



## Avaya Solution & Interoperability Test Lab

---

# **Application Notes for configuring Aculab's ApplianX IP Gateway to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for provisioning Aculab ApplianX IP Gateway to permit Avaya Aura® Communication Manager R8.1 using a SIP trunk via Avaya Aura® Session Manager R8.1 to communicate with a third-party Private Branch Exchange via a TDM trunk.

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 for provisioning an Aculab ApplianX IP Gateway to permit Avaya Aura® Communication Manager R8.1 using a SIP trunk via Avaya Aura® Session Manager R8.1 to communicate with a third-party Private Branch Exchange via a Time Division Multiplex (TDM) QSIG trunk.

The ApplianX IP Gateway can be used in a variety of TDM and VoIP migration strategies, whether it is connecting a TDM-based Private Branch Exchange (PBX) to a new IP network, or IP PBX, or providing a PSTN front end to SIP-based solutions. The ApplianX IP Gateway is a 'plug & play' gateway. On the PSTN side, the ApplianX IP Gateway provides one, two or four universal T1/E1 (USA, Japan, Europe, worldwide) interfaces, with a wide range of signalling protocols, including, SIP, PRI/ISDN types, T1 robbed bit and E1 CAS, R1, R2 and DTMF, plus PBX protocols, such as QSIG and DPNSS. A different protocol can be selected for each trunk.

## 2. General Test Approach and Test results

The general test approach was to configure a SIP trunk and an E1 QSIG trunk on the Aculab ApplianX IP Gateway (ApplianX). The SIP trunk connected to the VoIP port on the ApplianX then converted the signalling to QSIG and vice versa. A SIP Entity and Entity Link were configured on Session Manager to route calls to and from the ApplianX. Testing focused on verifying that SIP and QSIG signals were converted correctly.

**Note:** During compliance testing, the Communication Manager connected to the VoIP port on the ApplianX was known as the SIP PBX and the Communication Manager connected to the E1/T1 port on the ApplianX was known as the QSIG PBX.

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 the ApplianX did not include use of any specific encryption features to Session Manager as the ApplianX variant supplied did not support these features.

## 2.1. Interoperability Compliance Testing

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

- Verification of connectivity between Communication Manager (SIP PBX) and Communication Manager (QSIG PBX) via the ApplianX
- Basic call tests: Calls from SIP PBX to QSIG PBX and vice versa
- Calls on Hold/Release
- Transfers (Blind and Consultative)
- Conferences
- Call Waiting
- DTMF
- Route Optimisation (Path Replacement)
- Call Diverts
- Serviceability testing by simulating LAN failures

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

## 2.2. Test Results

Tests were performed to ensure full interoperability of ApplianX when configured for SIP (using Session Manager) and QSIG. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following noted observations:

1. Trunk Route Optimization (path replacement) was not occurring on the SIP trunk connection when callers are transferred or diverted, resulting in two phones talking to each other on the same side (same PBX). In all cases, SIP channels on the ApplianX were being used upon completion of the transfer or after the call was diverted. The QSIG channels were released. Aculab is investigating this issue.
2. During transfers the display was not being updated after the transfer was complete. On occasion this was just the A party not being updated with the correct CLID after the transfer was complete. On other occasions it was both the A and C parties not being updated. Aculab is investigating this issue.

## 2.3. Support

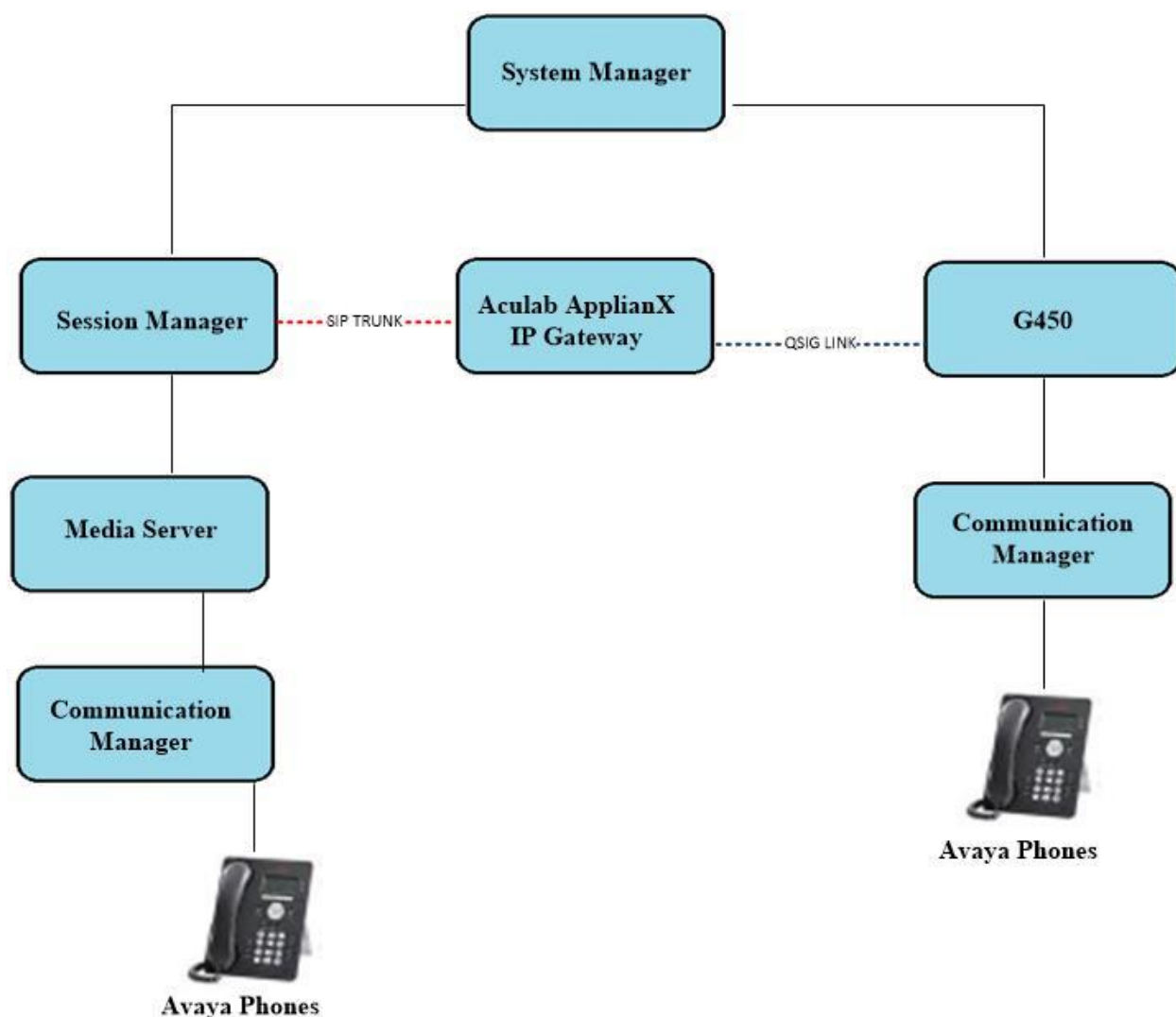
Technical support can be obtained for Aculab products as follows:

- **E-mail:** support@aculab.com
- **Phone:** +44(0)1908 273805

### 3. Reference Configuration

**Figure 1** illustrates the network configuration used during compliance testing. Communication Manager was configured to use SIP trunks to connect to the VoIP port on the ApplianX via Session Manager. An E1/T1 port on the ApplianX was configured for QSIG and connected directly to the E1/T1 port on the G450 gateway. Avaya H.323 and SIP telephones were used to make and receive calls via the ApplianX.

**Note:** Communication Manager, Session Manager, Media Server and System Manager were run on a virtual environment. During compliance testing the PBX hosting the QSIG trunk was a Communication Manager and G450 gateway.



**Figure 1: Network solution of Aculab ApplianX and Avaya Aura® Communication Manager and Avaya Aura® Session Manager**

## 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
Aculab Equipment	Software / Firmware Version
ApplianX IP Gateway Gateway Engine	2.3.10 build 13244 1.6.5-14

**Note:** The 3<sup>rd</sup> Party QSIG PBX was an Avaya Aura® Communication Manager 8.0 with Avaya G450 Gateway.

## 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 QSIG PSTN is outside the scope of these Application Notes. The ApplianX will interoperate with a wide range of PBXs supporting ISDN trunks.

### 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	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>		24000	319
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0

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

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	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 6**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options		Page 6 of 12
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? 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>		
Access Code 2:		
Automatic Callback Activation: *25 Deactivation: #25		

## 5.3. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM81vmppg**). 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
AMS81vmppg	10.10.40.61
G450	10.10.40.14
IPOffice	10.10.40.25
<b>SM81vmppg</b>	<b>10.10.40.32</b>
SM_Oceana	10.10.41.26
aes81vmppg	10.10.40.38
default	0.0.0.0
<b>procr</b>	<b>10.10.40.37</b>

( 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
```

Page 1 of 20

IP NETWORK REGION

Region: 1  
Location: 1      **Authoritative Domain: devconnect.local**  
Name: Default region

MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes  
    **Codec Set: 1**      Inter-region IP-IP Direct Audio: yes  
    UDP Port Min: 2048      IP Audio Hairpinning? n  
    UDP Port Max: 3329

DIFFSERV/TOS PARAMETERS  
    Call Control PHB Value: 46  
    Audio PHB Value: 46  
    Video PHB Value: 26

802.1P/Q PARAMETERS  
    Call Control 802.1p Priority: 6  
    Audio 802.1p Priority: 6  
    Video 802.1p Priority: 5

H.323 IP ENDPOINTS      AUDIO RESOURCE RESERVATION PARAMETERS  
    H.323 Link Bounce Recovery? y      RSVP Enabled? n  
    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 ApplianX. 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 ApplianX.

**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	Silence	Frames	Packet	
Codec	Suppression	Per Pkt	Size(ms)	
1: G.711A	n	2	20	
2: G.711MU	n	2	20	
3: G.729A	n	2	20	
4:				
Media Encryption			Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80				
2: none				
3:				

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

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the 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 was left blank to allow any/all domains.
- 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 the ApplianX and the Avaya phones.
- 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	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM81vmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from ApplianX (via Session Manager). Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 12		Page 1 of 5
TRUNK GROUP		
Group Number: 12	Group Type: sip	CDR Reports: y
Group Name: ApplianX	COR: 1	TN: 1 TAC: *812
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** was set to **private** and the **UI Treatment** was set to **service-provider**. 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>UI Treatment: service-provider</b>
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	
DSN Term? n	

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

- **Send Transferring Party Information?:** Enter y
- **Network Call Redirection?:** Enter y
- **Always Use re-INVITE for Display Updates?:** Enter y

change trunk-group 12	Page 5 of 5
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	<b>Send Transferring Party Information? y</b>
	<b>Network Call Redirection? y</b>
	Send Diversion Header? n
	Support Request History? y
	Telephone Event Payload Type: 101
	Convert 180 to 183 for Early Media? n
	<b>Always Use re-INVITE for Display Updates? y</b>
	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

The “QSIG PBX” has phones beginning with 2 so it was decided that all calls beginning with 2 with a length of 4 digits would be sent over the SIP trunk to Session Manager where they were then routed to the ApplianX.

### 5.4.1. Configure Route Pattern

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that ARS 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										
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				Sub	Dgts	Format	
1:	y	y	y	y	y	n	n	unre					lev0-pvt	none
2:	y	y	y	y	y	n	n	rest						none
3:	y	y	y	y	y	n	n	rest						none
4:	y	y	y	y	y	n	n	rest						none
5:	y	y	y	y	y	n	n	rest						none
6:	y	y	y	y	y	n	n	rest						none

### 5.4.2. Configure Uniform Dial Plan

It was decided for compliance testing that all calls to the “QSIG PBX” were calls that began with **2xxx** and these were to be sent across the SIP trunk to Session Manager and then onto ApplianX. To achieve this routing, Automatic Route Selection (ARS) will be used to route the calls. The dial plan and ARS 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 **2xxx** will use ARS No further digits are deleted or inserted. Calls are sent to **ARS** for further processing.

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

### 5.4.3. Configure Automatic Route Selection

Use the **change ars analysis** command to further configure the routing of the dialed digits. Calls to the ApplianX are achieved by dialing **2xxx** (calls from 2000 to 2999) 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 the ApplianX Gateway.

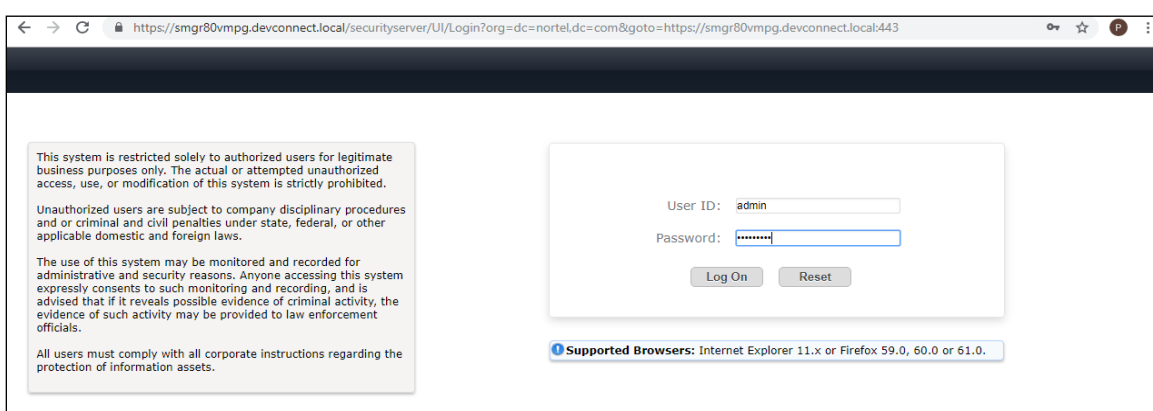
change ars analysis 1						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE						Percent Full: 3	
Location: all							
Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Req'd	
2	4	4	12	lpvt		n	
3	4	4	1	lpvt		n	
65	4	4	1	lpvt		n	
7	7	7	254	hnpa		n	
8	7	7	254	hnpa		n	
9	7	7	254	hnpa		n	

## 6. Configure Avaya Aura® Session Manager

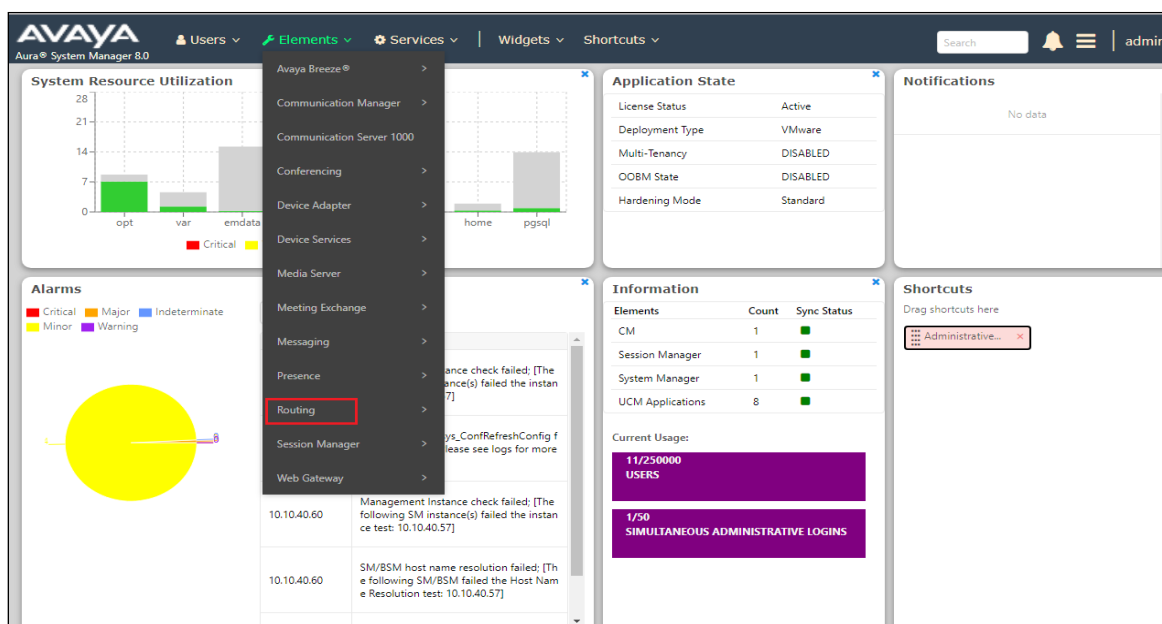
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure ApplianX SIP Entity
- Configure ApplianX Entity Link
- Configure Routing Policy for ApplianX
- Configure ApplianX 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.

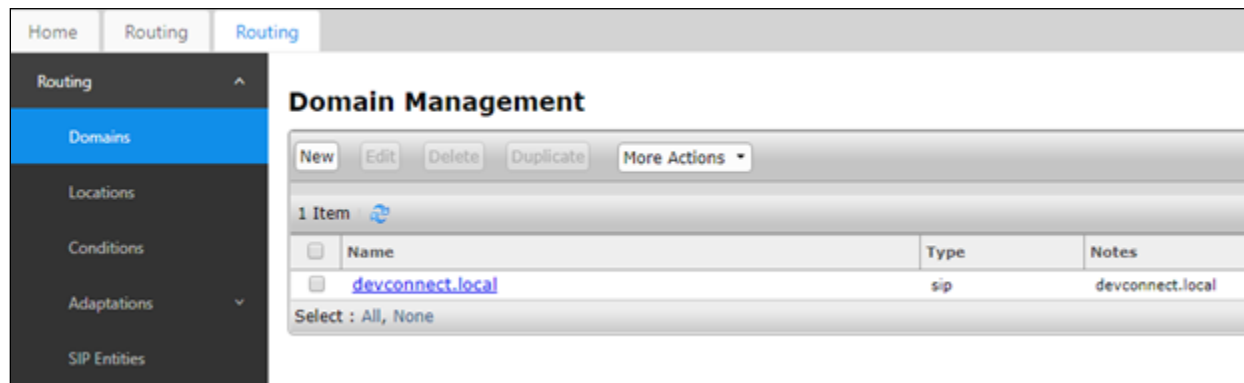


## 6.1. Domains and Locations

**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.

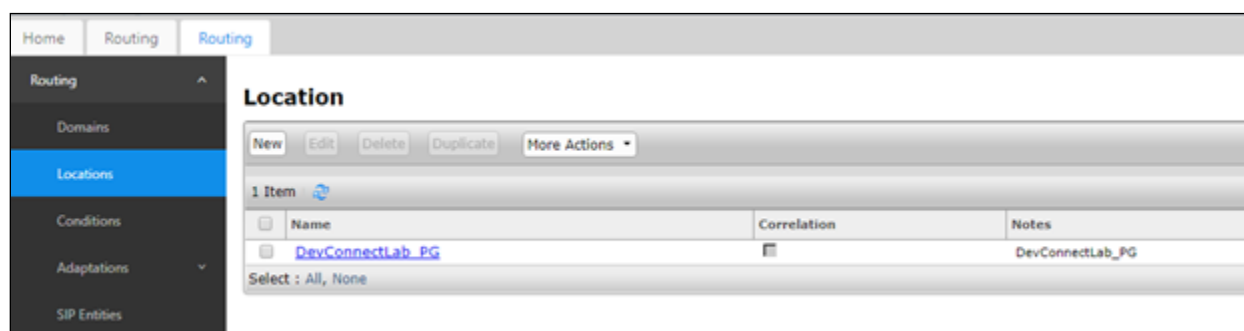
### 6.1.1. Display the Domain

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.



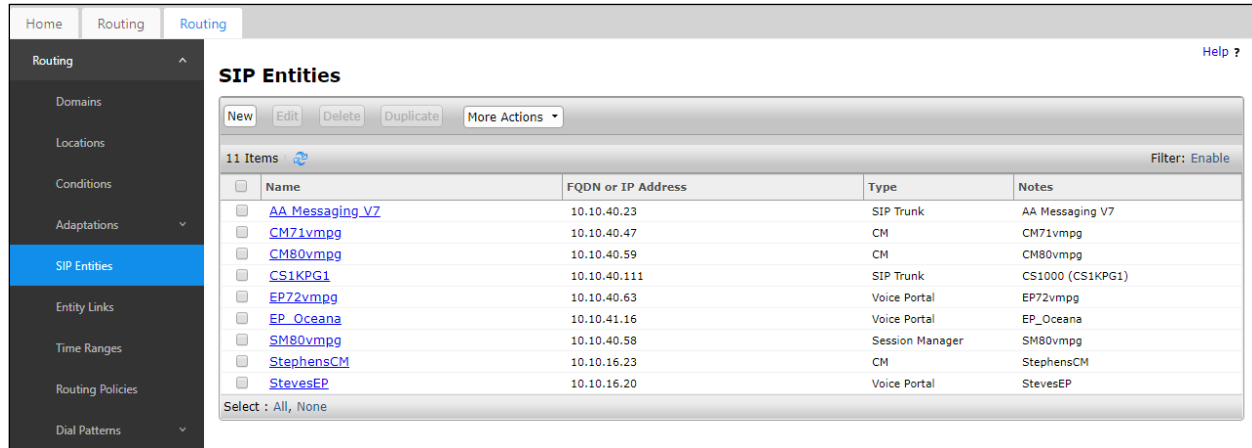
### 6.1.2. Display the Location

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.



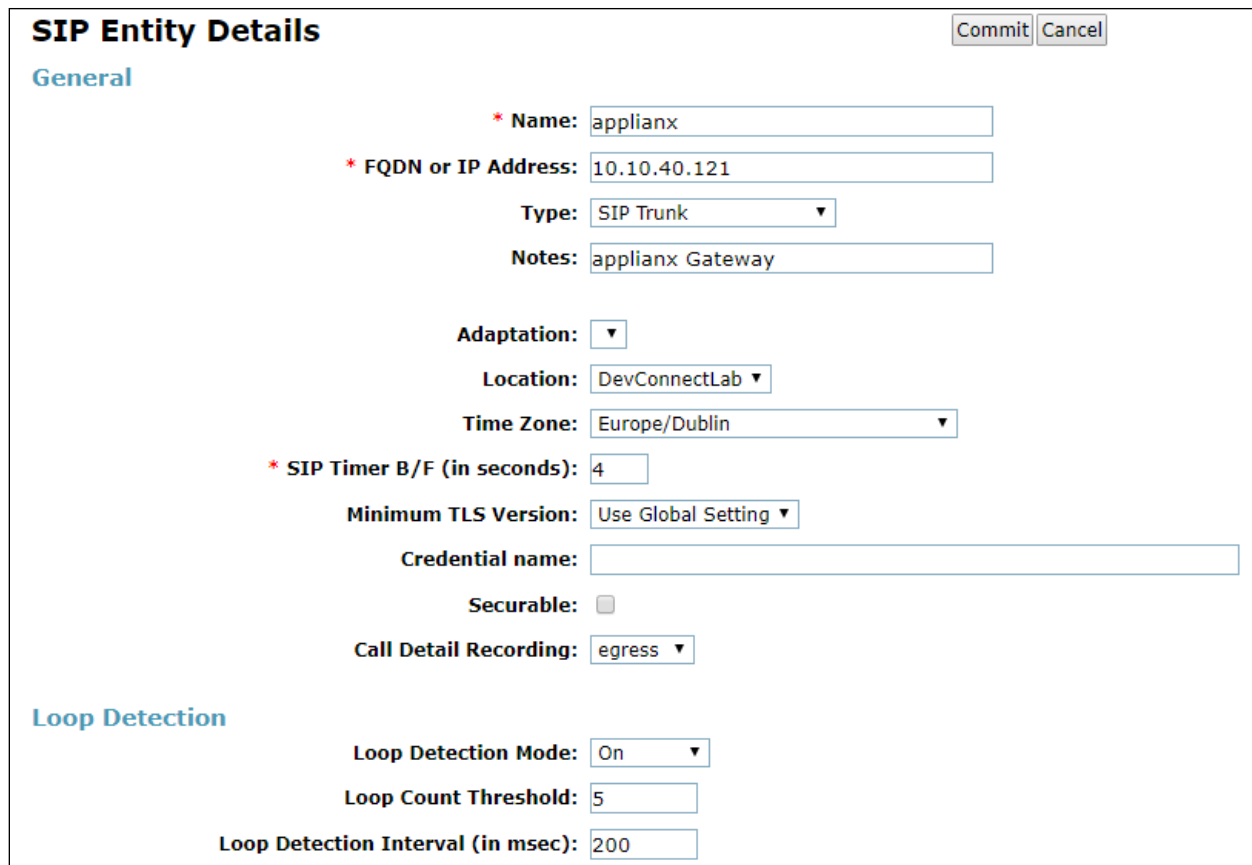
## 6.2. Configure ApplianX SIP Entity

The ApplianX is added on Session Manager as a SIP Entity with an Entity Link, every SIP endpoint that communicated over a SIP trunk would be added as such. 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 ApplianX. 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 ApplianX 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 has columns: 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 has columns: 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 ApplianX 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 has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The item added is:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM81vmg_applianx_506	SM81vmg	TCP	* 5060	applianx	* 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 has columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

## 6.4. Configure Routing Policy for ApplianX

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 **applianx** SIP Entity as shown below and click on **Select**.

**SIP Entities**
Select Cancel

---

**SIP Entities**

8 Items

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AAMessaging	10.10.40.23	Messaging	
<input checked="" type="radio"/>	applianx	10.10.40.121	SIP Trunk	applianx Gateway
<input type="radio"/>	cm80vmppg	10.10.40.59	CM	cm80vmppg
<input type="radio"/>	cm81vmppg - SIP PHONES	10.10.40.37	CM	Used for SIP Phones on CM
<input type="radio"/>	cm81vmppg - TRUNK	10.10.40.37	CM	For Trunk calls to CM
<input type="radio"/>	EP722	10.10.40.31	Voice Portal	EP722 and POM
<input type="radio"/>	IP Office	10.10.40.25	SIP Trunk	IP Office SE
<input type="radio"/>	TalkbaseServer	10.10.40.120	SIP Trunk	TalkbaseServer

Select : None

Select Cancel

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

**Routing Policy Details**
Commit Cancel

---

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
applianx	10.10.40.121	SIP Trunk	applianx Gateway

**Time of Day**

Add
Remove
View Gaps/Overlaps

1 Item

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
<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

Select : All, None

## 6.5. Configure ApplianX Dial Pattern

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
<input type="checkbox"/>	09173	9	9	<input type="checkbox"/>			-ALL-	To CM80vmpg from Syntec
<input type="checkbox"/>	2	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg
<input type="checkbox"/>	280	4	4	<input type="checkbox"/>			devconnect.local	To EP72vmpg
<input type="checkbox"/>	290	4	4	<input type="checkbox"/>			devconnect.local	To EP Oceana
<input type="checkbox"/>	30	4	4	<input type="checkbox"/>			devconnect.local	To CS1KPG1
<input type="checkbox"/>	351212455779	12	12	<input type="checkbox"/>			-ALL-	To SBC8 for Syntec
<input type="checkbox"/>	380	4	4	<input type="checkbox"/>			devconnect.local	To Steves EP
<input type="checkbox"/>	4	4	4	<input type="checkbox"/>			devconnect.local	To CM71vmpg
<input type="checkbox"/>	52	4	4	<input type="checkbox"/>			devconnect.local	To CM80vmpg for simulated PSTN to IPO
<input type="checkbox"/>	6666	4	4	<input type="checkbox"/>			devconnect.local	To AA Messaging V7
<input type="checkbox"/>	7080	4	6	<input type="checkbox"/>			devconnect.local	To Capita DMS
<input type="checkbox"/>	8000	5	5	<input type="checkbox"/>			devconnect.local	To Capita DS3000
<input type="checkbox"/>	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 **2** is used. This ensures that when 2xxx is dialed it will route to the ApplianX 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

**General**

\* **Pattern:** 2

\* **Min:** 4

\* **Max:** 4

**Emergency Call:** ☐

**SIP Domain:** devconnect.local ▼

**Notes:** To Applianx Gateway

**Originating Locations and Routing Policies**

**Add** **Remove**

1 Item

	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled
<input type="checkbox"/>					

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 ApplianX.

## Originating Location

SelectCancel

---

### 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

7 Items

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AA Messaging V7	<input type="checkbox"/>	AAMessaging	To AA Messaging V7
<input checked="" type="checkbox"/>	To Applianx	<input type="checkbox"/>	applianx	To Applianx Gateway
<input type="checkbox"/>	To CM80vmpg	<input type="checkbox"/>	cm80vmpg	To CM80vmpg
<input type="checkbox"/>	To cm81xvmpg	<input type="checkbox"/>	cm81vmpg - TRUNK	To cm81xvmpg
<input type="checkbox"/>	To EP722	<input type="checkbox"/>	EP722	To EP722
<input type="checkbox"/>	To IP Office	<input type="checkbox"/>	IP Office	To IP Office
<input type="checkbox"/>	To Talkbase	<input type="checkbox"/>	TalkbaseServer	To Talkbase

Select : All, None

SelectCancel

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

## Dial Pattern Details

CommitCancel

---

### General

\* Pattern: 2

\* Min: 4

\* Max: 4

Emergency Call: ☐

SIP Domain: devconnect.local

Notes: To Applianx Gateway

---

### Originating Locations and Routing Policies

AddRemove

1 Item

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

Select : All, None

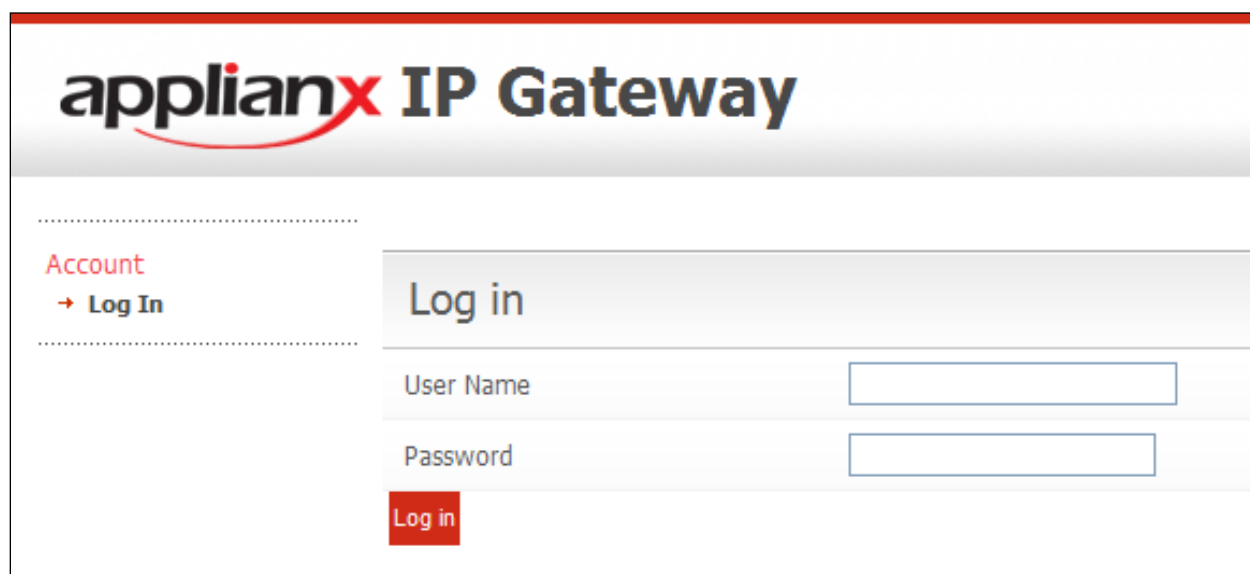
## 7. Configure Aculab ApplianX IP Gateway

A number of steps are required to configure the ApplianX. The initial assigning of the administration IP address, administration user name and password are assumed to be completed. The configuration operations described in this section can be summarized as follows:

- Login to ApplianX
- Run the Setup Wizard
- Configure QSIG Trunk
- Configure SIP Trunk
- Configure Endpoints
- Configure Groups
- Configure Routes
- Configure Clocking
- Configure SIP
- Configure Codecs
- Save configuration
- Use configuration

### 7.1. Login to ApplianX IP Gateway

Login by accessing the browser-based GUI, using the URL *http://<ip-address>* assigned to the ApplianX. Once the ApplianX IP Gateway web page opens, log in with the appropriate credentials and click on the **Log in** button.



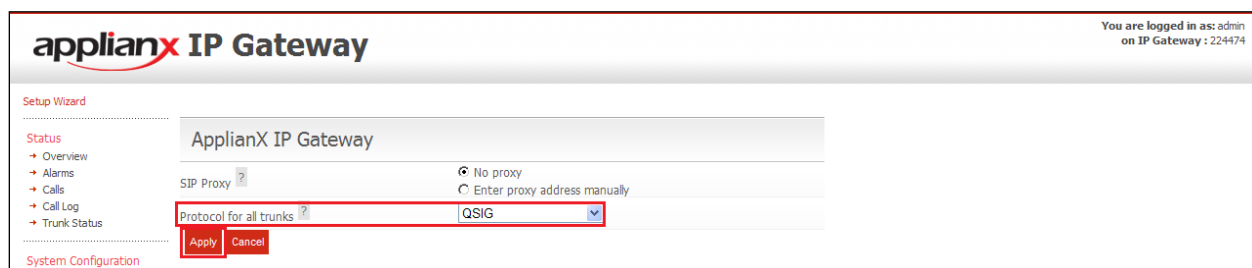
The screenshot shows the web interface for the ApplianX IP Gateway. At the top, the logo 'applianx IP Gateway' is displayed. Below the logo, there is a 'Log in' section. On the left side of this section, there is a link labeled 'Account' with a red arrow pointing to 'Log In'. The 'Log in' section itself contains two input fields: 'User Name' and 'Password'. Below these fields is a red button labeled 'Log in'.

## 7.2. Run the Setup Wizard

After the main web page opens, select **Setup Wizard** from **System Configuration** section.



Once the **Setup Wizard** page opens, select **QSIG** from the **Protocol for all trunks** drop-down box, and click on the **Apply** button.



After clicking the **Apply** button in the previous step, the **Edit Configurations** page opens. Click on the **Edit** button for **My Configuration**.

The screenshot shows the 'applanx IP Gateway' interface. In the top right corner, it says 'You are logged in as: admin on IP Gateway : 224474'. The left sidebar contains navigation links for 'Status' (Overview, Alarms, Calls, Call Log, Trunk Status), 'System Configuration' (Global Configuration, Networking, Setup Wizard, SIP Credentials), and 'Gateway Configuration' (Alias Registrar, DOI Barring, Edit Configurations). The main content area is titled 'Edit Configurations' and features two sections: 'Active configuration' and 'Available configurations'. The 'Active configuration' section has a table with columns 'Name', 'Description', and 'Last updated'. It lists one configuration: 'Change with Bridge media Qsig - DG' with a last updated time of '2013-12-06 06:14:08' and a status of 'Running'. The 'Available configurations' section also has a table with the same columns. It lists one configuration: 'My configuration' with a last updated time of '2014-02-05 08:51:34'. The 'My configuration' entry is highlighted with a red box, and its 'Edit' button is also highlighted.

In the **General** tab, give a descriptive name to the configuration. During compliance testing, **Avaya SIP to QSIG Test** was used.

The screenshot shows the 'applanx IP Gateway' interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Editing: Avaya SIP to QSIG Test'. It features a tabbed interface with tabs for 'General', 'Trunks', 'Endpoints', 'Groups', 'Routes', 'Clocking', 'SIP', 'Codecs', 'Survivability', and 'Test'. The 'General' tab is selected. Below the tabs is a section titled 'General Configuration Information' with two fields: 'Configuration name' and 'Configuration description'. The 'Configuration name' field contains the text 'Avaya SIP to QSIG Test'.



## 7.3. Configure QSIG Trunk

Click on the **Trunks** Tab followed by the **Trunk 1 Edit** button. This trunk was configured for QSIG. A cable was connected between the E1/T1 Trunk 1 port on the front of the ApplianX and the T1/E1 port on the G450 Gateway of the Communication Manager. Please note that the configuration of the QSIG trunk is dependent on the configuration of the connecting PBX, pay special attention to the Master/Slave configuration. The screenshots in this section relate to the configuration used during compliance testing of this solution.

The screenshot displays the 'ApplianX IP Gateway' configuration interface. The main heading is 'Editing: Avaya SIP to QSIG Test'. Below this, there is a navigation bar with tabs: General, **Trunks**, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'Trunks' tab is selected. The interface is divided into two sections: 'SIP trunks' and 'TDM trunks'. The 'SIP trunks' section contains a table with one row: 'Trunk 5' with Type 'SIP' and Group 'No group'. The 'TDM trunks' section contains a table with four rows: 'Trunk 1', 'Trunk 2', 'Trunk 3', and 'Trunk 4', all with Type 'TDM[QSIG]' and Group 'TDM trunks'. The 'Trunk 1' row is highlighted with a red border, and its 'Edit' button is also highlighted. On the left side, there is a sidebar menu with categories: Status, System Configuration, Gateway Configuration, and Diagnostics. The 'Edit Configurations' link under Gateway Configuration is selected. At the bottom, there are three buttons: 'Save Changes', 'Save and Return', and 'Cancel Changes'.

Name	Description	Type	Group	
Trunk 5		SIP	No group	Edit

Name	Description	Type	Group	
Trunk 1		TDM[QSIG]	TDM trunks	Edit
Trunk 2		TDM[QSIG]	TDM trunks	Edit
Trunk 3		TDM[QSIG]	TDM trunks	Edit
Trunk 4		TDM[QSIG]	TDM trunks	Edit

In the **Trunk name** field enter a name for the trunk (i.e., Avaya QSIG Trunk) and in the **Trunk description** field enter a description (i.e., Trunk to Avaya G450). Configure the remaining fields as shown in the following screen shot. Click on the **Change** button in the **Protocol configuration** section.

aplianx IP Gateway

Edit Configurations > Trunk Overview > Edit Trunk

**Status**

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

**System Configuration**

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

**Gateway Configuration**

- Alias Registrar
- DDI Barring
- **Edit Configurations**
- Interoperability
- Cause Mappings

**Diagnostics**

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

**Account**

- Log Out
- Change Password

**Editing: Avaya SIP to QSIG Test**

Apply Cancel

**General settings**

Trunk name Avaya QSIG Trunk

Trunk description Trunk to Avaya G450

Open inward speech path before answer ☒

Routing group TDM trunks

Block trunk from call activity ☐ No

Outgoing timeslot allocation strategy ☐ Highest available

Minimum digit count

Interdigit timeout (milliseconds)

Interdigit timeout for virtual calls (milliseconds)

Send sending complete on outgoing calls ☒

Send overlap digits on outgoing calls ☒

Response to unroutable incoming calls

**SNMP configuration**

Enable SNMP traps ☒

**Protocol configuration**

Protocol QSIG Edit Change

Click on the **Select** button for **QSIG**.

Select a protocol

Protocol	Description	Select
DPNSS	DPNSS Enhanced. Conforming to BTNR-188.	Select
<b>QSIG</b>	QSIG, also known as PSS1. Conforming to ECMA-143.	Select
ETS300	EuroISDN. Conforming to ETS300-102.	Select
INS1500	T1 Q.931 variant conforming to the INS-Net Interface and Services specification published by the NTT.	Select

Configure all the fields as is shown in the following screen shots.

**aplianx IP Gateway**

**Protocol Options**

**Status**

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

**System Configuration**

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

**Gateway Configuration**

- Alias Registrar
- DDI Barring
- Edit Configurations
- Interoperability
- Cause Mappings

**Diagnostics**

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

**Account**

- Log Out
- Change Password

**QSIG**

**General settings**

Trunk mode
E1

Impedence
120 Ohms (default)

CRC enabled
☒

Master/Slave configuration
Master, Priority B

**Basic features**

Display direction
Send and receive

Loop avoidance mapping
☐ Disabled  
☒ Transparent  
☐ Transit

Global transit limit
25

Insert loop avoidance in outgoing calls
☐

Do-not-disturb mapping
☒

Party Category Mode
Send using ANF-CMN (default)

Send progress indicators
☒

Allow incoming data calls
☒

Use 3.1kHz Audio bearer for speech
☐

Hold method
None (default)

Call Offer Enabled
☒

Call Transfer Enabled
☒

**Call Diversion Supplementary Service Support**

Continuation....

<b>Call Diversion Supplementary Service Support</b>	
Call Diversion Enabled ?	<input checked="" type="checkbox"/>
Divert as proxy ?	<input type="checkbox"/>
Divert unmatched to outgoing group ?	<input checked="" type="checkbox"/>
Send Diverted Address ?	<input checked="" type="checkbox"/>
Automatic Diversion Validation ?	<input type="checkbox"/>
Basic Service Type ?	Speech
Subscription Option Type ?	Notify With Number
'divertingLegInformation3.imv' Send Mode ?	Presentation Allowed
Default Party Number Type ?	Unknown
Include pSS1InfoElement Progress Indicator ?	<input checked="" type="checkbox"/>
<b>CBWF/CBWNNU (CC) Supplementary Service Support</b>	
CBWF/CBWNNU (CC) Enabled ?	<input checked="" type="checkbox"/>
Retain Signalling Connection ?	<input type="checkbox"/>
<b>Message Waiting Supplementary Service Support</b>	
Message Waiting Method ?	Facility (default)
<b>Path Replacement Additional Network Feature</b>	
Path Replacement Enabled ?	<input checked="" type="checkbox"/>
Dummy QSIG call identity ?	9999
Operate as originating end if other side cannot ?	<input checked="" type="checkbox"/>
Operate as terminating end if other side cannot ?	<input checked="" type="checkbox"/>
Allow Path Replacement proposal by terminating end also ?	<input type="checkbox"/>
Accept Path Replacement proposal when originating end ?	<input checked="" type="checkbox"/>
Delay in seconds after transfer before a Route Optimisation/Path Replacement proposal can be sent	30
Delay in seconds after a Route Optimisation/Path Replacement rejection before a new proposal can be sent	30

Select the remaining values and click on the **Apply** button.

<b>QSIG Protocol Compatibility</b>	
Length of invoke ids (in bytes) ?	2
Facility protocol profile ?	0x9F - ISO (default)
Send NFE and Interpretation APDUs ?	<input checked="" type="checkbox"/>
Use global IDs in Facility ?	<input type="checkbox"/>
<b>Raw configuration options</b>	
Options ?	
<b>Apply</b> <b>Cancel</b>	

After returning to the **Edit Trunk** page, click on the **Apply** button.

**aplianx IP Gateway**

Edit Configurations > Trunk Overview > Edit Trunk

Status

→ Overview

→ Alarms

→ Calls

→ Call Log

→ Trunk Status

System Configuration

→ Global Configuration

→ Networking

→ Setup Wizard

→ SIP Credentials

Gateway Configuration

→ Alias Registrar

→ DDI Barring

→ **Edit Configurations**

→ Interoperability

→ Cause Mappings

Diagnostics

→ Remote Logging

→ Network Diagnostics

→ Watchdog Status

→ Restart

→ Diagnostic Log

→ Endpoint Status

→ About

→ Hardware

Account

→ Log Out

→ Change Password

Editing: Avaya SIP to QSIG Test

Apply

Cancel

General settings

Trunk name

Avaya QSIG Trunk

Trunk description

Trunk to Avaya G450

Open inward speech path before answer ?

☒

Routing group

TDM trunks ▼

Block trunk from call activity ?

No ▼

Outgoing timeslot allocation strategy ?

Highest available ▼

Minimum digit count ?

0

Interdigit timeout (milliseconds) ?

3000

Interdigit timeout for virtual calls (milliseconds) ?

1000

Send sending complete on outgoing calls ?

☒

Send overlap digits on outgoing calls ?

☒

Response to unroutable incoming calls ?

Release ▼

SNMP configuration

Enable SNMP traps

☒

Protocol configuration

Protocol

QSIG

Edit

Change

## 7.4. Configure SIP Trunk

To configure the SIP trunk, click on the **Trunk 5 Edit** button.

Edit Configurations > Trunk Overview

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status

Editing: Avaya SIP to QSIG Test

General Trunks Endpoints Groups Routes Clocking SIP Codecs Survivability Test

SIP trunks

Name	Description	Type	Group	
Trunk 5		SIP	No group	Edit

TDM trunks

Name	Description	Type	Group	
Avaya QSIG Trunk	Trunk to Avaya G450	TDM[QSIG]	TDM trunks	Edit
Trunk 2		TDM[QSIG]	TDM trunks	Edit
Trunk 3		TDM[QSIG]	TDM trunks	Edit
Trunk 4		TDM[QSIG]	TDM trunks	Edit

Save Changes Save and Return Cancel Changes

Enter a descriptive name in the **Trunk name** field (i.e., Avaya SIP Trunk) and in the **Trunk description** field enter a description (i.e., SIP Trunk to Avaya SM). Configure the remaining fields as shown in the following screen shot. Click on the **Apply** button to save the changes.

Edit Configurations > Trunk Overview > Edit Trunk

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

Account

- Log Out
- Change Password

Editing: Avaya SIP to QSIG Test

Apply Cancel

General settings

Trunk name Avaya SIP Trunk

Trunk description SIP trunk to Avaya SM

Open inward speech path before answer ? ☒

Block trunk from call activity ? No

Response to unroutable incoming calls ? Release

SNMP configuration

Enable SNMP traps ☒

For use under supervision of Aculab Technical Support

**WARNING:** Setting this value too high may result in system performance issues.

Override default SIP Trunk Capacity ? ☐

SIP Trunk Capacity ? 120

## 7.5. Configure Endpoints

The ApplianX requires information relating to Session Manager so as to communicate with Communication Manager. After clicking on the **Endpoints** tab, click on the icon for **Proxy** as shown in the screen shot below.

Edit Configurations > SIP Endpoint Overview

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations

Editing: Avaya SIP to QSIG Test

General Trunks Endpoints Groups Routes Clocking SIP Codecs Survivability Test

Default SIP Endpoint	Default endpoint to match incoming SIP calls that don't match any other endpoint.	
ApplianX IP Gateway self	Certain supplementary services can result in the ApplianX IP Gateway being asked to call itself. This endpoint matches those calls and allows them to be routed correctly.	
ApplianX IP Gateway registered users	Destination for calls to registered users.	
Avaya SIP Trunk	SIP trunk to Avaya SM	

Add a new endpoint

Save Changes Save and Return Cancel Changes

Enter a descriptive name in the **Name** and in the **Description** fields. Configure the following in the remaining fields with the others as shown in the screen shot below.

- **Routing Group** Select **Proxy group** from the dropdown box
- **Endpoint address** Enter the IP address of the Session Manager (this is the same IP address as configured in **Section 5.1**)
- **UDP/TCP ports** Enter **5060**

Edit Configurations > SIP Endpoint Overview > Edit SIP Endpoint

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About
- Hardware

Account

- Log Out
- Change Password

Editing: Avaya SIP to QSIG Test

Apply Cancel

General

Name ? Avaya SIP Trunk

Description ? SIP trunk to Avaya SM

Routing group ? Proxy group

Endpoint Options

Endpoint address ? 10.10.40.32

UDP port ? 5060

TCP port ? 5060

Monitor this endpoint ? ☒

Trust this endpoint ? ☒

During call transfers, allow sending of 'INVITE with Replaces' ? ☒

During call transfers, allow sending of 'REFER with Replaces' ? ☒

During call transfers, allow sending of 'REFER' ? ☒

This endpoint is an Aculab ApplianX IP Gateway ? ☐

This endpoint is the central PBX ? ☐

Continuation....

After configuring the remaining fields, click on the **Apply** button on the top of the screen (not shown) to save the changes.

T.38 Fax Gateway Configuration	
Allow T.38 on this endpoint ?	<input checked="" type="checkbox"/>
Allow ECM negotiation for this endpoint ?	<input checked="" type="checkbox"/>
Allow V.17 Modem to be negotiated for this endpoint ?	<input checked="" type="checkbox"/>
Redundancy level ?	<input type="text" value="2"/>
Re-INVITE delay ?	<input type="text" value="500"/>

## 7.6. Configure Groups

During compliance testing no group configuration changes were required as the default **TDM trunks** and **Proxy group** groups were used. If changes are required, please refer to the Aculab documentation (see **Section 10**).

## 7.7. Configure Routes

To configure the QSIG Route, click on the **Routes** tab and uncheck **Use the same rules for all groups** check box.

Edit Configurations > Manage Routing

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- Edit Configurations**
- Interoperability
- Cause Mappings

Diagnostics

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart

Editing: Avaya SIP to QSIG Test

General Trunks Endpoints Group **Routes** Blocking SIP Codecs Survivability Test

**Routing Options**

Use the same rules for all groups ? ☐

Allow calls from unknown endpoints ? ☐

**Routing Rules**

Select the group for which you want to configure the routing TDM trunks

Name ?	DDI/DID criteria ?	DDI/DID man. ?	CLI/ANI criteria ?	CLI/ANI man. ?	Destination ?
ToAvaya	%	%	%	%	Proxy group

Add new rule Use these rules for all groups

Save Changes Save and Return Cancel Changes



### 7.7.1. Configure QSIG Route

- Select **TDM trunks** from the **Select the group for which you want to configure the routing** dropdown box
- **Name** Enter a descriptive name (i.e., QSIG to SIP)
- **Destination** Select **Proxy group** from the dropdown box

Click on the **Save Changes** button.

The screenshot shows the 'Edit Configurations > Manage Routing' interface. The title is 'Editing: Avaya SIP to QSIG Test'. The 'Routing Rules' section is active, showing a table with columns: Name, DDI/DID criteria, DDI/DID man., CLI/ANI criteria, CLI/ANI man., and Destination. A rule is defined with Name 'ToAvaya' and Destination 'Proxy group'. The 'Destination' dropdown is highlighted with a red box. Below the table are buttons for 'Add new rule' and 'Use these rules for all groups'. At the bottom are 'Save Changes', 'Save and Return', and 'Cancel Changes' buttons.

### 7.7.2. Configure SIP Route

- Select **Proxy group** from the **Select the group for which you want to configure the routing** dropdown box
- Click on the **Add new rule** button
- **Name** Enter a descriptive name (i.e., SIP to QSIG)
- **Destination** Select **TDM trunks** from the dropdown box

Click on the **Save Changes** button.

The screenshot shows the 'Edit Configurations > Manage Routing' interface. The title is 'Editing: Avaya SIP to QSIG Test'. The 'Routing Rules' section is active, showing a table with columns: Name, DDI/DID criteria, DDI/DID man., CLI/ANI criteria, CLI/ANI man., and Destination. A rule is defined with Name 'ToQSIG' and Destination 'TDM trunks'. The 'Destination' dropdown is highlighted with a red box. Below the table are buttons for 'Add new rule' and 'Use these rules for all groups'. At the bottom are 'Save Changes', 'Save and Return', and 'Cancel Changes' buttons.

## 7.8. Configure Clocking

During compliance testing, clocking was provided by the Avaya QSIG trunk. To configure clocking, click on the **Clocking** tab and using the left and right buttons, make sure only the Avaya QSIG Trunk is in the **Selected clock sources** list. Click on the **Save Changes** button.

The screenshot shows the 'ApplianX IP Gateway' configuration interface. The breadcrumb trail is 'Edit Configurations > Clocking'. The left sidebar contains several sections: 'Status' (Overview, Alarms, Calls, Call Log, Trunk Status), 'System Configuration' (Global Configuration, Networking, Setup Wizard, SIP Credentials), 'Gateway Configuration' (Alias Registrar, DDI Barring, Edit Configurations, Interoperability, Cause Mappings), and 'Diagnostics' (Remote Logging, Network Diagnostics, Watchdog Status, Restart, Diagnostic Log, Endpoint Status, About, Hardware). The main content area is titled 'Editing: Avaya SIP to QSIG Test' and has tabs for General, Trunks, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'Clocking' tab is active. It features two lists: 'Available clock sources' containing 'Trunk 2', 'Trunk 3', and 'Trunk 4'; and 'Selected clock sources' containing 'Avaya QSIG Trunk'. Between these lists are four buttons: '>', '>>', '<', and '<<'. At the bottom of the main area are 'Move up' and 'Move down' buttons. A checkbox 'Fall back to local clock' is checked. At the very bottom are three buttons: 'Save Changes', 'Save and Return', and 'Cancel Changes'.

## 7.9. Configure SIP

To configure the SIP settings, click on the **SIP** tab and enter all the information as shown in the screen shot below. **TCP** or **UDP** can be selected as both are supported in this configuration. For compliance testing TCP was chosen as per the SIP Entity Link configured in **Section 6.3**.

The screenshot shows the 'applanx IP Gateway' web interface. The breadcrumb trail is 'Edit Configurations > SIP Configuration'. The left sidebar contains several sections: 'Status' (Overview, Alarms, Calls, Call Log, Trunk Status), 'System Configuration' (Global Configuration, Networking, Setup Wizard, SIP Credentials), 'Gateway Configuration' (Alias Registrar, DDI Barring, Edit Configurations, Interoperability, Cause Mappings), 'Diagnostics' (Remote Logging, Network Diagnostics, Watchdog Status, Restart, Diagnostic Log, Endpoint Status, About, Hardware), and 'Account' (Log Out, Change Password). The main content area is titled 'Editing: Avaya SIP to QSIG Test' and has tabs for General, Trunks, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'SIP' tab is active. Below the tabs are three red section headers: 'Transport for outgoing calls', 'Media options', and 'Jitter Buffer'. The 'Transport for outgoing calls' section contains a 'Transport protocol' dropdown menu with 'TCP' selected. The 'Media options' section contains several settings: 'DTMF over IP send method' (RFC2833 encoded RTP), 'Tone duration of regenerated DTMF' (250), 'Interdigit duration of regenerated DTMF' (250), 'Support comfort noise' (checked), 'Send 183 for Ringing' (checked), 'Discontinuous Transmission (DTX)' (Enabled - With Comfort Noise), 'Enable Packet Loss Concealment (PLC)' (checked), 'Enable RTCP' (unchecked), 'Use 'sendonly' for Hold' (radio button selected), 'Use 'inactive' for Hold' (radio button), and 'Use 'recvonly' for Hold' (radio button). The 'Jitter Buffer' section is partially visible at the bottom.

Section	Setting	Value
Transport for outgoing calls	Transport protocol	TCP
	Media options	
Media options	DTMF over IP send method	RFC2833 encoded RTP
	Tone duration of regenerated DTMF	250
	Interdigit duration of regenerated DTMF	250
	Support comfort noise	<input checked="" type="checkbox"/>
	Send 183 for Ringing	<input checked="" type="checkbox"/>
	Discontinuous Transmission (DTX)	Enabled - With Comfort Noise
	Enable Packet Loss Concealment (PLC)	<input checked="" type="checkbox"/>
	Enable RTCP	<input type="checkbox"/>
	Use 'sendonly' for Hold	<input checked="" type="radio"/>
	Use 'inactive' for Hold	<input type="radio"/>
Jitter Buffer	Use 'recvonly' for Hold	<input type="radio"/>
	Bridge media streams	<input type="checkbox"/>

Continuation....

After configuring the remaining fields, click on the **Save Changes** button to save the changes.

[Change Password](#)

>> Jitter Buffer

Manual jitter buffer configuration ? ☐

>> Listening ports

UDP listen port (0 to disable)

TCP listen port (0 to disable)

>> Endpoint monitoring

Polling interval ?

>> Message Waiting Supplementary Service Support

Accept unsolicited message summary ? ☒

Send unsolicited message summary ? ☒

>> Call Diversion Supplementary Service Support

Call Diversion Enabled ? ☒

History-Info Method Preferred ? ☒

Divert as proxy ? ☐

Divert unmatched to outgoing group ? ☒

Send Diverted Address ? ☒

>> Custom messages conveying non-SIP features

Exchange transfer information ? ☒

Exchange Route Optimisation/Path Replacement information ? ☒

CBWF/CBWNUI Enabled ? ☒

Save Changes

Save and Return

Cancel Changes

## 7.10. Configure Codecs

During compliance testing the codec settings were left as default. The screen shot below shows the configured codecs.

The screenshot displays the 'ApplianX IP Gateway' web interface. The main title is 'Editing: Avaya SIP to QSIG Test'. Below the title is a navigation bar with tabs: General, Trunks, Endpoints, Groups, Routes, Clocking, SIP, **Codecs**, Survivability, and Test. The 'Codecs' tab is highlighted. The interface is divided into two main sections: 'Available codecs' and 'Configured codecs'. The 'Available codecs' list contains 'G729'. The 'Configured codecs' list contains 'G711\_Alaw' and 'G711\_Mulaw'. Between these lists are four red buttons: '>', '>>', '<', and '<<'. At the bottom right of the configuration area are 'Move Up' and 'Move Down' buttons. At the bottom of the page are three red buttons: 'Save Changes', 'Save and Return', and 'Cancel Changes'. On the left side, there is a sidebar menu with categories: Status (Overview, Alarms, Calls, Call Log, Trunk Status), System Configuration (Global Configuration, Networking, Setup Wizard, SIP Credentials), Gateway Configuration (Alias Registrar, DDI Barring, Edit Configurations, Interoperability, Cause Mappings), and Diagnostics (Remote Logging, Network Diagnostics, Watchdog Status, Restart, Diagnostic Log, Endpoint Status, About).

## 7.11. Save Configuration

Once all the configuration changes have been made, click on the **Save and Return** button.

**applianx IP Gateway**

Edit Configurations > Codec Configuration

**Status**

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

**System Configuration**

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

**Gateway Configuration**

- Alias Registrar
- DDI Barring
- **Edit Configurations**
- Interoperability
- Cause Mappings

**Diagnostics**

- Remote Logging
- Network Diagnostics
- Watchdog Status
- Restart
- Diagnostic Log
- Endpoint Status
- About

**Editing: Avaya SIP to QSIG Test**

General Trunks Endpoints Groups Routes Clocking SIP Codecs **Survivability** Test

**Available codecs**

- G729

**Configured codecs**

- G711\_Alaw
- G711\_Mulaw

Move Up Move Down

Save Changes **Save and Return** Cancel Changes

## 7.12. Use Configuration

Once all the configurations have been made and saved, click on the **Use** button for this configuration (Avaya SIP to QSIG Test) to apply them to the ApplianX.

**applianx IP Gateway**

Edit Configurations

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DDI Barring
- **Edit Configurations**
- Interoperability

Changes saved

Edit Configurations

Active configuration

Name	Description	Last updated	
My configuration		2015-09-02 20:27:32	Running <a href="#">View</a> <a href="#">Copy</a>

Available configurations

Name	Description	Last updated	
Avaya SIP to QSIG Test		2015-09-02 21:41:11	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Use</a>

Click on the **Yes** button to confirm.

**applianx IP Gateway**

Edit Configurations

Question

Are you sure you want to use the configuration Avaya SIP to QSIG Test?

[Yes](#) [No](#)

Once the configuration is active, the web page should update to something similar to the screen below.

**applianx IP Gateway**

Edit Configurations

Status

- Overview
- Alarms
- Calls
- Call Log
- Trunk Status

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Active configuration

Name	Description	Last updated	
Avaya SIP to QSIG Test		2015-09-02 21:41:11	Running <a href="#">View</a> <a href="#">Copy</a>

## 8. Verification Steps

The connection to Session Manager can be ultimately verified by making and receiving calls across the ApplianX.

1. Make a call to the SIP PBX from the QSIG PBX. Ensure the call is connected and there is a two-way speech path.
2. Make a call to the QSIG PBX from the SIP PBX. Ensure the call is connected and there is a two-way speech path.

This connection can also be verified on the Session Manager and the ApplianX.

### 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  in-service/idle    no
0001/0002 T00002  in-service/idle    no
0001/0003 T00003  in-service/idle    no
0001/0004 T00004  in-service/idle    no
0001/0005 T00005  in-service/idle    no
0001/0006 T00006  in-service/idle    no
0001/0007 T00007  in-service/idle    no
0001/0008 T00008  in-service/idle    no
0001/0009 T00009  in-service/idle    no
0001/0010 T00010  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 shown below.

```
status signaling-group 12

                                STATUS SIGNALING GROUP

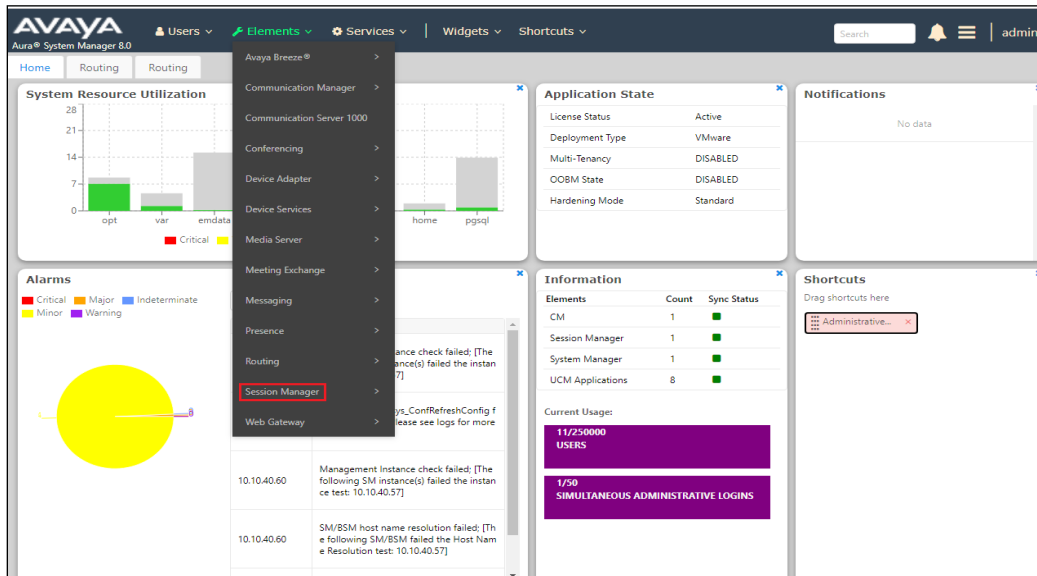
      Group ID: 12
      Group Type: sip

      Group State: in-service
```

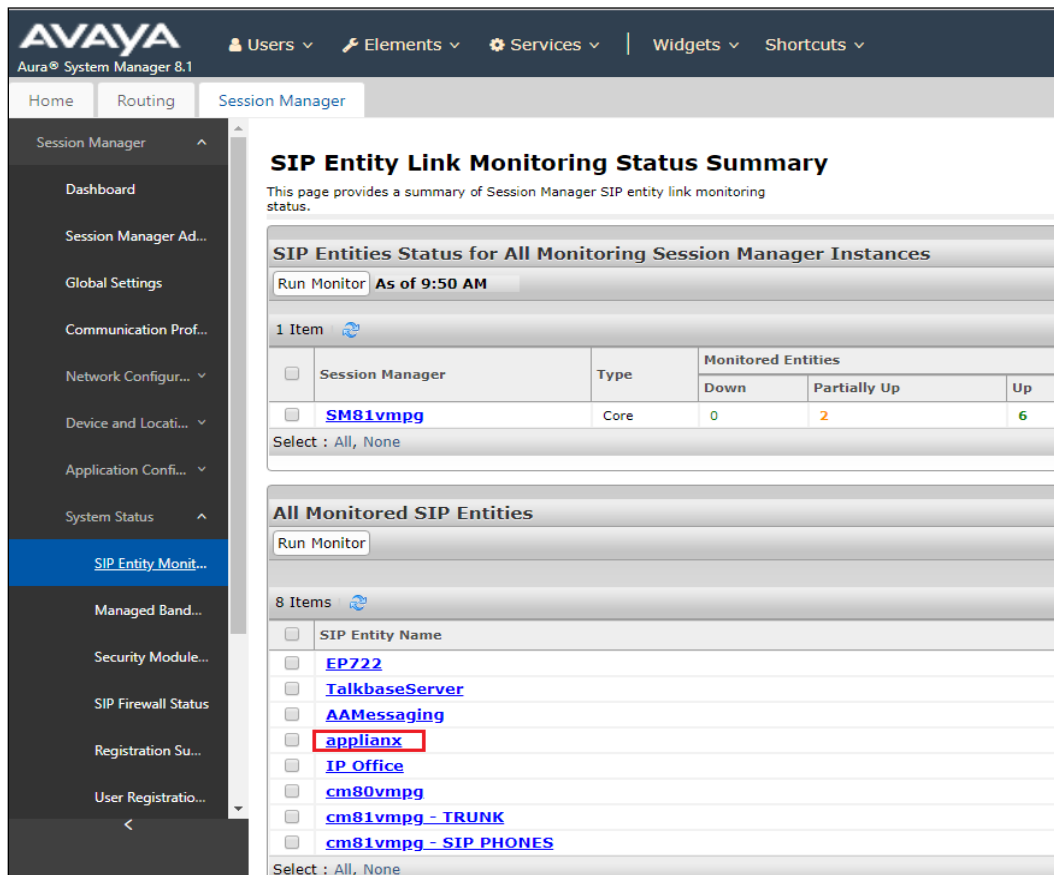


## 8.2. Verify ApplianX SIP Entity is up

Log into System Manager as per **Section 6**. Navigate to **Elements** → **Session Manager**.



Select the **ApplianX** SIP Entity.



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: applanx									
Summary View									
1 Item <span>Filter: Enable</span>									
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SM81vmpg	IPv4	10.10.40.121	5060	TCP	FALSE	UP	200 Ok	UP
Select : None									

### 8.3. Verify the connection from the ApplanX Gateway

Open a web connection to the ApplanX as per **Section 7**. Enter the appropriate credentials, once logged in navigate to **Call Log** from the left window, make a call across the ApplanX and the details of the call will be displayed in the main window as shown below with a call to **2000** from **1001**.

applanx IP Gateway				
Call Activity Log				
Status				
→ Overview				
→ Alarms				
→ Calls				
→ Trunk Status				
System Configuration				
→ Global Configuration				
→ Networking				
→ Setup Wizard				
→ SIP Credentials				
Gateway Configuration				
→ Alias Registrar				
→ DDI Barring				
→ Edit Configurations				
→ Interoperability				
→ Cause Mappings				
Diagnostics				
Call Activity Log				
Clear activity log Download activity log				
Time	Location	Numbers	Message	
2019-09-27 09:44:41.571	Avaya SIP Trunk Ts: 3		Got SIP msg: INVITE sip:2000@devconnect.local SIP/2.0,	
2019-09-27 09:44:41.572	Avaya SIP Trunk Ts: 3		Parsing INVITE, User: 1001 Host: devconnect.local	
2019-09-27 09:44:41.573	Avaya SIP Trunk Ts: 3	From: 1001@devconnect.local To: 2000@devconnect.local	Incoming call detected	
2019-09-27 09:44:41.573	Avaya SIP Trunk Ts: 3	From: 1001@devconnect.local To: 2000@devconnect.local	Matched routing rule "To QSIG"	
2019-09-27 09:44:41.574	Avaya SIP Trunk Ts: 3	From: 1001@devconnect.local To: 2000@devconnect.local	Making outgoing call on endpoint: Trunk 2	
2019-09-27 09:44:41.578	QSIG to CM Trunk Ts: 1	To: 2000 From: 1001	Dialing	
2019-09-27 09:44:45.269	QSIG to CM Trunk Ts: 1	To: 2000 From: 1001	Outgoing leg connected	
2019-09-27 09:44:45.280	Avaya SIP Trunk Ts: 3	From: 1001@devconnect.local To: 2000@devconnect.local	Incoming leg connected	
2019-09-27 09:44:45.294	Avaya SIP Trunk Ts: 3	From: 1001@devconnect.local To: 2000@devconnect.local	Got SIP msg: ACK sip:2000@10.10.40.121;transport=tcp;asm=1 SIP/2.0,	

This same call can be witnessed under the Calls section as shown below where the TDM and SIP channels are shown as green when the call is active.

applanx IP Gateway				
Call Status				
Status				
→ Overview				
→ Alarms				
→ Calls				
→ Call Log				
→ Trunk Status				
System Configuration				
→ Global Configuration				
Call Status				
QSIG to IP Office	TDM			
QSIG to CM Trunk	TDM			
Trunk 3	TDM			
Trunk 4	TDM			
Avaya SIP Trunk	SIP			

## 9. Conclusion

These Application Notes describe the configuration steps required to integrate Aculab ApplianX IP Gateway with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1. All feature and serviceability test cases were completed successfully with any issues and observations outlined in **Section 2.2**.

## 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

Product Documentation for ApplianX IP Gateway can be at the following location:

<http://www.aculab.com/documents/>

---

**©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).