Avaya Solution & Interoperability Test Lab

Application Notes for configuring Aculab's ApplianX IP Gateway to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 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 so as to route calls to and from the ApplianX. Testing focused on verifying that SIP and QSIG signals were converted correctly.

Note: During compliance testing Communication Manager was 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 and 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 with the following observations:

- Music on Hold is not a supported feature on the ApplianX IP Gateway in this solution.
- Message Waiting Indication is not supported on this version of ApplianX IP Gateway software.

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 G430. Avaya 9608 (H.323), 9641G (H.323) and Avaya 2420 digital telephones were used to make and receive calls via the ApplianX. System Manager was used to manage the Communication Manager.

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 G430 media gateway.

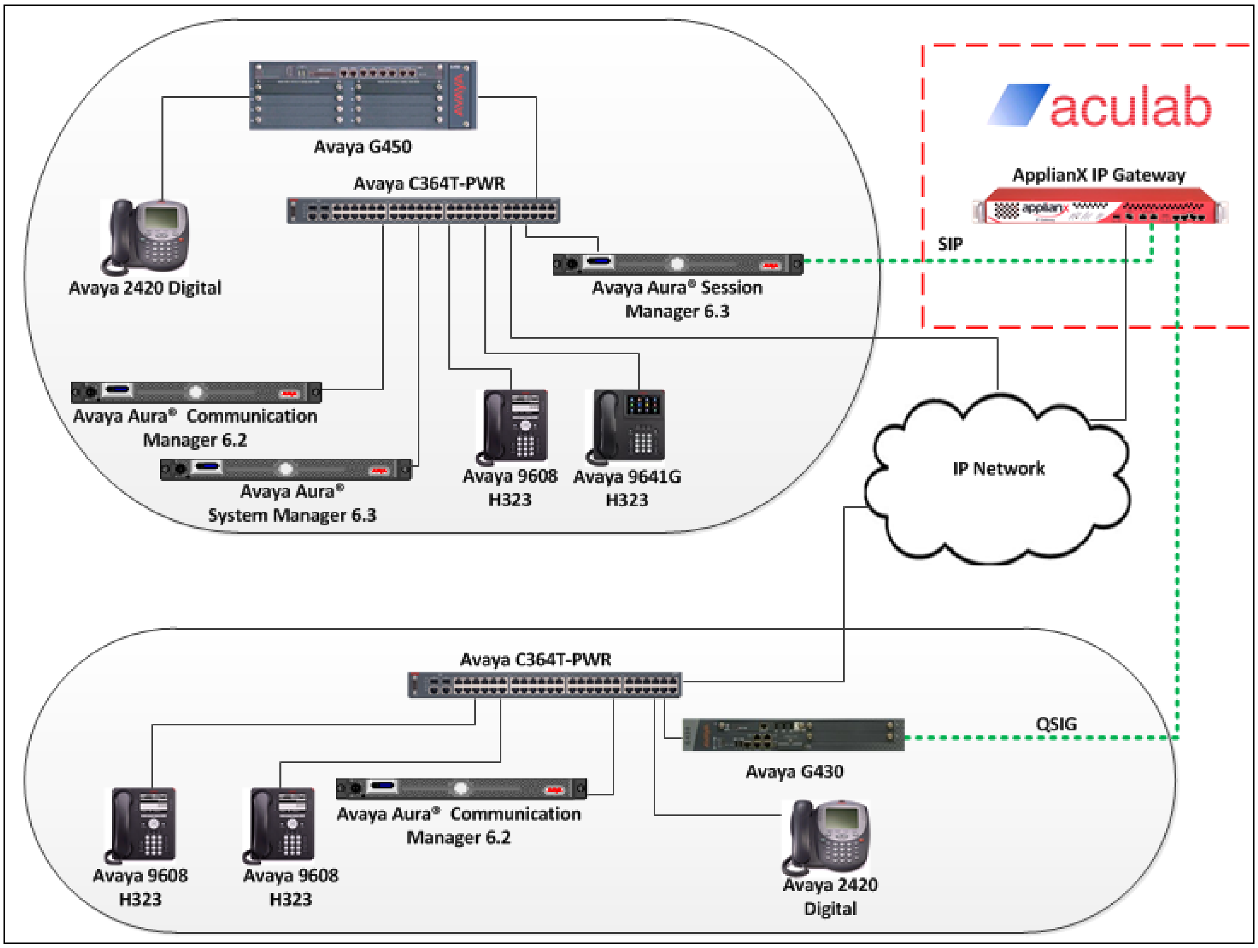


Figure 1: Avaya Aura® Communication Manager/Avaya Aura® Session Manager and Aculab ApplianX IP Gateway Reference Configuration

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	Avaya Aura® Communication Manager R6.2 Build R016x.02.0.832.0
Avaya Aura® Session Manager	R6.3 Build 6.3.0.8.5682-6.3.8.2826 Update 6.3.5.52017
Avaya Aura® System Manager	R6.3 Build 6.3.5.0.635005
Avaya 9608 IP phone	S9608_11HALBR6_2_4_08_V452
Avaya 9641G IP Phone	S9621_11HALBR6_2_4_08_V452
Avaya 2420 Digital phone	Rel 6.0, FWV 6
Aculab Equipment	**Software Version**
ApplianX IP Gateway Gateway Engine	Version 2.3.1 release 792 Version 1.5.2-208

Table 1: Hardware and Software Version Numbers

Note: The 3rd –Party QSIG PBX was an Avaya Aura® Communication Manager 6.3 and Avaya G430 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 for the Session manager node **(**i.e. **sm62vmmc-sig**)
- **IP Address** Enter the IP address of the Session Manager (10.10.60.14)

.

```
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              ::
sm62vmmc-sig        10.10.60.14
```

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 **sm62vmmc-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: sm62vmcmc-sig
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? 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 SM62VMMC)**
- **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 SM62VMMC                 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
                                                UUI 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
GROUP MEMBER ASSIGNMENTS                  Total Administered Members:  15

       Port            Name
  1: T00001            To SM62VMM
  2: T00002            To SM62VMM
  3: T00003            To SM62VMM
  4: T00004            To SM62VMM
  5: T00005            To SM62VMM
  6: T00006            To SM62VMM
  7: T00007            To SM62VMM
  8: T00008            To SM62VMM
  9: T00009            To SM62VMM
 10: T00010            To SM62VMM
 11: T00011            To SM62VMM
 12: T00012            To SM62VMM
 13: T00013            To SM62VMM
 14: T00014            To SM62VMM
 15: T00015            To SM62VMM
```

6. Configuring Avaya Aura® Session Manager

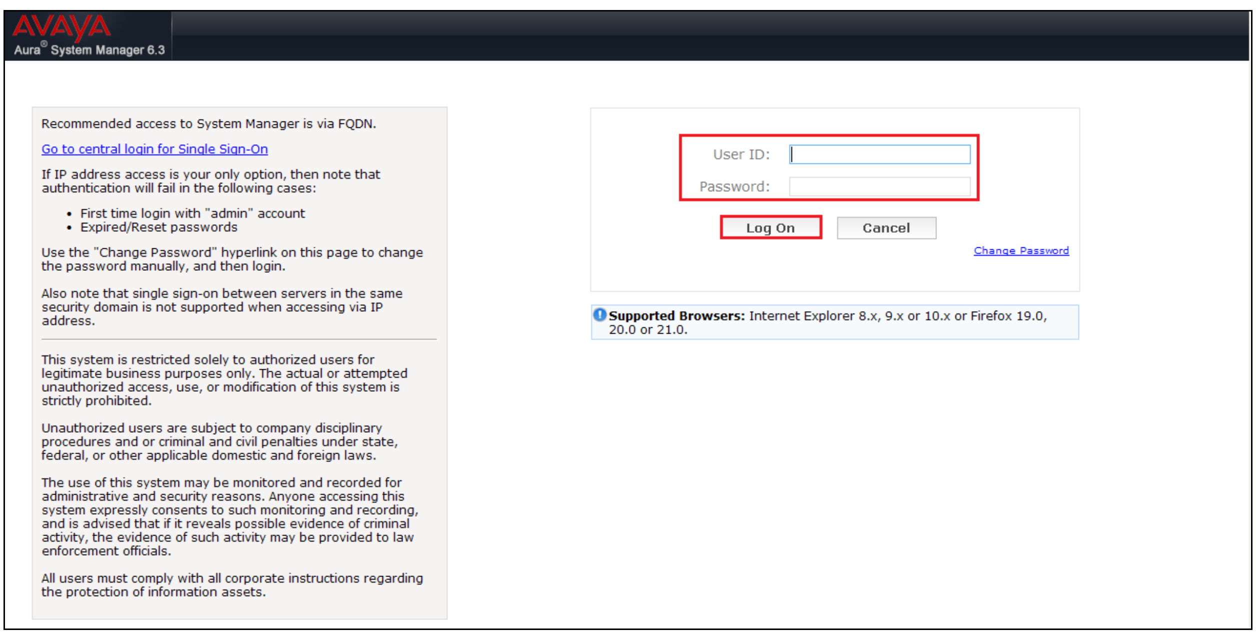
A number of configurations are required to enable Session Manager to route calls between Communication Manager and ApplianX. All configurations of Session Manager are performed using System Manager. The configuration operations described in this section can be summarized as follows:

- 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.

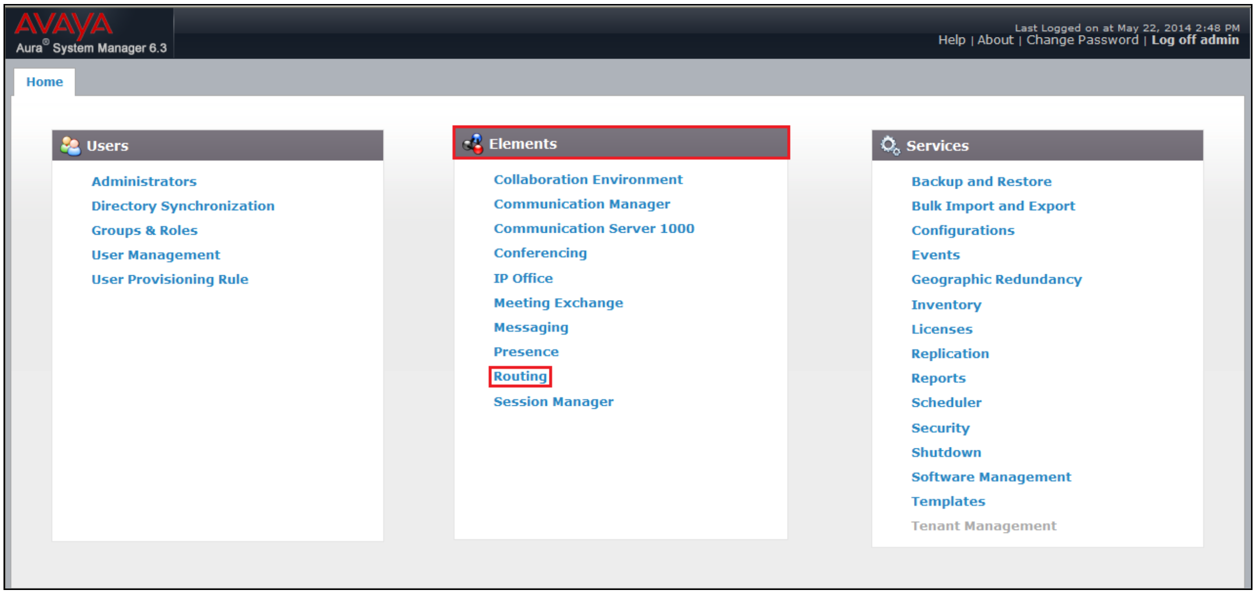
6.1. Logging on to Avaya Aura® System Manager

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.

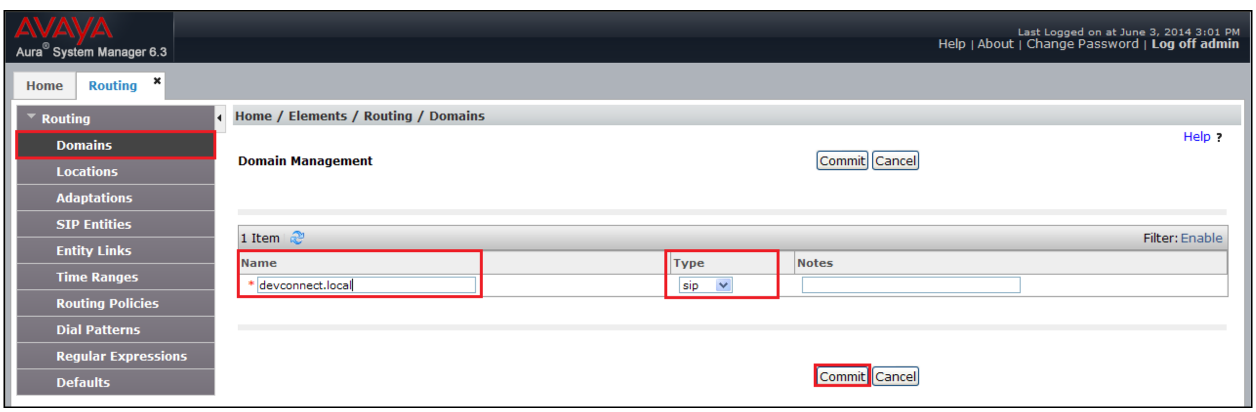


6.2. Administer SIP Domain

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

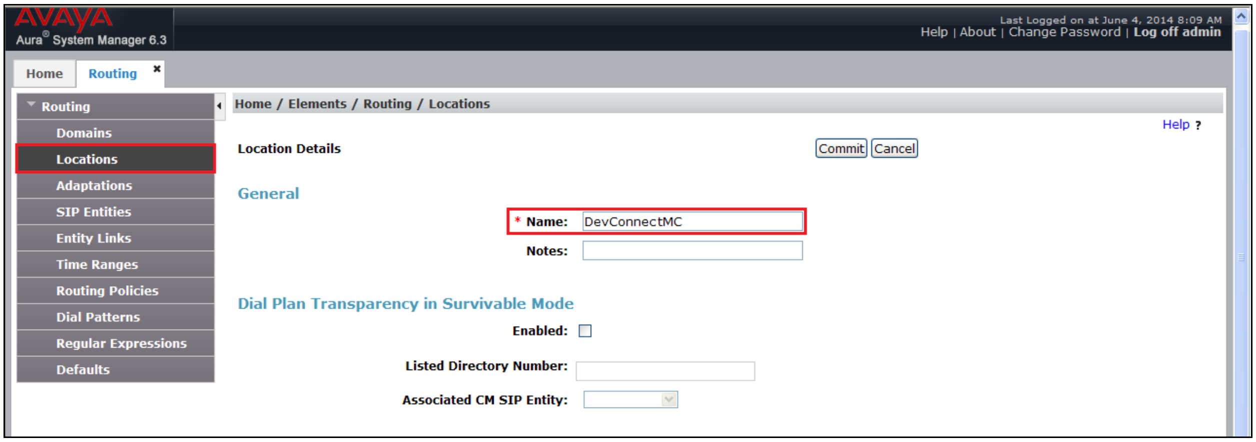


Select **Domains** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter the domain of the enterprise (i.e., devconnect.local) and select **sip** from the dropdown box. Click **Commit** to save changes.

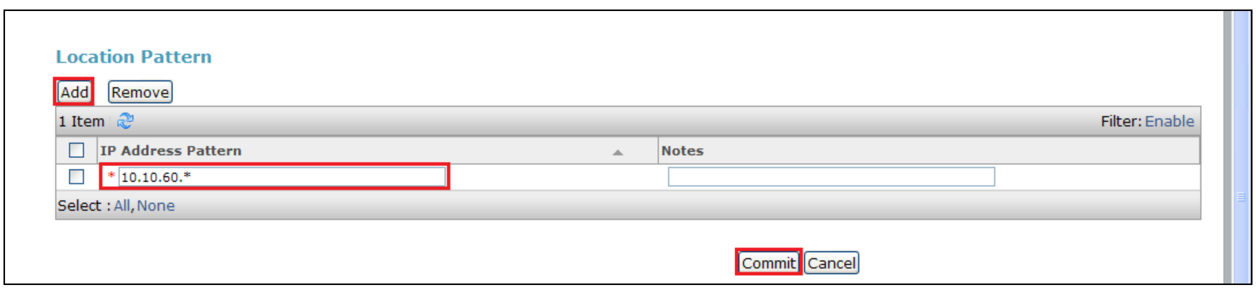


6.3. Administer Locations

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.



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.



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).

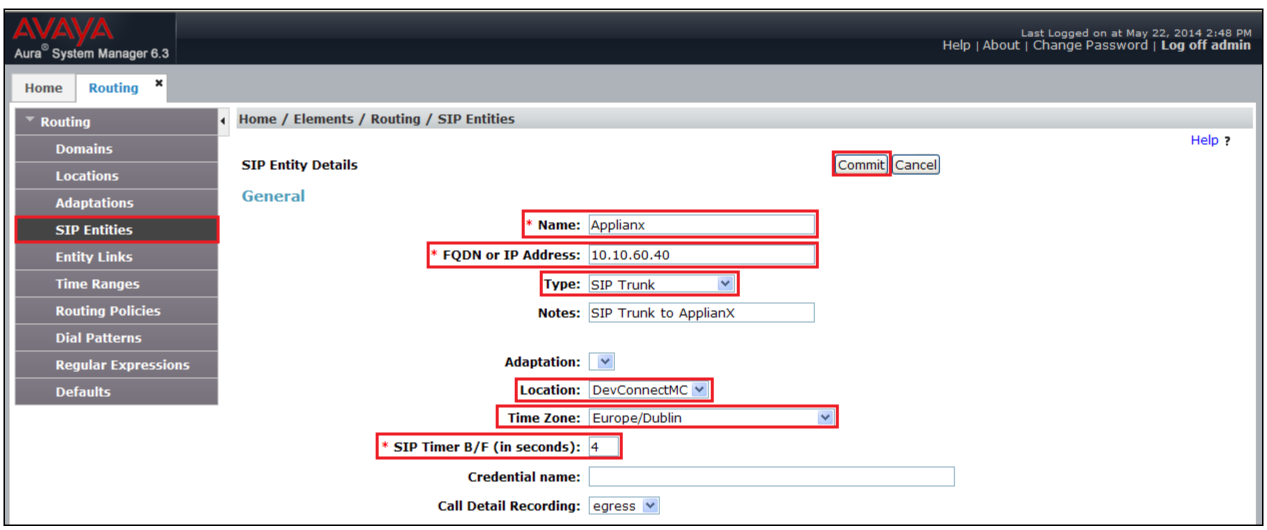
Note: A SIP Entity was already configured for Communication Manager and was called **CM63**.

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.

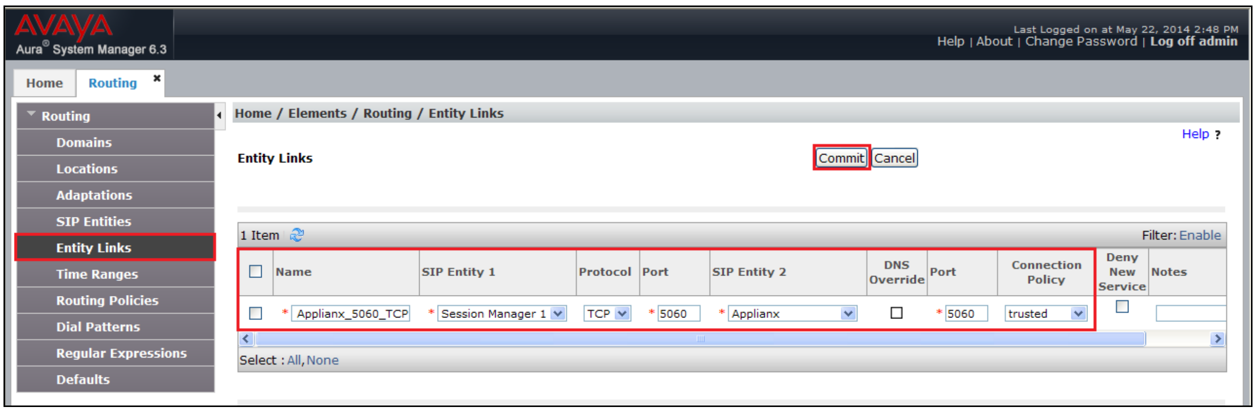


6.5. Create an Entity Link for ApplianX

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:

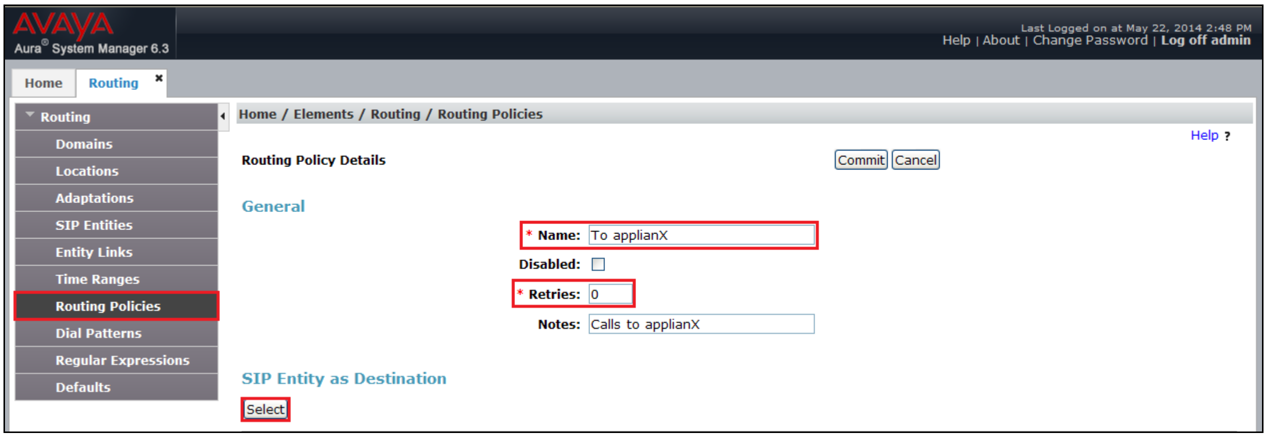
- **Name** An informative name, (e.g. **Applianx_5060_TCP**)
- **SIP Entity 1** Select **Session Manager 1** from the **SIP Entity 1** dropdown box
- **Protocol** Select **TCP** from the Protocol drop down box
- **Port** Enter **5060**
- **SIP Entity 2** Select **applianx** from the **SIP Entity 2**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

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

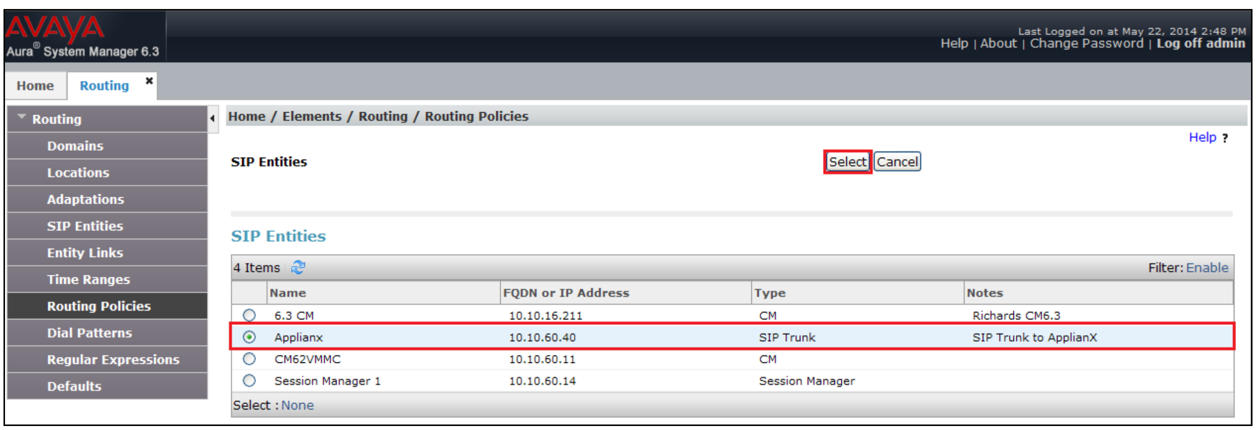


6.6. Create a Routing Policy for ApplianX

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, (example **To appliianx**), 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.



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.

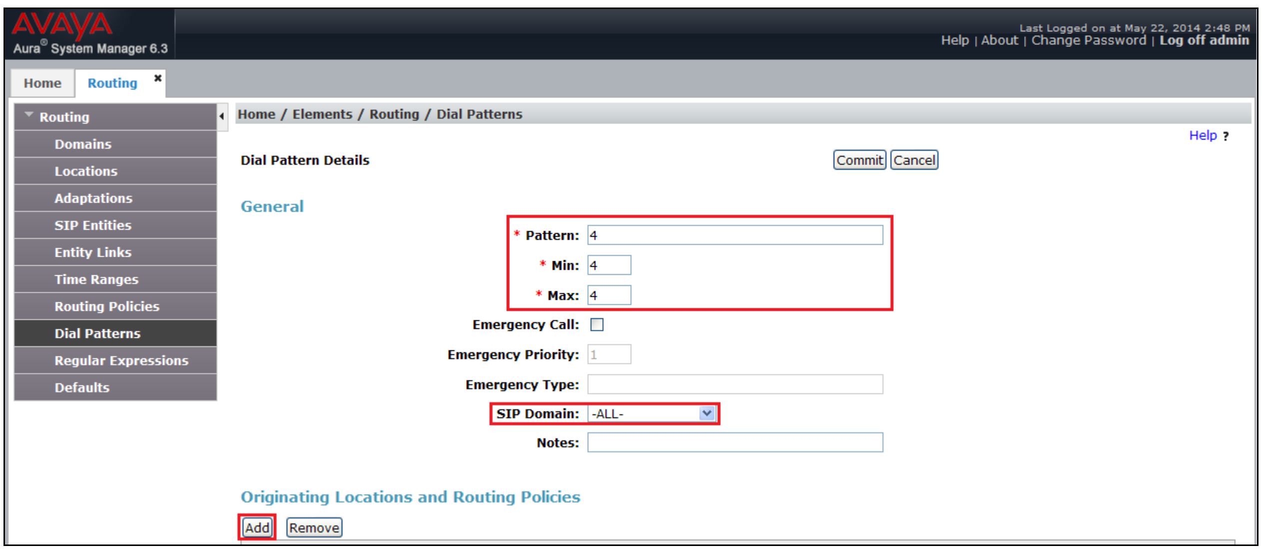


6.7. Create a Dial Pattern for ApplianX

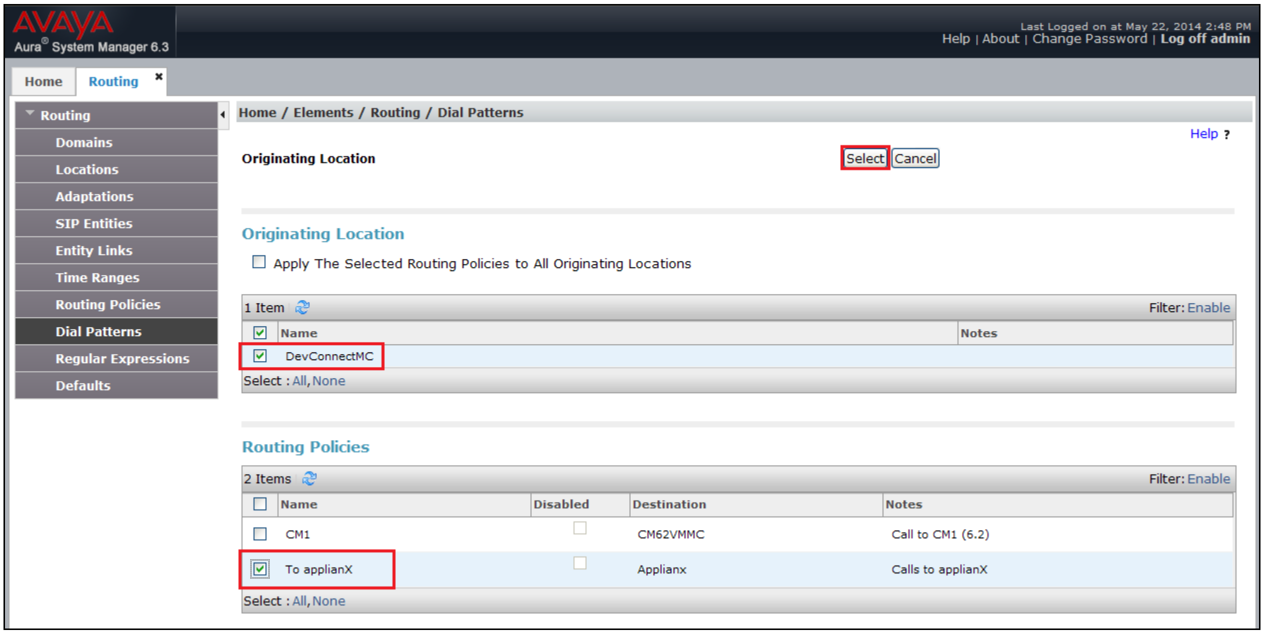
A dial pattern must be created on Session Manager to route calls to and from the ApplianX. During compliance testing a number of patterns were used. The example below shows 4. To configure the Dial Pattern to route calls to the ApplianX, select **Dial Patterns** on the left panel menu and then click 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 out 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**.



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).



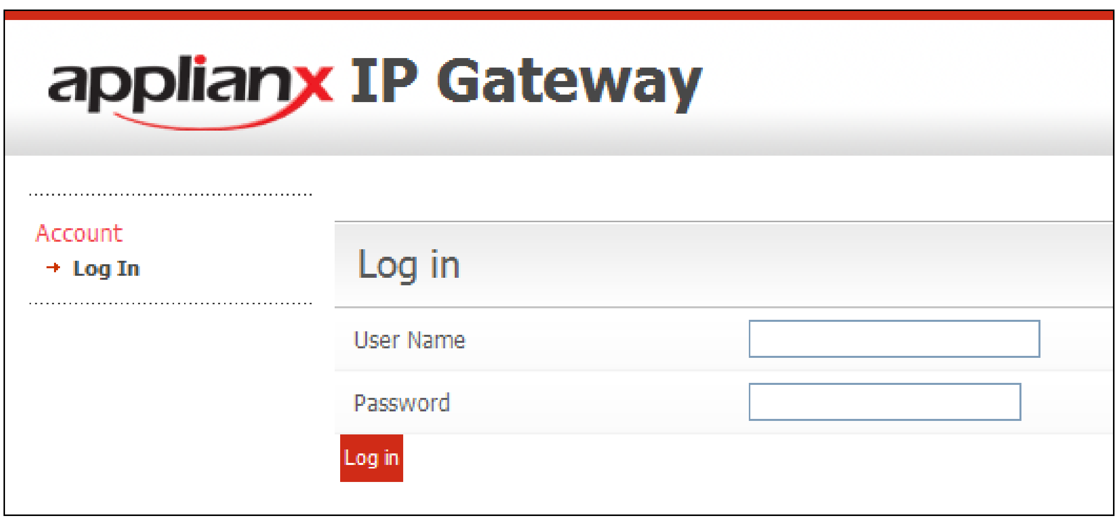
7. Configure Aculab ApplianX IP Gateway

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

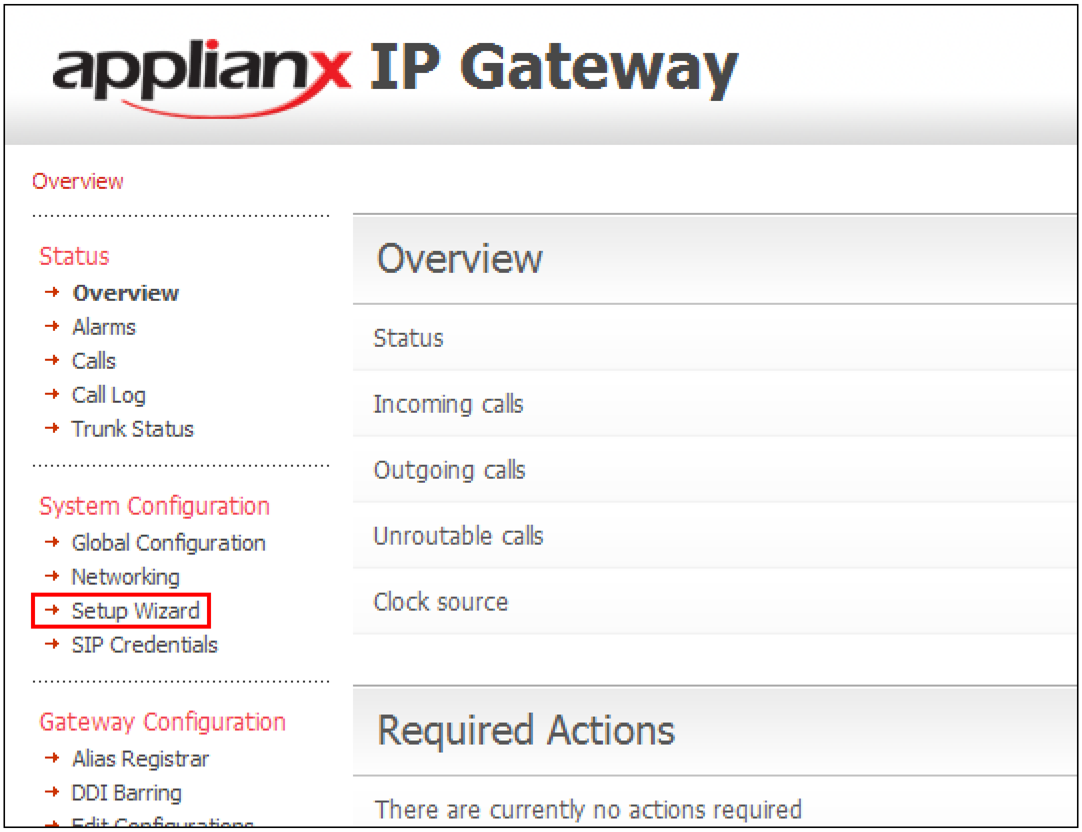
7.1. Login to ApplianX IP Gateway

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.

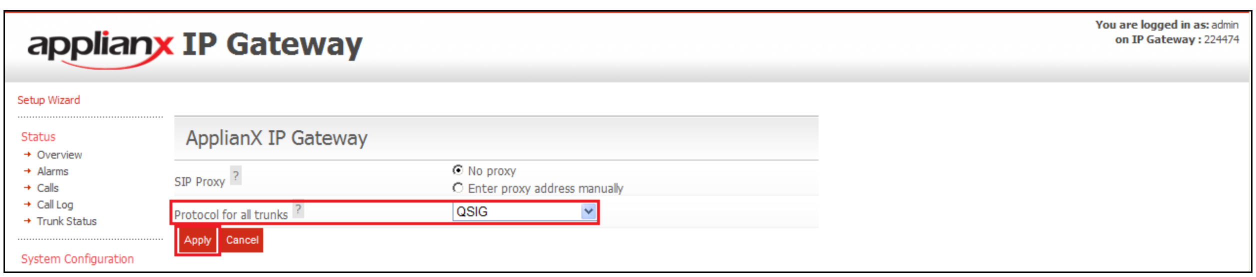


7.2. Run the Setup Wizard

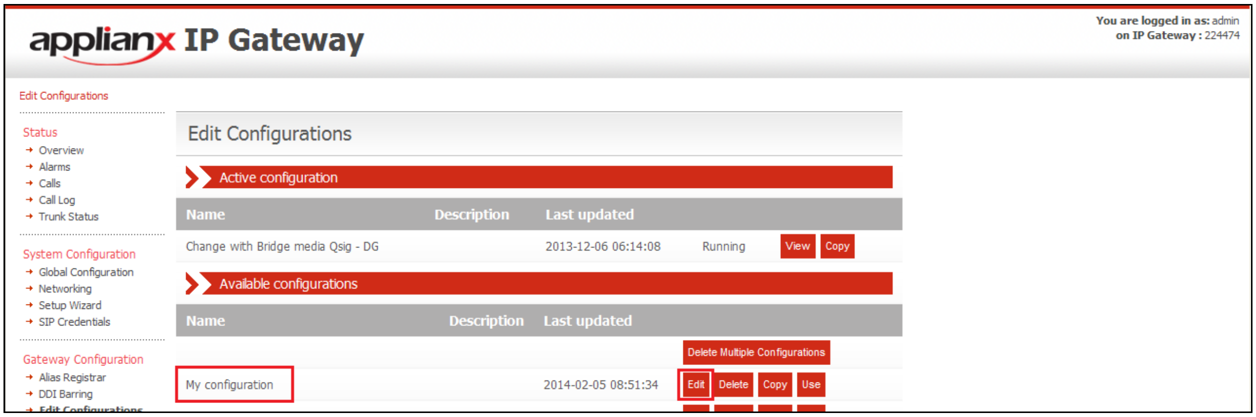
After the main web page opens, select **Setup Wizard** from System Configuration section.



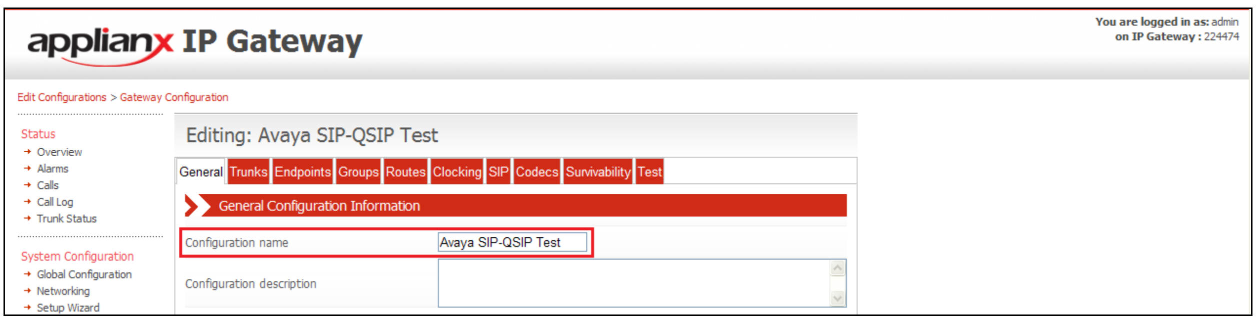
Once the **Setup Wizard** page opens, select **QSIG** from the **Protocol for all trunks**, drop-down box, and click on the **Apply** button.



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

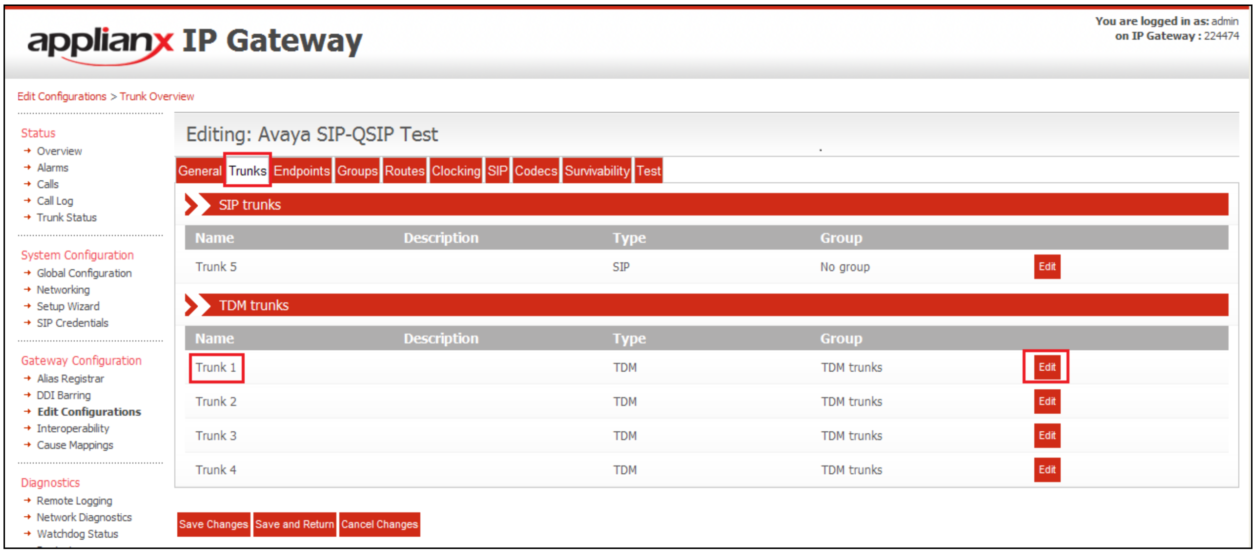


In the **General** tab, give a descriptive name to the configuration. During compliance testing, **Avaya SIP-QSIG Test** was used.

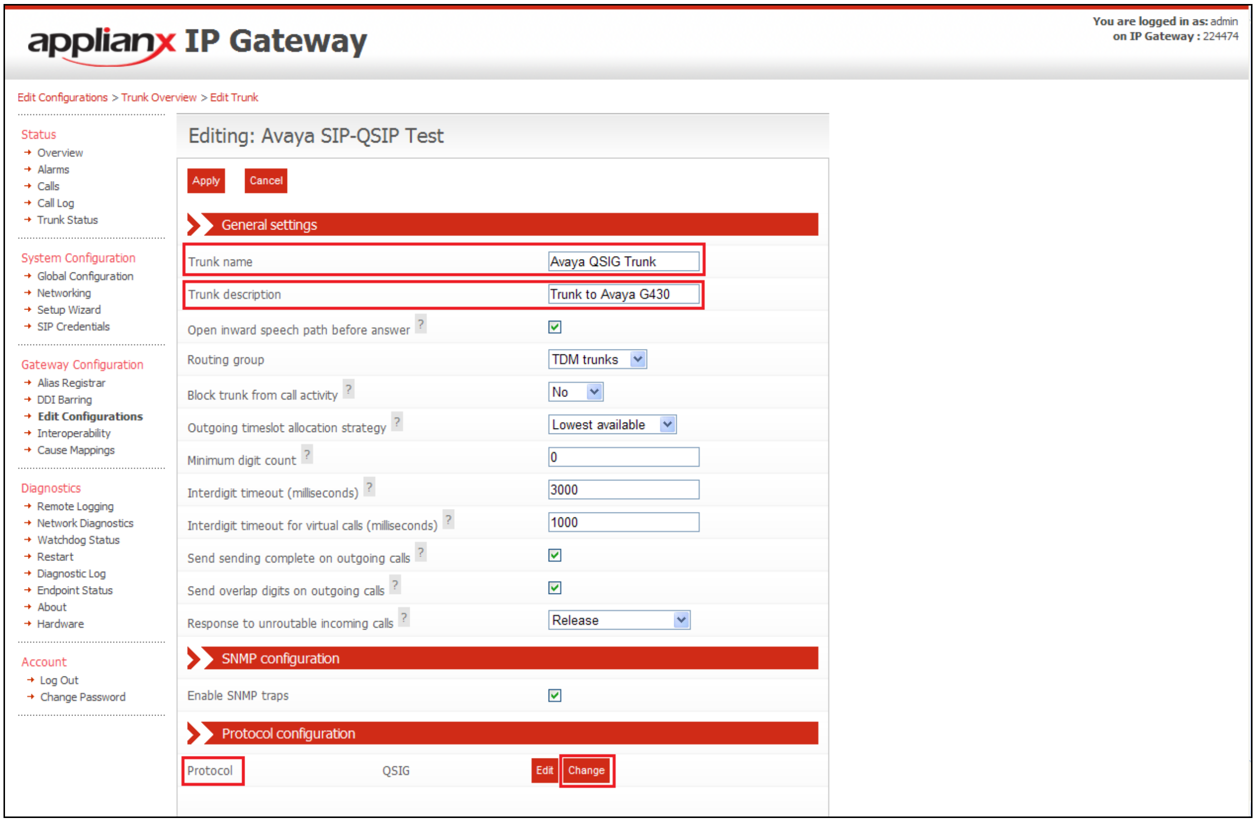


7.3. Configure QSIG Trunk

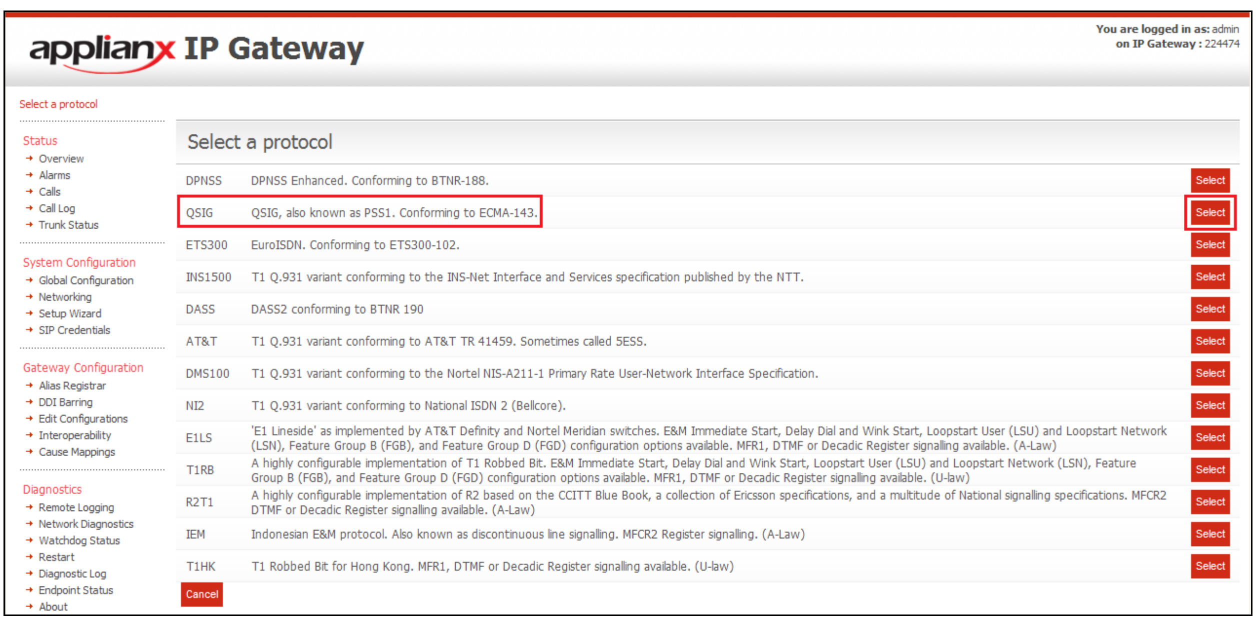
Click on the **Trunks** Tab followed by the **Trunk 1 Edit** button. This trunk was configured for QSIG. A cable was connected between the E1/T1 Trunk 1 port on the front of the ApplianX and the T1/E1 port on the G430 Gateway of the Communication Manager. Please note that the configurations of the QSIG 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.



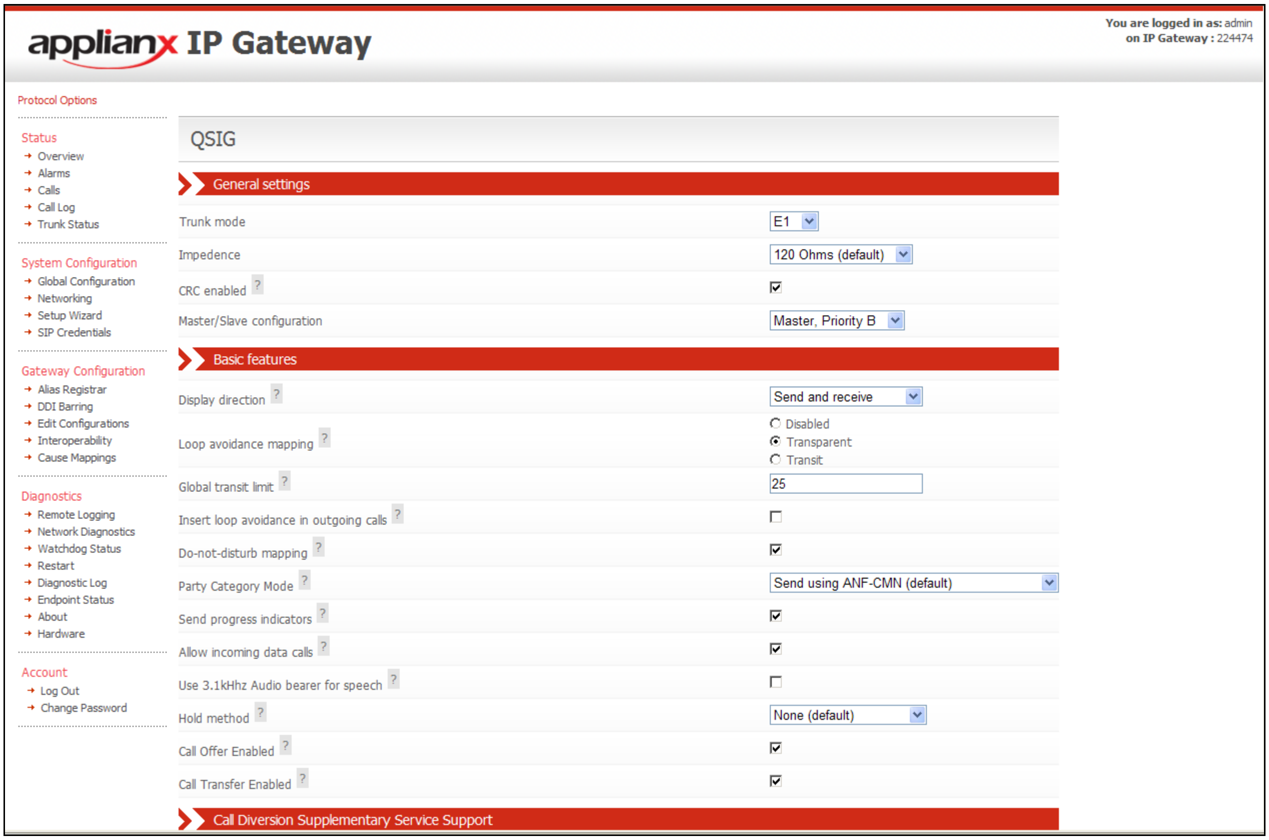
In the **Trunk Name** field (i.e., Avaya QSIG Trunk) and in the **Trunk description** field enter a description (i.e., Trunk to Avaya G430). Configure the remaining fields as shown in the following screen shot. Click on the **Change** button in the **Protocol configuration** section**.**



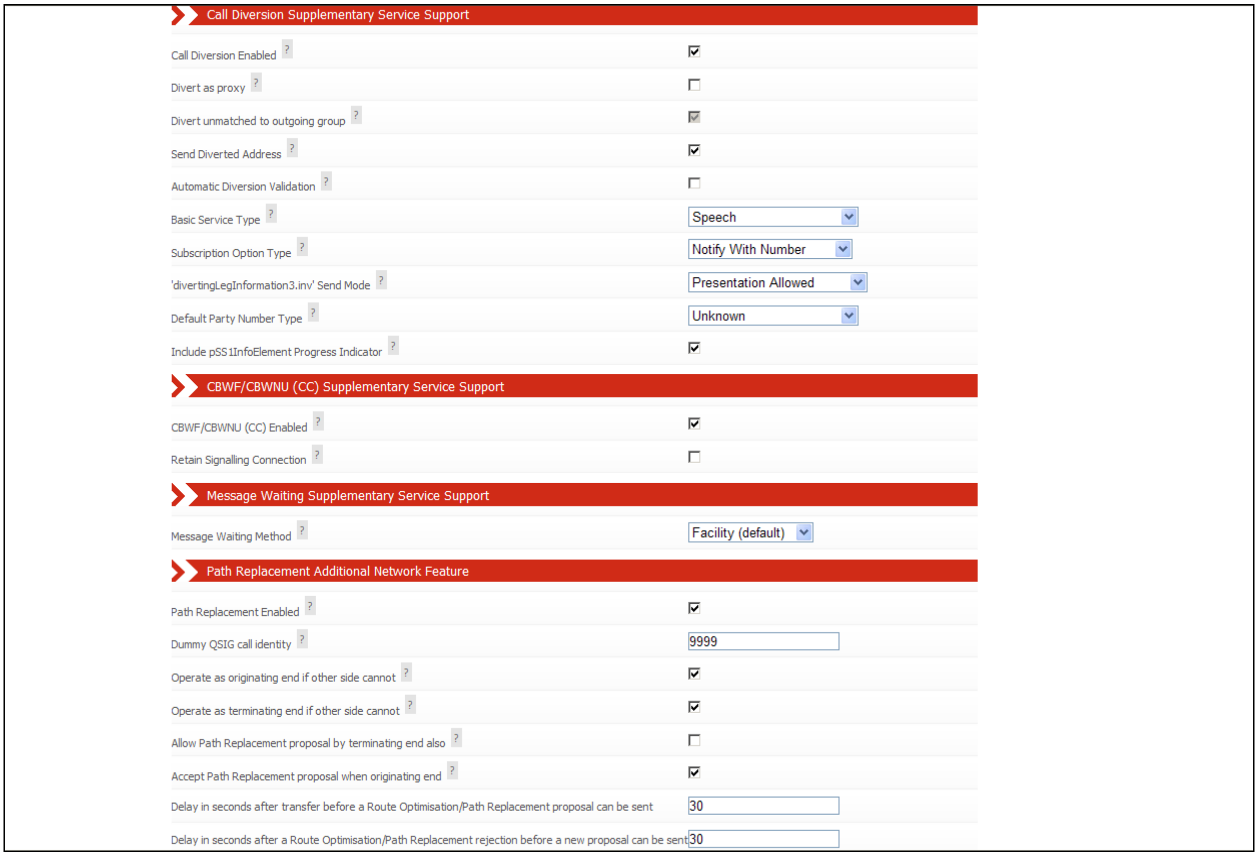
Click on the **Select** button for **QSIG**.



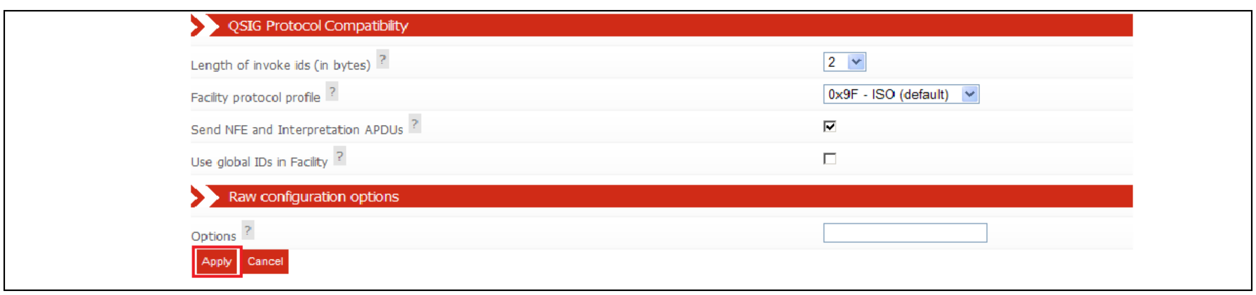
Configure all as is shown in the following screen shots.



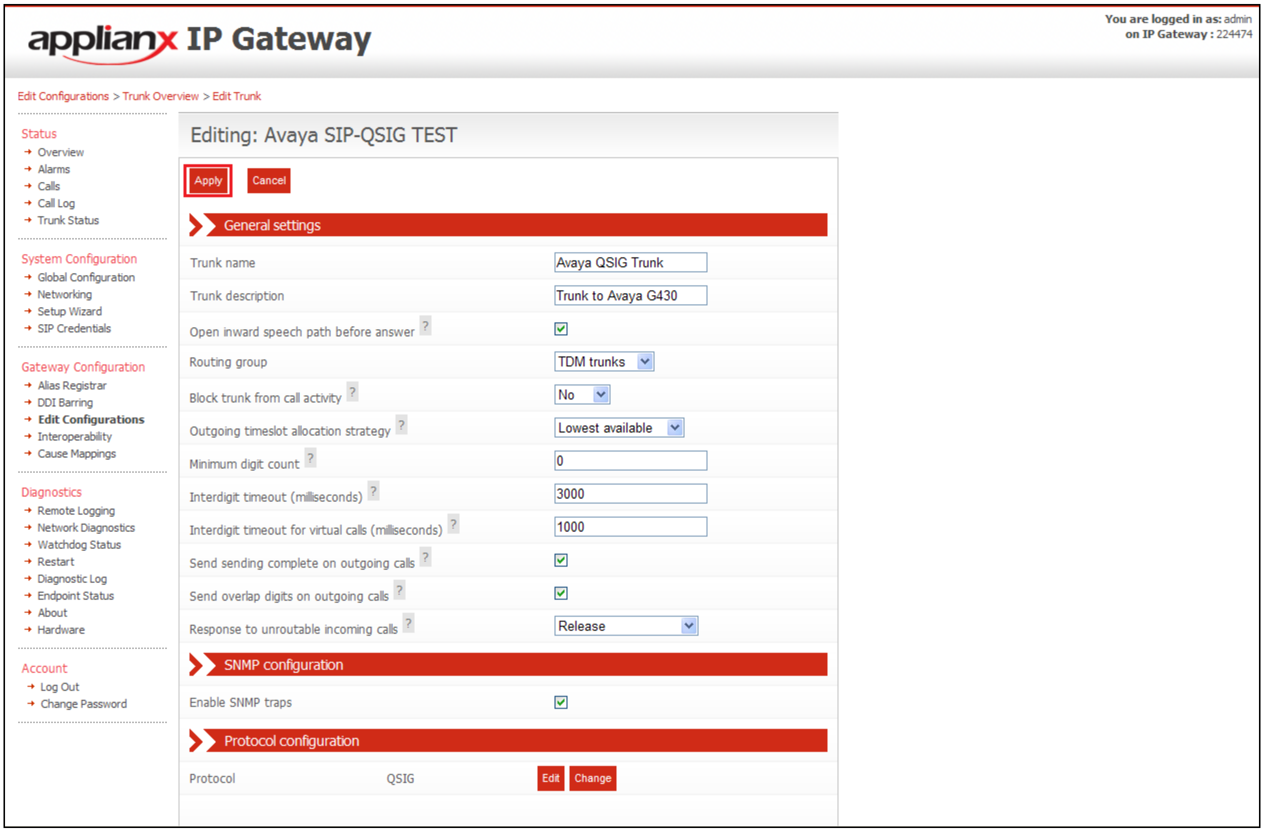
Continuation….



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

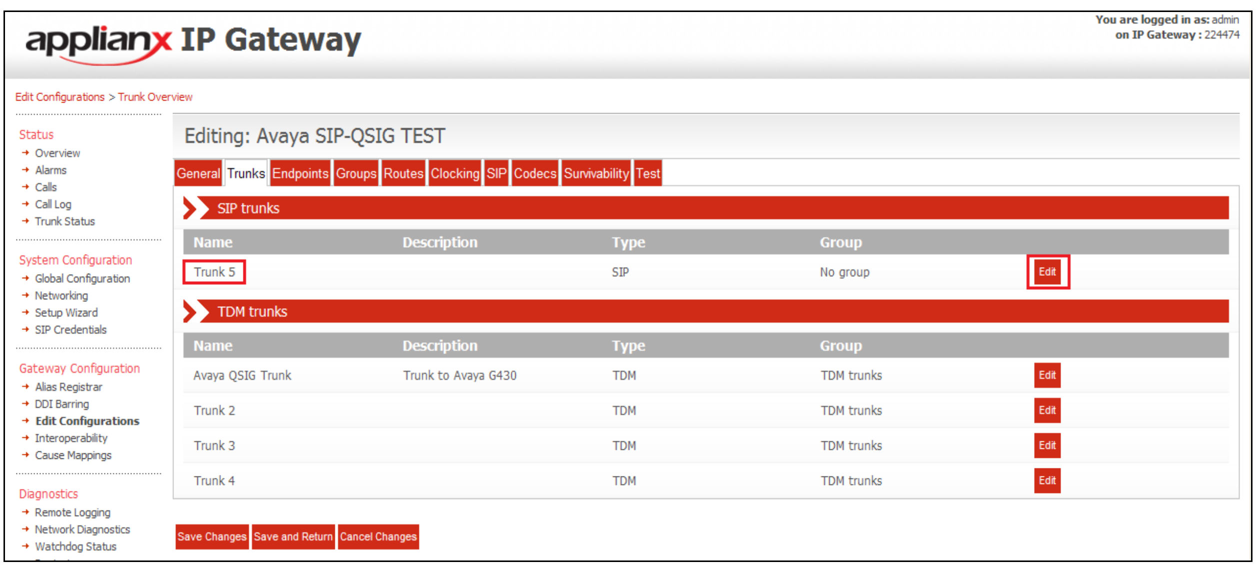


After returning to the **Editing** page, click on the **Apply** button.

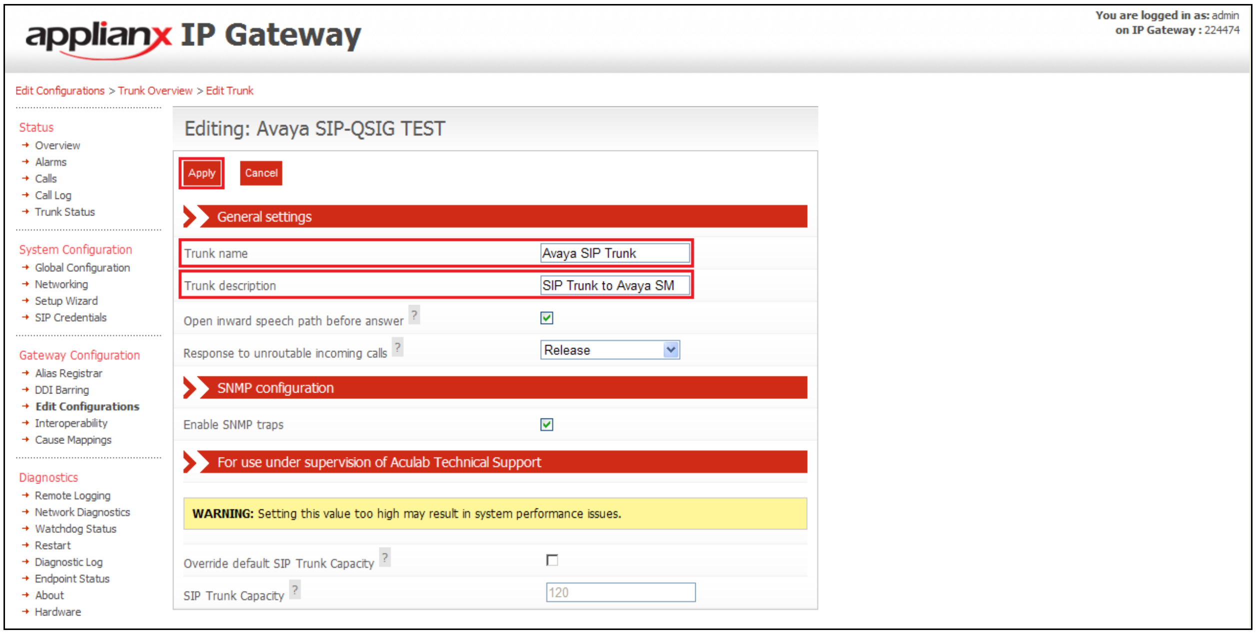


7.4. Configure SIP Trunk

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

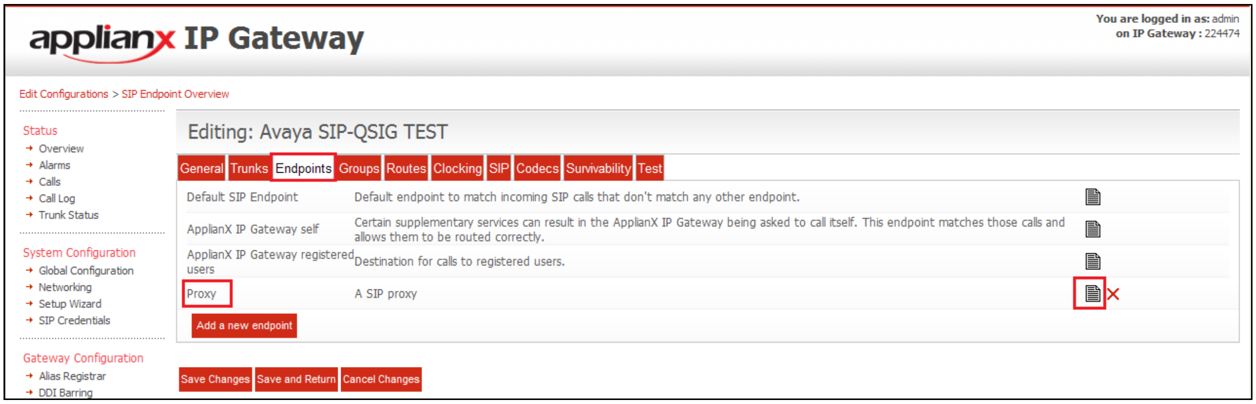


Enter a descriptive name in the **Trunk Name** field (i.e., Avaya SIP Trunk) and in the **Trunk description** field enter a description (i.e., SIP Trunk to Avaya SM). Configure the remaining fields as shown in the following screen shot. Click on the **Apply** button to save the changes.



7.5. Configure Endpoints

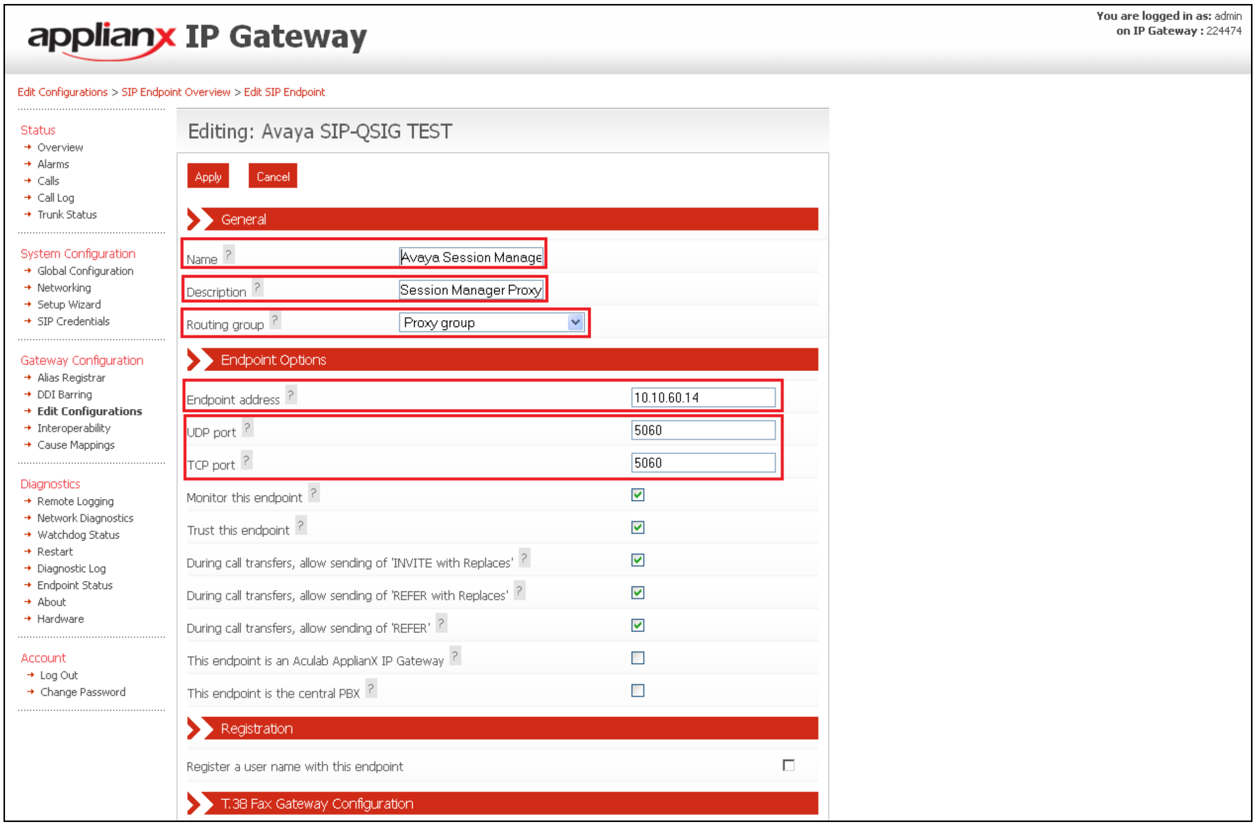
The ApplianX requires information relating to Session Manager so as to communicate with Communication Manager. After clicking on the **Endpoints** tab, click on the icon for **Proxy** as shown in the screen shot below.



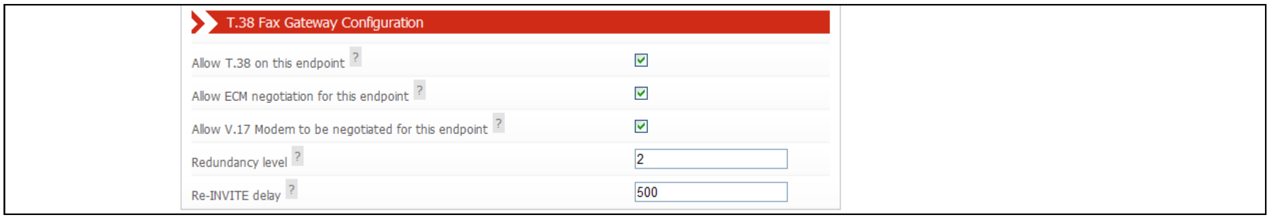
Enter a descriptive name in the **Name** field (i.e., Avaya Session Manager) and in the **Description** field enter a description (i.e., Avaya Session Manager Proxy). Configure the following in the remaining fields:

- **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.



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

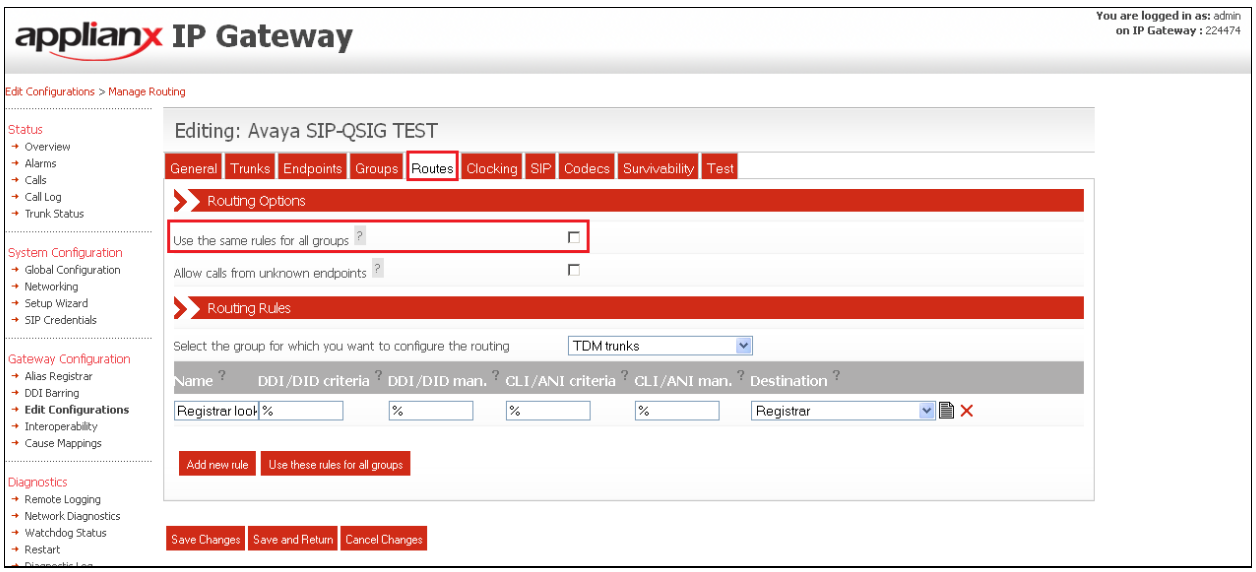


7.6. Configure Groups

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

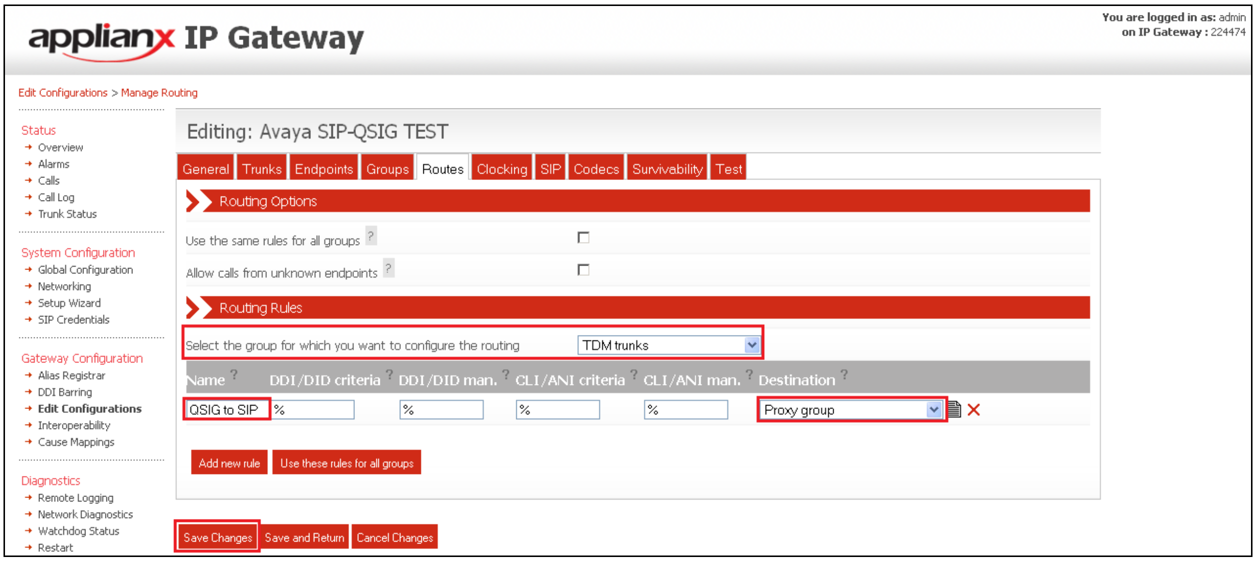
To configure the QSIG Route, click on the **Routes** tab and uncheck **Use the same rules for all groups**the check box.



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

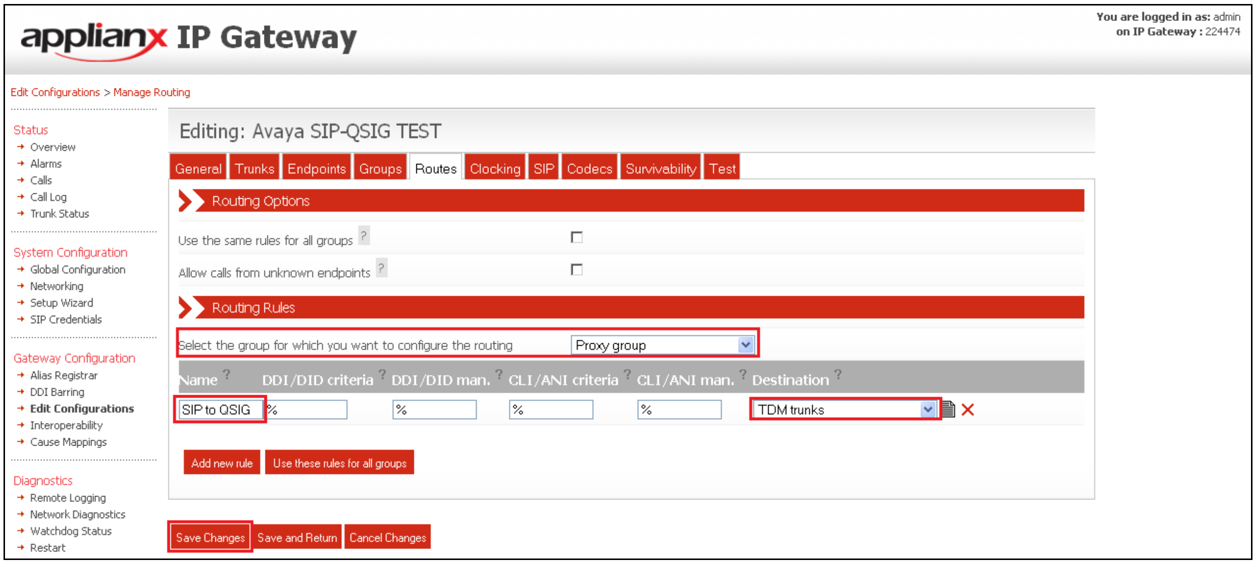
Click on the **Save Changes** button.



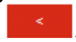
7.7.2. Configure SIP Route

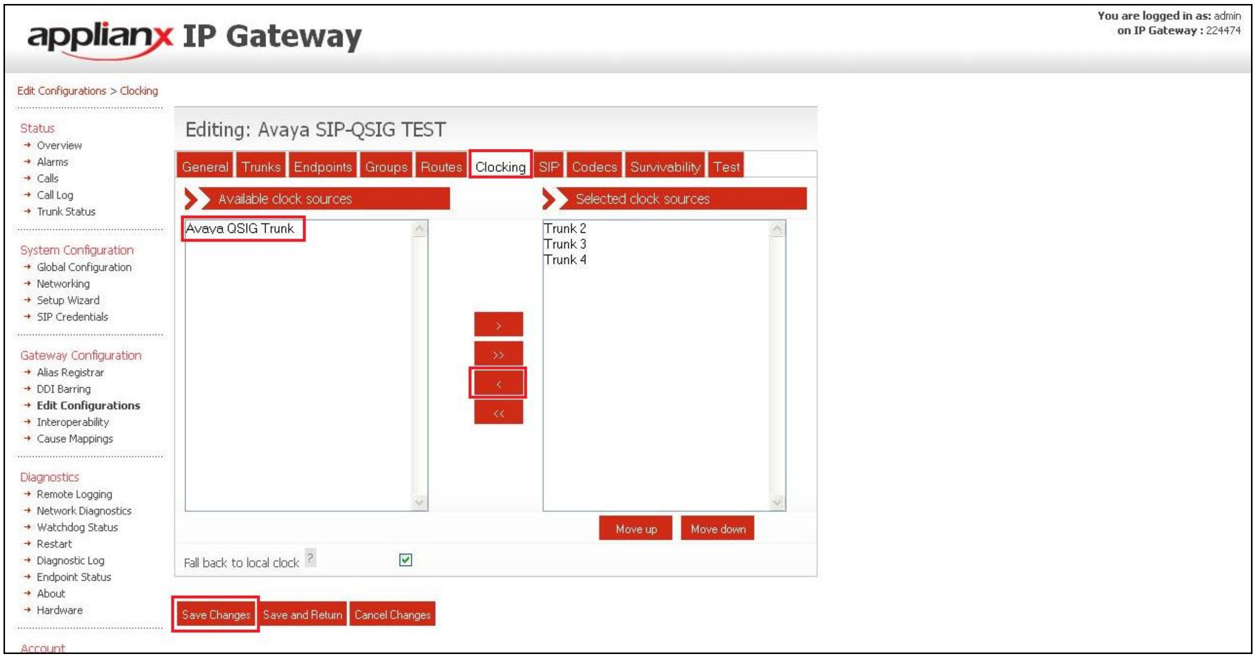
- Select **Proxy group** from the **Select the group for which you want to configure the routing** dropdown box
- Click on the **Add new rule** button
- **Name** Enter a descriptive name (i.e. SIP to QSIG)
- **Destination** Select **TDM trunks** from the dropdown box

Click on the **Save Changes** button.



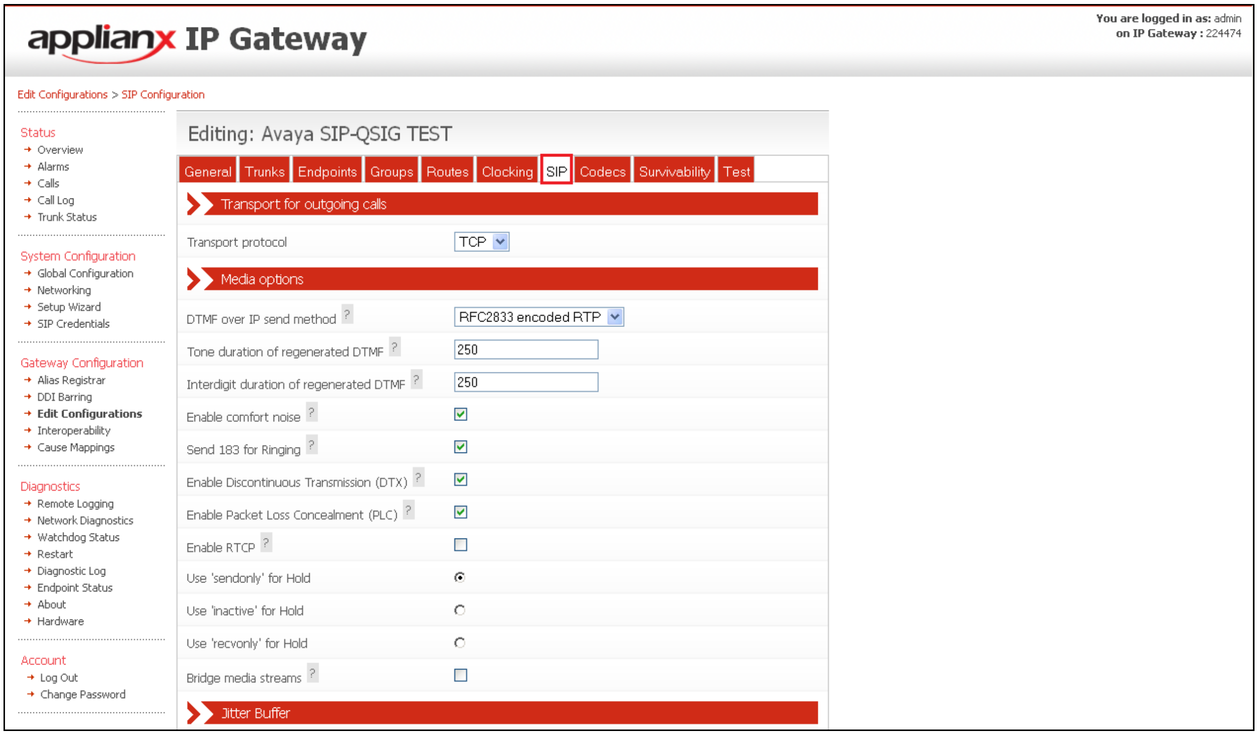
7.8. Configure Clocking

During compliance testing clocking was provided by the Avaya QSIG trunk. To configure clocking, click on the **Clocking** tab and highlight the **QSIG Trunk** from the **Selected clock sources** frame and click on the left icon button . Click on the **Save Changes** button.

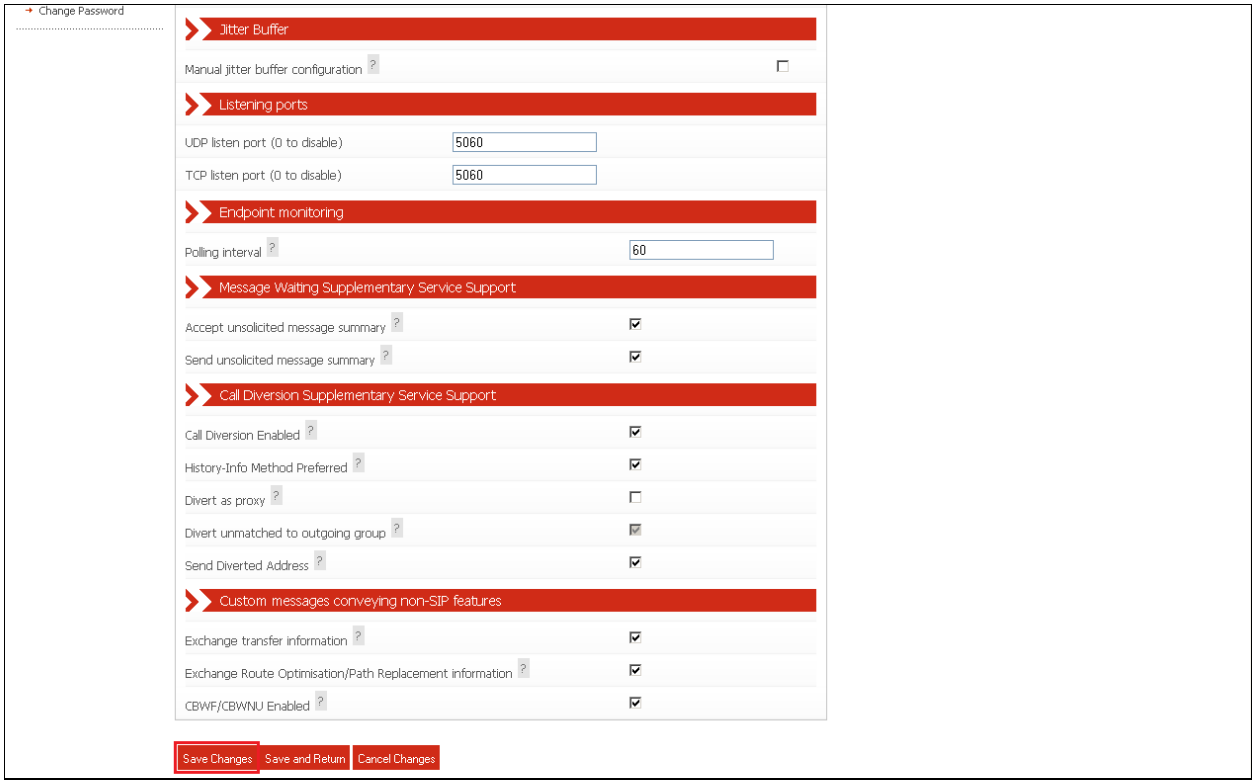


7.9. Configure SIP

To configure the SIP settings click on the **SIP** tab and enter all the information as shown in the screen shot below.

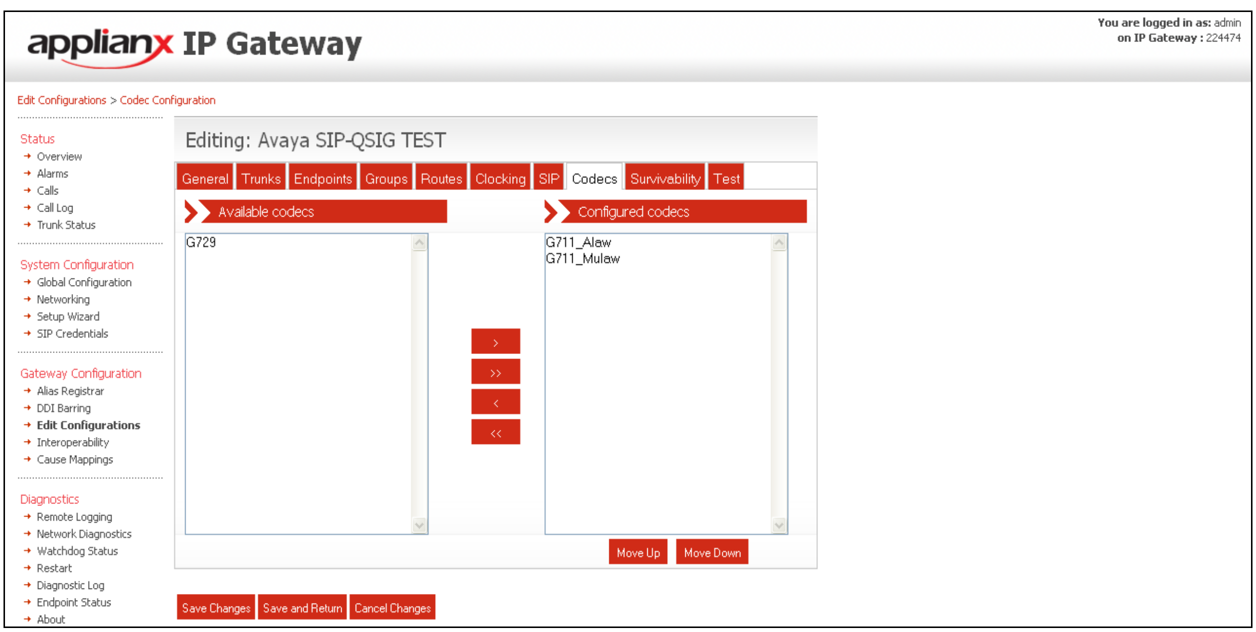


Continuation….
After configuring the remaining fields, click on the **Save Changes** button to save the changes.



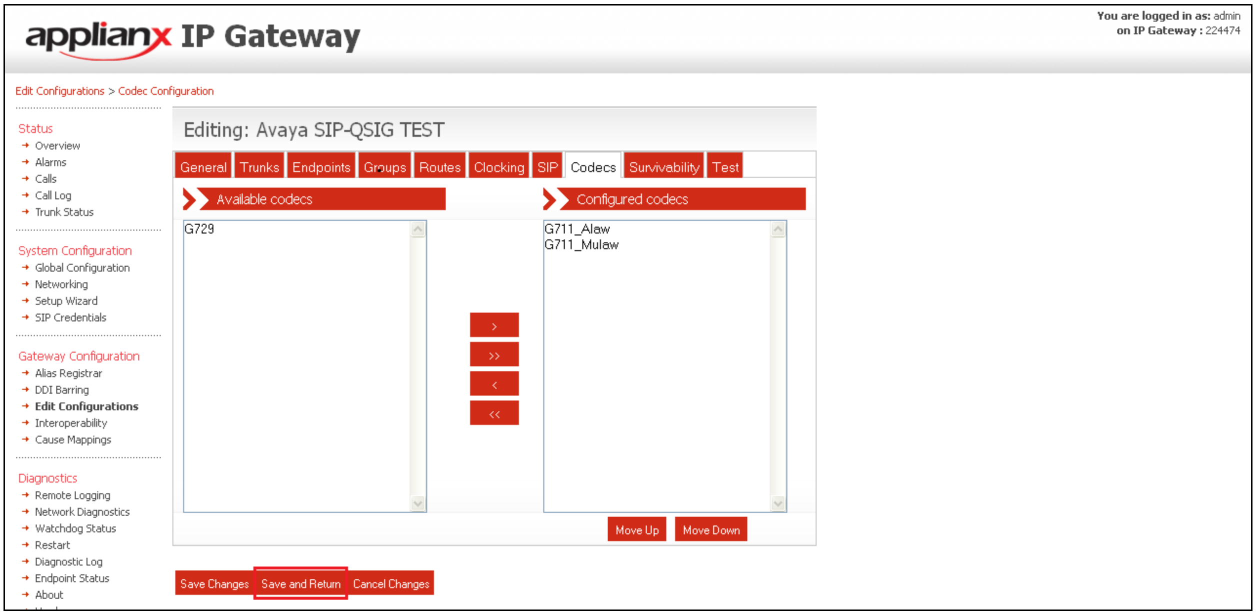
7.10. Configure Codecs

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



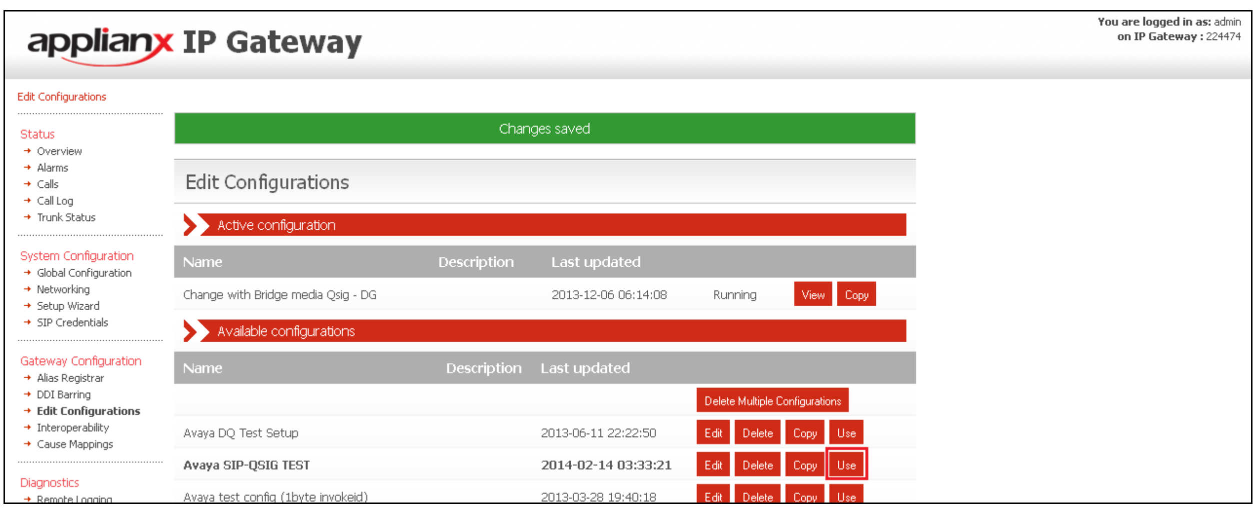
7.11. Save Configuration

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

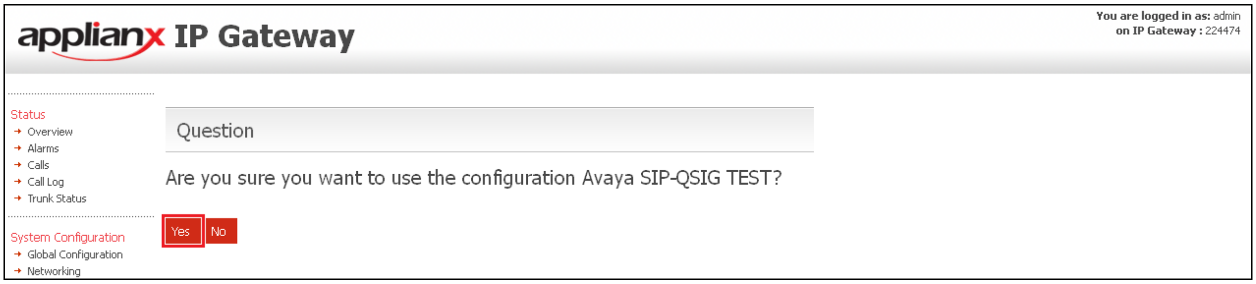


7.12. Use Configuration

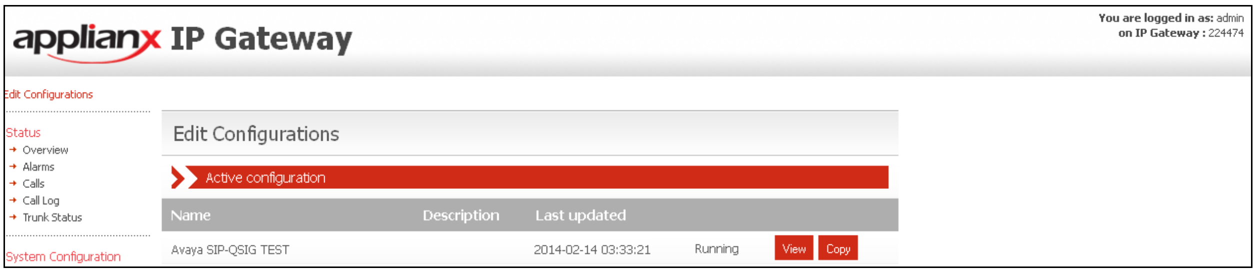
Once all the configurations have been made and saved, click on the **Use** button for this configuration (Avaya SIP-QSIG Test) to apply them to the ApplianX.



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



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

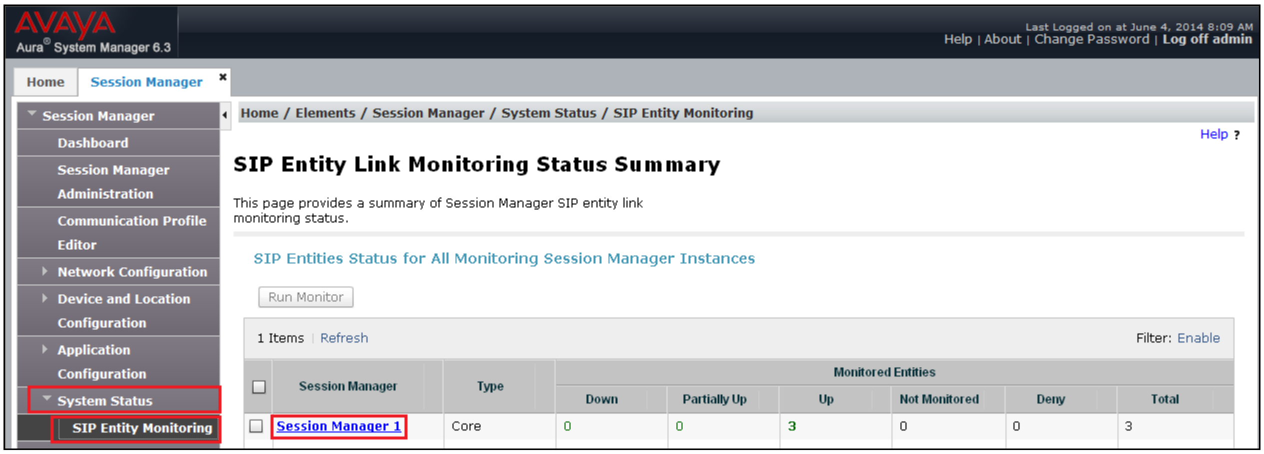


8. Verification Steps

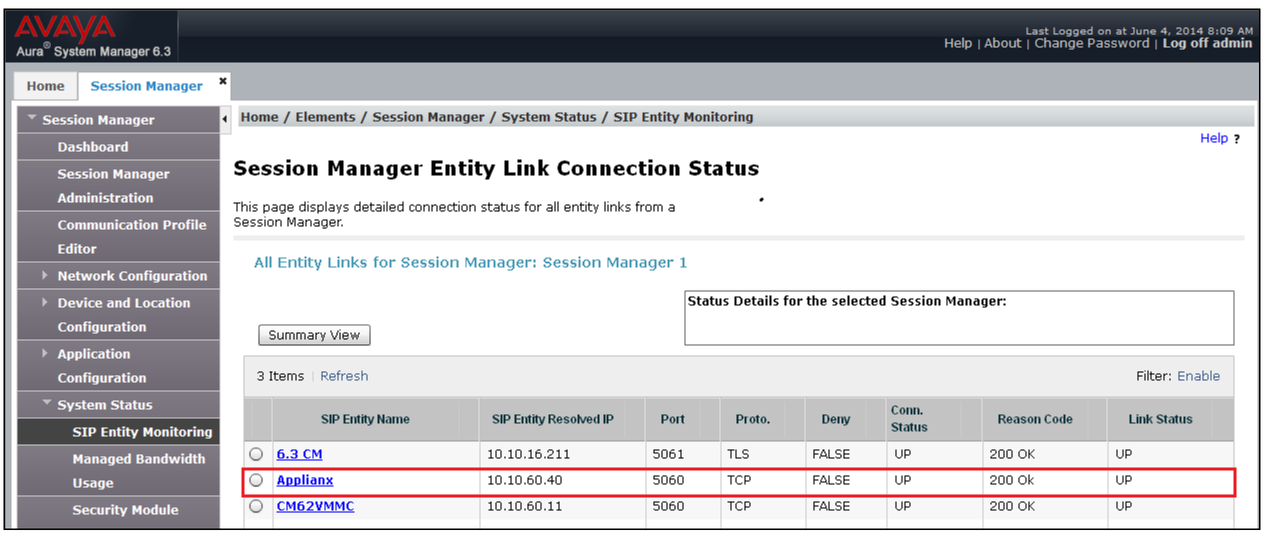
This section provides the tests that can be performed to verify correct configuration of the Avaya and Aculab solution.

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**.



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.



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 6.2 using a SIP trunk to interoperate with a QSIG trunk. All test cases have passed and met the objectives with two observations outlined in **Section 2.2**.

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 6.2, Issue 9.0, February 2012, Document Number 555-245-205.
[2] Administering Avaya Aura® Communication Manager, Release 6.2, Issue 7.0, February 2012, Document Number 03-300509.
[3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013
[4] Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013

Product Documentation for ApplianX IP Gateway can be at the following location:
http://www.aculab.com/documents/

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*.