icon.



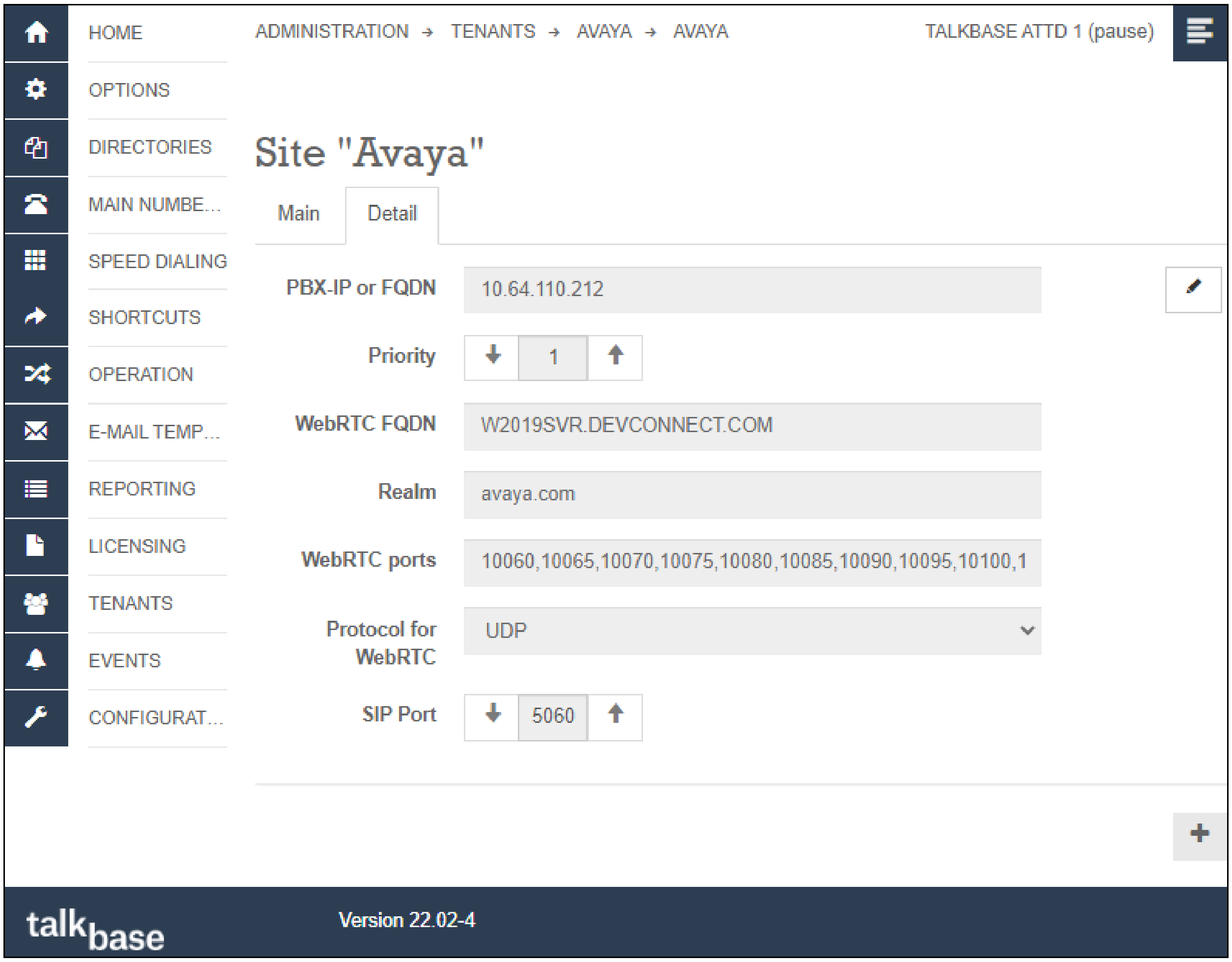
Enter the SIP login name and Communication Profile Password from **Section 6.6** for **PBX-User** and **PBX-Password.** The **Phone number** is the CM Endpoint Profile Extension of the SIP user.



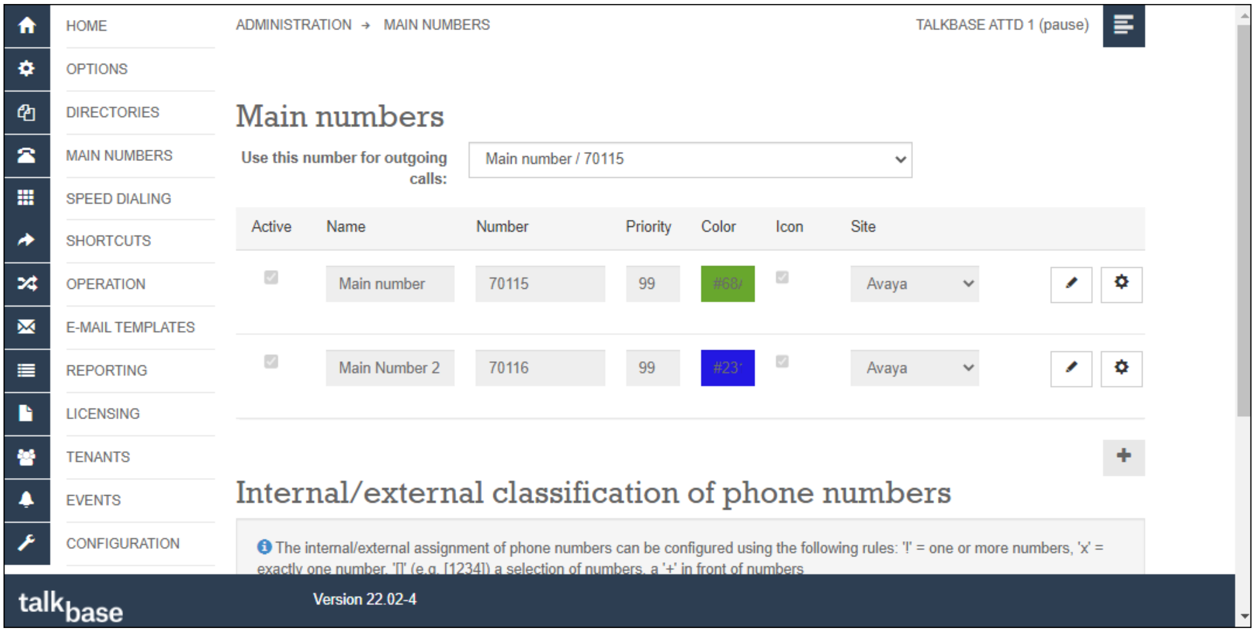
After configuring Users, select the **Sites** tab. The site should be configured so a Main Number can be assigned. To create a site, click the **+** icon. Compliance testing used a **Name** of **Avaya,** SIP **Domain** of **avaya.com**, and set **Default** (not shown).



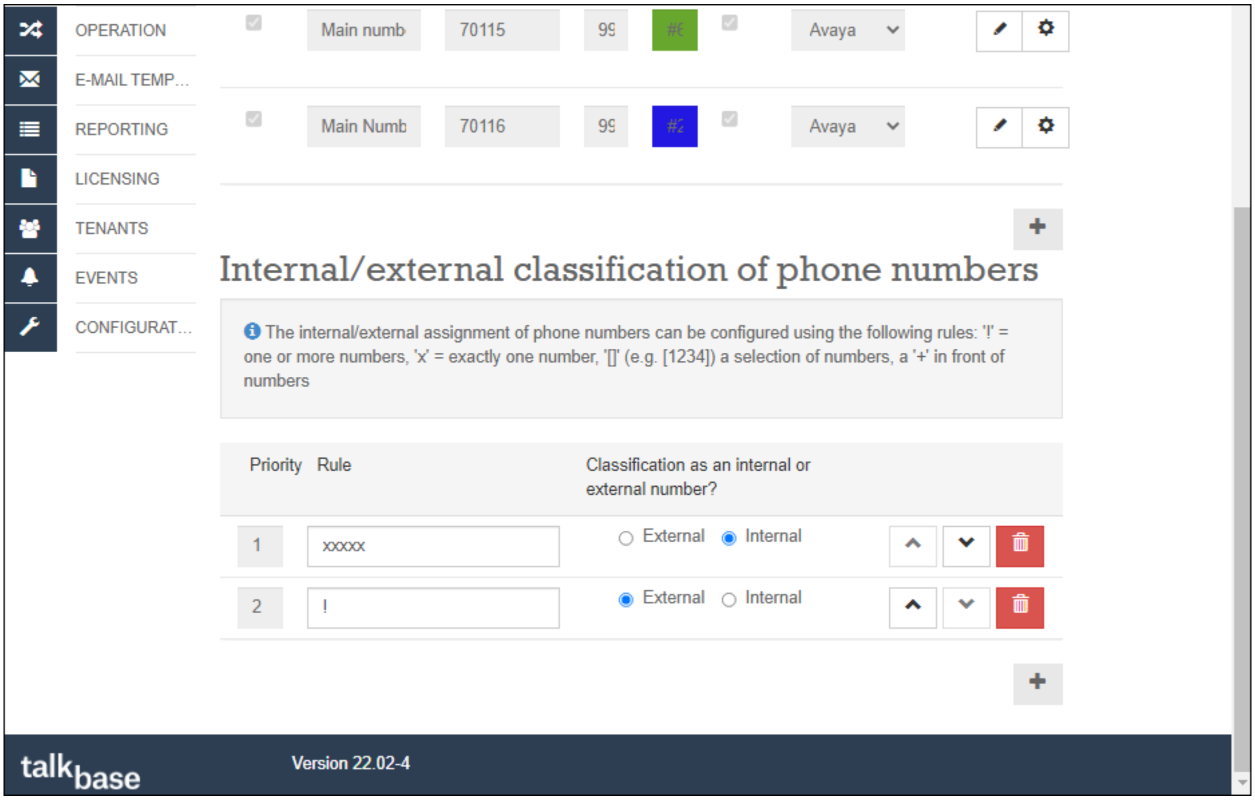
Select the **Edit** icon for the Avaya Site. Once open, select the **Detail** tab. Click the **Edit** icon to configure the following. The **PBX-IP or** FQDN should be se to the Session Manager IP Address (e.g., **10.64.110.212**) Set the **WebRTC FQDN** to the talkbase server FQDN (e.g., **W2019SVR.DEVCONNECT.COM**). Set the **Realm** to the SIP domain from **Section 6.1** (e.g., **avaya.com**). Add the **WebRTC ports** noted from **Section 7.2**. Set the **Protocol for WebRTC to UDP**. Set the **SIP Port** to **5060**.



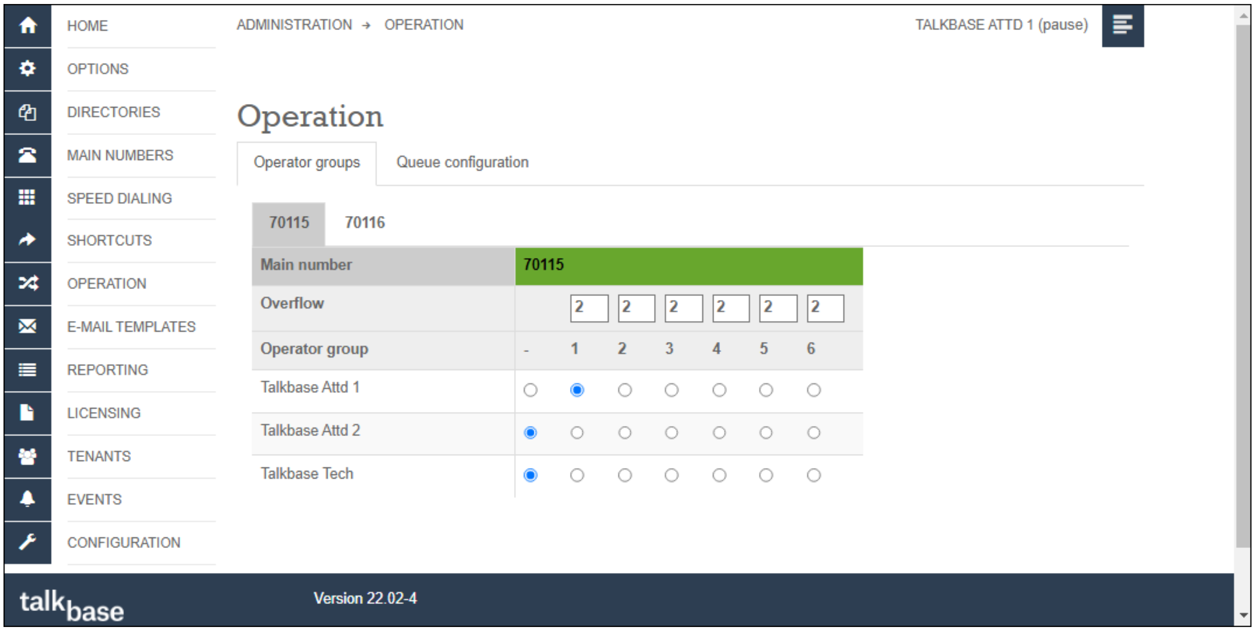
Return to the **Administration** menu and select **Main numbers** from the **Dashboard** (not shown) to configure the main numbers that will be assigned to attendants. The following shows that two numbers (e.g., **70115** and **70116**) are configured for the Avaya Tenant. To add a main number, Click on the **+** icon to add a new row and input an extension that has been configured to route from Session Manager to talkbase and select the **Avaya** Tenant.

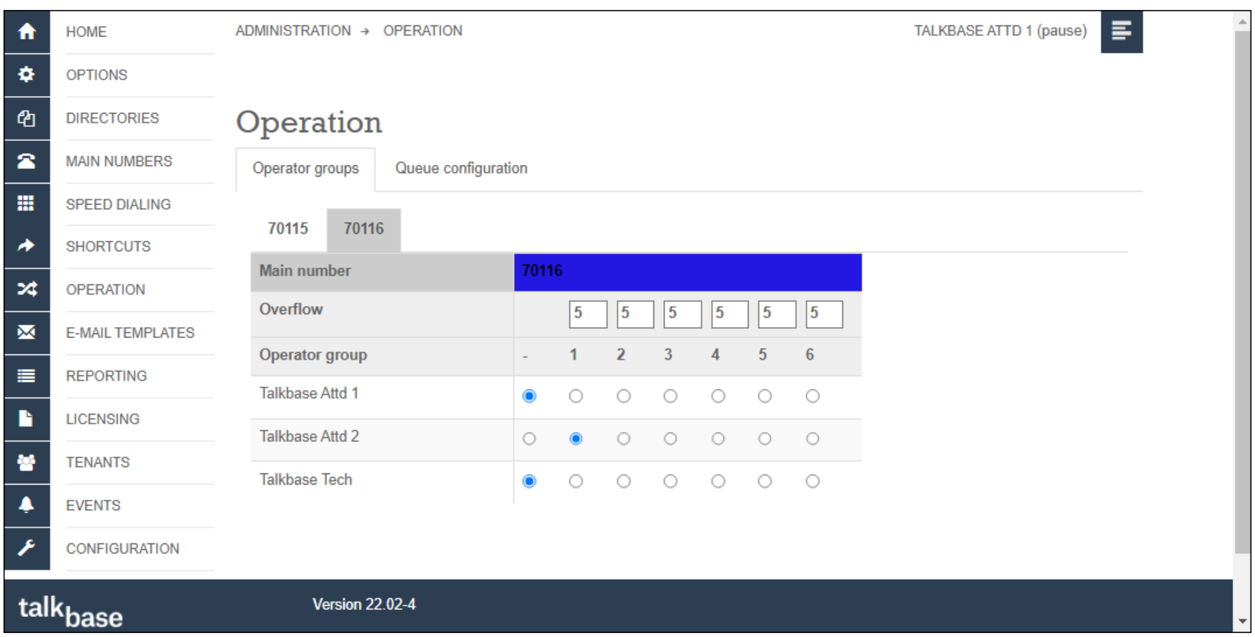


Scroll down to add **Internal/external classification of phone numbers** to classify incoming calls to talkbase as internal or external. Click on the **+** icon to add a new row. Input the **Rule** and specify the classification as **Internal** or **External**. Priority can be adjusted by moving the rule up or down by clicking the arrow icons for the row. The following rules are added for compliance testing. 5-digit extensions are classified as internal.

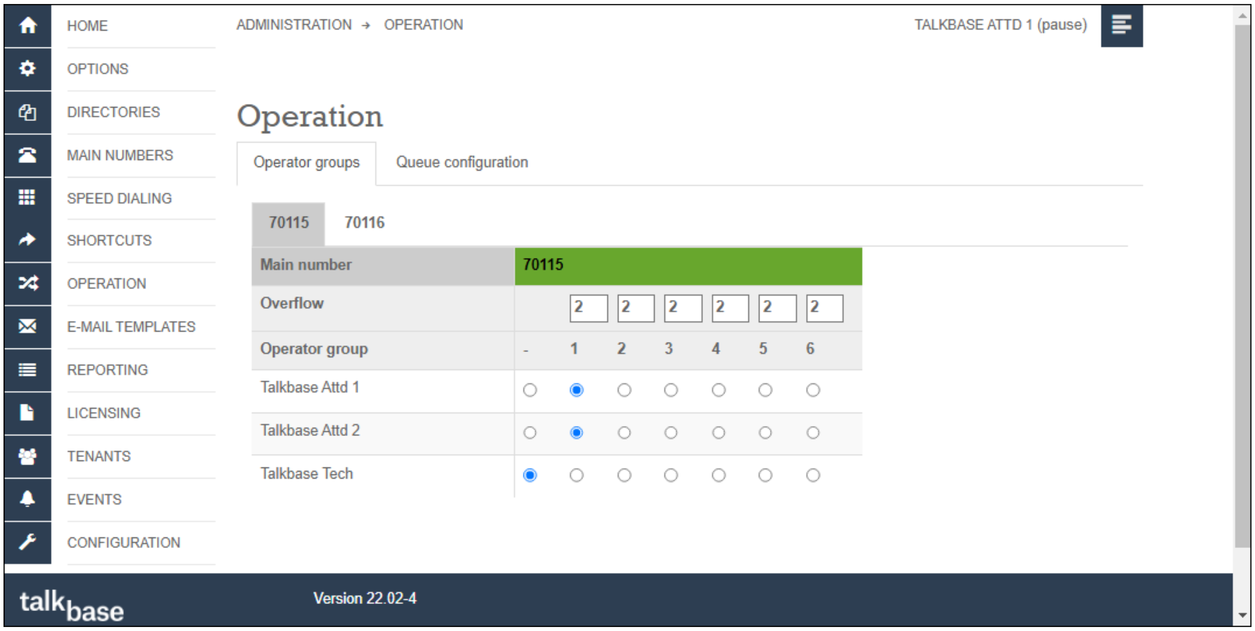


Return to the **Administration** menu and select **Operation** from the **Dashboard** (not shown) to assign attendants to receive calls from main numbers. The **Operator Groups** tab and **Main numbers** subtabs show numbers configured along with attendants administered. **Overflow** shows the number of calls in queue needed before another **Operator group** will receive calls from the main number. Compliance testing administered **Talkbase Attd 1** and **Talkbase Attd 2** to different main numbers as seen below.





The example below shows both **Talkbase Attd 1** and **Talkbase Attd 2** assigned to the **Main number 70115**.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of talkbase with Communication Manager and Session Manager.

8.1. Verify the SIP Trunk connection

The SIP trunk connection can be verified from both Communication Manager and Session Manager.

8.1.1. Verify Avaya Aura® Communication Manager Trunk

From the SAT interface, verify the status of the SIP trunk groups by using the **status trunk n** command, where "n" is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the **in-service/idle** state.

```
status trunk 12
                             TRUNK GROUP STATUS

Member    Port    Service State      Mtce Connected Ports
                                     Busy

0012/0001 T000026 in-service/idle    no
0012/0002 T000027 in-service/idle    no
0012/0003 T000028 in-service/idle    no
0012/0004 T000029 in-service/idle    no
0012/0005 T000030 in-service/idle    no
0012/0006 T000031 in-service/idle    no
0012/0007 T000032 in-service/idle    no
0012/0008 T000033 in-service/idle    no
0012/0009 T000034 in-service/idle    no
0012/0010 T000035 in-service/idle    no
```

Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where "n" is the signaling group number administered in **Section 5.3**. Verify that the signaling group is **in-service** as indicated in the **Group State** field.

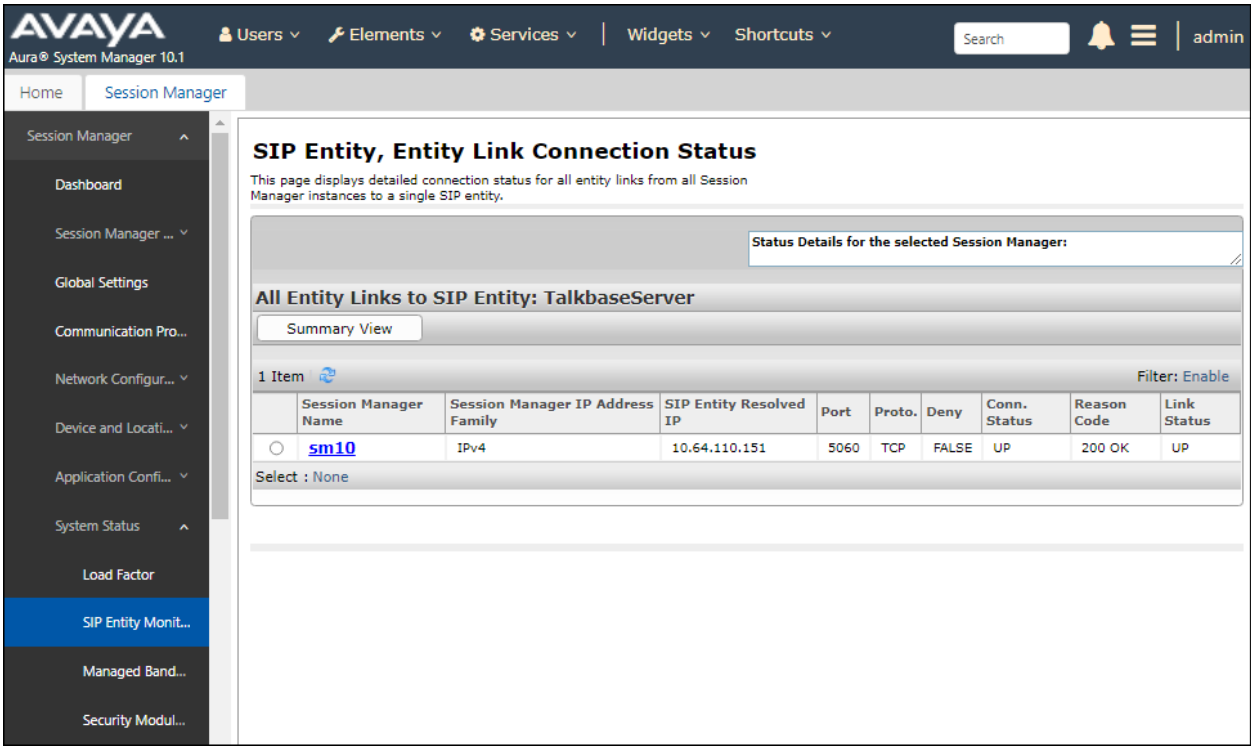
```
status signaling-group 12
                         STATUS SIGNALING GROUP

        Group ID: 12
      Group Type: sip

     Group State: in-service
```

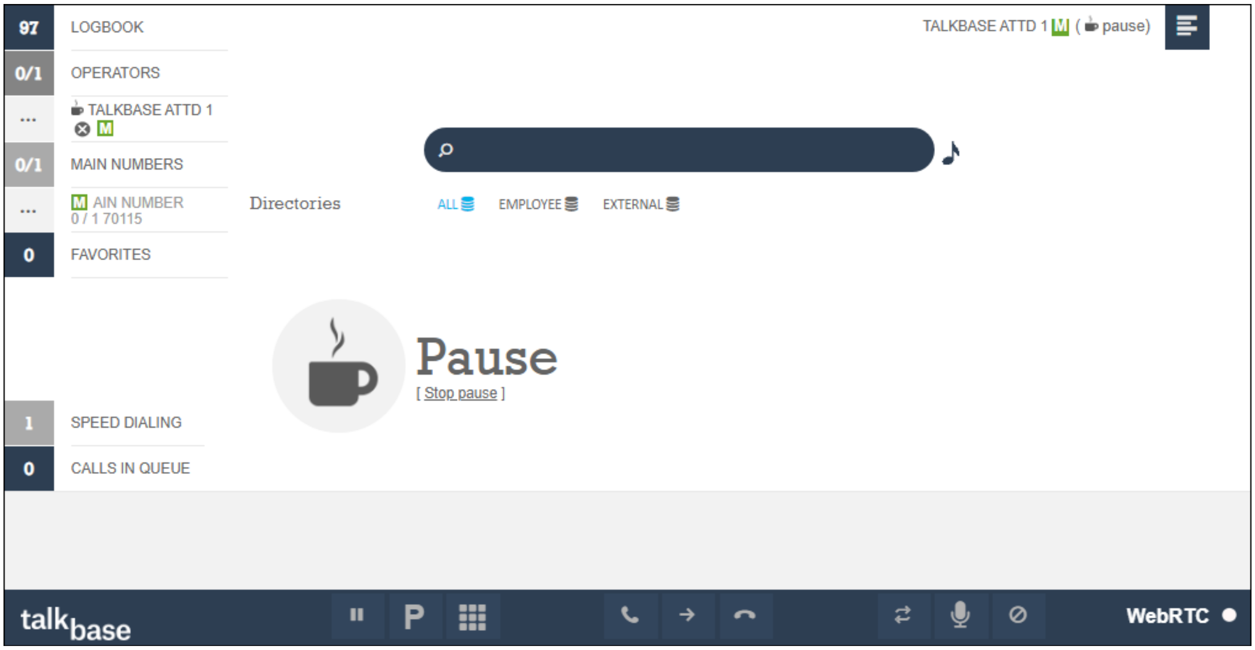
8.2. Verify talkbase SIP Entity is Connected

Log into System Manager as per **Section 6**. Navigate to **Elements → Session Manager→System Status→ SIP Entity Monitoring**. Click on the name of the talkbase SIP entity created in **Section 6.2** e.g., **TalkbaseServer** (not shown). The SIP Entity Link's **Conn. Status** should show **UP**.

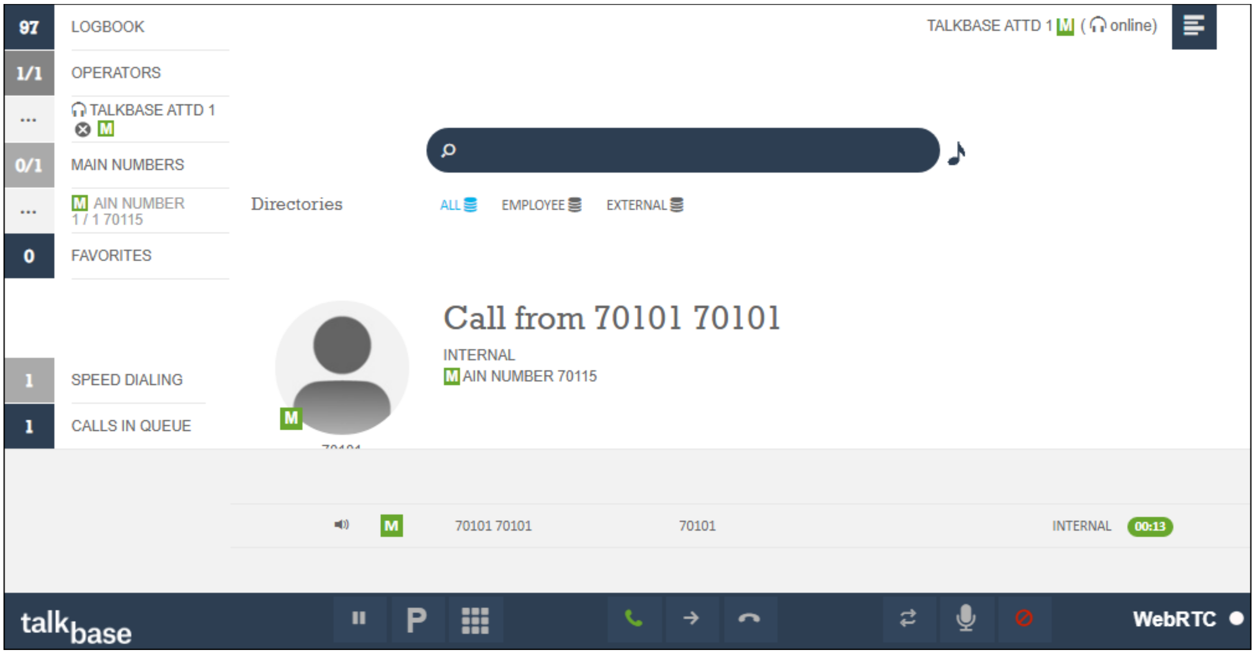


8.3. Verify talkbase Attendant

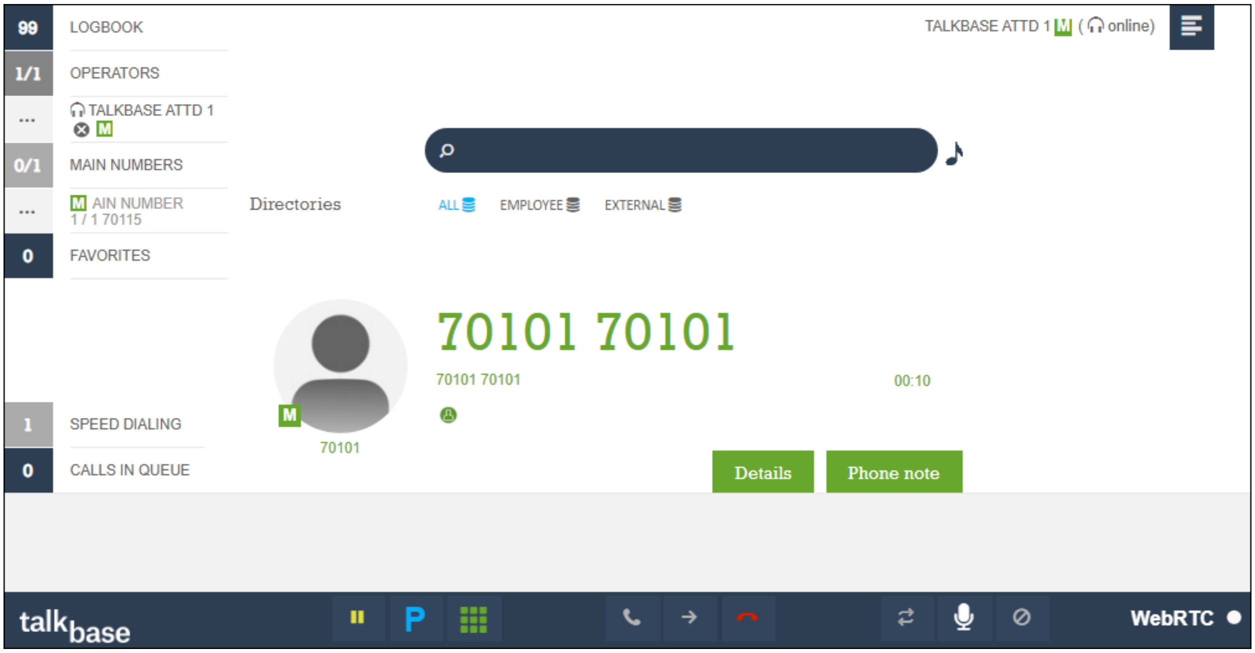
Open a web connection to the talkbase server as per **Section 7.2.** Enter the appropriate credentials and click on **Sign in** (not shown). The following screen should display showing the agent and the message **Pause** showing that the Attendant is not idle. **WebRTC** displayed in white at the bottom of the screen indicates that the Attendant is connected correctly with the SIP user created in **Section 6.6**.



Clicking on **Pause** will place the Attendant into a state ready to receive calls. When a call from **70101** is placed to the main number **70115** the following should display as shown below. Clicking on either the message in the middle of the screen or on the green telephone icon at the very bottom of the screen will answer the call.



Once the call is answered, verify the call can be put on hold, forwarded, or ended using the icons located at the bottom of the screen. The CLID displayed in the middle of the screen turns green also indicting the call is answered.



After answering the call, verify two-way audio.

9. Conclusion

These Application Notes describe the configuration steps required to integrate FROX AG talkbase with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022.

[2] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022.

The following documentation related to talkbase may be obtained from Frox AG.

[3] Talkbase Administration Guide, Release 2.17, January 4, 2019

[4] Talkbase Installation Guide, Release 22.02, September 22, 2022

[5] Talkbase Operator’s Guide, Release 1.72, February 8, 2017

[6] Talkbase Prerequisites, Release 22.02, August 25,2022

11. Appendix 1 Talkbase server Configuration File

The talkbase server configuration file can be modified for specific configurations as illustrated in **Section 7.2**. The configuration file used for compliance testing is listed here excepting password credentials.


```
server:
    port: 8080
    address: localhost
    servlet:
        session:
            timeout: 180 # Session timeout. If a duration suffix is not specified, seconds will
be used.

spring:
    profiles: prod
    datasource:
        type: com.zaxxer.hikari.HikariDataSource
        url: jdbc:postgresql://localhost:5432/talkbase
        name:
        username: talkbase
        password: ******
        driver-class-name: org.postgresql.Driver
        statementCacheNumDeferredCloseThreads: 1
        unreturnedConnectionTimeout: 180
        debugUnreturnedConnectionStackTraces: true
        maximumPoolSize: 150
    jpa:
        database-platform: com.noser.hunter.common.util.FixedPostgreSQL82Dialect
        database: POSTGRESQL
        show-sql: false
        properties:
            hibernate.cache.use_second_level_cache: true
            hibernate.cache.use_query_cache: false
            hibernate.generate_statistics: true
            hibernate.javax.cache.provider: org.ehcache.jsr107.EhcacheCachingProvider
            hibernate.javax.cache.uri: ${spring.cache.jcache.config}
            hibernate.cache.region.factory_class:
com.noser.hunter.common.util.SpringCacheRegionFactory
#    datasource:
#       dataSourceClassName: com.microsoft.sqlserver.jdbc.SQLServerDataSource
#       url: jdbc:sqlserver://localhost:1434;databaseName=talkbase;trustServerCertificate=true
#       databaseName:
#       serverName:
#       username: sa
#       password: ******
#       maximumPoolSize: 100
#       driver-class-name: com.microsoft.sqlserver.jdbc.SQLServerDriver
#   jpa:
#       database-platform: org.hibernate.dialect.SQLServer2012Dialect
#       database: SQL_SERVER
#       openInView: false
#       show_sql: false
#       generate-ddl: false
#       hibernate:
#           ddl-auto: none
#           naming-strategy: org.hibernate.cfg.EJB3NamingStrategy
#       properties:
#           hibernate.cache.use_second_level_cache: false
#           hibernate.cache.use_query_cache: false
#           hibernate.generate_statistics: false
#           hibernate.cache.region.factory_class:
org.hibernate.cache.ehcache.SingletonEhCacheRegionFactory
    cache:
        jcache:
            config: ehcache.xml

    thymeleaf:
```

```
        mode: XHTML
        cache: true

    mail:
        host: mail.tblab.frox.com
        port: 25
        user: TBTech
        password: ******
        from: TBTech@DEVCONNECT.COM
        protocol: smtp
        tls: false
        auth: false

metrics:
    jmx.enabled: true
    graphite:
        enabled: false
        host: localhost
        port: 2003
        prefix: test

elasticsearch:
    host: 127.0.0.1
    port: 9300
    adminPort: 9200
    clusterName: elasticsearch
Talkbase:
    presence: none
    callForwarding: avaya

talkbase:
    ui:
        company:
            toolbar_logo:   # Absolute path to custom company logo (i.e. D:/toolbar-logo.jpg,
JPG/JPEG formats are supported, preferred size - 30 x 30) that display on the main screen in the
bar at the bottom of the screen left to the Talkbase logo
            login_logo:     # Absolute path to custom logo (i.e. D:/login-logo.jpg, JPG/JPEG
formats are supported, preferred size - 75 x 75) that should display on the login screen near
Talkbase logo
    sites:
        configuration:
            path: ../sitesConfiguration          # Path to Talkbase tenant sites configuration
file
            file: sites-config.json              # The name of the Talkbase tenant sites
configuration file
    telephony:
        vendor: avaya                       # Possible values: skype_for_business, cisco, avaya,
cloud_pbx, innovaphone
        pbx: 10.64.110.212                            # Comma-separated list of FQDNs or IP
adresses of one or more PBXes to which talkbase can connect (empty for Skype for Business)
        sipdomain: avaya.com                # SIP domain to be used for outgoing calls
    search:
        path: ../elasticsearch                # Path to the Elastic Search Engine
    security:
        domain: DEVCONNECT.COM                     # Active Directory Domain
        ldap:
            globalCatalogPort: 3268           # default(3268)  for SSL (3269)  Active Directory
Search Port (Global Catalog)
            ldapPort: 389                     # default(389)  for SSL (636)
            prefix: ldap                      # ldaps for SSL
            adFQDN:                           # If this property is set it will be taken as the
FQDN of your Active Directory server
            account:
                user: TBTech           # Technical Active Directory Username
                password: ******   # Password of the technical AD user
        lyncserver:
            domain: DEVCONNECT.COM                   # Domain of the Skype for Business Server
            sipdomain: DEVCONNECT.COM             # Used for autodiscovering Skype for Business
(lyncdiscoverinternal must be defined in DNS)
            techauth_use_domain: true
```

```
            mediation_server:                   # Pool FQDN of the mediation server; leave empty
to let talkbase autodiscover it
            account:
                user: TBTech           # Technical user to use for Skype for Business
Authentication
                password: ******   # Password of the technical user
            localurl: localhost                 # Should be the local host IP address
            port: 5074                          # Configured Skype for Business SIP server port
            allowInsecureConnection: true # This property is needed if there's no valid
certificate for https
        xmppserver:
            enabled: false
            host: 0.0.0.0                 # FQDN of the presence server
            port: 5222                          # XMPP port (default: 5222)
            serviceName: DEVCONNECT.COM           # presence domain as configured on the presence
server (everything after @)
            iMUserFormat: pbxUser               #pbxUser or phoneNumber
            autodiscoverDomain: DEVCONNECT.COM    # used for autodiscover if empty the security
domain is fallback
            iMKeyField: email_address           # Which DB field contains the IM & Presence
Usernames? Default: ad_username Possible values: ad_username, user_principal_name, email_address,
sip_address, jabber_id, im_username
            adPresenceKey: email                # Which AD field contains the IM & Presence
Usernames of Operator? Default: sAMAccountName
            useAvayaPresenceSymbols: false
            account:
                user: username               # id of the XMPP user (Cisco End User or Avaya
presence user )
                password: ******       # password of XMPP user
            resource: Talkbase                  # Informational name of the talkbase resource
            reconnectionDelay: 120    # fixed delay in seconds between the XMPP reconnection
attempts
            connectionRetryDelay: 60  # fixed delay in seconds for establishing XMPP connection
if initial was failed
            replyTimeout: 3000        # number of milliseconds to wait for a response from the
XMPP server
            fixedRateToActualizeRoster: 300000 # fixed period in milliseconds between invocations
        sipphonestatus:                         #Used for Cisco and Avaya
            host: 10.64.110.212                        # FQDN of the Cisco Unified Communication
Manager or the Avaya Session Manager SIP Entity
            domain: avaya.com                # The SIP domain used for phones
            clientport: 5065                    # The talkbase side SIP port on which talkbase
will listen for status changes, default 5065
            serverport: 5060                    # The PBX side SIP port to use for phone status
subscriptions, default 5060
            account:
                username: 70110     # User name of technical user configured on the PBX
                password: ****** # Password of the technical user
            phonefields: phone # Which db fields should be considered for phoneStatus (order
matters)  example : phone, phone2, phone3, mobile
        sippresence:                            # Used for Innovaphone
            host: 10.64.110.212                        # FQDN or IP address of the PBX
            clientport: 5065                    # Port to be used on the talkbase server (default
5065)
            serverport: 5060                    # Port to be used on the PBX (default 5060)
            iMKeyField: ad_username             # Which DB field contains the IM & Presence
Usernames? Default: ad_username Possible values: ad_username, user_principal_name, email_address,
sip_address, jabber_id, im_username, phone
            account:
                username: TBTech       # User name of technical user configured on the PBX
                password: ******   # Password of the technical user
        jtapi:
            host: 10.64.110.212                        # FQDN of the Cisco Unified Communication
Manager
            account:
                user:     # User name of the technical application user (this is an Application
User on the CUCM)
                password:  # Password of the technical application user
        sipwebrtc:
            realm: 10.64.110.212                       # FQDN of the PBX
```

```
            domain: DEVCONNECT.COM                # Domain to use for WebRTC, phone numbers will
be composed like <phoneNumber>@<domain>
            websocket:
            - wss://W2019SVR.DEVCONNECT.COM:10060;ws:10061;udp:10061;c2c:10062;c2cs:10063
            - wss://W2019SVR.DEVCONNECT.COM:10065;ws:10066;udp:10066;c2c:10067;c2cs:10068
            - wss://W2019SVR.DEVCONNECT.COM:10070;ws:10071;udp:10071;c2c:10072;c2cs:10073
            - wss://W2019SVR.DEVCONNECT.COM:10075;ws:10076;udp:10076;c2c:10077;c2cs:10078
            - wss://W2019SVR.DEVCONNECT.COM:10080;ws:10081;udp:10081;c2c:10082;c2cs:10083
            - wss://W2019SVR.DEVCONNECT.COM:10085;ws:10086;udp:10086;c2c:10087;c2cs:10088
            - wss://W2019SVR.DEVCONNECT.COM:10090;ws:10091;udp:10091;c2c:10092;c2cs:10093
            - wss://W2019SVR.DEVCONNECT.COM:10095;ws:10096;udp:10096;c2c:10097;c2cs:10098
            - wss://W2019SVR.DEVCONNECT.COM:10100;ws:10101;udp:10101;c2c:10102;c2cs:10103
            - wss://W2019SVR.DEVCONNECT.COM:10105;ws:10106;udp:10106;c2c:10107;c2cs:10108
            - wss://W2019SVR.DEVCONNECT.COM:10110;ws:10111;udp:10111;c2c:10112;c2cs:10113
            - wss://W2019SVR.DEVCONNECT.COM:10115;ws:10116;udp:10116;c2c:10117;c2cs:10118
            - wss://W2019SVR.DEVCONNECT.COM:10120;ws:10121;udp:10121;c2c:10122;c2cs:10123
            - wss://W2019SVR.DEVCONNECT.COM:10125;ws:10126;udp:10126;c2c:10127;c2cs:10128
            - wss://W2019SVR.DEVCONNECT.COM:10130;ws:10131;udp:10131;c2c:10132;c2cs:10133
            - wss://W2019SVR.DEVCONNECT.COM:10135;ws:10136;udp:10136;c2c:10137;c2cs:10138
            - wss://W2019SVR.DEVCONNECT.COM:10140;ws:10141;udp:10141;c2c:10142;c2cs:10143
            - wss://W2019SVR.DEVCONNECT.COM:10145;ws:10146;udp:10146;c2c:10147;c2cs:10148
            - wss://W2019SVR.DEVCONNECT.COM:10150;ws:10151;udp:10151;c2c:10152;c2cs:10153
            - wss://W2019SVR.DEVCONNECT.COM:10155;ws:10156;udp:10156;c2c:10157;c2cs:10158
            - wss://W2019SVR.DEVCONNECT.COM:10160;ws:10161;udp:10161;c2c:10162;c2cs:10163
            - wss://W2019SVR.DEVCONNECT.COM:10165;ws:10166;udp:10166;c2c:10167;c2cs:10168
            - wss://W2019SVR.DEVCONNECT.COM:10170;ws:10171;udp:10171;c2c:10172;c2cs:10173
            - wss://W2019SVR.DEVCONNECT.COM:10175;ws:10176;udp:10176;c2c:10177;c2cs:10178
            - wss://W2019SVR.DEVCONNECT.COM:10180;ws:10181;udp:10181;c2c:10182;c2cs:10183
            - wss://W2019SVR.DEVCONNECT.COM:10185;ws:10186;udp:10186;c2c:10187;c2cs:10188
            - wss://W2019SVR.DEVCONNECT.COM:10190;ws:10191;udp:10191;c2c:10192;c2cs:10193
            - wss://W2019SVR.DEVCONNECT.COM:10195;ws:10196;udp:10196;c2c:10197;c2cs:10198
            - wss://W2019SVR.DEVCONNECT.COM:10200;ws:10201;udp:10201;c2c:10202;c2cs:10203
            - wss://W2019SVR.DEVCONNECT.COM:10205;ws:10206;udp:10206;c2c:10207;c2cs:10208
            - wss://W2019SVR.DEVCONNECT.COM:10210;ws:10211;udp:10211;c2c:10212;c2cs:10213
            - wss://W2019SVR.DEVCONNECT.COM:10215;ws:10216;udp:10216;c2c:10217;c2cs:10218
            - wss://W2019SVR.DEVCONNECT.COM:10220;ws:10221;udp:10221;c2c:10222;c2cs:10223
            - wss://W2019SVR.DEVCONNECT.COM:10225;ws:10226;udp:10226;c2c:10227;c2cs:10228
            - wss://W2019SVR.DEVCONNECT.COM:10230;ws:10231;udp:10231;c2c:10232;c2cs:10233
            outboundProxy: udp://10.64.110.212:5060                # FQDN of the PBX
    atiras:
        atiras_interface_enabled: false
        host: <atiras_server_fqdn_or_ip_address>
        port: 8089
    ivr:
        audioContainer: C:/Talkbase/IVR/Container/prompt/ulaw       # do not change, setup
installs the files there
        audioSubPath: talkbase                                          # do not change, setup
installs the files there
        audioQueueContainer: C:/Talkbase/IVR/Container/queue/ulaw   # do not change, setup
installs the files there
    servicenumber:
        soundContainer: ../sounds                                       # do not change, setup
installs the files there
    licencing:
        path: ../licence                                                # do not change, setup
installs the files there
        file: talkbase-licence.dat                                      # the name of the
talkbase license file
    exchange:
        enabled: true                                                   # true or false, if true,
exchange is connected at startup
        url: #https://exchangeserver.contoso.com/EWS/Exchange.asmx
        proxy:
            url:
            domain:
            port:
            user:
            password:
        account:
            domain: DEVCONNECT.COM
            user: TBTech
```

```
            password: ******
            email: TBTech@DEVCONNECT.COM
        timewindow: 30 # in days (max 41)
        amountOfEvents: 15
        timeout: 100000 # milliseconds
    exchange_online:
        enabled: false
        client_id:
        client_secret:
        tenant_id:
        eMail_domains:
            - frox.ch
            - frox.com
    ldap:
        configuration_folder_path: C:\Talkbase\LdapConfiguration
        page_size: 1000
        schedule: 0 0 1 ? * *
        use_change_notifications: false
    csvImport:
        location: C:\Talkbase\CsvFiles
        charSet:
        numberOfBCKs: 5
        schedule: 0 10 2 * * *
        delimiterChar: ';'
        enclosingChar: '"'
        dateFormat: 'dd.MM.yyyy HH:mm:ss'
        supportedFileTypes: csv
    logCleanup:
        logDirectories:
            - C:\Talkbase\Logs
            - C:\Talkbase\apache-tomcat\logs
            - C:\Talkbase\elasticsearch\logs
        deleteAfterDays: 30
        taskSchedule: 0 0 1 * * *
    voicerecording:
        voiceRecordingDirectory: C:\Talkbase\WebRTC\RecordedCalls
        deleteMarkedCallsAfterDays: 7
        deleteUnmarkedCallsAfterDays: 0
        cleanup:
            schedule: 00 30 1 * * *
    innovaphone:
        username: TBTech
        password: ******
        userkey: ad_username             # Default: ad_username Possible values: ad_username,
user_principal_name, email_address, sip_address, jabber_id, im_username
        host:
    avaya:
        callforwarding:
            aesServer: https://10.64.110.247                                # The FQDN of the
Avaya AES Server
            username: TBTech                                # The CM user (must be able to access
SAT
            password: ******                            # The CM user password
            request.timeout: 5000
    breather:
            extendDuration: 10           # amount of seconds the breather will be extended by
            maxExtensionsCount: 3        # amount of times the breather can be extended

cache:
    timeToLiveSeconds: 3600
    ehcache:
        maxBytesLocalHeap: 512M
        directoryEntryImages:
              maxSizeMemory: 256
              maxSizeDisk: 1024
              timeToLiveInCache: 3600
        audioFiles:
              maxSizeMemory: 128
              maxSizeDisk: 1024
              timeToLiveInCache: 3600
```

```
attendantStatistics:                                                    # do not change, it is
installed like this by AttendantStatisticsSetup.exe
    enabled: false
    datasource:
        dataSourceClassName: org.postgresql.ds.PGSimpleDataSource
        url: jdbc:postgresql://localhost:5431/AttendantStatistics
        databaseName:
        serverName:
        username: postgres
        password: ******
        maximumPoolSize: 10
    jpa:
        database-platform: com.noser.hunter.common.util.FixedPostgreSQL82Dialect
        database: POSTGRESQL
        show-sql: false

subscription:
    polling: # not for exchange online
        schedule: 0 * * * * *
    favorites:
        polling:
            schedule: 0 */5 * * * *
```

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 Dev*Connec*t Program at devconnect@avaya.com.