



## Avaya Solution & Interoperability Test Lab

---

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

### **Abstract**

These Application Notes describe the configuration steps required to integrate FROX AG talkbase with Avaya Aura® Communication Manager using a SIP connection to 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 R8.1 using a SIP connection to Avaya Aura® Session Manager R8.1. 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.

talkbase is a web-based attendant console which works with a number of telephony platforms including Communication Manager and Session Manager. talkbase is a replacement for an older attendant console called Atiras. The new solution is built with technologies like Spring, Java 8, HTML5, AngularJS and it uses WebRTC as operator phones, while communicating with SIP (Trunk). Also, it interfaces with Active Directory, Presence and Exchange servers.

## 2. General Test Approach and Test Results

The general test approach evaluated the ability of the talkbase to communicate with Communication Manager by registering as a SIP user and utilizing the SIP trunk to route calls.

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, as it does not include any user management of its own. One user account is required per operator, along with one phone device to be used as WebRTC device by the operator console. While the talkbase server internally calls these WebRTC devices and operator consoles do automatically answer the calls from talkbase, they don't answer calls that are not announced by the talkbase server. That means that operators cannot receive private calls on their operator consoles.

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 Director controller otherwise there may be an issue with the trust of the certificates issued.

A SIP user was created for each talkbase Operator. Please note that Application Sequences must not be defined on these users. A SIP Entity was added on System Manager for the talkbase server and a dialplan was added to route calls to the Operator, this typically would be the “main number” of the company so that calls would be answered by one of more Operators at a reception.

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 the talkbase operator. Calls were never made to that SIP user directly only to the main number. The SIP user is configured without any Application Sequences, these are purposely left blank.

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.

## 2.1. Interoperability Compliance Testing

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

- talkbase attendant is used to login/logout Operators.
- talkbase attendant is used to make/receive basic calls.
- talkbase attendant is used to receive PSTN calls.
- talkbase attendant is used to hold/transfer/forward calls.
- Serviceability testing by simulating LAN failures.

The serviceability testing focused on verifying the ability of the talkbase solution to recover from adverse conditions, such as power failures and network disconnects.

## 2.2. Test Results

All test cases were executed and verified. All test cases passed successfully.

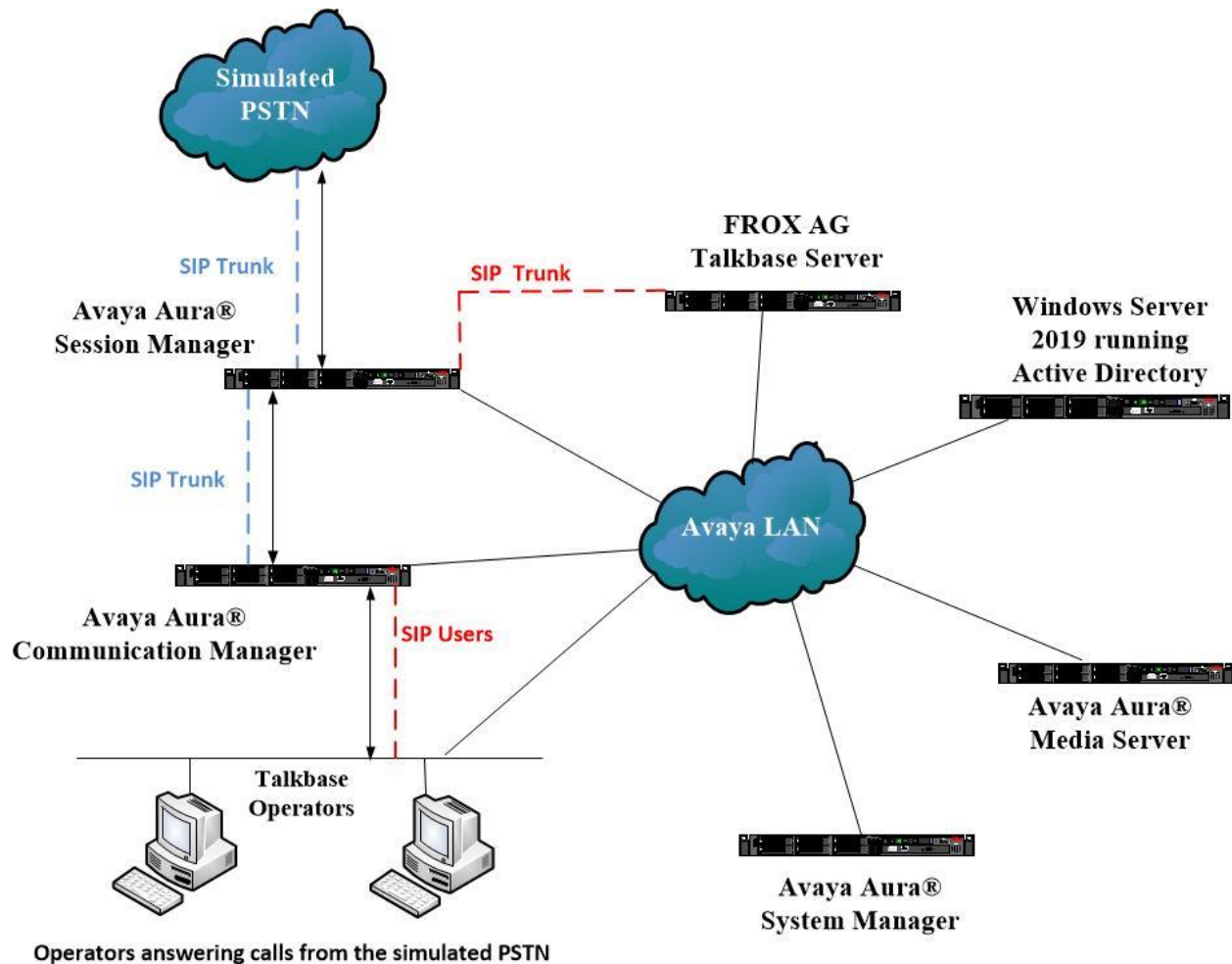
## 2.3. Support

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

- **Phone:** +41 55 254 12 54/89
- **Email:** [info@talkbase.com](mailto:info@talkbase.com)
- **Web:** <https://talkbase.com/en/>

### 3. Reference Configuration

**Figure 1** shows the network topology during compliance testing. The talkbase server was placed on the Avaya telephony LAN. Session Manager provides the talkbase SIP connection to Communication Manager. The talkbase operator 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 R8.1**

## 4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Media Server	Appliance Version R8.0.0.12 Media Server 8.0.0.169 Element Manager 8.0.0.169
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
FROX AG Equipment	Software / Firmware Version
FROX AG talkbase server	19.08
FROX AG talkbase Client Web Application	Chrome Version 76.0.3809.100

## 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 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- System Features and Access Codes
- 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 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	250
Maximum Concurrently Registered IP Stations:		18000	2
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>319</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	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
<b>ARS?</b>	<b>y</b>	Computer Telephony Adjunct Links?	y
<b>ARS/AAR Partitioning?</b>	<b>y</b>	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options		Page 5 of 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	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	
	<b>Uniform Dialing Plan? y</b>	
Private Networking? y	Usage Allocation Enhancements? y	

## 5.2. System Features and Access Codes

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 10** for supporting documentation.

display system-parameters features		Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled? n		
<b>Trunk-to-Trunk Transfer: all</b>		
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		

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

display feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:		
Attendant Access Code:		
<b>Auto Alternate Routing (AAR) Access Code: 8</b>		
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>		
Automatic Callback Activation: *25		Access Code 2: Deactivation: #25

### 5.3. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM81vmpg**). 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
                                IP NODE NAMES
      Name                      IP Address
AMS81vmpg                     10.10.40.61
G450                          10.10.40.14
IPOffice                      10.10.40.25
SM81vmpg                     10.10.40.32
SM_Oceana                    10.10.41.26
aes81vmpg                    10.10.40.38
default                       0.0.0.0
procr                        10.10.40.37

( 16 of 18  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 configured to match the domain name configured on Session Manager. In this configuration, the domain name is **devconnect.local**. 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
                                IP NETWORK REGION
      Region: 1
Location: 1      Authoritative Domain: devconnect.local
      Name: Default region
MEDIA PARAMETERS
      Codec Set: 1
      UDP Port Min: 2048
      UDP Port Max: 3329
      Intra-region IP-IP Direct Audio: yes
      Inter-region IP-IP Direct Audio: yes
      IP Audio Hairpinning? n
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
      H.323 Link Bounce Recovery? y
      Idle Traffic Interval (sec): 20
      Keep-Alive Interval (sec): 5
      Keep-Alive Count: 5
      RSVP Enabled? n
```

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to talkbase. 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), **G.711MU** (mu-law) and **G729A** which are supported by talkbase

**Media Encryption** is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any extension not capable of handling encryption.

display ip-codec-set 1				Page 1 of 2
IP MEDIA PARAMETERS				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	
1: <b>G.711A</b>	n	2	20	
2: <b>G.711MU</b>	n	2	20	
3: <b>G.729A</b>	n	2	20	
4:				
<b>Media Encryption</b>		Encrypted SRTCP: enforce-unenc-srtcp		
1:	<b>1-srtp-aescm128-hmac80</b>			
2:	<b>none</b>			
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 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 **SM81vmpg**), also shown above.
- Ensure that the recommended TLS port value of **5061** 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**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region.
- 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 get setup directly between talkbase and the caller.
- The default values for the other fields may be used.

**Note:** These were the 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 2
SIGNALING GROUP		
Group Number: 1	<b>Group Type: sip</b>	
IMS Enabled? n	<b>Transport Method: tls</b>	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
<b>Peer Detection Enabled? y</b>	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		
<b>Near-end Node Name: procr</b>	<b>Far-end Node Name: SM81vmpg</b>	
<b>Near-end Listen Port: 5061</b>	<b>Far-end Listen Port: 5061</b>	
	<b>Far-end Network Region: 1</b>	
<b>Far-end Domain: devconnect.local</b>		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
<b>DTMF over IP: rtp-payload</b>	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	<b>Direct IP-IP Audio Connections? y</b>	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	<b>Initial IP-IP Direct Media? y</b>	
	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	<b>Group Type: sip</b>	CDR Reports: y
Group Name: talkbase	COR: 1	TN: 1 <b>TAC: *812</b>
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
<b>Service Type: tie</b>	Auth Code? n	
	Member Assignment Method: auto	
	<b>Signaling Group: 12</b>	
	<b>Number of Members: 10</b>	

On **Page 3** of the trunk-group form the **Numbering Format** was set to **private** and the **UII Treatment** was set to **shared**. The rest of the fields were set as shown.

change trunk-group 12	Page 3 of 5
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: private</b>
	<b>UII Treatment: shared</b>
	Maximum Size of UII Contents: 128
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Send UCID? y	
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	
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	

## 5.4. Administer Call Routing

It was decided to assign a range of numbers to the Attendant as main numbers, where the Communication Manager users can dial to or the PSTN can call. For compliance testing the range of numbers used was 1550 to 1559 and 1555 and 1556 were used specifically during testing. The basis is to route calls 155x 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 *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, Route Pattern Number **12** is used to route calls to trunk group (**Grp No**) **12**, this is the SIP Trunk configured in **Section 5.3**. The **Numbering Format** was set to **lev0-pvt**.

change route-pattern 12															Page 1 of 3	
Pattern Number: 1 Pattern Name: Talkbase																
SCCAN? n Secure SIP? n Used for SIP stations? n																
<b>Grp</b> FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC																
<b>No</b> 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 <b>Numbering</b> LAR																
0 1 2 M 4 W Request Dgts <b>Format</b>																
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

### 5.4.2. Configure Uniform Dialplan

It was decided for compliance testing that all calls to the “Attendant” were calls that began with **155x** and these were to be sent across the SIP trunk to Session Manager and then onto talkbase. To achieve this routing, Automatic Alternate Routing (AAR) will be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this routing.

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to **155x** will use Automatic Alternate Routing (AAR). No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 6						Page 1 of 2	
UNIFORM DIAL PLAN TABLE							
Percent Full: 0							
Matching			Insert			Node	
Pattern	Len	Del	Digits	Net	Conv	Num	
155	4	0		aar	n		
					n		
					n		
					n		
					n		
					n		

### 5.4.3. Configure Automatic Alternate Routing

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to the ‘Attendant’ are achieved by dialing **155x** (calls from 1550 to 1559) and are matched with the **Dialed String** entry shown below. Calls are sent to **Route Pattern 12**, configured in **Section 5.4.1**, which contains the SIP Trunk Group to talkbase.

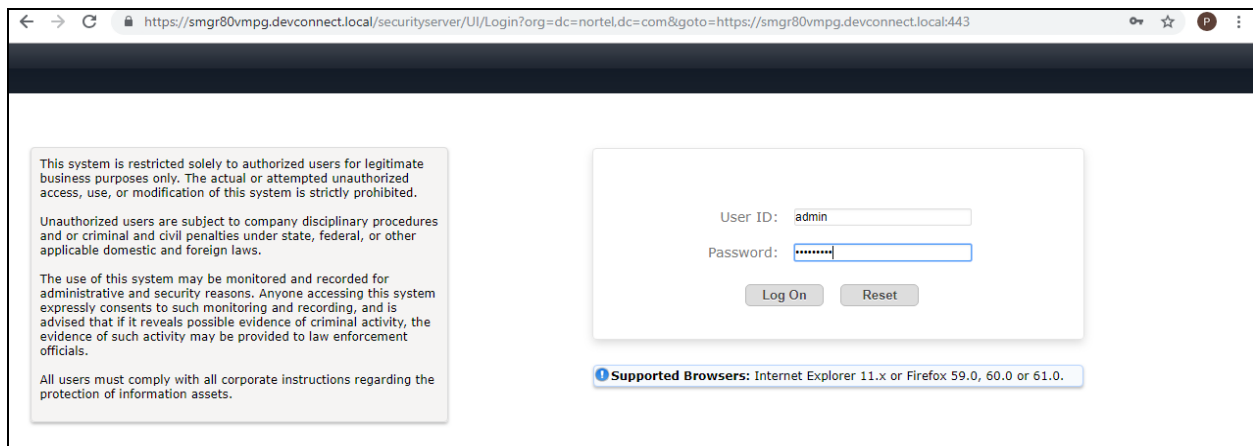
change aar analysis 1						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 3		
Dialed String	Total		Route	Call	Node	ANI	
	Min	Max	Pattern	Type	Num	Reqd	
155	4	4	12	lev0		n	
3	4	4	1	aar		n	
65	4	4	1	aar		n	
7	7	7	254	aar		n	
8	7	7	254	aar		n	
9	7	7	254	aar		n	
						n	
						n	
						n	
						n	

## 6. Configure Avaya Aura® Session Manager

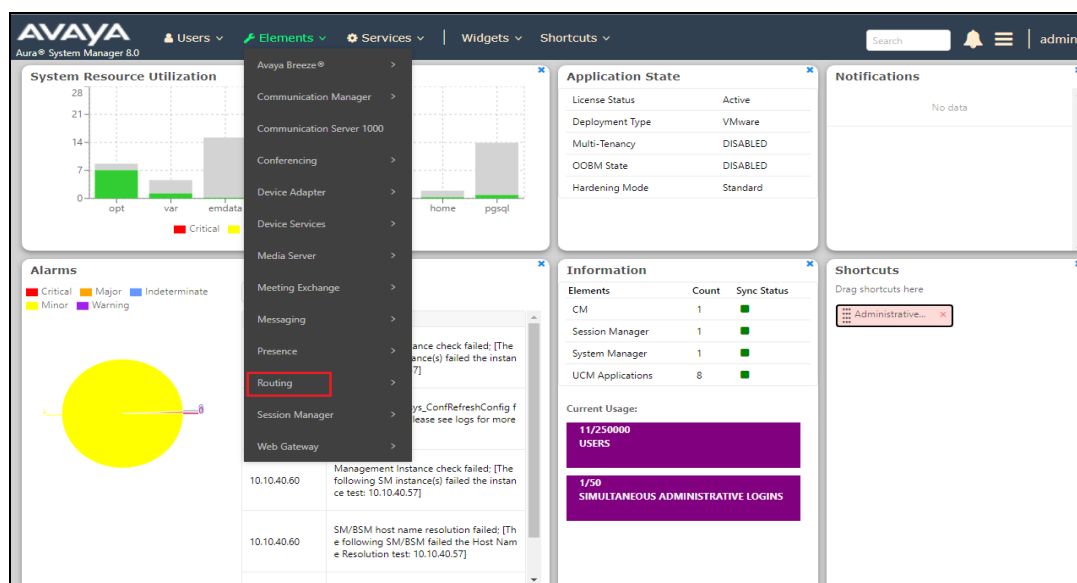
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern

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** highlighted below.

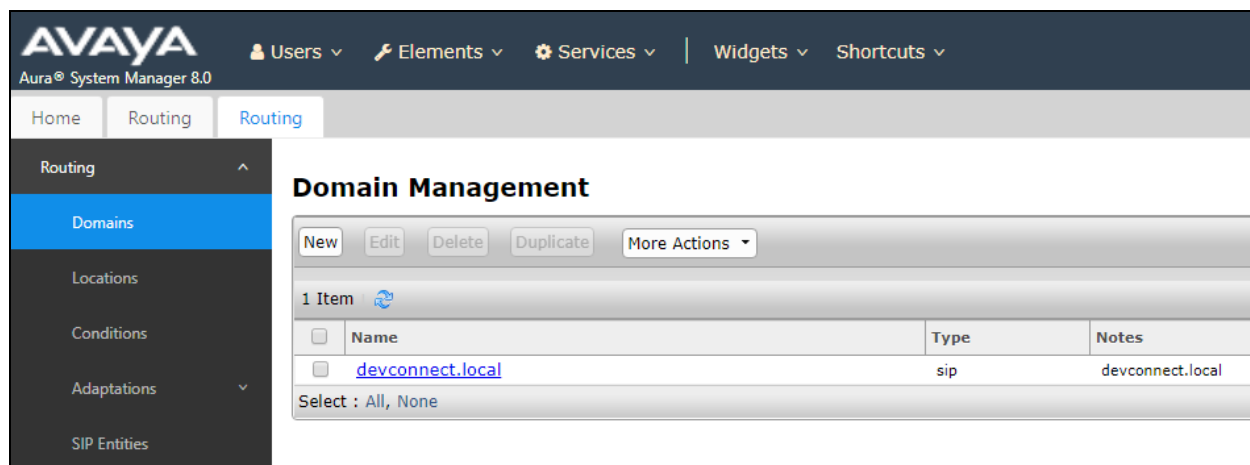


## 6.1. Domains and Locations

**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.

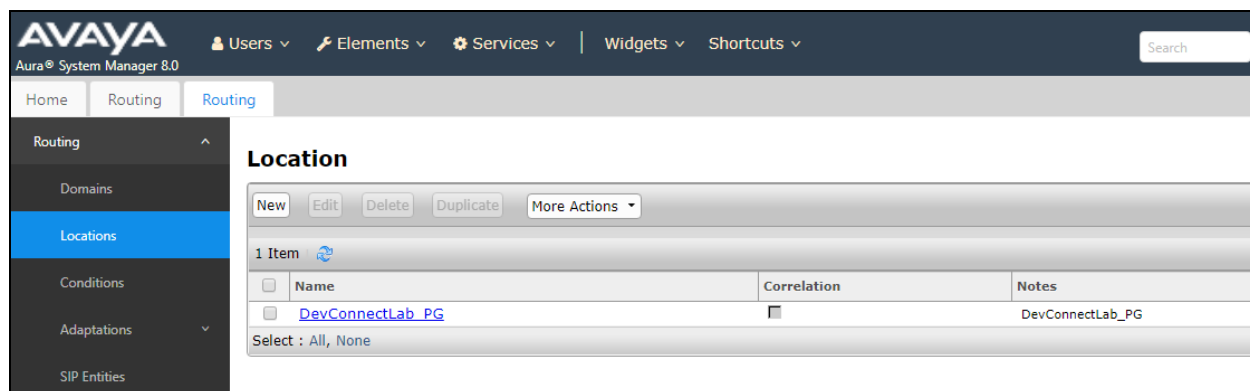
### 6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** 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

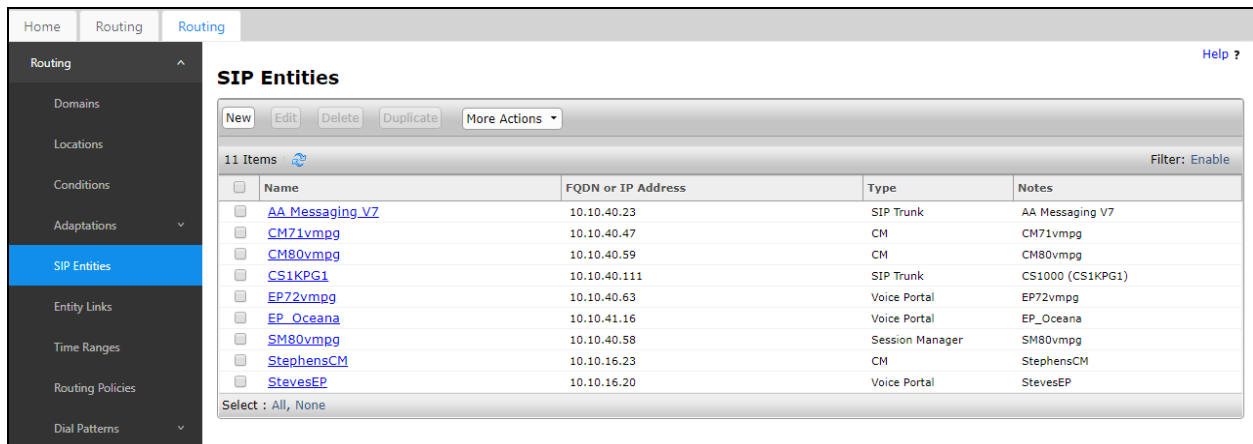
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab\_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click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



## 6.2. Configure talkbase SIP Entity

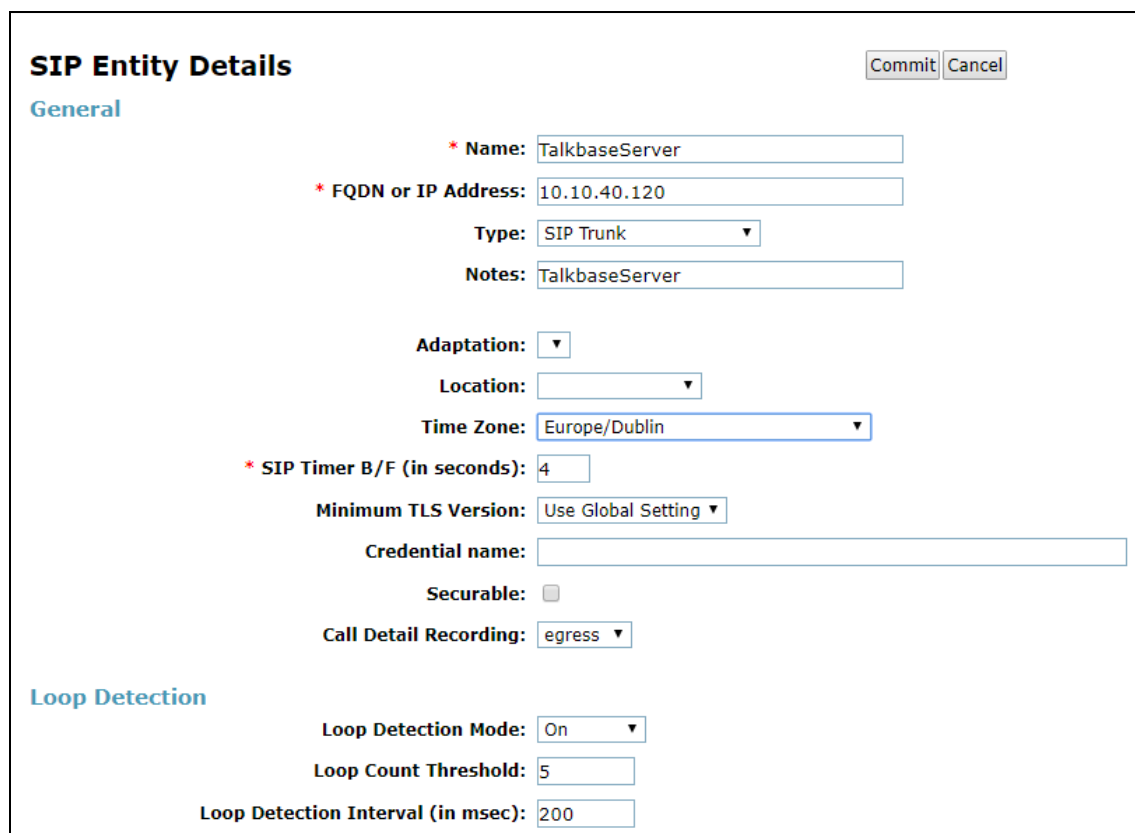
Each SIP device (other than Avaya SIP phones) that communicates with Session Manager requires a SIP Entity and Entity Link configuration.

Click on **SIP Entities** in the left column and select **New** in the right window.



Name	FQDN or IP Address	Type	Notes
AA Messaging VZ	10.10.40.23	SIP Trunk	AA Messaging V7
CM71vmppg	10.10.40.47	CM	CM71vmppg
CM80vmppg	10.10.40.59	CM	CM80vmppg
CS1KPG1	10.10.40.111	SIP Trunk	CS1000 (CS1KPG1)
EP72vmppg	10.10.40.63	Voice Portal	EP72vmppg
EP_Oceana	10.10.41.16	Voice Portal	EP_Oceana
SM80vmppg	10.10.40.58	Session Manager	SM80vmppg
StephensCM	10.10.16.23	CM	StephensCM
StevesEP	10.10.16.20	Voice Portal	StevesEP

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the talkbase server. Enter the correct **Time Zone** and **Location** and scroll down to SIP Entity Links.



**SIP Entity Details** [Commit] [Cancel]

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

\* SIP Timer B/F (in seconds):

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

**Loop Detection**

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

## 6.3. Configure talkbase SIP Entity Link

An Entity link can be added from the SIP Entities page. Using the page from the previous page scroll down to Entity Links.

Upon scrolling down to **Entity Links** click on **Add**.

The screenshot shows the 'Monitoring' section with the following settings:

- SIP Link Monitoring: Use Session Manager Configuration
- CRLF Keep Alive Monitoring: Use Session Manager Configuration
- Supports Call Admission Control: ☐
- Shared Bandwidth Manager: ☐
- Primary Session Manager Bandwidth Association: [Dropdown]
- Backup Session Manager Bandwidth Association: [Dropdown]

The 'Entity Links' section has the 'Override Port & Transport with DNS SRV' checkbox unchecked. Below it is a table with 0 items and a 'Filter: Enable' link. The table headers are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. Below the table is the 'SIP Responses to an OPTIONS Request' section, which also has 0 items and a 'Filter: Enable' link. The table headers for this section are: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created talkbase SIP Entity for **SIP Entity 2**. Ensure that **TCP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.

The screenshot shows the 'Entity Links' section with the 'Override Port & Transport with DNS SRV' checkbox unchecked. Below it is a table with 1 item and a 'Filter: Enable' link. The table headers are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The single item in the table is:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM81vmpg_TalkbaseServ	SM81vmpg	TCP	* 5060	TalkbaseServer	* 5060	trusted	<input type="checkbox"/>

Below the table is the 'SIP Responses to an OPTIONS Request' section, which has 0 items and a 'Filter: Enable' link. The table headers for this section are: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

## 6.4. Configure Routing Policy for talkbase

Click on **Routing Policies** in the left window and select **New** in the main window.

<input type="checkbox"/>	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	<a href="#">To AA Messaging V7</a>	<input type="checkbox"/>	0	AA Messaging V7	To AA Messaging V7
<input type="checkbox"/>	<a href="#">To ASCBE</a>	<input type="checkbox"/>	0	ASBCE8vmppg	To Session Border Controller
<input type="checkbox"/>	<a href="#">To Capita DMS</a>	<input type="checkbox"/>	0	Capita DMS	To Capita DMS
<input type="checkbox"/>	<a href="#">To Capita_DS3000</a>	<input type="checkbox"/>	0	Capita DS3000	To Capita DS3000
<input type="checkbox"/>	<a href="#">To_CM71vmppg</a>	<input type="checkbox"/>	0	CM71vmppg	To CM71vmppg
<input type="checkbox"/>	<a href="#">To_CM80vmppg</a>	<input type="checkbox"/>	0	CM80vmppg	To CM80vmppg
<input type="checkbox"/>	<a href="#">To_CS1KPG1</a>	<input type="checkbox"/>	0	CS1KPG1	To CS1KPG1
<input type="checkbox"/>	<a href="#">To_EP72vmppg</a>	<input type="checkbox"/>	0	EP72vmppg	To EP72vmppg
<input type="checkbox"/>	<a href="#">To_EP_Oceana</a>	<input type="checkbox"/>	0	EP_Oceana	To EP Oceana
<input type="checkbox"/>	<a href="#">To Stephens CM</a>	<input type="checkbox"/>	0	StephensCM	To StephensCM
<input type="checkbox"/>	<a href="#">To Steves EP</a>	<input type="checkbox"/>	0	StevesEP	To Steves EP

Select : All, None

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.

### Routing Policy Details

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Select the **TalkbaseServer** SIP Entity as shown below and click on **Select**.

**SIP Entities**

SelectCancel

**SIP Entities**

4 Items

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AAMessaging	10.10.40.23	Messaging	
<input type="radio"/>	cm81vmpg	10.10.40.37	CM	cm81vmpg
<input type="radio"/>	EP722	10.10.40.31	Voice Portal	EP722 and POM
<input checked="" type="radio"/>	TalkbaseServer	10.10.40.120	SIP Trunk	TalkbaseServer

Select : None

SelectCancel

The selected destination is now shown, click on **Commit** to save this.

**Routing Policy Details**

CommitCancel

**General**

\* Name:

To Talkbase

Disabled:

☐

\* Retries:

0

Notes:

To Talkbase

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
TalkbaseServer	10.10.40.120	SIP Trunk	TalkbaseServer

**Time of Day**

AddRemoveView Gaps/Overlaps

1 Item

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 6.5. Configure talkbase Dial Patterns

Select **Dial Patterns** in the left window and select **New** in the main window.

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
09173	9	9	<input type="checkbox"/>			-ALL-	To CM80vmpg from Syntec
2	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg
280	4	4	<input type="checkbox"/>			devconnect.local	To EP72vmpg
290	4	4	<input type="checkbox"/>			devconnect.local	To EP Oceana
30	4	4	<input type="checkbox"/>			devconnect.local	To CS1KPG1
351212455779	12	12	<input type="checkbox"/>			-ALL-	To SBC8 for Syntec
380	4	4	<input type="checkbox"/>			devconnect.local	To Steves EP
4	4	4	<input type="checkbox"/>			devconnect.local	To CM71vmpg
52	4	4	<input type="checkbox"/>			devconnect.local	To CM80Vmpg for simulated PSTN to IPO
6666	4	4	<input type="checkbox"/>			devconnect.local	To AA Messaging V7
7080	4	6	<input type="checkbox"/>			devconnect.local	To Capita DMS
8000	5	5	<input type="checkbox"/>			devconnect.local	To Capita DS3000
823	7	7	<input type="checkbox"/>			devconnect.local	To Stephens CM 823 000x

Enter the required digits for the Routing Pattern, in the example below **155** is used. This ensures that when 155x is dialled it will route to the talkbase server. Enter the appropriate domain for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating Locations and Routing Policies** to select this Routing Policy.

**Dial Pattern Details** [Commit] [Cancel]

**General**

\* Pattern: 155

\* Min: 4

\* Max: 4

Emergency Call: ☐

SIP Domain: devconnect.local ▼

Notes: To Talkbase

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item

Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination

Select : All, None

Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created Routing Policy for talkbase.

Originating Location

Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnectLab	DevConnectLab

Select : All, None

Routing Policies

4 Items

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AA Messaging V7	<input type="checkbox"/>	AAMessaging	To AA Messaging V7
<input type="checkbox"/>	To cm81xvmpg	<input type="checkbox"/>	cm81xvmpg	To cm81xvmpg
<input type="checkbox"/>	To EP722	<input type="checkbox"/>	EP722	To EP722
<input checked="" type="checkbox"/>	To Talkbase	<input type="checkbox"/>	TalkbaseServer	To Talkbase

Select : All, None

Select Cancel

With the Routing Policy selected click on **Commit** to finish adding the Dial Pattern.

Dial Pattern Details

Commit Cancel

General

\* Pattern: 155  
\* Min: 4  
\* Max: 4  
Emergency Call: ☐  
SIP Domain: devconnect.local  
Notes: To Talkbase

Originating Locations and Routing Policies

Add Remove
1 Item
Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnectLab	DevConnectLab	To Talkbase	0	<input type="checkbox"/>	TalkbaseServer	To Talkbase

Select : All, None

Denied Originating Locations

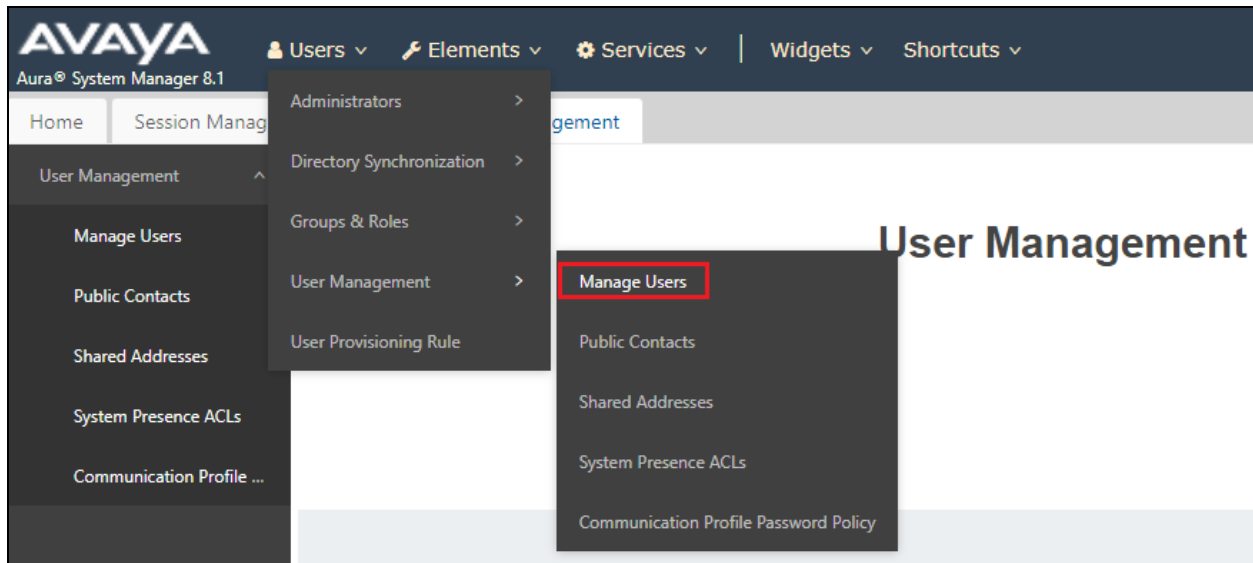
Add Remove
0 Items

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

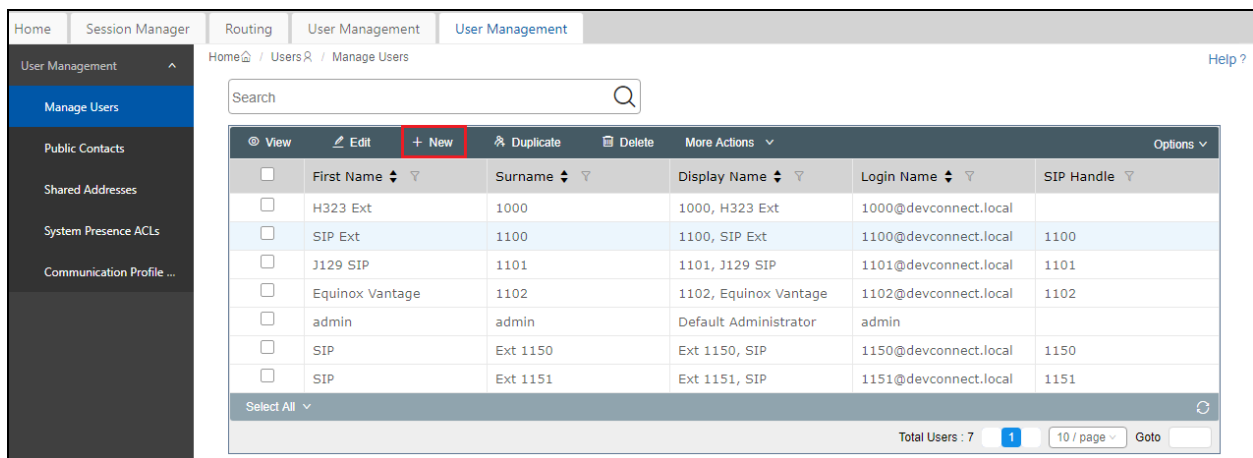
Commit Cancel

## 6.6. Configure SIP talkbase SIP User

Navigate to Users → User Management → Manager Users as shown below.



Select **New** highlighted, to add a new user.



Under the **Identity** tab, information on the user name is filled in.

User Profile | Edit | 1150@devconnect.local

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule :

\* Last Name : Ext 1150

\* First Name : SIP

\* Login Name : 1150@devconnect.local

Description : Talkbase User

Password :

Confirm Password :

Endpoint Display Name : Ext 1150, SIP

Language Preference : English (United States)

Employee ID : Employee Id Of User

Last Name (Latin Translation) : Ext 1150

First Name (Latin Translation) : SIP

Middle Name : Middle Name Of User

Email Address : Email Address Of User

User Type : Basic

Localized Display Name : Ext 1150, SIP

Title Of User : Title Of User

Time Zone : (+1:0)GMT : Dublin, Edin...

Department : Department Of User

Under the **Communication Profile** tab, the user's **Password** is filled in, this will be used in **Section 7.3**.

Identity Communication Profile Membership Contacts

Comm-Profile Password

Comm-Profile Password : .....

Re-enter Comm-Profile Password : ..... ✓

Generate Comm-Profile Password

Cancel OK

Click in **Communication Address** in the left window and add the SIP user information which should be the extension and the domain as shown below.

The screenshot shows a configuration window for 'Communication Address'. On the left, there's a sidebar with 'Communication Profile Password' and 'PROFILES' (Session Manager Profile, CM Endpoint Profile). The main area has a table with columns: Type, Handle, and Domain. There is one row with 'Avaya SIP', '1150', and 'devconnect.local'. At the bottom, it says 'Total: 1' and '10 / page'.

Type	Handle	Domain
Avaya SIP	1150	devconnect.local

Click on **Session Manager Profile** in the left menu and enter the Session Manager information as shown. Note that there are no **Application Sequences** configured for this user.

The screenshot shows the 'Session Manager Profile' configuration window. The left sidebar has 'Session Manager Profile' selected. The main area is titled 'SIP Registration' and contains fields for 'Primary Session Manager' (SM81vmpg), 'Secondary Session Manager' (Start typing...), 'Survivability Server' (Start typing...), 'Max. Simultaneous Devices' (1), and 'Block New Registration When Maximum Registrations Active?' (unchecked). Below this is the 'Application Sequences' section with 'Origination Sequence' and 'Termination Sequence' both set to 'Select'.

Click on **CM Endpoint Profile**, in the left window and note that the **9608SIP** template was used for the compliance testing. The default configuration was used for the station after that. Click on **Commit** to save the new user.

User Profile | Edit | 1150@devconnect.local

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

\* System :

cm81xvmpg

\* Profile Type :

Endpoint

Use Existing Endpoints :

\* Extension :

1150

Template :

9608SIP\_DEFAULT\_CM\_8\_1

\* Set Type :

9608SIP

Security Code :

Enter Security Code

Port :

IP

Voice Mail Number :

6666

Preferred Handle :

Select

Calculate Route Pattern :

Sip Trunk :

aar

SIP URI :

Select

Enhanced Callr-Info Display for 1-line phones :

Delete on Unassign from User or on Delete User :

Override Endpoint Name and Localized Name :

Allow H.323 and SIP Endpoint Dual Registration :

## 7. Configure FROX AG talkbase

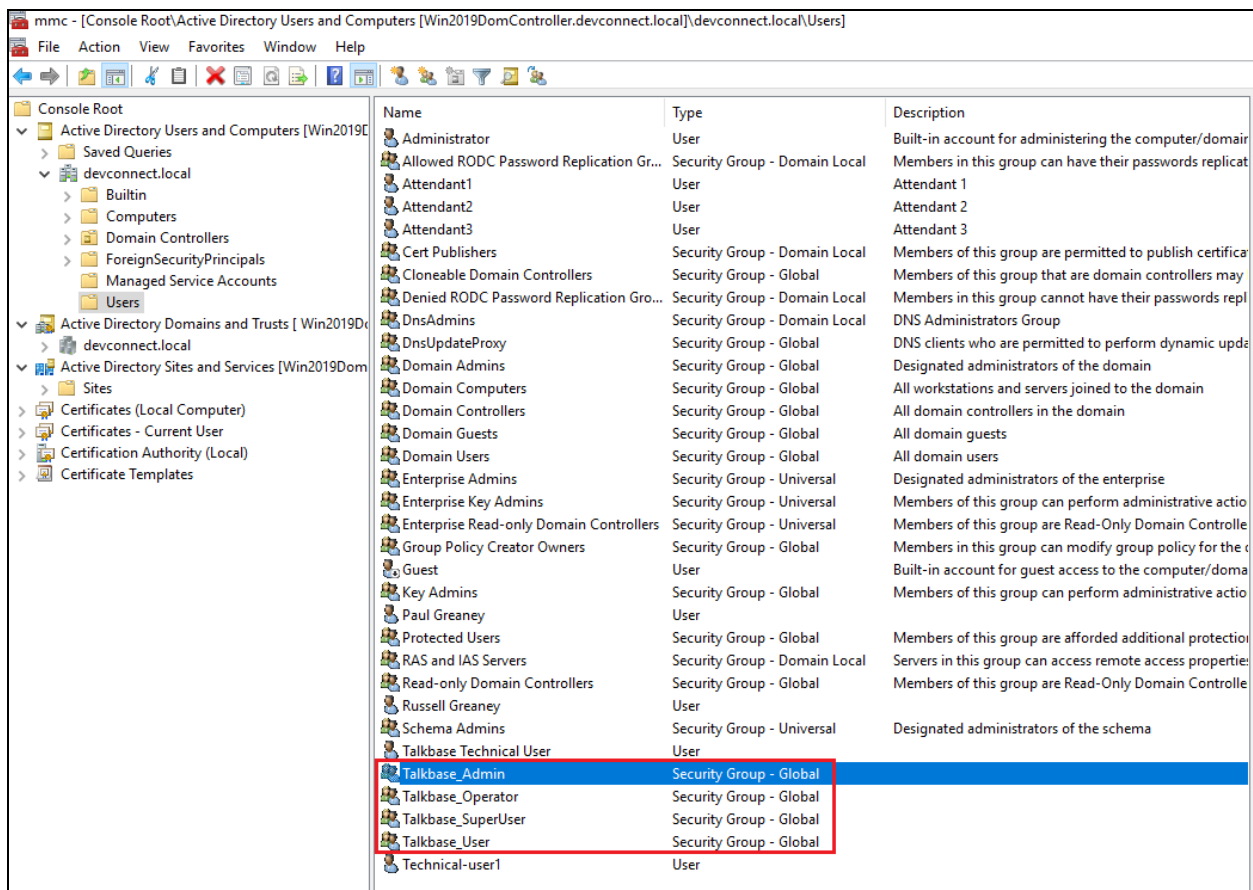
The configuration for talkbase to communicate with Session Manager is made both on the talkbase server directly and a GUI using a web connection to the server. talkbase is dependant on having a Windows domain already in place with Active Directory setup and running. The talkbase server along with the client PC's must all be a part of this domain. There is a certificate share between the talkbase server and the client PC's that can only take place if they are part of the same domain. talkbase users are synchronized with the Active Directory and again this must be part of the setup also.

### 7.1. Configure Active Directory for talkbase

The Active Directory must be configured for the following groups.

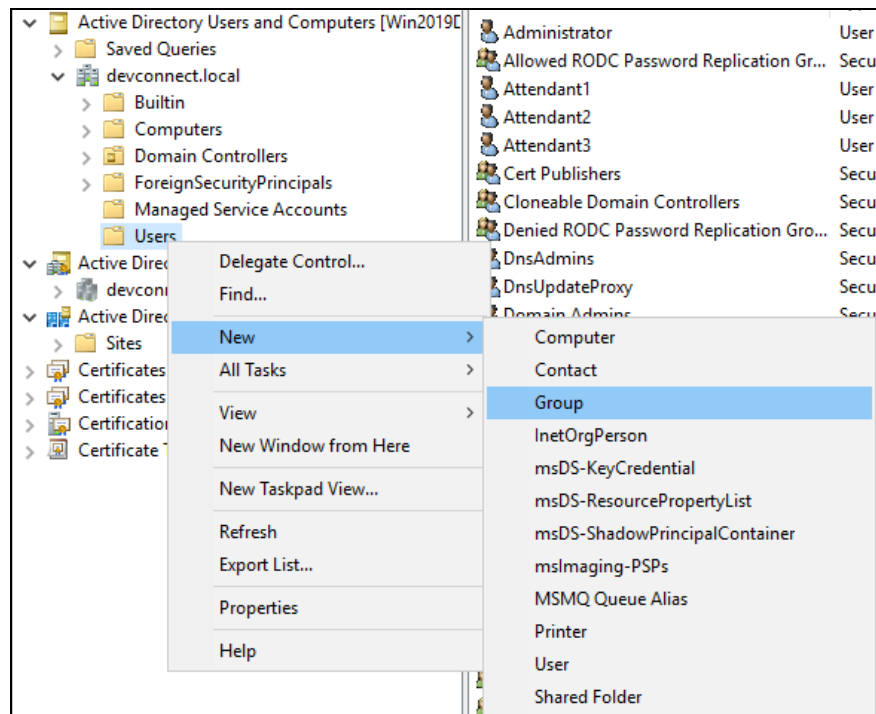
- **Talkbase\_Admin**
- **Talkbase\_Operator**
- **Talkbase\_SuperUser**
- **Talkbase\_User**

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.

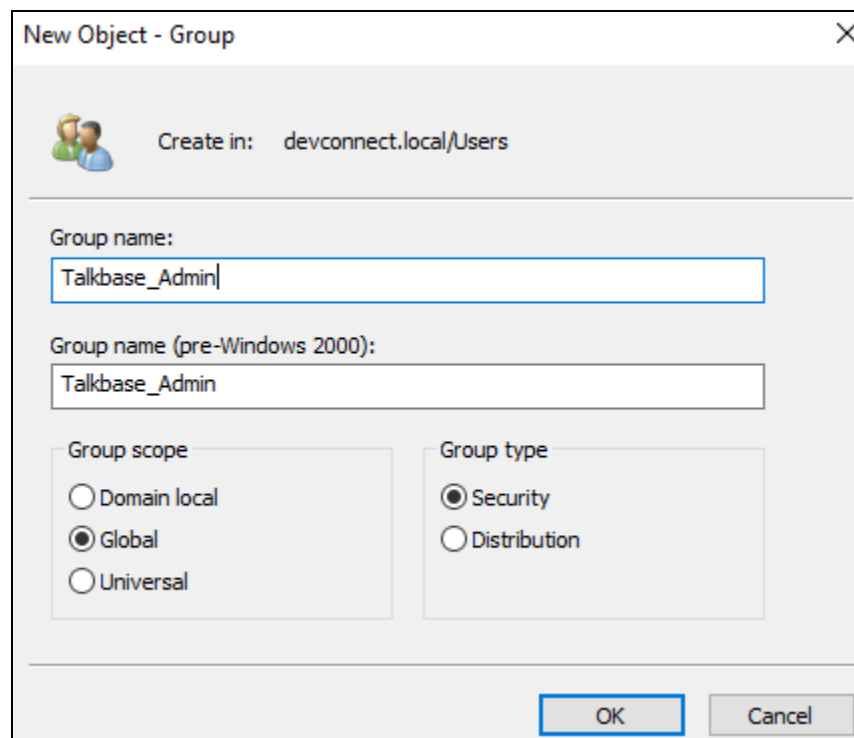


Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Gr...	Security Group - Domain Local	Members in this group can have their passwords replicat
Attendant1	User	Attendant 1
Attendant2	User	Attendant 2
Attendant3	User	Attendant 3
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certica
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may
Denied RODC Password Replication Gro...	Security Group - Domain Local	Members in this group cannot have their passwords repl
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic upda
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative actio
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controlle
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the c
Guest	User	Built-in account for guest access to the computer/doma
Key Admins	Security Group - Global	Members of this group can perform administrative actio
Paul Greaney	User	
Protected Users	Security Group - Global	Members of this group are afforded additional protection
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controlle
Russell Greaney	User	
Schema Admins	Security Group - Universal	Designated administrators of the schema
Talkbase Technical User	User	
Talkbase_Admin	Security Group - Global	
Talkbase_Operator	Security Group - Global	
Talkbase_SuperUser	Security Group - Global	
Talkbase_User	Security Group - Global	
Technical-user1	User	

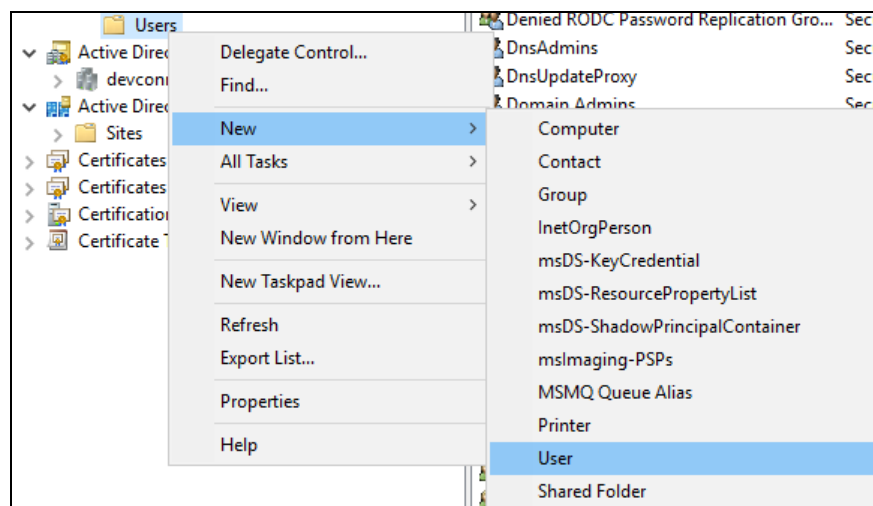
To add a new group, right-click on **Users** and select **New** and then **Group** as shown below.



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 **Attendant1** that was setup and used for testing. These are the users name details under the **General** tab.

A screenshot of the 'Attendant1 Properties' dialog box, specifically the 'General' tab. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Remote control', 'Remote Desktop Services Profile', 'COM+', 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'General', 'Address', 'Account', 'Profile', 'Telephones', and 'Organization'. The 'General' tab is selected. It features a user icon and the name 'Attendant1'. Below this are several text input fields: 'First name' (containing 'TBUser1'), 'Initials' (empty), 'Last name' (containing 'Frox'), 'Display name' (containing 'Attendant1'), 'Description' (containing 'Attendant 1'), and 'Office' (empty). At the bottom are fields for 'Telephone number' (containing '3150'), 'E-mail' (empty), and 'Web page' (empty). There are 'Other...' buttons next to the 'Telephone number' and 'Web page' fields. At the very bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

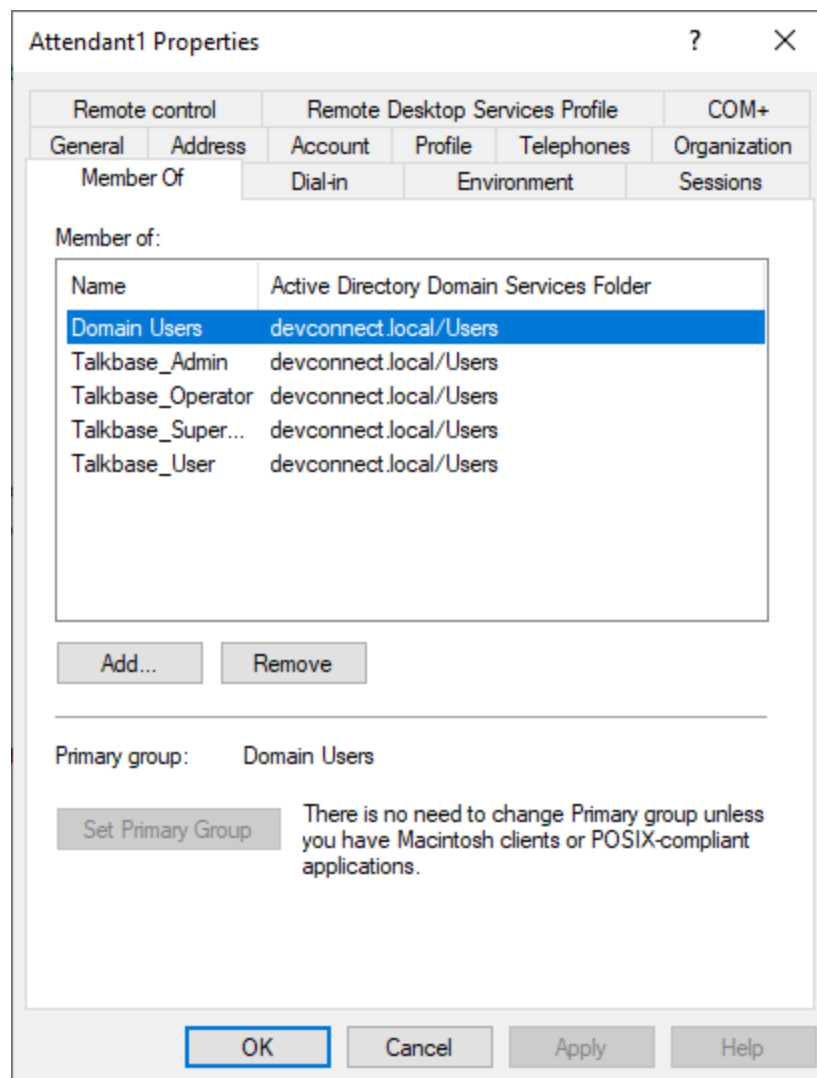
This is the account information under the **Account** tab.

The screenshot shows the 'Attendant1 Properties' dialog box with the 'Account' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with tabs for 'Remote control', 'Remote Desktop Services Profile', 'COM+', 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'General', 'Address', 'Account' (selected), 'Profile', 'Telephones', and 'Organization'. The 'Account' tab contains the following fields and options:

- User logon name:** A text box containing 'Attendant1' and a dropdown menu showing '@devconnect.local'.
- User logon name (pre-Windows 2000):** Two text boxes, the first containing 'DEVCONNECT\' and the second containing 'tuser1'.
- Logon Hours...** and **Log On To...** buttons.
- ☐ **Unlock account**
- Account options:** A list box containing four items:
  - ☐ User must change password at next logon
  - ☐ User cannot change password
  - ☒ Password never expires
  - ☐ Store password using reversible encryption
- Account expires:** A section with two radio buttons:   
- ☒ **Never**  
- ☐ **End of:** followed by a date picker showing 'Sunday 22 September 2019'.

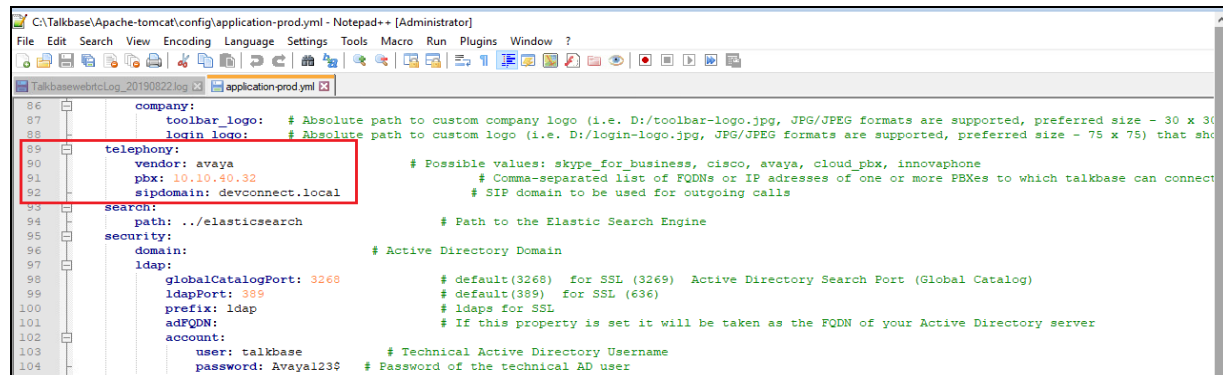
At the bottom of the dialog are four buttons: **OK**, **Cancel**, **Apply**, and **Help**.

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



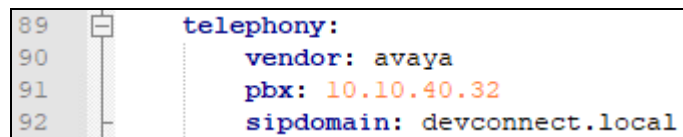
## 7.2. Configure talkbase server

Configuration of the talkbase server is made by amending a file called **application-prod.yml**. Navigate to **C:\Talkbase\Apache-tomcat\config** and edit the **application-prod.yml** file located in that config folder. Below shows an example of that file.



```
86     company:
87       toolbar logo: # Absolute path to custom company logo (i.e. D:/toolbar-logo.jpg, JPG/JPEG formats are supported, preferred size - 30 x 30)
88       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 be used for login
89     telephony:
90       vendor: avaya # Possible values: skype_for_business, cisco, avaya, cloud_pbx, innovaphone
91       pbx: 10.10.40.32 # Comma-separated list of FQDNs or IP addresses of one or more PBXes to which talkbase can connect
92       sipdomain: devconnect.local # SIP domain to be used for outgoing calls
93     search:
94       path: ../elasticsearch # Path to the Elastic Search Engine
95     security:
96       domain: # Active Directory Domain
97       ldap:
98         globalCatalogPort: 3268 # default(3268) for SSL (3269) Active Directory Search Port (Global Catalog)
99         ldapPort: 389 # default(389) for SSL (636)
100         prefix: ldap # ldaps for SSL
101         adFQDN: # If this property is set it will be taken as the FQDN of your Active Directory server
102         account:
103           user: talkbase # Technical Active Directory Username
104           password: Avaya1234 # Password of the technical AD user
```

Upon a closer look, the IP address of Session Manager is added for the **pbx** value and the **sipdomain** value is that of the domain configured in **Section 6.1.1**.



```
89     telephony:
90       vendor: avaya
91       pbx: 10.10.40.32
92       sipdomain: devconnect.local
```

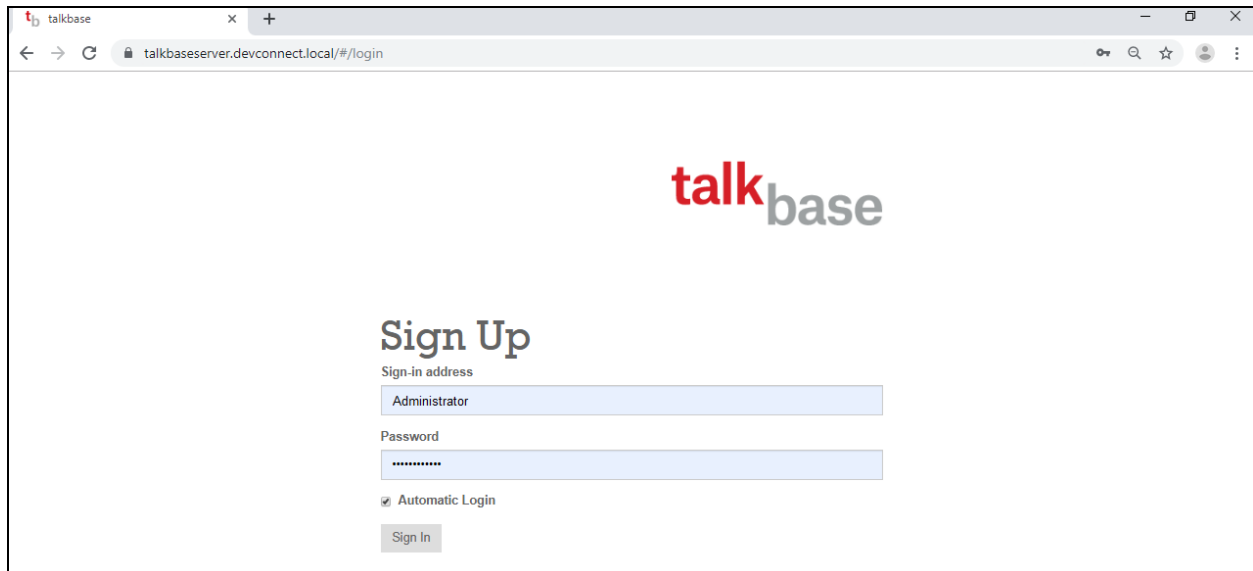
Further down the page information on the **sipwebrtc** is shown again including the Session Manager IP address along with the **outboundproxy** information.



```
sipwebrtc:
  realm: 10.10.40.32 # FQDN of the PBX
  domain: devconnect.local # Domain to use for WebRTC, phone numbers will be composed like <phoneNumber>@<domain>
  websocket:
    - wss://talkbaseserver.devconnect.local:10060/ws:10061:udp:10061:c2c:10062:c2cs:10063
    - wss://talkbaseserver.devconnect.local:10065/ws:10066:udp:10066:c2c:10067:c2cs:10068
    - wss://talkbaseserver.devconnect.local:10070/ws:10071:udp:10071:c2c:10072:c2cs:10073
    - wss://talkbaseserver.devconnect.local:10075/ws:10076:udp:10076:c2c:10077:c2cs:10078
    - wss://talkbaseserver.devconnect.local:10080/ws:10081:udp:10081:c2c:10082:c2cs:10083
    - wss://talkbaseserver.devconnect.local:10085/ws:10086:udp:10086:c2c:10087:c2cs:10088
    - wss://talkbaseserver.devconnect.local:10090/ws:10091:udp:10091:c2c:10092:c2cs:10093
    - wss://talkbaseserver.devconnect.local:10095/ws:10096:udp:10096:c2c:10097:c2cs:10098
    - wss://talkbaseserver.devconnect.local:10100/ws:10101:udp:10101:c2c:10102:c2cs:10103
    - wss://talkbaseserver.devconnect.local:10105/ws:10106:udp:10106:c2c:10107:c2cs:10108
    - wss://talkbaseserver.devconnect.local:10110/ws:10111:udp:10111:c2c:10112:c2cs:10113
    - wss://talkbaseserver.devconnect.local:10115/ws:10116:udp:10116:c2c:10117:c2cs:10118
    - wss://talkbaseserver.devconnect.local:10120/ws:10121:udp:10121:c2c:10122:c2cs:10123
    - wss://talkbaseserver.devconnect.local:10125/ws:10126:udp:10126:c2c:10127:c2cs:10128
    - wss://talkbaseserver.devconnect.local:10130/ws:10131:udp:10131:c2c:10132:c2cs:10133
    - wss://talkbaseserver.devconnect.local:10135/ws:10136:udp:10136:c2c:10137:c2cs:10138
    - wss://talkbaseserver.devconnect.local:10140/ws:10141:udp:10141:c2c:10142:c2cs:10143
    - wss://talkbaseserver.devconnect.local:10145/ws:10146:udp:10146:c2c:10147:c2cs:10148
    - wss://talkbaseserver.devconnect.local:10150/ws:10151:udp:10151:c2c:10152:c2cs:10153
    - wss://talkbaseserver.devconnect.local:10155/ws:10156:udp:10156:c2c:10157:c2cs:10158
    - wss://talkbaseserver.devconnect.local:10160/ws:10161:udp:10161:c2c:10162:c2cs:10163
    - wss://talkbaseserver.devconnect.local:10165/ws:10166:udp:10166:c2c:10167:c2cs:10168
    - wss://talkbaseserver.devconnect.local:10170/ws:10171:udp:10171:c2c:10172:c2cs:10173
    - wss://talkbaseserver.devconnect.local:10175/ws:10176:udp:10176:c2c:10177:c2cs:10178
    - wss://talkbaseserver.devconnect.local:10180/ws:10181:udp:10181:c2c:10182:c2cs:10183
    - wss://talkbaseserver.devconnect.local:10185/ws:10186:udp:10186:c2c:10187:c2cs:10188
    - wss://talkbaseserver.devconnect.local:10190/ws:10191:udp:10191:c2c:10192:c2cs:10193
    - wss://talkbaseserver.devconnect.local:10195/ws:10196:udp:10196:c2c:10197:c2cs:10198
    - wss://talkbaseserver.devconnect.local:10200/ws:10201:udp:10201:c2c:10202:c2cs:10203
    - wss://talkbaseserver.devconnect.local:10205/ws:10206:udp:10206:c2c:10207:c2cs:10208
    - wss://talkbaseserver.devconnect.local:10210/ws:10211:udp:10211:c2c:10212:c2cs:10213
    - wss://talkbaseserver.devconnect.local:10215/ws:10216:udp:10216:c2c:10217:c2cs:10218
    - wss://talkbaseserver.devconnect.local:10220/ws:10221:udp:10221:c2c:10222:c2cs:10223
    - wss://talkbaseserver.devconnect.local:10225/ws:10226:udp:10226:c2c:10227:c2cs:10228
    - wss://talkbaseserver.devconnect.local:10230/ws:10231:udp:10231:c2c:10232:c2cs:10233
  outboundProxy: udp://10.10.40.32:5060 # FQDN of the PBX
```

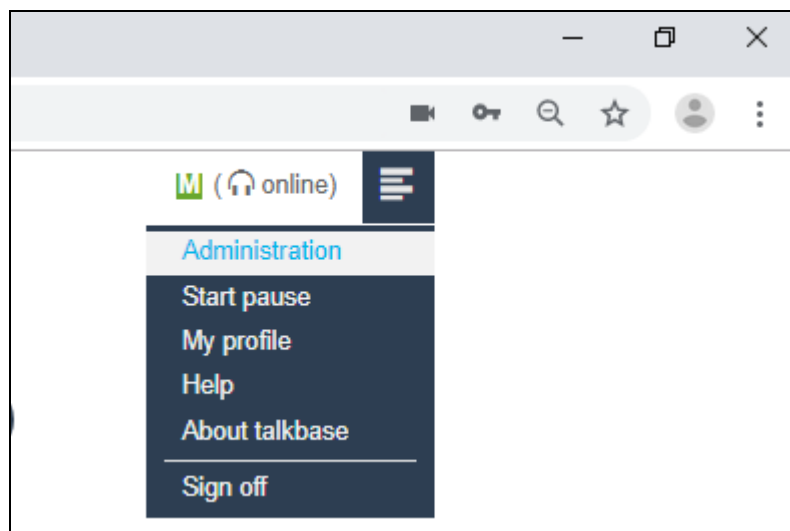
### 7.3. Configure talkbase Attendant

Further configuration of the talkbase server is carried out by opening a web browser to the talkbase server's IP address. Open a URL to **http://<FQDN of Talkbase Server>**. Enter the appropriate credentials and click on **Sign in**.



The screenshot shows a web browser window with the URL `talkbaseserver.devconnect.local/#/login`. The page features the "talkbase" logo at the top. Below it, the heading "Sign Up" is displayed. Under "Sign Up", there is a "Sign-in address" field containing "Administrator", a "Password" field with masked characters, a checked "Automatic Login" checkbox, and a "Sign In" button.

Once signed in, click on the icon at the top right of the page and select **Administration** as shown below.



The following screen is displayed showing the various modules. Click on **Tenants** at the bottom of the screen.

talkbaseserver.devconnect.local/#/admin

ATTENDANT1 (pause)

## Dashboard

- Options**: General options
- Directories**: Management of directories and their GUI representation.
- Main numbers**: Management of main numbers, opening hours, alternative destinations, music & sounds.
- Speed Dialing**: Management of Speed Dialing Buttons.
- Shortcuts**: Management of keyboard-shortcuts.
- Operation**: Management of general parameters, calling queue and operator groups.
- E-mail templates**: Management of e-mail templates.
- Licensing**: License management.
- Reporting**: Centralized call journal for investigations.
- Tenants**: Management of tenants. (Highlighted with a red box)
- Events**: Event Viewer for the latest information about the operating status of talkbase

The **Tenant** called **Avaya** was setup by the FROX engineers as part of the original connection setup. Click on the icon highlighted to display the information on this tenant.

ADMINISTRATION → TENANTS

ATTENDANT1 (pause)

## Tenants







Name	Number of users ( 5 / 5 )	Actions
Avaya	5	

The users listed are automatically populated as these are taken directly from the Active Directory of the domain that talkbase is a part of. **Attendant 1**, **Attendant2** and **Attendant3** were all added as domain users as per **Section 7.1**.

### Configuration

for Tenant Avaya

User Directories Main numbers Options

User ( 6 )	PBX-User	
Attendant1	1150	
Attendant2	1151	
Attendant3		
Paul Greaney		
Russell Greaney		
TB Avaya		

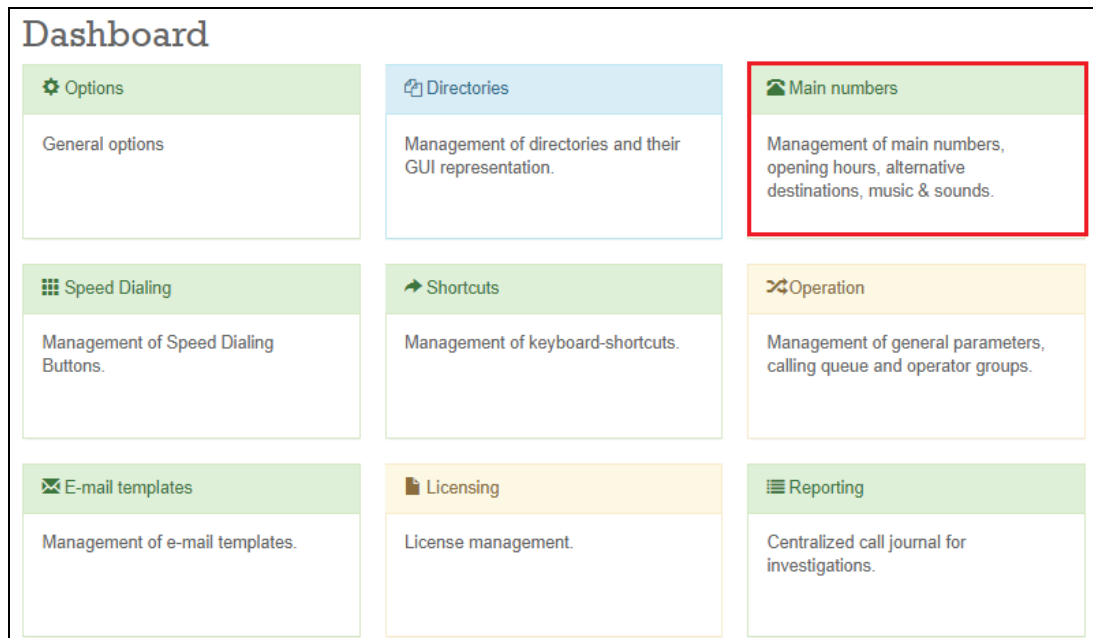
The **PBX-User** is the value configured in **Section 6.6** for the user name, along with the **PBX-Password** and the **Phone number** is the extension number assigned to the SIP user. In this case the extension number and user are the same, as they typically are in the DevConnect lab.

PBX-User ×

PBX-User	1150
PBX-Password	....
Confirm Password	....
Phone number	1150

Save Cancel

Navigate to **Main numbers** from the **Dashboard** menu.



Information on the number associated with the Attendant is set here. Clicking on the + icon will add a new “main number” and this can then be assigned to an Attendant.

## Main numbers

Use this number for outgoing calls: Main number / 1555

Active	Name	Number	Priority	Color	Icon	
<input checked="" type="checkbox"/>	Main number	1555	99	#532		
<input checked="" type="checkbox"/>	Main Nummer2	1556	99	#611	<input checked="" type="checkbox"/>	

## Internal/external classification of phone numbers

The internal/external assignment of phone numbers can be configured using the following rules: 'f' = one or more numbers, 'x' = exactly one number, 'I' (e.g. [1234]) a selection of numbers, a '+' in front of numbers

Priority	Rule	Classification as an internal or external number?	
1	xxxx	<input type="radio"/> External <input checked="" type="radio"/> Internal	
2	I	<input checked="" type="radio"/> External <input type="radio"/> Internal	

A new number **1557** has been added for the **Sales** line.

### Main numbers

Use this number for outgoing calls:

Active	Name	Number	Priority	Color	Icon	
<input checked="" type="checkbox"/>	Main number	1555	99	#687		
<input checked="" type="checkbox"/>	Main Nummer2	1556	99	#e11		
<input checked="" type="checkbox"/>	<input type="text" value="Sales"/>	<input type="text" value="1557"/>	<input type="text" value="99"/>			

Navigate to **Operation** from the **Dashboard** page.

### Dashboard

<b>Options</b> General options	<b>Directories</b> Management of directories and their GUI representation.	<b>Main numbers</b> Management of main numbers, opening hours, alternative destinations, music & sounds.
<b>Speed Dialing</b> Management of Speed Dialing Buttons.	<b>Shortcuts</b> Management of keyboard-shortcuts.	<b>Operation</b> Management of general parameters, calling queue and operator groups.
<b>E-mail templates</b> Management of e-mail templates.	<b>Licensing</b> License management.	<b>Reporting</b> Centralized call journal for investigations.

The numbers created from the previous page are now assigned to the various Attendants configured. The example below shows the number **1555** assigned to **Attendant1** only.

## Operation

Operator groups

Queue configuration

1555

1556

1557

Main number	1555						
Overflow		2	2	2	2	2	
Operator group	-	1	2	3	4	5	6
Attendant1							
Attendant2							
Attendant3							

The example below shows the new number **1557** assigned to both **Attendant1** and **Attendant2** in different **Operator groups**.

## Operation

Operator groups

Queue configuration

1555

1556

1557

Main number							
Overflow		5	5	5	5	5	
Operator group	-	1	2	3	4	5	6
Attendant1							
Attendant2							
Attendant3							

## 8. Verification Steps

The connection to AES can be verified on the AES side and on the talkbase side using the desktop to make and receive calls.

### 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

The following steps can be taken if there are any issues with calls being made. This should help verify the links between the products. 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 as shown below.

```
status trunk 12
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/0001	T00001	<b>in-service/idle</b>	no
0001/0002	T00002	<b>in-service/idle</b>	no
0001/0003	T00003	<b>in-service/idle</b>	no
0001/0004	T00004	<b>in-service/idle</b>	no
0001/0005	T00005	<b>in-service/idle</b>	no
0001/0006	T00006	<b>in-service/idle</b>	no
0001/0007	T00007	<b>in-service/idle</b>	no
0001/0008	T00008	<b>in-service/idle</b>	no
0001/0009	T00009	<b>in-service/idle</b>	no
0001/0010	T00010	<b>in-service/idle</b>	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 shown below.

```
status signaling-group 12
```

STATUS SIGNALING GROUP	
Group ID:	12
Group Type:	sip
Group State:	<b>in-service</b>

## 8.2. Verify talkbase SIP Entity is up

Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The 'Elements' menu is open, displaying a list of system components. 'Session Manager' is highlighted in red. The main dashboard includes several widgets: 'System Resource Utilization' with a bar chart, 'Alarms' with a circular gauge, 'Application State' with a table of system status, 'Information' with a table of element counts, and 'Notifications' with a list of alerts. The 'Session Manager' entry in the 'Elements' menu is highlighted in red.

Select the **TalkbaseServer** SIP Entity.

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page in the Avaya Aura System Manager 8.0 interface. The page provides a summary of Session Manager SIP entity link monitoring status. It includes a table of monitored SIP entities, with 'TalkbaseServer' highlighted. The table shows the status of various entities, including 'EP722', 'TalkbaseServer', 'cm81vmpg', and 'AAMessaging'. The 'TalkbaseServer' entity is shown as 'Up'.

SIP Entities Status for All Monitoring Session Manager Instances					
Run Monitor As of 1:48 PM					
1 Item					
	Session Manager	Type	Monitored Entities		
			Down	Partially Up	Up
<input type="checkbox"/>	SM81vmpg	Core	0	2	2

All Monitored SIP Entities	
Run Monitor	
4 Items	
<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	EP722
<input type="checkbox"/>	TalkbaseServer
<input type="checkbox"/>	cm81vmpg
<input type="checkbox"/>	AAMessaging

The SIP Entity should show as **UP** as it is shown below.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: TalkbaseServer

Summary View

1 Item

Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SM81vmpg	IPv4	10.10.40.120	5060	TCP	FALSE	UP	200 OK	UP

Select : None

### 8.3. Verify the talkbase Operator is functioning correctly

Open a web connection to the talkbase server as per **Section 7.2**. Enter the appropriate credentials, in this case this will be the Active Directory user shown in **Section 7.1**, and click on **Sign in**.

talkbaseserver.devconnect.local/#/login

talkbase

Sign Up

Sign-in address

attendant1

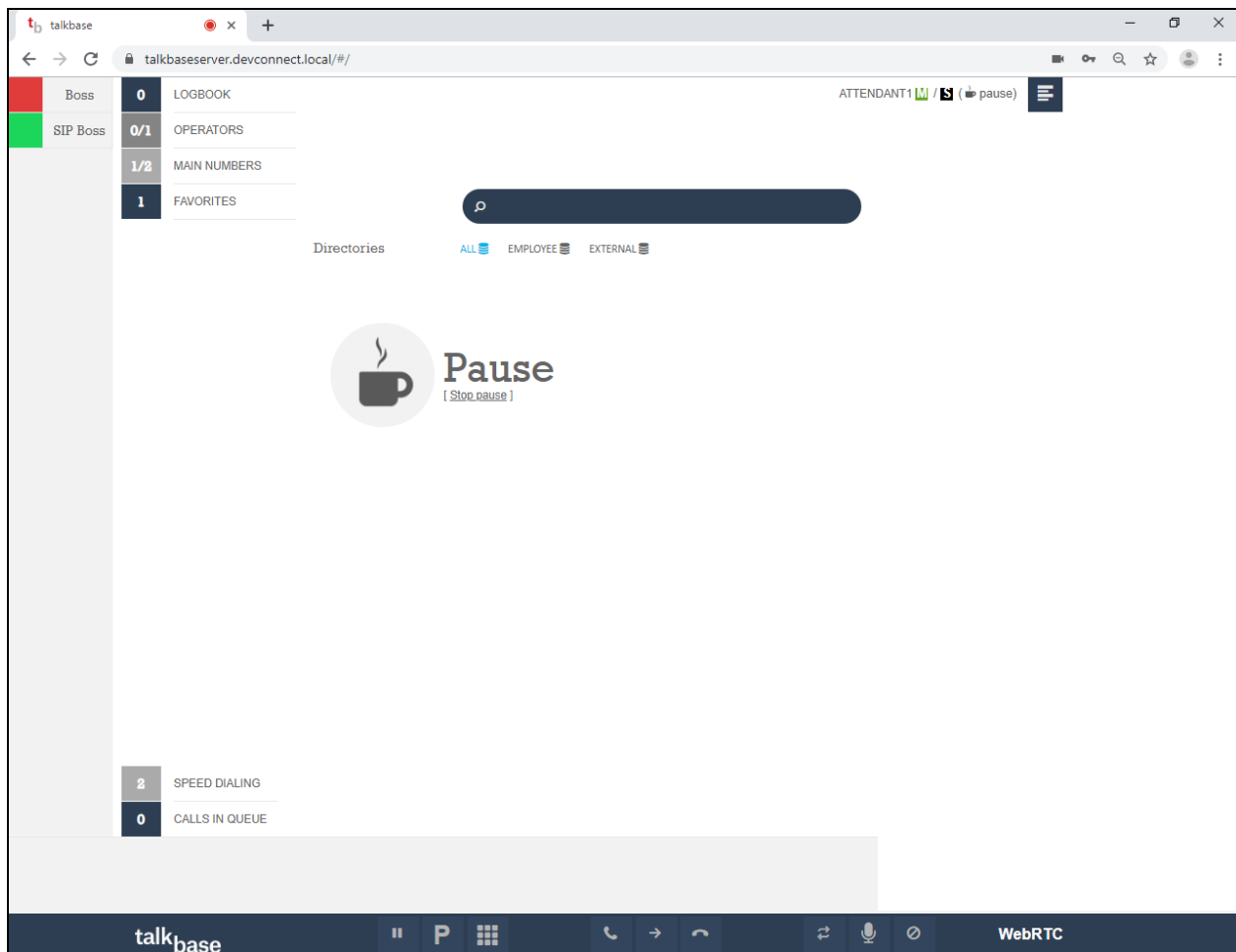
Password

\*\*\*\*\*

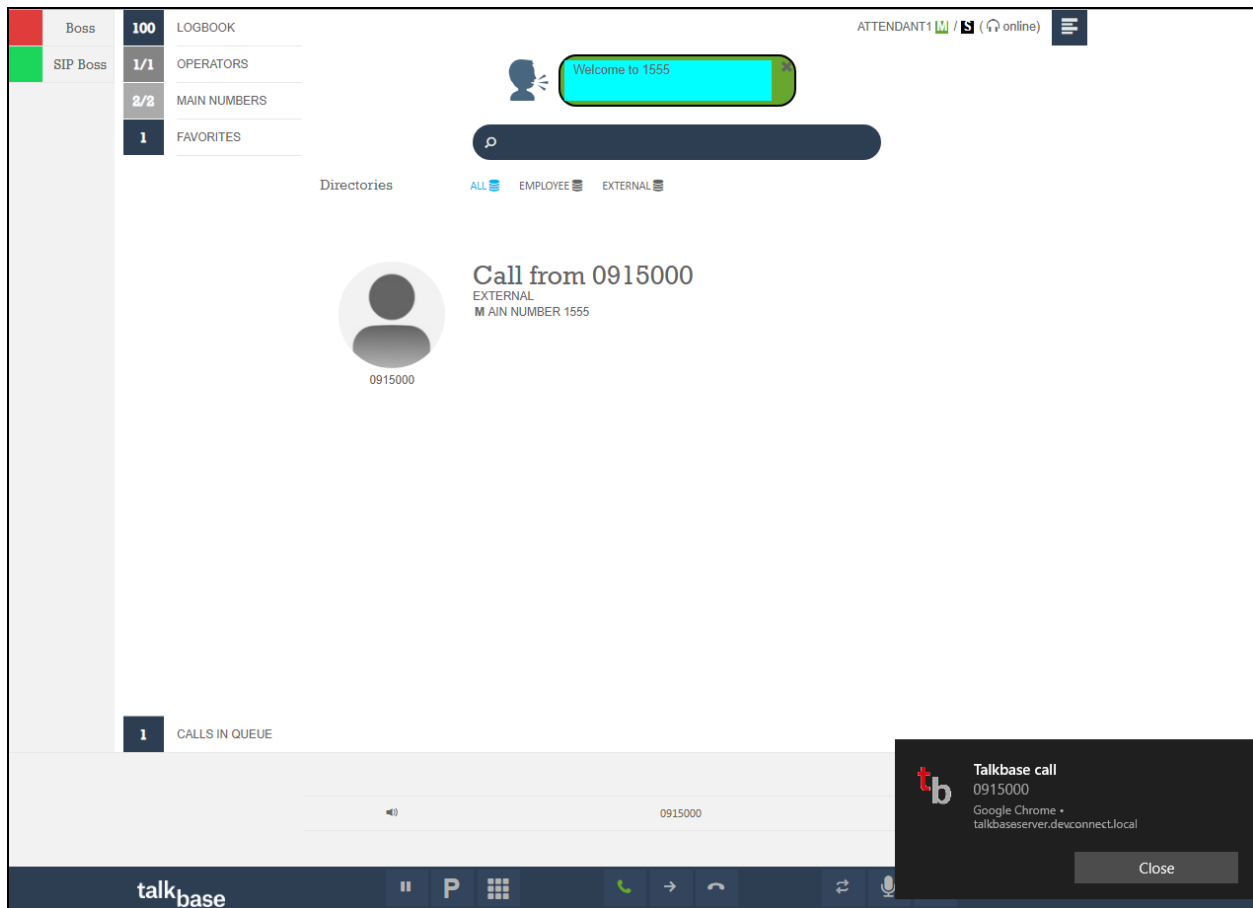
☒ Automatic Login

Sign In

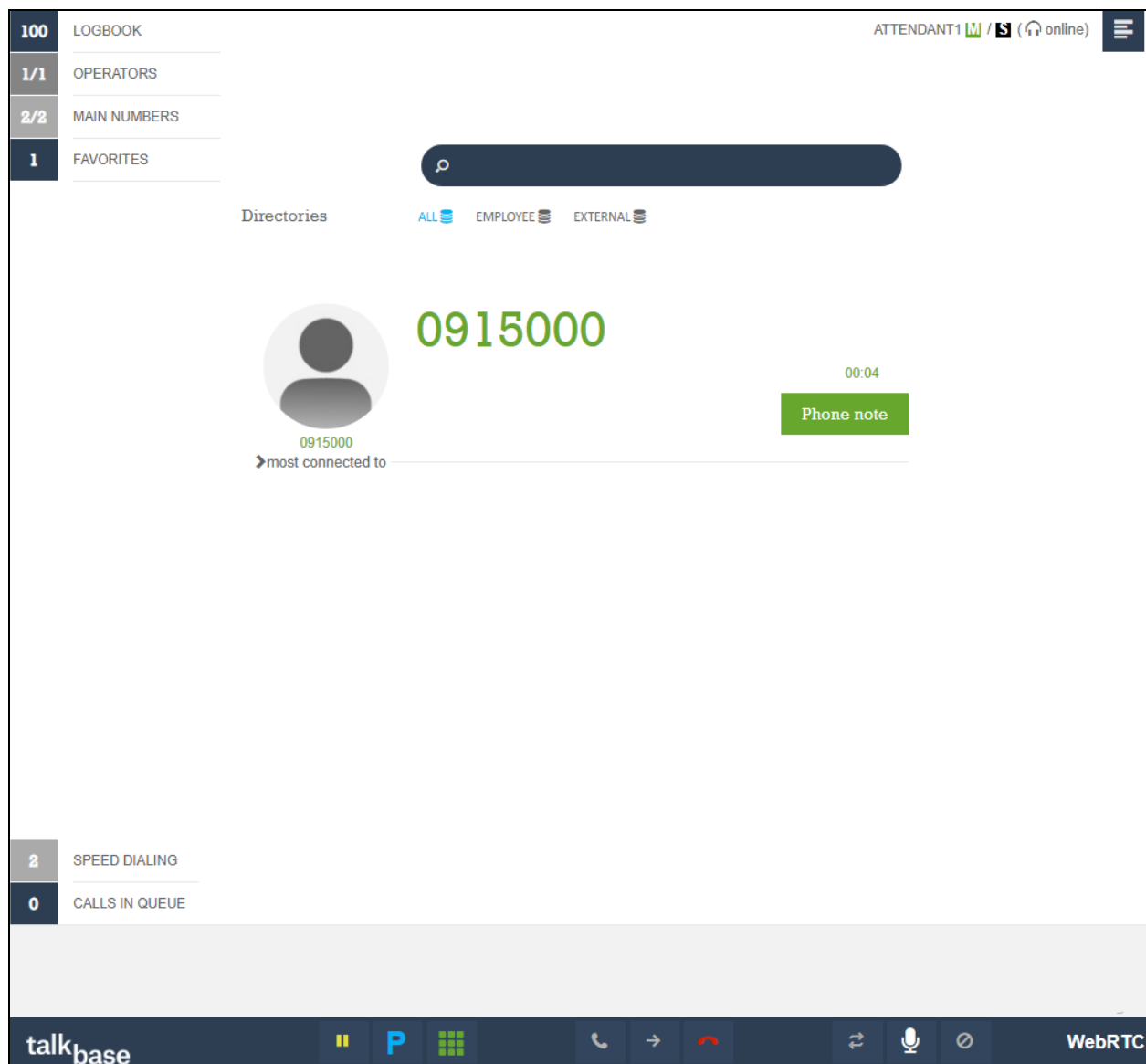
The following screen should be displayed showing the agent and the message **Pause** showing that the Operator is not idle. The **WebRTC** displayed in white at the bottom of the screen indicates that the Operator is connected correctly with the SIP user created in **Section 6.6**.



Clicking on **Pause** shown on the previous page will place the Operator into a state ready to receive calls. When a call from **0915000** is placed to the main number **1555** the following should be displayed 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, the call can be put on hold, transferred or hung up, using the icons located at the bottom of the screen. The CLID displayed in the middle of the screen turns green also indicating the call is answered.



## 9. Conclusion

These Application Notes describe the configuration steps required to integrate talkbase with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1. All feature and serviceability test cases were completed successfully.

## 10. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via <http://support.avaya.com>

- [1] Administering Avaya Aura® Communication Manager, Release 8.1
- [2] Administering Avaya Aura® Session Manager, Release 8.1

Documentation related to talkbase may directly be obtained from Frox AG as follows.

- **Phone:** +41 55 254 12 54/89
- **Email:** [info@talkbase.com](mailto:info@talkbase.com)
- **Web:** <https://talkbase.com/en/>

---

**©2019 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).