



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Aculab's ApplianX IP Gateway to interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Session Manager R7.0.1 using SIP Trunks - Issue 1.0

Abstract

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

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

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

1. Introduction

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.

2.1. Interoperability Compliance Testing

The testing included:

- Verification of connectivity between Communication Manager (SIP PBX) and Communication Manager (QSIG PBX) via the ApplianX IP Gateway
- 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

2.2. Test Results

Tests were performed to insure full interoperability of an Aculab ApplianX IP Gateway 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.

Note: Although during testing a Communication Manager and Media Gateway was configured with QSIG trunks, an ApplianX IP Gateway will function with any PBX supporting QSIG.

2.3. Support

Technical support can be obtained for Aculab products as follows:

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

Note: An Aculab support contract is required to gain access to Aculab support services.

3. Reference Configuration

Figure 1 illustrates the network configuration used during compliance testing. Communication Manager was configured to use SIP to connect to the VoIP port on the ApplianX via the Session Manager. An E1/T1 port on the ApplianX was configured for QSIG and connected directly to the E1/T1 port on the G450. Avaya 9611G (H.323) and Avaya 2420 digital telephones were used to make and receive calls via the ApplianX.

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

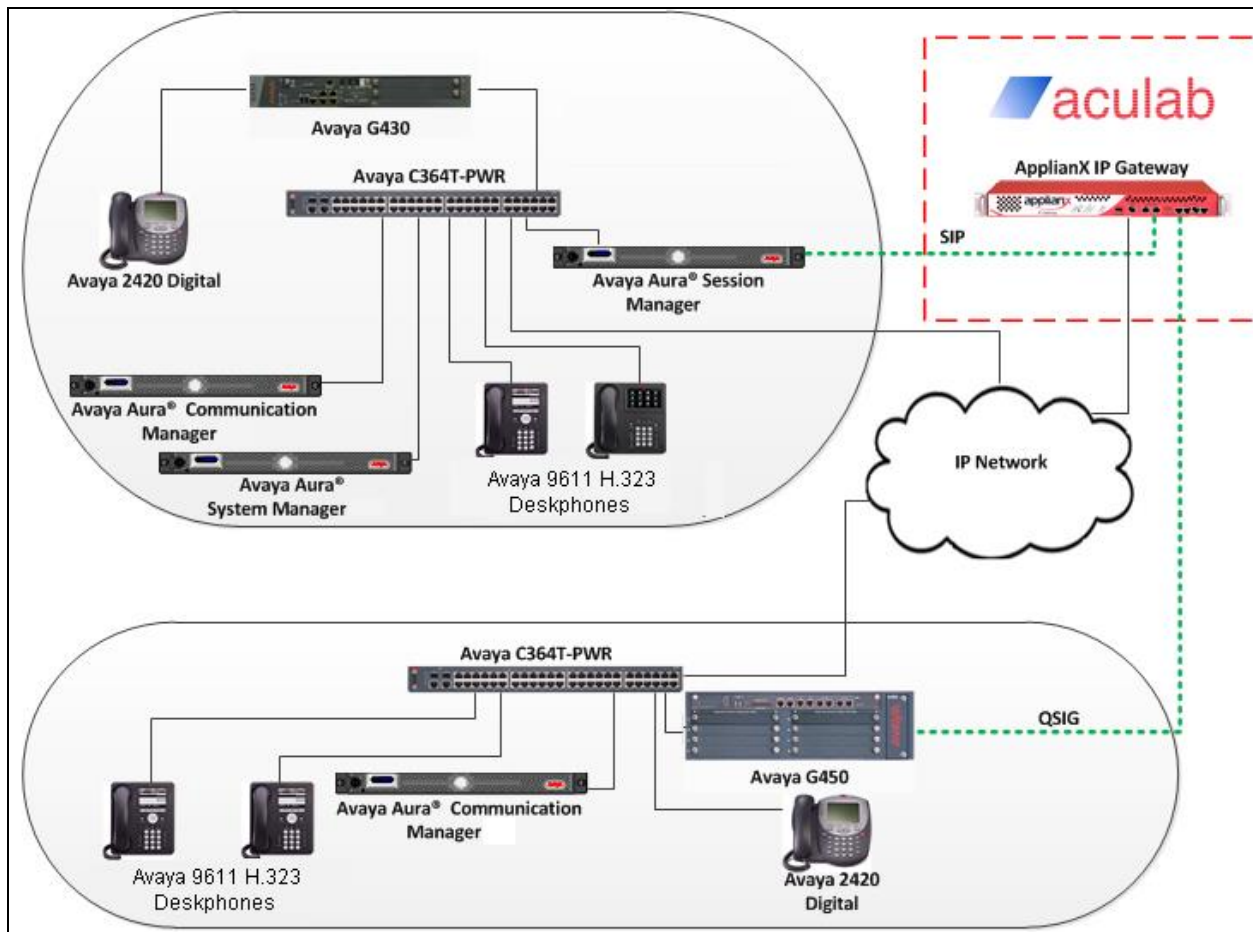


Figure 1: Avaya Aura® Communication Manager/Avaya Aura® Session Manager and Aculab ApplianX IP Gateway Reference Configuration

4. Equipment and Software Validated

The hardware and associated software used in the compliance testing is listed below.

Avaya Equipment	Software Version
Avaya Aura® Communication Manager running on a Virtual Platform	R7.0 Build R017x.00.0.441.0 Version 7.0.1.1.0.441.23169 Updates: 00.0.441.0-223169 PLAT-rhel6.5-0010
Avaya Aura® Session Manager running on a Virtual Platform	R7.0.1 Build 7.0.1.1.70114
Avaya Aura® System Manager running on a Virtual Platform	R7.0.1.2 Build 7.0.0.0.16266 Update 7.0.1.2.075662 Service Pack 2
Avaya 9611G IP Deskphone	6.6029
Avaya 2420 Digital Deskphone	Rel 6.0, FWV 6
Aculab Equipment	Software Version
ApplianX IP Gateway	2.3.6 Build 10551
Gateway Engine	1.6.1-87

Table 1: Hardware and Software Version Numbers

Note: The 3rd Party QSIG PBX was an Avaya Aura® Communication Manager 7.0 and Avaya G450 Gateway

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied that a working system is already in place. 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: (**Note:** during compliance testing all inputs not highlighted in bold were left as default)

- Configure Session Manager Node
- Configure Signaling-Group
- Configure Trunk Group

Note: The configuration of the QSIG PBX is outside of the scope of these Application Notes. The ApplianX will interoperate with a wide range of PBXs supporting QSIG trunks.

5.1. Configure Session Manager Node

For Communication Manager to communicate with Session Manager a node must be configured on Communication Manager. Use the **change node-name ip** command and configure the following:

- **Name** Enter an informative name for the Session manager node (i.e. **sm70vmmc-sig**)
- **IP Address** Enter the IP address of the Session Manager (10.10.60.40)

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
aes62vmmc	10.10.60.10	
default	0.0.0.0	
procr	10.10.60.11	
procr6	::	
sm70vmmc-sig	10.10.60.40	

5.2. Configure Signaling Group

A signaling group is required before a trunk-group can be configured. Use the **add signaling-group** command followed by next available signaling group number to configure the following:

- **Group Type:** Enter **SIP**
- **Transport Method** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **sm70vmmc-sig** (Session Manager Node as configured in **Section 5.1**)
- **Far-end Network Region:** Enter the appropriate Network region (i.e., 1)
- **Far-end Domain:** Enter the appropriate Domain (note: during compliance testing no Domain was used)
- **Initial IP-IP Direct Media:** Enter **y**
- **H323 Station Outgoing Direct Media:** Enter **y**

```
add signaling-group 1                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: procr              Far-end Node Name: sm70vmmc-sig
Near-end Listen Port: 5060            Far-end Listen Port: 5060
                                     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? y Initial IP-IP Direct Media? y
                                     Alternate Route Timer(sec): 6
```

5.3. Configure Trunk Group

This section describes the trunk group configuration used during compliance. Use the **add trunk-group** command followed by next available group number to configure the following:

- **Group Type:** Enter **sip**
- **Group Name:** Enter an informative name for the trunk (i.e., **To SM70VMC**)
- **TAC** Enter a TAC number i.e., **701**
- **Service Type:** Enter **tie**
- **Signaling Group:** Enter the Signaling Group number as configured in **Section 5.2**
- **Number of Members:** Enter the number of channels require to connect to the Session Manger (during compliance testing 15 channels were used)

```
add trunk-group 1                                     Page 1 of 21
TRUNK GROUP
Group Number: 1          Group Type: sip          CDR Reports: y
Group Name: To SM70VMC   COR: 1          TN: 1      TAC: 701
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: 1
                          Number of Members: 15
```

Go to **Page 3** and enter the following:

- **Numbering format:** Enter **private**

```
add trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n      Measured: none
Maintenance Tests? y

Numbering Format: private
                        UI Treatment: service-provider
                        Replace Restricted Numbers? n
                        Replace Unavailable Numbers? n

                        Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

Go to **Page 4** and enter the following:

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

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Send Diversion Header? n	
Support Request History? n	
Telephone Event Payload Type:	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

The screen shot below shows the trunk group members used during compliance testing.

add trunk-group 1	Page 5 of 21
TRUNK GROUP	
Administered Members (min/max): 1/15	
Total Administered Members: 15	
GROUP MEMBER ASSIGNMENTS	
Port	Name
1: T00001	To SM70VMM
2: T00002	To SM70VMM
3: T00003	To SM70VMM
4: T00004	To SM70VMM
5: T00005	To SM70VMM
6: T00006	To SM70VMM
7: T00007	To SM70VMM
8: T00008	To SM70VMM
9: T00009	To SM70VMM
10: T00010	To SM70VMM
11: T00011	To SM70VMM
12: T00012	To SM70VMM
13: T00013	To SM70VMM
14: T00014	To SM70VMM
15: T00015	To SM70VMM

6. Configuring Avaya Aura® Session Manager

A number of configurations are required to enable Session Manager to route calls between Communication Manager and ApplianX. All configurations of Session Manager are performed using System Manager. The configuration operations described in this section can be summarized as follows:

- Logging on to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Locations
- Create ApplianX as a SIP Entity
- Create an Entity Link for ApplianX
- Create a Routing Policy for ApplianX
- Create a Dial Pattern for ApplianX

Note: It is implied a working system is already in place, including a Location, a SIP Entity, an Entity Link, a Routing Policy and a Dial Pattern to route calls to Communication Manager, which are outside the scope of these Application Notes.

6.1. Logging on to Avaya Aura® System Manager

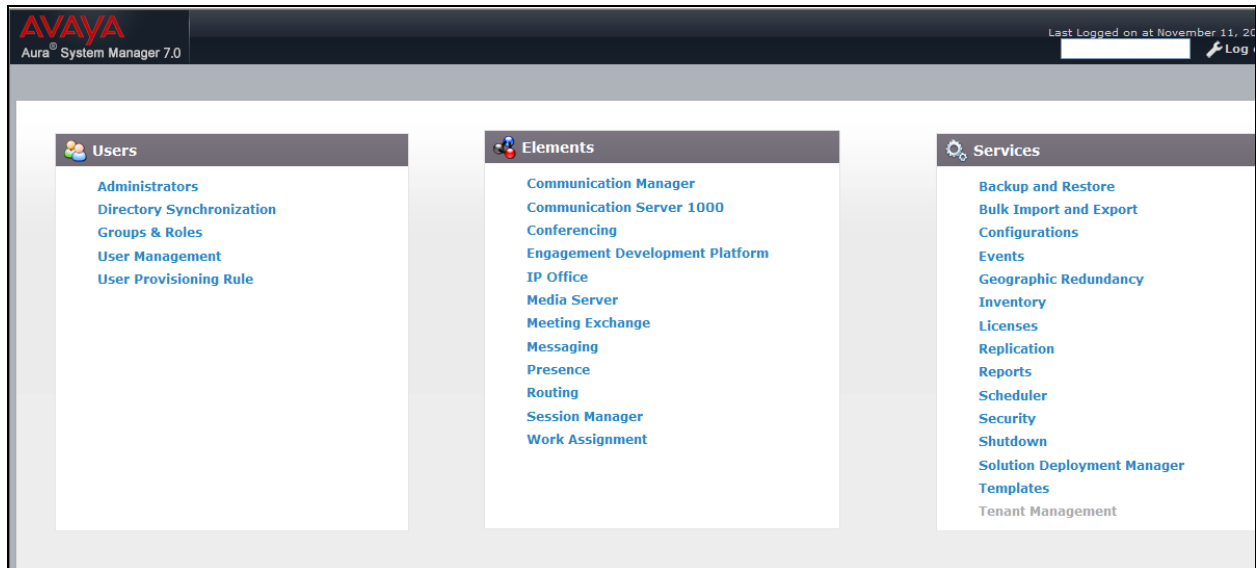
Log on by accessing the browser-based GUI of System Manager, using the URL “http://<fqdn>/SMGR” or “http://<ip-address>/SMGR”, where:

“<fqdn>” is the fully qualified domain name of System Manager or the “<ip-address>” is the IP address of System Manager.

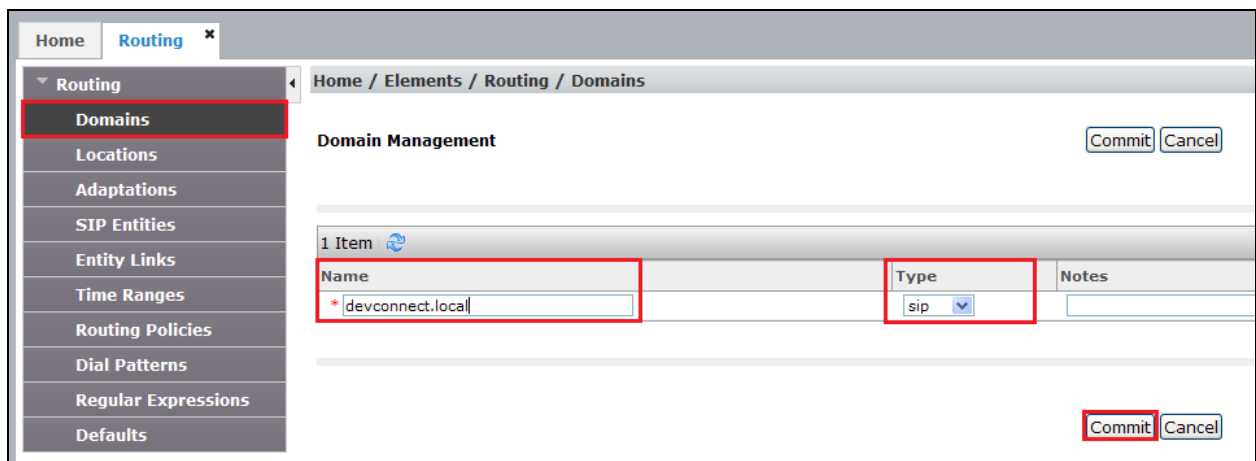
Once the System Manager Web page opens, log in with the appropriate credentials and click on the **Log On** button.

6.2. Administer SIP Domain

Once logged in, select **Routing** from under the **Elements** column.



Select **Domains** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter the domain of the enterprise (i.e., devconnect.local) and select **sip** from the dropdown box. Click **Commit** to save changes.



6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. Select **Locations** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter an informative name for the location (i.e., DevconnectMC). During compliance testing, all other fields were left at default values.

Home / Elements / Routing / Locations

Location Details

Commit Cancel

Help ?

General

* Name: DevConnectMC

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Scroll to the bottom of the page and under **Location Pattern**, click **Add**, and enter an **IP Address Pattern** in the resulting new row. The * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used during compliance testing.

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
10.10.60.	

Select : All, None

Commit Cancel

6.4. Create ApplianX as a SIP Entity

A SIP Entity must be added for the ApplianX. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown).

Note: A SIP Entity was already configured for Communication Manager and was called **CM70**.

Enter the following for the ApplianX SIP Entity:

Under **General** enter the following:

- **Name** Enter an informative name (e.g., **Applianx**)
- **FQDN or IP Address** Enter the IP address of the signalling interface of the ApplianX
- **Type** Select **SIP Trunk** from the dropdown box
- **Location** Select the location from the dropdown box that was configured in **Section 6.3**
- **Time Zone** Select Time zone for this location from the dropdown box
- **SIP Timer** Enter **4**

Once the correct information is entered click the **Commit** Button.

Note: During compliance testing **Adaptation** was left blank.

The screenshot displays the 'SIP Entity Details' configuration page for 'Applianx'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:

- Name:** Applianx
- FQDN or IP Address:** 10.10.60.40
- Type:** SIP Trunk
- Notes:** SIP Trunk to ApplianX
- Adaptation:** (blank)
- Location:** DevConnectMC
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Credential name:** (blank)
- Call Detail Recording:** egress

The 'Commit' button is highlighted in the top right corner.

6.5. Create an Entity Link for ApplianX

The SIP trunk between Session Manager and the ApplianX requires an Entity Link.

To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button, (not shown), enter the following:

- **Name** An informative name, (e.g. **Applianx_5060_TCP**)
- **SIP Entity 1** Select **Session Manager 1** from the **SIP Entity 1** dropdown box
- **Protocol** Select **TCP** or **UDP*** from the Protocol drop down box.
- **Port** Enter **5060**
- **SIP Entity 2** Select **Applianx** from the **SIP Entity 2** dropdown box (configured in **Section 6.4**)
- **Port** Enter **5060** as the Port
- **Connection Policy** Select **trusted** from the drop down box

Click **Commit** to save changes. The following screen shows the Entity Links used.

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* Applianx_5060_TCP	* Session Manager 1	TCP	* 5060	* Applianx	<input type="checkbox"/>	* 5060	trusted	<input type="checkbox"/>	

Select : All, None

***Note:** The UDP protocol was also used in this test and is also supported for the SIP trunk to the Applianx

6.6. Create a Routing Policy for ApplianX

Create routing policies to direct calls to the ApplianX via Session Manager. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). In **Routing Policy Details** enter an informative name in the **Name** field (e.g., **To applianx**), and enter **0** in the **Retries** field. At **SIP Entity as Destination**, click the **Select** button. A Routing Policy was also configured to direct calls to Communication Manager, but is outside the scope of these Application Notes.

Home / Elements / Routing / Routing Policies

Routing Policy Details [Commit] [Cancel]

General

* Name: To applianX

Disabled: ☐

* Retries: 0

Notes: Calls to applianX

SIP Entity as Destination

[Select]

Once the **SIP Entity** list screen opens, check the **applianx** radio button. Click on the **Select** button to confirm the chosen options and then return to the Routing Policies Details screen and select the **Commit** button (not shown) to save.

Home / Elements / Routing / Routing Policies

SIP Entities [Select] [Cancel] [Help ?]

SIP Entities

4 Items [Filter: Enable]

Name	FQDN or IP Address	Type	Notes
6.3 CM	10.10.16.211	CM	Richards CM6.3
Applianx	10.10.60.40	SIP Trunk	SIP Trunk to ApplianX
CM62VMC	10.10.60.11	CM	
Session Manager 1	10.10.60.14	Session Manager	

Select : None

6.7. Create a Dial Pattern for ApplianX

A dial pattern must be created on Session Manager to route calls to and from the ApplianX. During compliance testing a number of patterns were used. The example below shows 4. To configure the Dial Pattern to route calls to the ApplianX, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown). A Dial Pattern was also configured to route calls to Communication Manager, but is outside the scope of these Application Notes. Under **General** enter the following:

- **Pattern** Enter 4
- **Min** Enter 4 as the minimum length of dialed number
- **Max** Enter 4 as the maximum length of dialed number
- **SIP Domain** Select **All** from the drop down box

Click the **Add** button in **Originating Locations and Routing Policies**.

The screenshot displays the Session Manager web interface for configuring a Dial Pattern. The left sidebar shows the 'Routing' menu with 'Dial Patterns' selected. The main area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- * Pattern:** 4
- * Min:** 4
- * Max:** 4
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty field)
- SIP Domain:** -ALL- (dropdown menu)
- Notes:** (empty text area)

At the bottom, the 'Originating Locations and Routing Policies' section contains an 'Add' button (highlighted with a red box) and a 'Remove' button.

In **Originating Location** check the **DevConnectMC** check box. Under **Routing Policies** check the **To applianX** check box. Click on the **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save (not shown).

Home
Routing

Home / Elements / Routing / Dial Patterns

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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"/>	DevConnectMC	

Select : All, None

Routing Policies

2 Items

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	CM1	<input type="checkbox"/>	CM62VMC	Call to CM1 (6.2)
<input checked="" type="checkbox"/>	To applianX	<input type="checkbox"/>	Applianx	Calls to applianX

Select : All, None

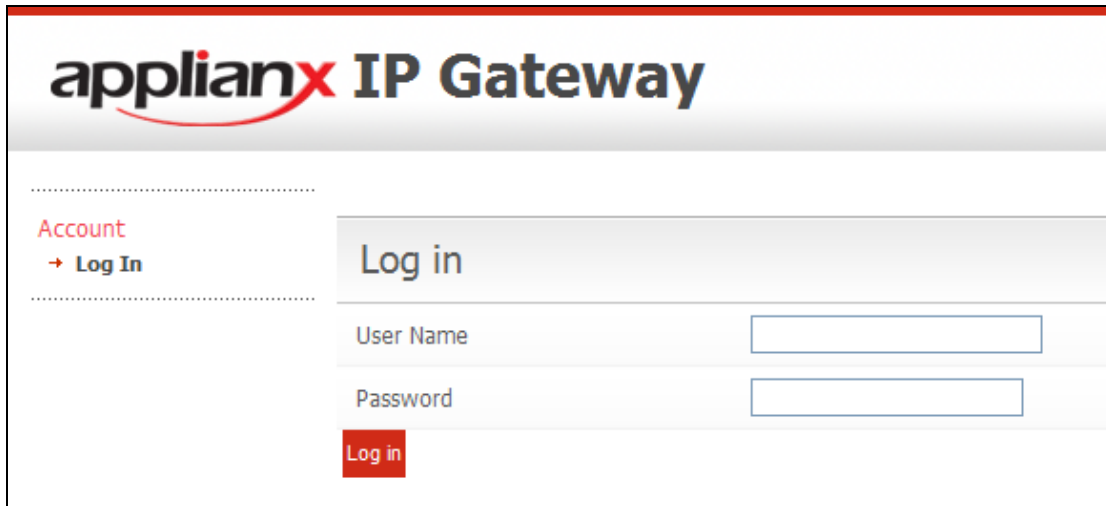
7. Configure Aculab ApplianX IP Gateway

A number of steps are required to configure the Aculab ApplianX IP Gateway. 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 IP Gateway
- Run the Setup Wizard
- Configure QSIG Trunk
- Configure SIP Trunk
- Configure Endpoints
- Configure Groups
- Configure Routes
- 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.



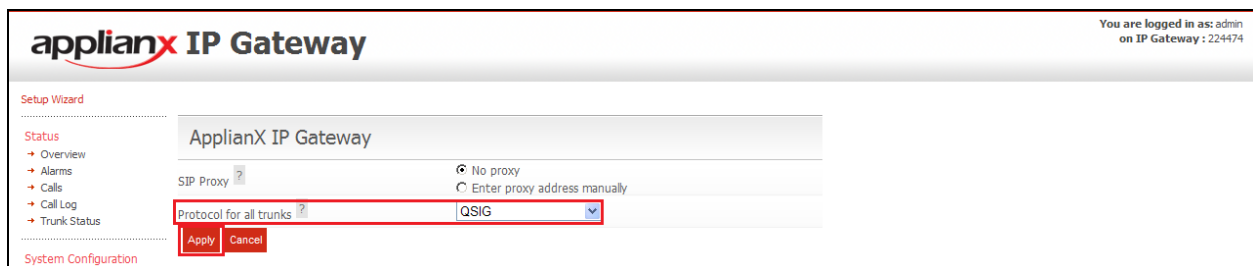
The screenshot shows the login interface for the ApplianX IP Gateway. At the top, the logo "applianx IP Gateway" is displayed, with "applianx" in red and "IP Gateway" in blue. Below the logo, there is a horizontal line. On the left side, the word "Account" is written in red, followed by a red arrow pointing to the text "Log In". On the right side, there is a "Log in" button in a light gray box. Below this button, there are two input fields: "User Name" and "Password". Below the "Password" field, there is a red "Log in" button.

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**.

applianX IP Gateway

You are logged in as: admin
on IP Gateway : 224474

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**

Edit Configurations

Active configuration

Name	Description	Last updated		
Change with Bridge media Qsig - DG		2013-12-06 06:14:08	Running	View Copy

Available configurations

Name	Description	Last updated		
My configuration		2014-02-05 08:51:34	Edit	Delete Copy Use

[Delete Multiple Configurations](#)

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

applianX IP Gateway

Edit Configurations > Gateway Configuration

Status

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

System Configuration

- Global Configuration
- Networking
- Setup Wizard

Editing: Avaya SIP to QSIG Test

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

General Configuration Information

Configuration name:

Configuration description:

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 configurations of the QSIG trunk are dependent on the configuration of the QSIG gateway of 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 left sidebar contains navigation menus for Status, System Configuration, Gateway Configuration, and Diagnostics. The main area is titled 'Editing: Avaya SIP to QSIG Test' and features a tabbed interface with 'Trunks' selected. Below the tabs, there are sections for 'SIP trunks' and 'TDM trunks'. The 'TDM trunks' table lists four trunks, with 'Trunk 1' highlighted and its 'Edit' button also highlighted. At the bottom, there are buttons for '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 (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.

The screenshot shows the 'Edit Configurations > Trunk Overview > Edit Trunk' page for 'Avaya SIP to QSIG Test'. The left sidebar contains navigation links for Status, System Configuration, Gateway Configuration, Diagnostics, and Account. The main content area is titled 'Editing: Avaya SIP to QSIG Test' and includes 'Apply' and 'Cancel' buttons. It is divided into three sections: General settings, SNMP configuration, and Protocol configuration. In the General settings section, the 'Trunk name' is 'Avaya QSIG Trunk' and the 'Trunk description' is 'Trunk to Avaya G450'. Other settings include 'Open inward speech path before answer' (checked), 'Routing group' (TDM trunks), 'Block trunk from call activity' (No), 'Outgoing timeslot allocation strategy' (Highest available), 'Minimum digit count' (0), 'Interdigit timeout' (3000), 'Interdigit timeout for virtual calls' (1000), 'Send sending complete on outgoing calls' (checked), 'Send overlap digits on outgoing calls' (checked), and 'Response to unroutable incoming calls' (Release). The SNMP configuration section has 'Enable SNMP traps' checked. The Protocol configuration section shows a table with one entry: 'QSIG'. The 'Protocol' column is highlighted with a red box, and the 'Change' button is also highlighted with a red box.

Editing: Avaya SIP to QSIG Test																																																		
<div>Apply Cancel</div> <div>General settings</div> <tr> <td>Trunk name</td> <td colspan="2">Avaya QSIG Trunk</td> </tr> <tr> <td>Trunk description</td> <td colspan="2">Trunk to Avaya G450</td> </tr> <tr> <td>Open inward speech path before answer</td> <td colspan="2"><input checked="" type="checkbox"/></td> </tr> <tr> <td>Routing group</td> <td colspan="2">TDM trunks</td> </tr> <tr> <td>Block trunk from call activity</td> <td colspan="2">No</td> </tr> <tr> <td>Outgoing timeslot allocation strategy</td> <td colspan="2">Highest available</td> </tr> <tr> <td>Minimum digit count</td> <td colspan="2">0</td> </tr> <tr> <td>Interdigit timeout (milliseconds)</td> <td colspan="2">3000</td> </tr> <tr> <td>Interdigit timeout for virtual calls (milliseconds)</td> <td colspan="2">1000</td> </tr> <tr> <td>Send sending complete on outgoing calls</td> <td colspan="2"><input checked="" type="checkbox"/></td> </tr> <tr> <td>Send overlap digits on outgoing calls</td> <td colspan="2"><input checked="" type="checkbox"/></td> </tr> <tr> <td>Response to unroutable incoming calls</td> <td colspan="2">Release</td> </tr> <tr> <td colspan="3">SNMP configuration</td> </tr> <tr> <td>Enable SNMP traps</td> <td colspan="2"><input checked="" type="checkbox"/></td> </tr> <tr> <td colspan="3">Protocol configuration</td> </tr> <tr> <td>Protocol</td> <td>QSIG</td> <td> <div>Edit Change</div> </td> </tr>			Trunk name	Avaya QSIG Trunk		Trunk description	Trunk to Avaya G450		Open inward speech path before answer	<input checked="" type="checkbox"/>		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	<input checked="" type="checkbox"/>		Send overlap digits on outgoing calls	<input checked="" type="checkbox"/>		Response to unroutable incoming calls	Release		SNMP configuration			Enable SNMP traps	<input checked="" type="checkbox"/>		Protocol configuration			Protocol	QSIG	<div>Edit Change</div>
Trunk name	Avaya QSIG Trunk																																																	
Trunk description	Trunk to Avaya G450																																																	
Open inward speech path before answer	<input checked="" type="checkbox"/>																																																	
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	<input checked="" type="checkbox"/>																																																	
Send overlap digits on outgoing calls	<input checked="" type="checkbox"/>																																																	
Response to unroutable incoming calls	Release																																																	
SNMP configuration																																																		
Enable SNMP traps	<input checked="" type="checkbox"/>																																																	
Protocol configuration																																																		
Protocol	QSIG	<div>Edit Change</div>																																																

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

The screenshot shows the 'Select a protocol' dialog box. It has a sidebar with navigation links for Status, System Configuration, and Network Configuration. The main content area is titled 'Select a protocol' and contains a table with four rows: DPNSS, QSIG, ETS300, and INS1500. The 'QSIG' row is highlighted with a red box, and the 'Select' button in the rightmost column of this row is also highlighted with a red box.

Select a protocol		
DPNSS	DPNSS Enhanced. Conforming to BTNR-188.	Select
QSIG	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 as is shown in the following screen shots.

Protocol Options

Status

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

System Configuration

- Global Configuration
- Networking
- Setup Wizard
- SIP Credentials

Gateway Configuration

- Alias Registrar
- DOI 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

applanx IP Gateway

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
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....

Call Diversion Supplementary Service Support	
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.inv' Send Mode ?	Presentation Allowed
Default Party Number Type ?	Unknown
Include pSS1InfoElement Progress Indicator ?	<input checked="" type="checkbox"/>
CBWF/CBWN (CC) Supplementary Service Support	
CBWF/CBWN (CC) Enabled ?	<input checked="" type="checkbox"/>
Retain Signalling Connection ?	<input type="checkbox"/>
Message Waiting Supplementary Service Support	
Message Waiting Method ?	Facility (default)
Path Replacement Additional Network Feature	
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

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

QSIG Protocol Compatibility	
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"/>
Raw configuration options	
Options ?	
Apply Cancel	

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

The screenshot shows the 'Editing: Avaya SIP to QSIG Test' configuration page. The left sidebar contains navigation menus for Status, System Configuration, Gateway Configuration, Diagnostics, and Account. The main content area has tabs for General settings, SNMP configuration, and Protocol configuration. The General settings tab is active, showing fields for Trunk name, Trunk description, Open inward speech path before answer, Routing group, Block trunk from call activity, Outgoing timeslot allocation strategy, Minimum digit count, Interdigit timeout, Interdigit timeout for virtual calls, Send sending complete on outgoing calls, Send overlap digits on outgoing calls, and Response to unroutable incoming calls. The Apply button is highlighted in red.

7.4. Configure SIP Trunk

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

The screenshot shows the 'Editing: Avaya SIP to QSIG Test' configuration page with the 'SIP' tab selected. The 'SIP trunks' section displays a table with columns: Name, Description, Type, and Group. The table lists 'Trunk 5' with Type 'SIP' and Group 'No group'. The 'Edit' button for 'Trunk 5' is highlighted in red. Below the table, there are buttons for 'Save Changes', 'Save and Return', and 'Cancel Changes'.

Name	Description	Type	Group
Trunk 5		SIP	No group

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.

The screenshot shows the 'Edit Trunk' configuration page for 'Avaya SIP to QSIG Test'. The left sidebar contains navigation menus for Status, System Configuration, Gateway Configuration, Diagnostics, and Account. The main content area has tabs for General settings, SNMP configuration, and a warning section. The 'General settings' tab is active, showing fields for Trunk name (Avaya SIP Trunk), Trunk description (SIP trunk to Avaya SM), Open inward speech path before answer (checked), Block trunk from call activity (No), Response to unroutable incoming calls (Release), Enable SNMP traps (checked), and SIP Trunk Capacity (120).

7.5. Configure Endpoints

The ApplanX 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.

The screenshot shows the 'Edit SIP Endpoint Overview' page for 'Avaya SIP to QSIG Test'. The left sidebar contains navigation menus for Status, System Configuration, Gateway Configuration, and Account. The main content area has tabs for General, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'Endpoints' tab is active, showing a table of endpoints. The 'Avaya SIP Trunk' endpoint is highlighted, and the 'Proxy' icon (a document with an 'X') is visible in the right column.

Enter a descriptive name in the **Name** field (i.e., Avaya Session Manager) and in the **Description** field enter a description (i.e., Avaya Session Manager Proxy). Configure the following in the remaining fields:

- **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 port** Enter **5060**
- **TCP port** Enter **5060**

Configure the remaining fields as shown in the following screen shot.

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 ? 10.10.60.40

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 ? ☐

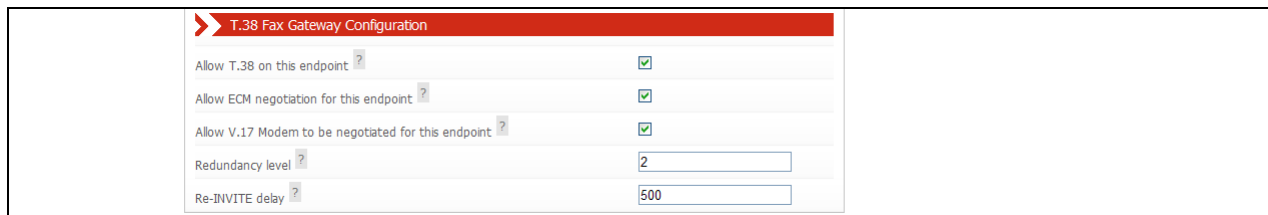
This endpoint is the central PBX ? ☐

Registration

Register a user name with this endpoint ☐

Continuation....

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



The screenshot shows the 'T.38 Fax Gateway Configuration' screen. It has a red header bar with the title. Below the header, there are five configuration items, each with a help icon (question mark) and a checkbox or input field:

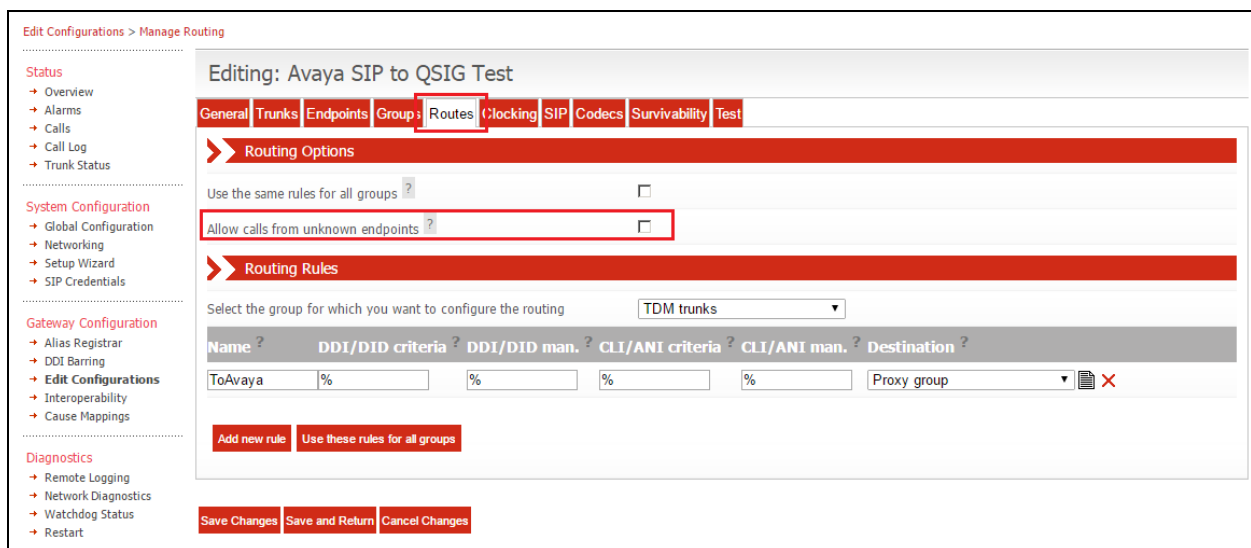
Configuration Item	Value/Status
Allow T.38 on this endpoint	<input checked="" type="checkbox"/>
Allow ECM negotiation for this endpoint	<input checked="" type="checkbox"/>
Allow V.17 Modem to be negotiated for this endpoint	<input checked="" type="checkbox"/>
Redundancy level	2
Re-INVITE delay	500

7.6. Configure Groups

During compliance testing no group configuration was required as only one TDM trunk was configured. If multiple TDM trunks 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.



The screenshot shows the 'Edit Configurations > Manage Routing' screen. The left sidebar contains a navigation menu with sections: Status, System Configuration, Gateway Configuration, and Diagnostics. The main content area is titled 'Editing: Avaya SIP to QSIG Test' and has a red header bar with the title. Below the header, there are several tabs: General, Trunks, Endpoints, Group, Routes, Locking, SIP, Codecs, Survivability, and Test. The 'Routes' tab is selected and highlighted with a red box. Below the tabs, there are three sections: 'Routing Options', 'Routing Rules', and 'Routing Rules'. The 'Routing Options' section has two checkboxes: 'Use the same rules for all groups' (unchecked) and 'Allow calls from unknown endpoints' (unchecked). The 'Routing Rules' section has a dropdown menu for 'Select the group for which you want to configure the routing' set to 'TDM trunks'. Below this, there is a table with columns: Name, DDI/DID criteria, DDI/DID man., CLI/ANI criteria, CLI/ANI man., and Destination. The first row has the following values: 'ToAvaya', '%', '%', '%', '%', and 'Proxy group'. Below the table, there are two buttons: 'Add new rule' and 'Use these rules for all groups'. At the bottom, there are three buttons: 'Save Changes', 'Save and Return', and '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.

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 Groups Routes Clocking 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

7.7.2. 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.

Edit Configurations > Manage Routing

Editing: Avaya SIP to QSIG Test

General Trunks Endpoints Groups Routes Clocking 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 Proxy group

Name ?	DDI/DID criteria ?	DDI/DID man. ?	CLI/ANI criteria ?	CLI/ANI man. ?	Destination ?
ToQSIG	%	%	%	%	TDM trunks

Add new rule Use these rules for all groups

Save Changes Save and Return Cancel Changes

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 left sidebar contains a navigation menu with 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.

The screenshot displays the 'aplianx IP Gateway' configuration interface. The left sidebar contains a navigation menu with 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 features a tabbed interface with 'SIP' selected. The 'SIP' tab is divided into sections: 'Transport for outgoing calls' (Transport protocol: TCP), '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: 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: selected, Use 'inactive' for Hold: unselected, Use 'recvonly' for Hold: unselected, Bridge media streams: unchecked), and 'Jitter Buffer'.

aplianx IP Gateway

Edit Configurations > SIP 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
- Hardware

Account

- Log Out
- Change Password

Editing: Avaya SIP to QSIG Test

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

Transport for outgoing calls

Transport protocol TCP

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 ☒

Send 183 for Ringing ☒

Discontinuous Transmission (DTX) Enabled - With Comfort Noise

Enable Packet Loss Concealment (PLC) ☒

Enable RTCP ☐

Use 'sendonly' for Hold ☒

Use 'inactive' for Hold ☐

Use 'recvonly' for Hold ☐

Bridge media streams ☐

Jitter Buffer

Continuation....

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

The screenshot shows the configuration page for the Avaya SIP Gateway. The page is divided into several sections, each with a red header and a right-pointing arrow. The sections are: Jitter Buffer, Listening ports, Endpoint monitoring, Message Waiting Supplementary Service Support, Call Diversion Supplementary Service Support, and Custom messages conveying non-SIP features. Each section contains various configuration options, some with checkboxes and some with input fields. At the bottom of the page, there are three buttons: Save Changes, Save and Return, and Cancel Changes.

Section	Configuration Option	Value / Status
Jitter Buffer	Manual jitter buffer configuration	<input type="checkbox"/>
	Listening ports	
Listening ports	UDP listen port (0 to disable)	5060
	TCP listen port (0 to disable)	5060
Endpoint monitoring	Endpoint monitoring	
	Polling interval	60
Message Waiting Supplementary Service Support	Accept unsolicited message summary	<input checked="" type="checkbox"/>
	Send unsolicited message summary	<input checked="" type="checkbox"/>
Call Diversion Supplementary Service Support	Call Diversion Enabled	<input checked="" type="checkbox"/>
	History-Info Method Preferred	<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"/>
Custom messages conveying non-SIP features	Exchange transfer information	<input checked="" type="checkbox"/>
	Exchange Route Optimisation/Path Replacement information	<input checked="" type="checkbox"/>
	CBWF/CBWFU Enabled	<input checked="" type="checkbox"/>

7.10. Configure Codecs

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

The screenshot shows the 'Edit Configurations > Codec Configuration' page. The page has a sidebar with navigation links and a main content area. The main content area has a tabbed interface with tabs for General, Trunks, Endpoints, Groups, Routes, Clocking, SIP, Codecs, Survivability, and Test. The 'Codecs' tab is selected. The 'Codecs' tab has two sub-tabs: 'Available codecs' and 'Configured codecs'. The 'Available codecs' list contains 'G729'. The 'Configured codecs' list contains 'G711_Alaw' and 'G711_Mulaw'. There are buttons for moving codecs between the two lists: '>', '>>', '<<', and '<'. At the bottom of the page, there are three buttons: Save Changes, Save and Return, and Cancel Changes.

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 Configured codecs

G729

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 View Copy

Available configurations

Name	Description	Last updated	
Avaya SIP to QSIG Test		2015-09-02 21:41:11	Edit Delete Copy Use

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

The screenshot shows the 'Applianx IP Gateway' web interface. On the left is a navigation menu with 'Status' (Overview, Alarms, Calls, Call Log, Trunk Status) and 'System Configuration' (Global Configuration, Networking, Setup Wizard, SIP Credentials). The main area displays a 'Question' box with the text: 'Are you sure you want to use the configuration Avaya SIP to QSIG Test?'. Below the question are two buttons: 'Yes' and 'No'.

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

The screenshot shows the 'Applianx IP Gateway' web interface with the 'Edit Configurations' page. The left navigation menu is the same. The main area has a title 'Edit Configurations' and a red bar indicating 'Active configuration'. Below this is a table with columns 'Name', 'Description', and 'Last updated'. The table contains one entry: 'Avaya SIP to QSIG Test' with a description of '2015-09-02 21:41:11' and a status of 'Running'. To the right of the table are 'View' and 'Copy' buttons.

Name	Description	Last updated
Avaya SIP to QSIG Test	2015-09-02 21:41:11	Running

8. Verification Steps

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

8.1. Verify the SIP Entity Link status for the ApplianX IP Gateway

From System Manager select **Session Manager** from under the **Elements** column (not shown). When the **Session Manager** tab opens select **System Status** followed by **SIP Entity Monitoring**, then click on **Session Manager**.

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page. The left sidebar has 'System Status' and 'SIP Entity Monitoring' highlighted. The main content area shows a summary of monitoring status with a 'Run Monitor' button. Below is a table of monitored entities.

Session Manager	Type	Monitored Entities						Total
		Down	Partially Up	Up	Not Monitored	Deny		
Session Manager 1	Core	0	0	3	0	0	3	

When the **Session Manager Entity Link Connection Status** window opens, observe the **Conn Status** and **Link Status** and ensure that they are both showing as **up** for the **ApplianX** SIP Entity.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. The left sidebar has 'SIP Entity Monitoring' and 'Managed Bandwidth Usage' highlighted. The main content area shows a summary of connection status with a 'Summary View' button. Below is a table of entity links.

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	6.3 CM	10.10.16.211	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Applianx	10.10.60.40	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM62VMMC	10.10.60.11	5060	TCP	FALSE	UP	200 OK	UP

8.2. Verify calls via the ApplianX IP Gateway

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.

9. Conclusion

These Application Notes describe the configuration steps required for an Aculab ApplianX IP Gateway to interoperate with an Avaya Aura® Communication Manager 7.0 using a SIP trunk to interoperate with a QSIG trunk. All test cases have passed and met the objectives.

10. Additional References

This section references the Avaya and Aculab documentation that is relevant to these Application Notes. Product documentation for Avaya products may be found at:

<http://support.avaya.com>

[1] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.0, August 2015, Document Number 555-245-205.*

[2] *Administering Avaya Aura® Communication Manager, Release 7.0, August 2015, Document Number 03-300509.*

[3] *Administering Avaya Aura® Session Manager, Release 7.0, August 2015*

[4] *Administering Avaya Aura® System Manager, Release 7.0, August, 2015*

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

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

©2016 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.