Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.3 to Support Belgacom SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Belgacom SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Belgacom is a member of the DevConnect Global SIP Service Provider program..

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Belgacom SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server provided to the customer as a service. Customers using this Avaya SIP-enabled enterprise solution with the Belgacom SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. An AudioCodes VoIP Gateway is provided for fax functionality to replace the Communication Manager Media Gateway functionality that would normally be present at the customer's site. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Session Manager and Communication Manager. The enterprise site was configured to use the SIP Trunk Service provided by Belgacom. An AudioCodes MP-118 was provided to test T.38 fax functionality. The T.38 fax testing took priority over standard voice telephony testing, this having been previously successfully tested and documented in Application Notes "BELGACOM_ASM62".

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 interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Belgacom. Incoming PSTN calls were made to H.323, SIP and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Belgacom to the PSTN. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP and Analogue telephones.
- Calls using G.729 and G.711A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode. The group 3 fax machine was connected via the AudioCodes MP-118 gateway which was connected to the Session Manager using TCP as the transport protocol.
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.

- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones was disabled during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Belgacom SIP Trunk Service with the following observations:

- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Calls to the Emergency Services were not tested as no test was booked with the Operator
- During test, “600 Busy Everywhere” was received from the network when dialling a busy number. The more commonly used response for busy is “486 Busy Here”
- .
- During test, “603 Decline” was received from the network when dialing an unassigned number. The more commonly used response for an unassigned number is “404 Not Found”.
- No media attributes were present in the SDP answer from the network for Payload Type 18 (G.729). As media format “annexb=no” wasn’t present, G.729A was not being correctly negotiated. Media was lost on equipment that doesn’t support G.729B, for example Flare and one-X Communicator.
- When no matching codec was found for an incoming call, Communication Manager sent “488 Not Acceptable Here”. The network re-attempted the call several times resulting in delay before the caller heard a tone.
- During test, “482 Merged Request” was received from the network when dialling a toll free number from the enterprise (080055800).
- During test, “603 Decline” was received from the network when dialling a directory Enquiries number (1405).
- Fallback of T.38 fax calls to G.711 was successful when 488 “Not Acceptable Here” was received from the network. It was not successful, however, when “415 Unsupported Media Type” was received. A workaround was put in place using Header Manipulation Rules in the Acme Packet network SBC to change the “415 Unsupported media type” to “488 Not Acceptable Here”. A permanent fix will be delivered on the Communication Manager in release 7.0.
- EC500 Confirmed Answer failed when initial IP direct media was used i.e., the Signalling Group setting “Initial IP-IP Direct Media” is set to “y”.
- When testing one-X Communicator in Telecommuter mode, call transfers to the PSTN were unreliable. The trace on the Session Manager showed a SIP INVITE dropped due to Firewall rules. It is recommended to upgrade the Session Manager to Service Pack 1 as Firewall sensitivity issues have been resolved in this build.
- When testing one-X Communicator in Telecommuter mode conference with internal extension failed. The trace on the Session Manager showed a SIP INVITE dropped due to

Firewall rules. It is recommended to upgrade to Service Pack 1 as Firewall sensitivity issues have been resolved in this build.

- Media failed on an incoming long duration call and was recovered after a hold and resume.
- The Communication Manager returned a SIP 503 "Service Unavailable" message when all trunks were busy. The network re-attempted the call several times and the caller heard a tone after approximately 25 seconds. This failure could be more graceful.
- The Session Manager returned a SIP 500 "Server Link Monitor Status Down" message when signalling to the CM failed. The network re-attempted the call several times and the caller heard a tone after approximately 25 seconds. This failure could be more graceful.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Belgacom products please contact an authorized Belgacom representative at: ippbx.certification@belgacom.be.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Belgacom SIP Trunk Service. Located at the enterprise site is a Session Manager and Communication Manager. Endpoints are Avaya 9600 and 4600 series IP telephones, Analogue Telephone, an Avaya Desktop Video Device, a PC running Avaya one-X Communicator, and a Fax Machine connected via an AudioCodes MP-118 gateway. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

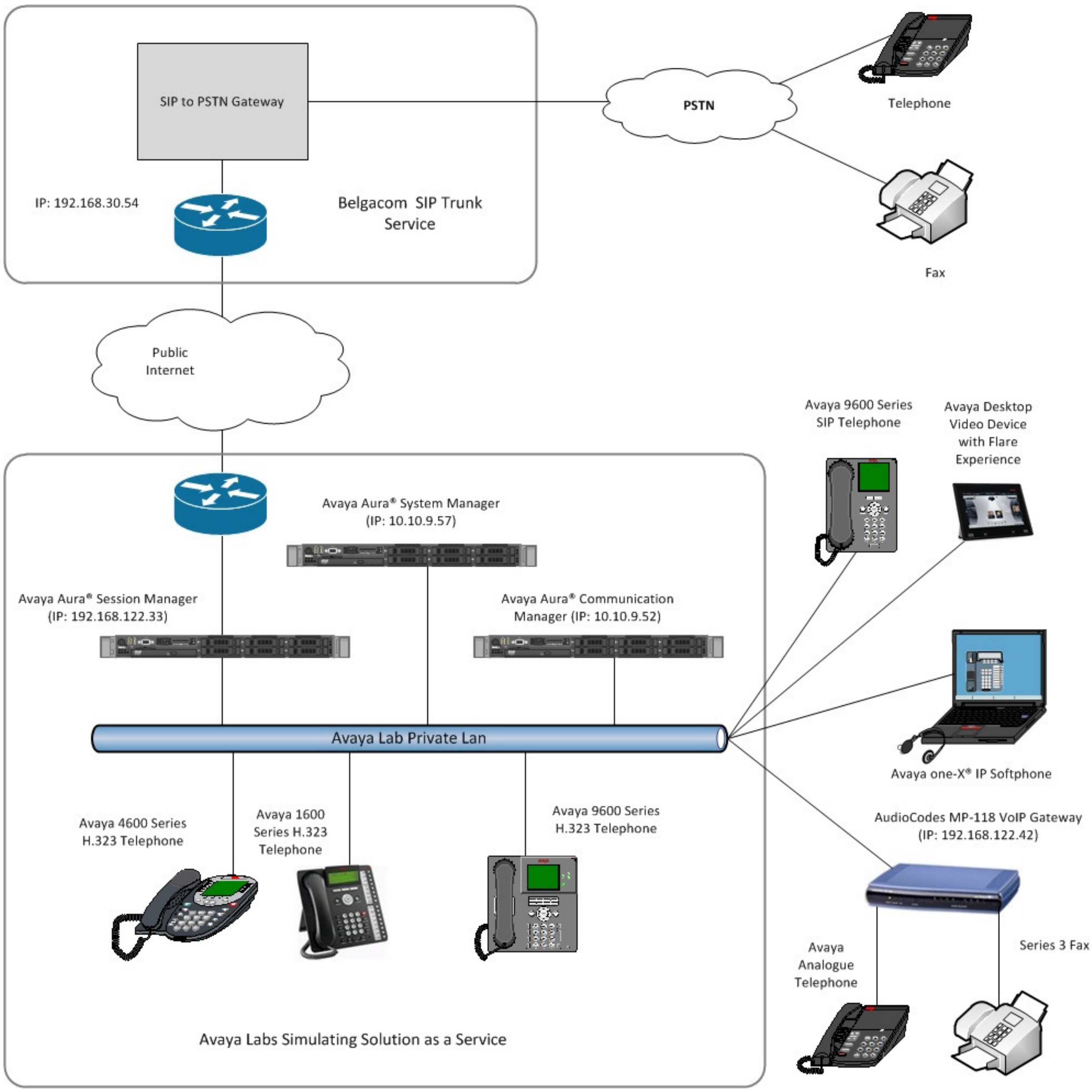


Figure 1: Belgacom SIP Solution Topology

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya S8800 Server running Session Manager	6.3
Avaya S8800 Server running System Manager	6.3
Avaya S8800 Server running Communication Manager	6..2 SP 4 (R016x.02.0.823.0)
AudioCodes MP-118 VoIP Gateway	6.20A.062.003
Avaya 9600 series Handsets SIP H.323	 2.6.02 3.1
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1.2
Analogue Handset	NA
Analogue Fax	NA
Belgacom	
IMS	REL10.1
MGC/MGW	MGC12 – T.38 enabled

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signaling associated with Belgacom SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Belgacom and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Belgacom network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Server and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Belgacom network, and any other SIP trunks used.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 20
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 4**, verify that **IP Trunks** field is set to **y.**

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? y
     External Device Alarm Admin? y                Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **192.168.122.33** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100               192.168.122.33
Sipera-SBC          10.10.9.71
default             0.0.0.0
procr               10.10.9.52
procr6              ::
```

Note: During test, the Session Manager was assigned a public IP address so that it could communicate directly with the Belgacom network. The address has been altered to a private address for this document.

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager (see **Section 6.2**). In this configuration, the domain name is **imst.belgacom.be**.
- By default, **IP-IP Direct Audio** (both **Intra**- and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is established with initial direct media or is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.
- The **UDP Port Min** and **UDP Port Max** values were set to define a range of ports that would be compatible with the Belgacom firewall rules at the time of test.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: imst.belgacom.be
    Name: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 10000                     IP Audio Hairpinning? n
   UDP Port Max: 10201
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by Belgacom were configured, namely **G.729A**, and **G.711A**.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.729A            n          2        20
 2: G.711A            n          2        20
```

The Belgacom SIP Trunk service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **FAX - Mode** to **t.38-standard** as shown below

```
change ip-codec-set 1                                           Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Belgacom SIP Trunk service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)
- Set **Direct IP-IP Audio Connections** to **y**
- Set **Initial IP-IP Direct Media** to **y**

The default values for the other fields may be used.

```
add signaling-group 1                                          Page   1 of   1
                                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? n
  Peer Detection Enabled? y  Peer Server: SM


   Near-end Node Name: procr                 Far-end Node Name: SM100
 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? n              Alternate Route Timer(sec): 6
```

Note: The previous screenshot shows **Initial IP-IP Direct Media** set **y**. This was set during test to avoid additional signalling required when shuffling from connection to the media gateway to a direct connection. It was observed during test, however, that this caused failure of EC500 Confirmed Answer as described in **Section 2.2**. If this feature is required, **Initial IP-IP Direct Media** should be set to **n.**

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk**
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

```
add trunk-group 1                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 1                  Group Type: sip           CDR Reports: y
  Group Name: Group 1                   COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Belgacom to prevent unnecessary SIP messages during call setup.

```
add trunk-group 1                                                Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 300

 Disconnect Supervision - In? y  Out? y
```

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI with leading zeros.

```
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
```

On **Page 4** of this form:

- Set **Support Request History** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Belgacom (this Payload Type is not applied to calls from SIP end-points)
- Set **Always Use re-INVITE for Display Updates** to **n** as Belgacom support UPDATE
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

```
add trunk-group 1                                                 Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? n
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? n
                      Network Call Redirection? y
                         Send Diversion Header? n
                       Support Request History? y
                  Telephone Event Payload Type: 101


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? n
            Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
                                 Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change private-numbering** command to configure Communication Manager to send the calling party number in national format with leading 0. In the test configuration, individual stations were mapped to send numbers allocated from the Belgacom DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

```
change private-numbering 0                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 4  2208           1          027nnnnn3        9     Total Administered: 9
 4  2296           1          027nnnnn2        9        Maximum Entries: 540
 4  2316           1          027nnnnn4        9
 4  2346           1          027nnnnn1        9
 4  2396           1          027nnnnn0        9
 4  2400           1          027nnnnn7        9
 4  2401           1          027nnnnn8        9
 4  2602           1          027nnnnn5        9
 4  2701           1          027nnnnn6        9
```

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Belgacom SIP Trunk service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

```
change feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

```
change ars analysis 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total      Route     Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
    0                     8    14     1        pubu          n
    00                    13   17     1        pubu          n
    00353                 10   14     1        pubu          n
    0044                  12   14     1        pubu          n
    0800                  11   11     1        pubu          n
    1405                  4    4      1        pubu          n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **Numbering Format** of **unk-unk** allows sending of private calling party number.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: all calls
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                               n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Belgacom can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Belgacom for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **+3227nnnnn0** to **+3227nnnnn9** to the 4 digit extension by deleting all (**11**) of the incoming digits and inserting the extension number. Note that the significant digits beyond the area code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11 +3227979420      11  2396
 public-ntwrk    11 +3227979421      11  2346
 public-ntwrk    11 +3227979422      11  2296
 public-ntwrk    11 +3227979423      11  2208
 public-ntwrk    11 +3227979424      11  2316
 public-ntwrk    11 +3227979425      11  2602
 public-ntwrk    11 +3227979426      11  2701
 public-ntwrk    11 +3227979427      11  6101
```

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 2396                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 2396             EC500        -      0035386nnnnnnn   1          1
                               -
```

Save Communication Manager changes by entering **save translation** to make them permanent.

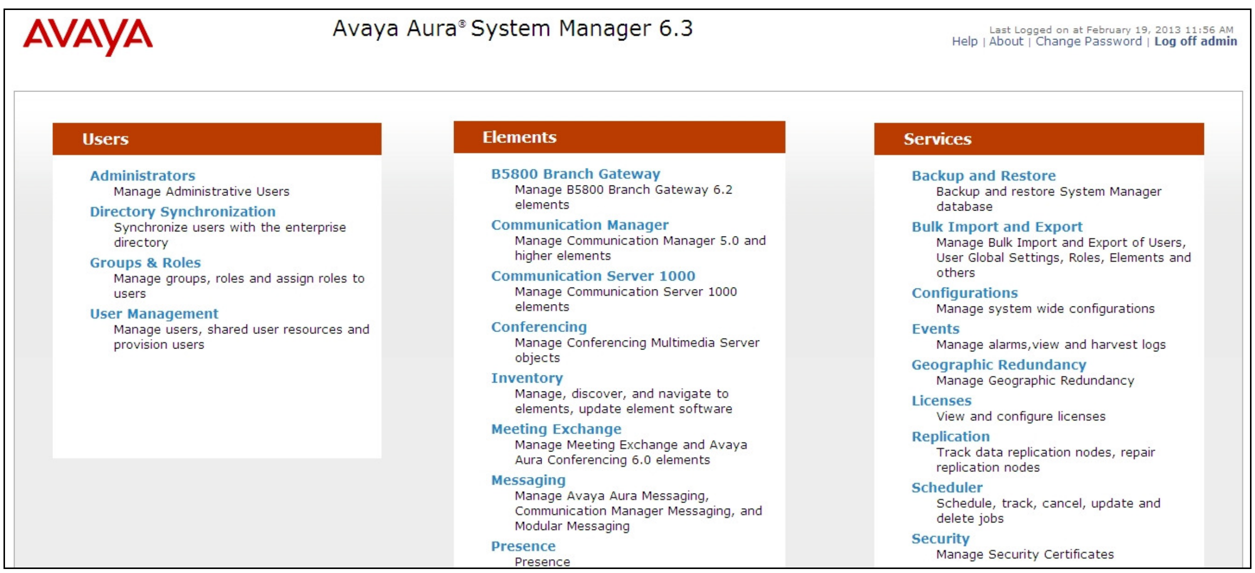
6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

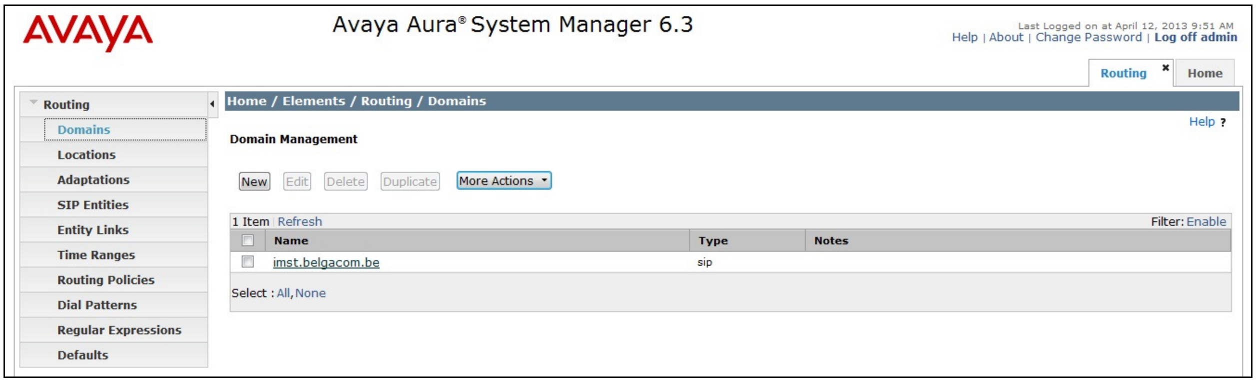
6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



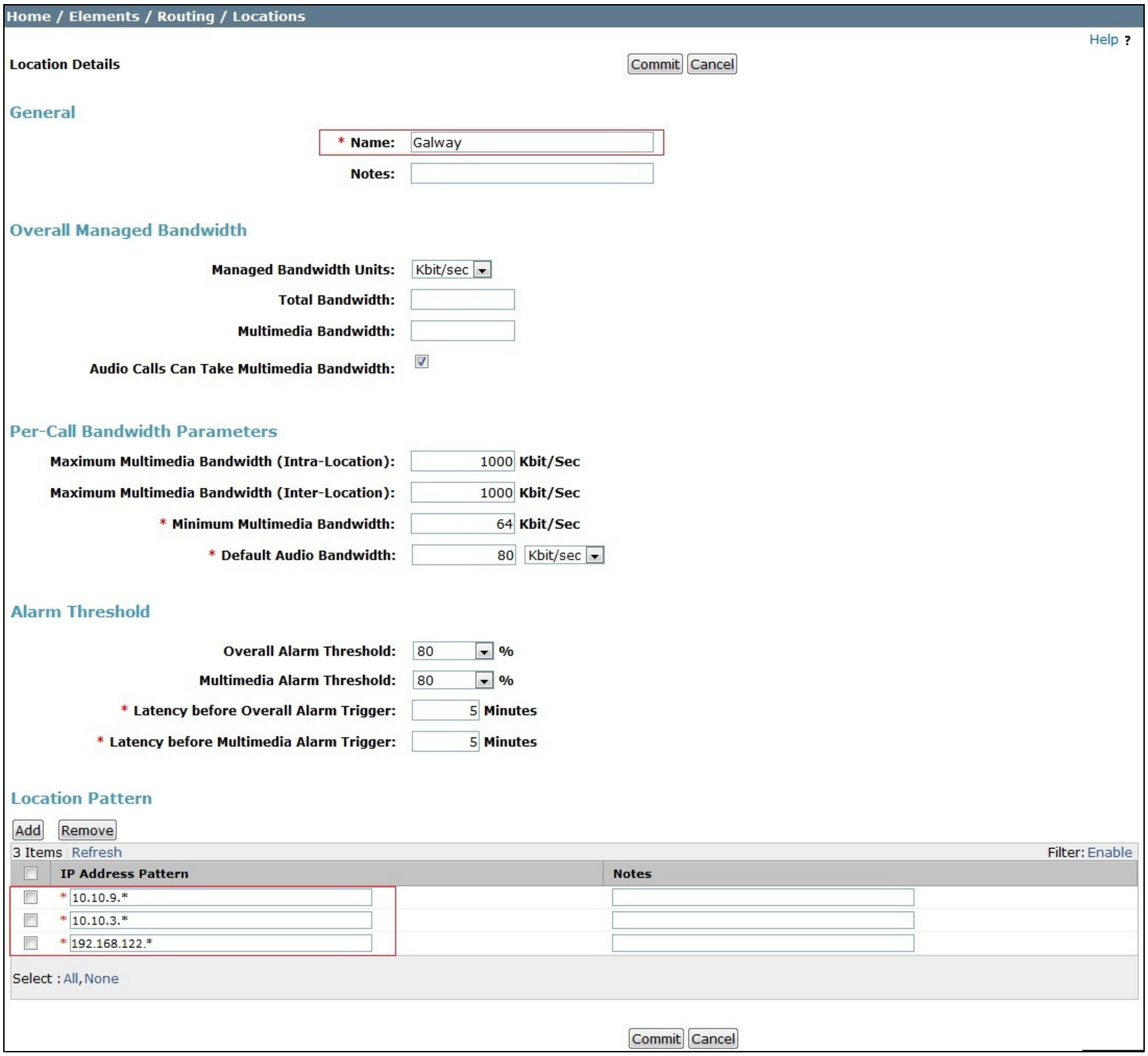
6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with Belgacom; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on the Communication Manager. Refer to **Section 5.3** for details. In test, **imst.belgacom.be** was used. Optionally, a description for the domain can be entered in the Notes field. Click **Commit** (not shown) 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. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.



6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system, supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General**:

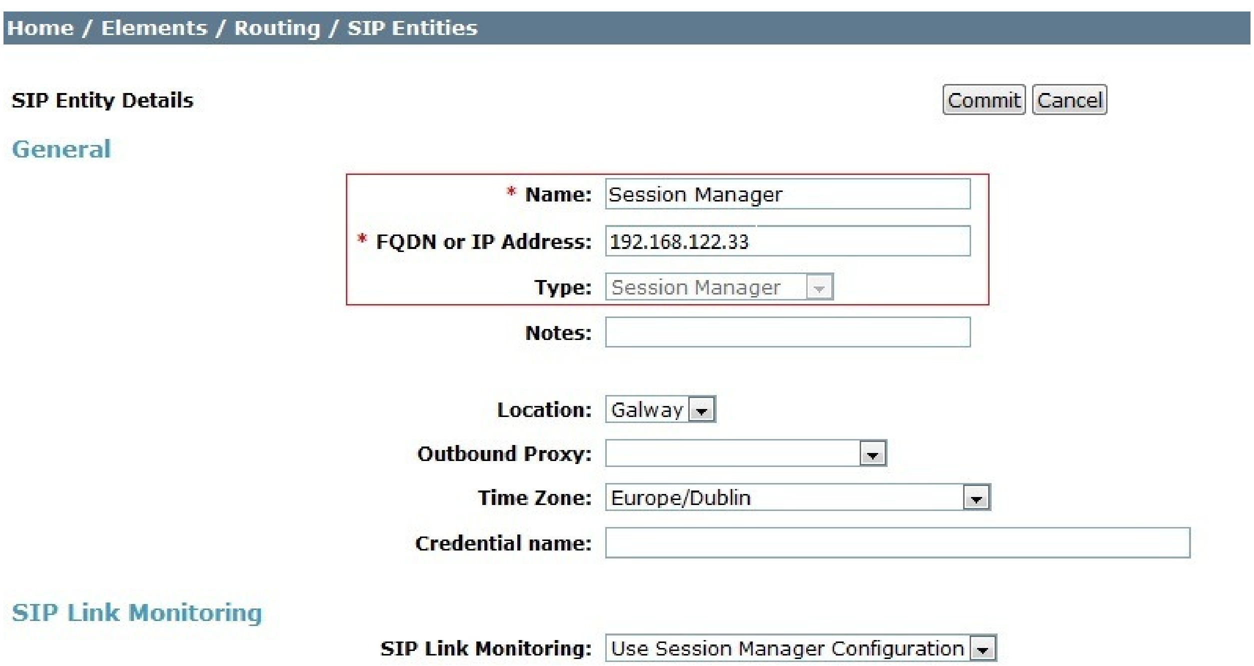
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of the Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Manager SIP entity and **SIP Trunk** for the Belgacom Network SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Belgacom Network SIP Entity

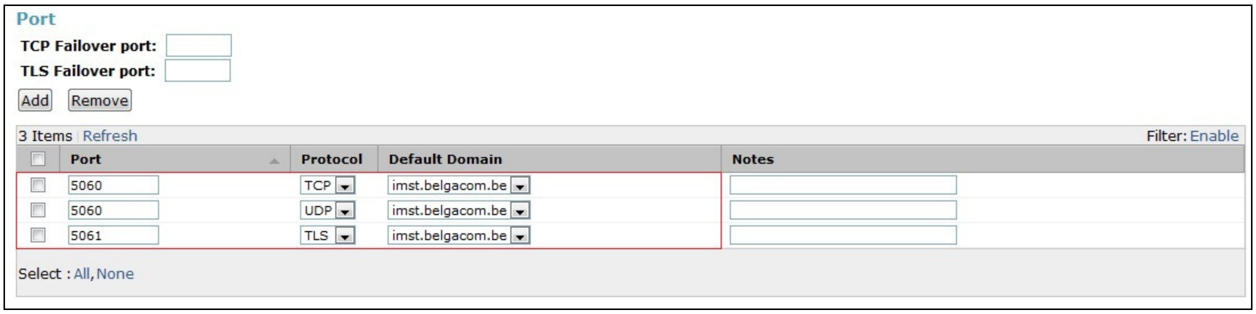
6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.



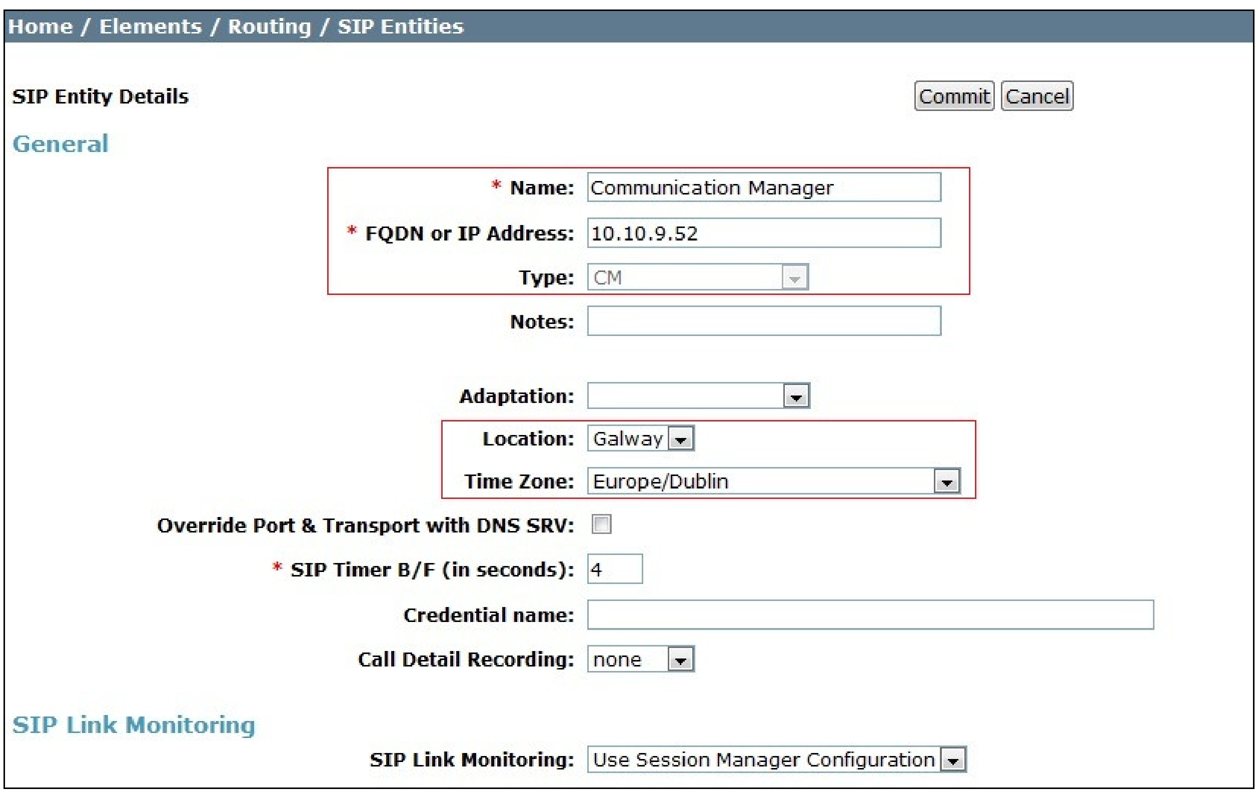
The Session Manager must be configured with the port numbers of the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain



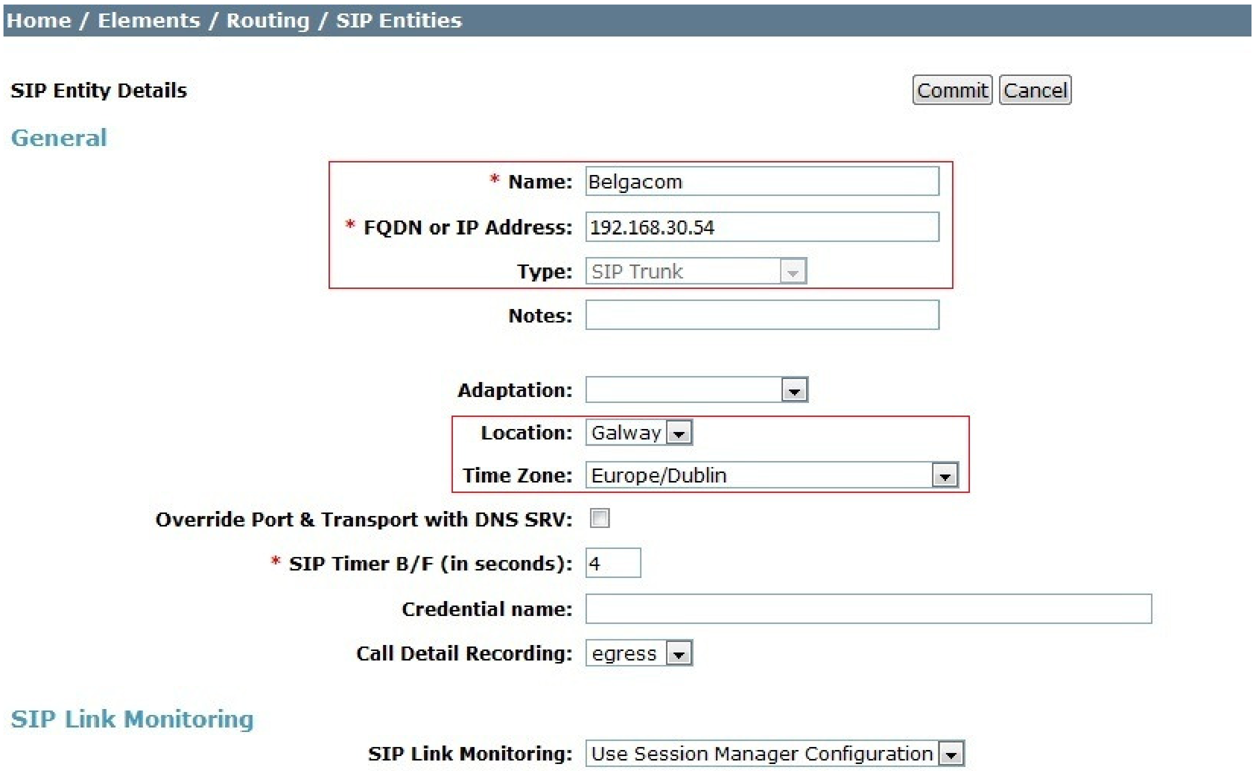
6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



6.4.3. Belgacom Network SIP Entity

The following screen shows the SIP Entity for the Belgacom network. The **FQDN or IP Address** field is set to the IP address provided by Belgacom for their interface (see **Figure 1**). Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

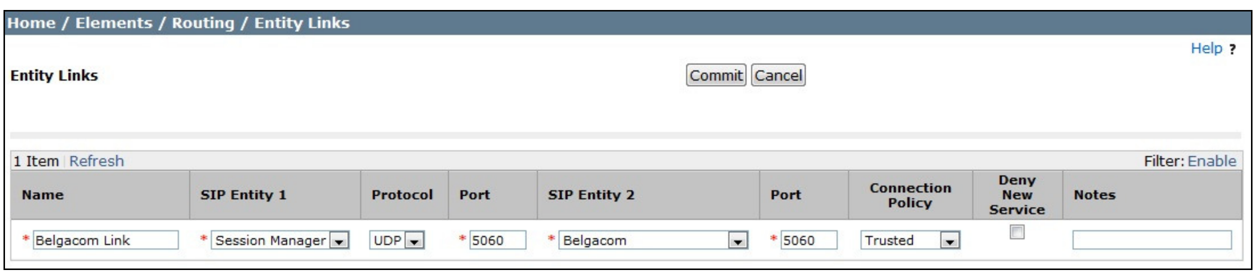


6.5. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager**
- In the **Protocol** field enter the transport protocol to be used to send SIP requests
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted

Click **Commit** to save changes. The following screens show the Entity Links used in this configuration.



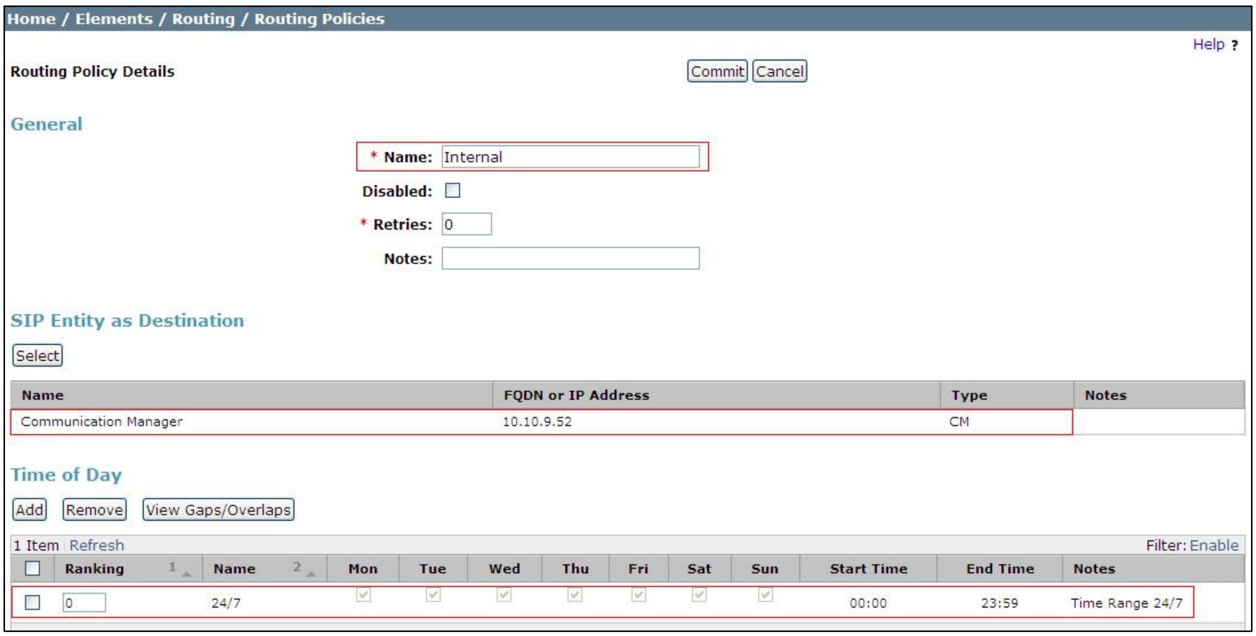
6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

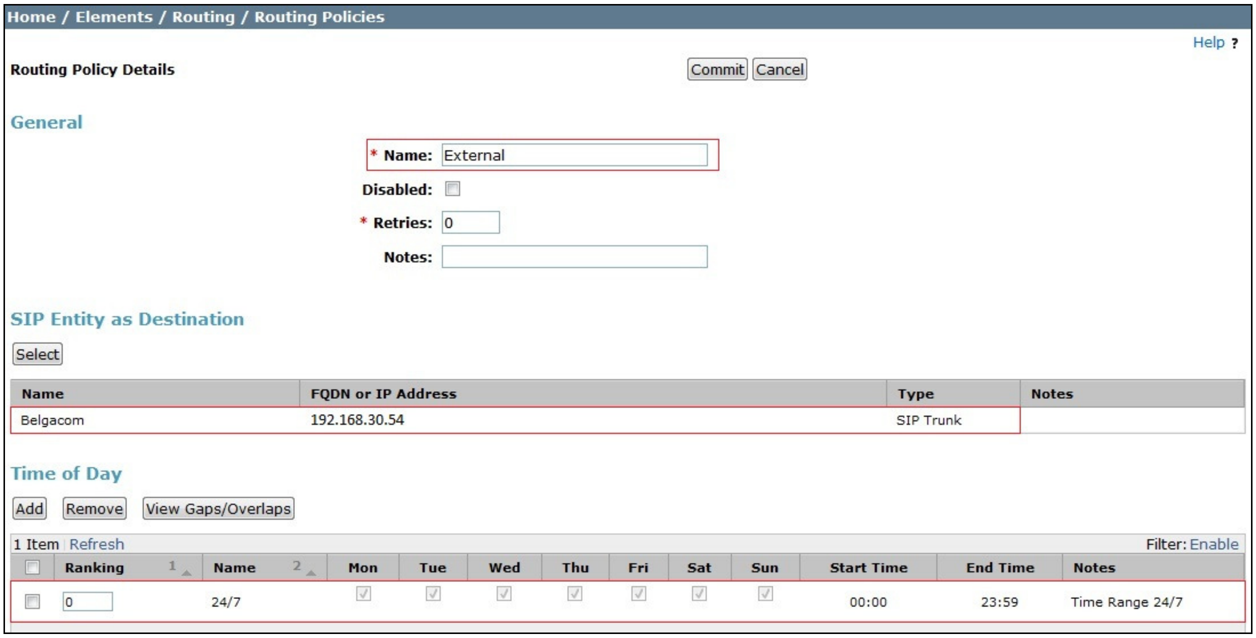
Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies in a pop-up window (not shown)
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the Belgacom network.



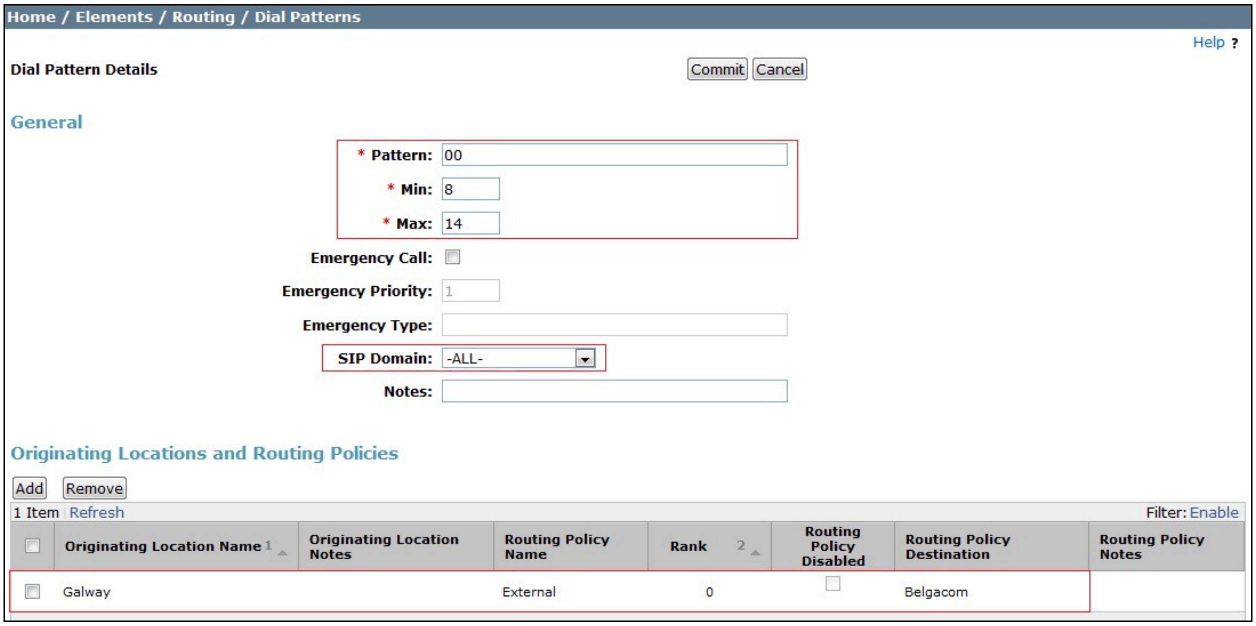
6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

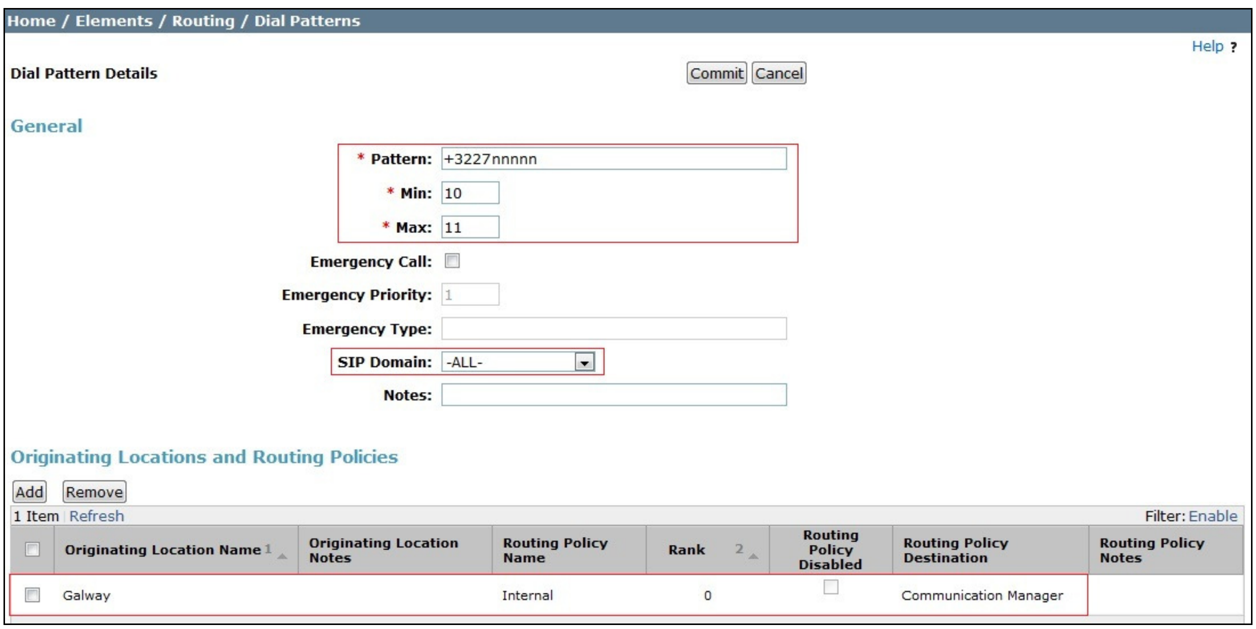
Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select the location defined in **Section 6.3** or **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6.** Click **Select** button to save. The following screen shows an example dial pattern configured for the Belgacom network which will route the calls out to the PSTN.



The following screen shows the test dial pattern configured for Communication Manager.

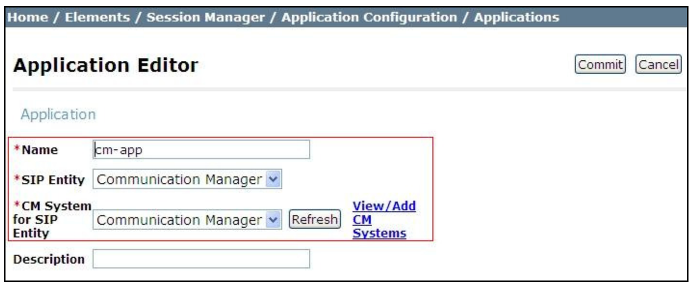


Note: The pattern to be matched has been obscured.

6.8. Administer Application for Avaya Aura® Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New**.

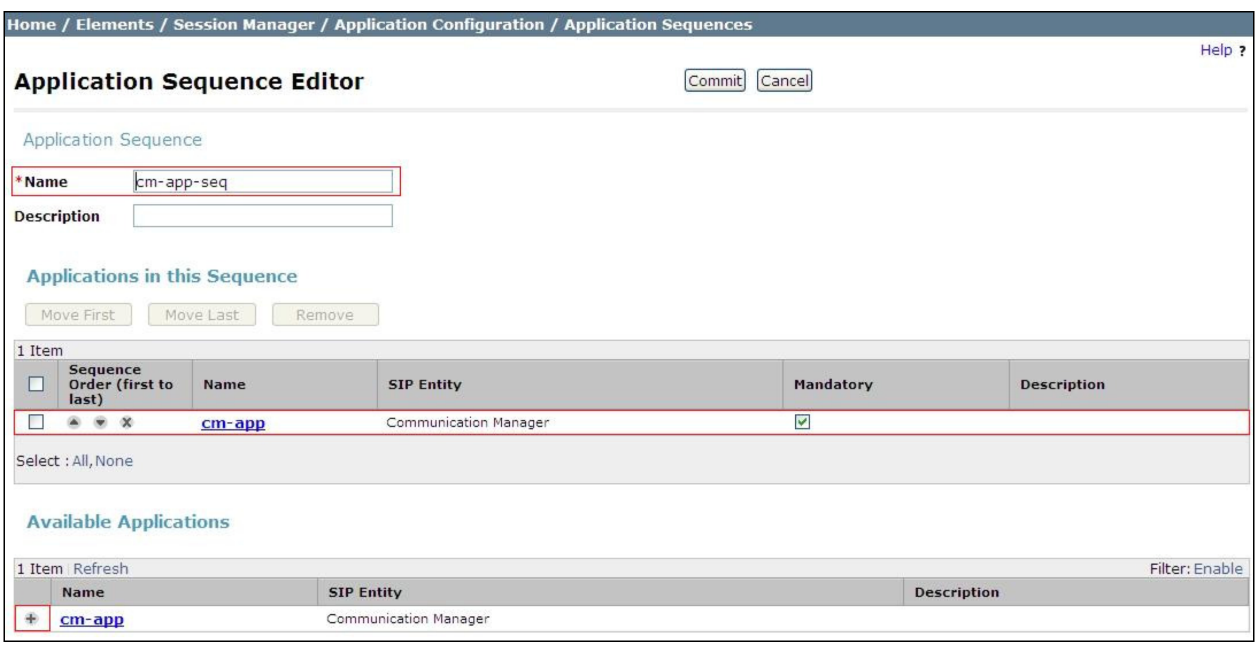
- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager and select **Commit** to save the configuration.



6.9. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New** (not shown).

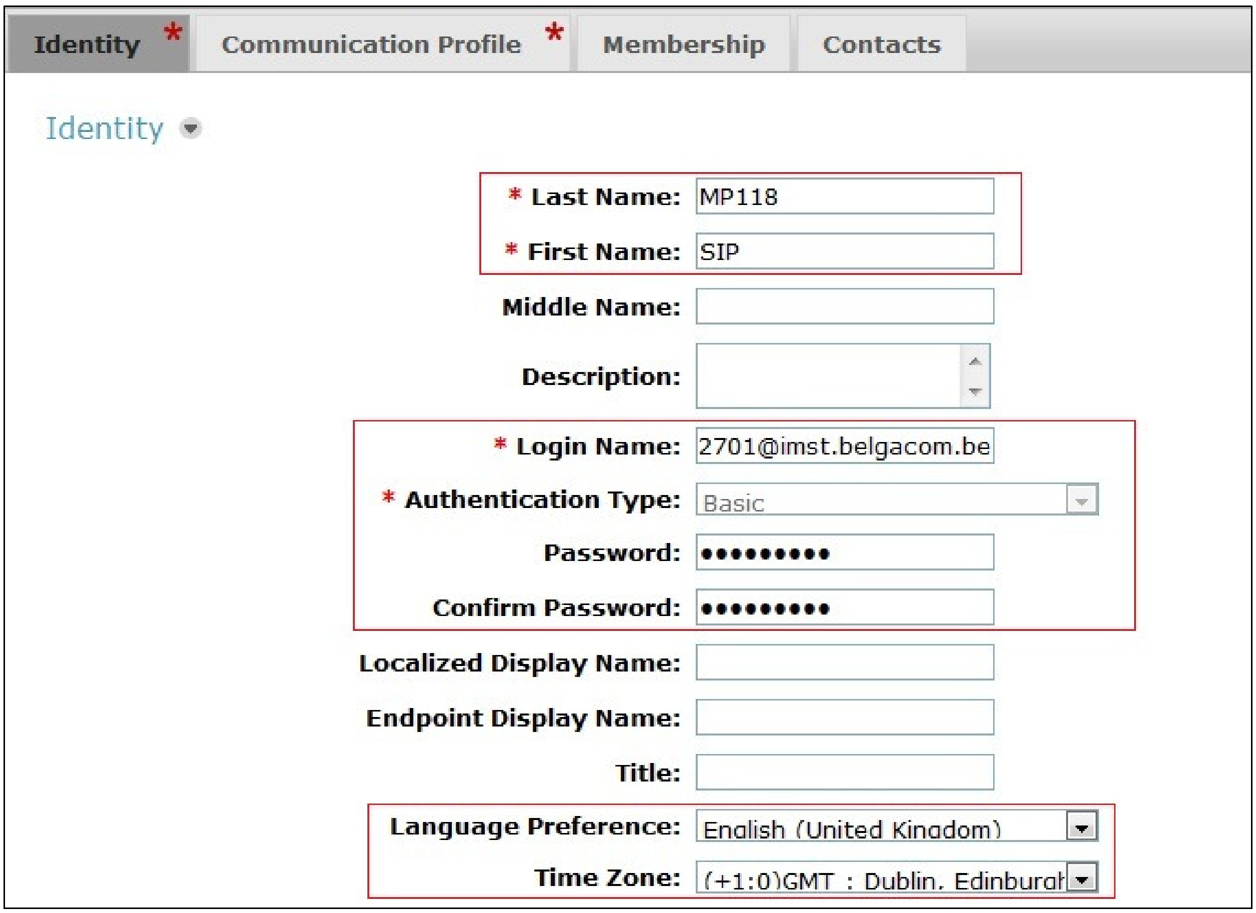
- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.



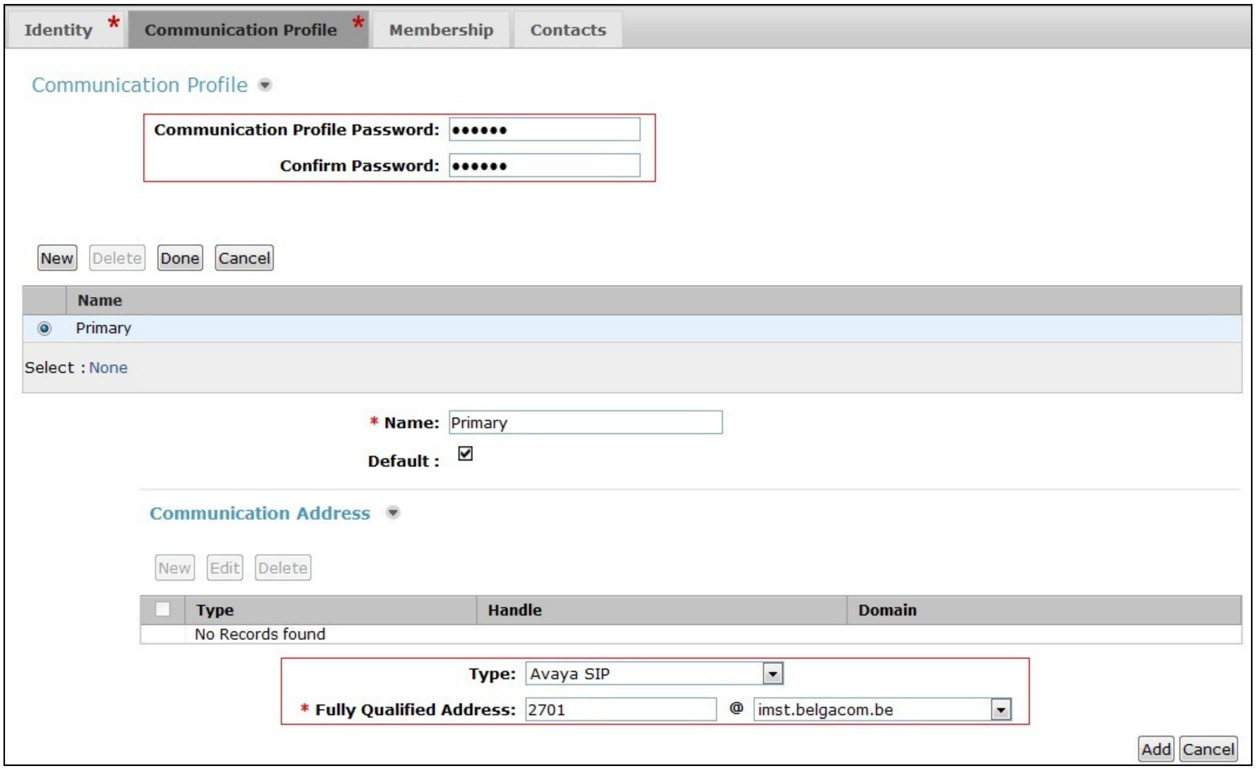
6.10. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. The AudioCodes MP-118 is registered as a SIP extension to provide fax capability at the customer's premises. The following example shows the configuration of the MP-118 for the test environment. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).
On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. **2701@imst.belgacom.be**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password
- Set the **Language Preference** and **Time Zone** as required



On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

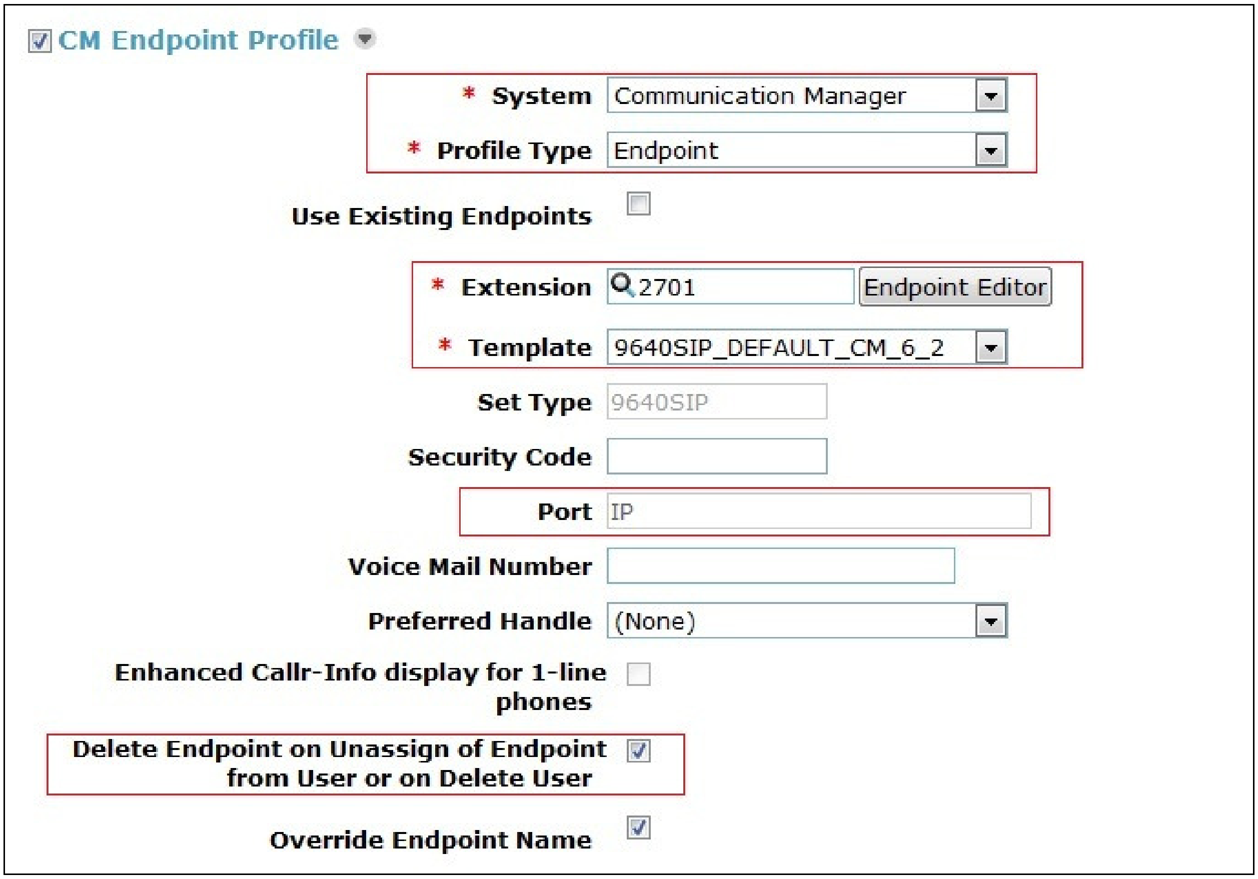


Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field

Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (Not Shown) to save changes and the System Manager will add the Communication Manager user configuration automatically



7. Configure AudioCodes MP-118

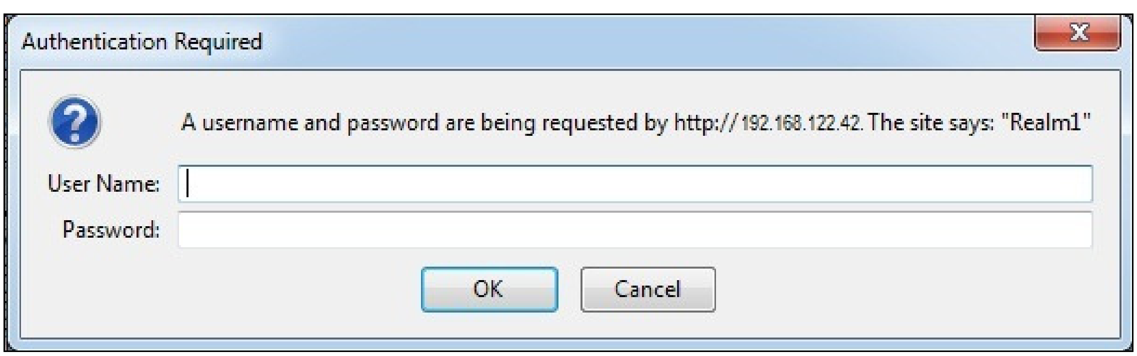
The AudioCodes MP-118 is used to provide fax functionality at the customer's site. The MP-118 is configured as a SIP endpoint and registered on the Session Manager. The MP-118 provides the coding and decoding between T.38 and Group3 / Super Group 3 fax. The solution also allows for fallback to G.711 where T.38 is not supported by the network media gateway. The configuration of the MP-118 can be summarised as follows:

- Logging into the AudioCodes MP-118
- Configure IP Settings
- Configure Security Settings for TLS
- Configure Voice Settings
- Configure Fax/Modem/CID Settings
- Configure RTP/RTCP Settings
- Configure IP Group Table
- Configure Proxy Sets Table
- Configure SIP General Parameters
- Configure Proxy & Registration
- Configure Coders
- Configure Tel Profile T.38 for Fax
- Configure IP Profile T.38 for Fax
- Configure Endpoint Phone numbers
- Configure IP to Trunk Group Routing
- Saving all Configurations to Flash Memory

Note: During compliance testing a standard WEB browser was used for the complete configuration of the AudioCodesMP-118. Some pre-configuration can be done by modifying a Configuration File which can be loaded on to the MP-118.

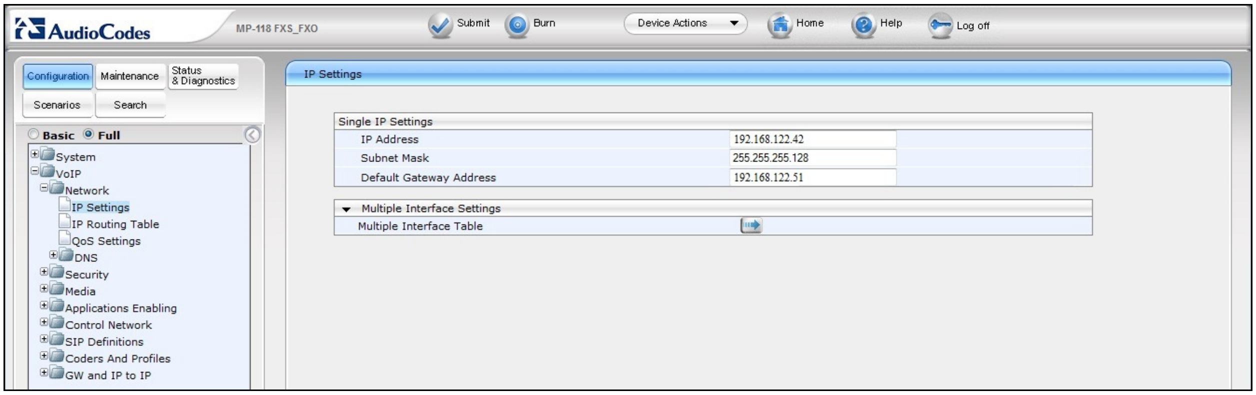
7.1. Logging into the AudioCodes MP-118

Enter the IP address of the AudioCodes into a web browser. At first time log in enter the appropriate credentials and click on the OK button.



7.2. Configure IP Settings

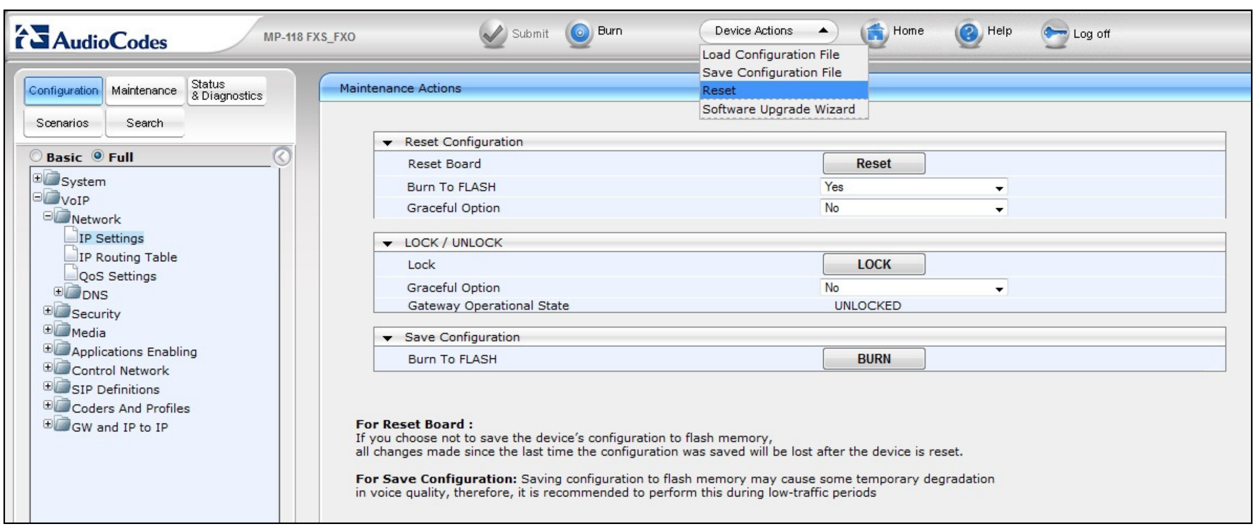
Once the web page opens click on the **Configuration** button and check the **Full** radio button and navigate to **VoIP → Network → IP Settings**. Enter the IP address of the MP-118 along with the mask and default gateway:



Click on the **Apply** button (not shown) to save.

Once the configuration is saved a Gateway Reset is required. The following steps are required:

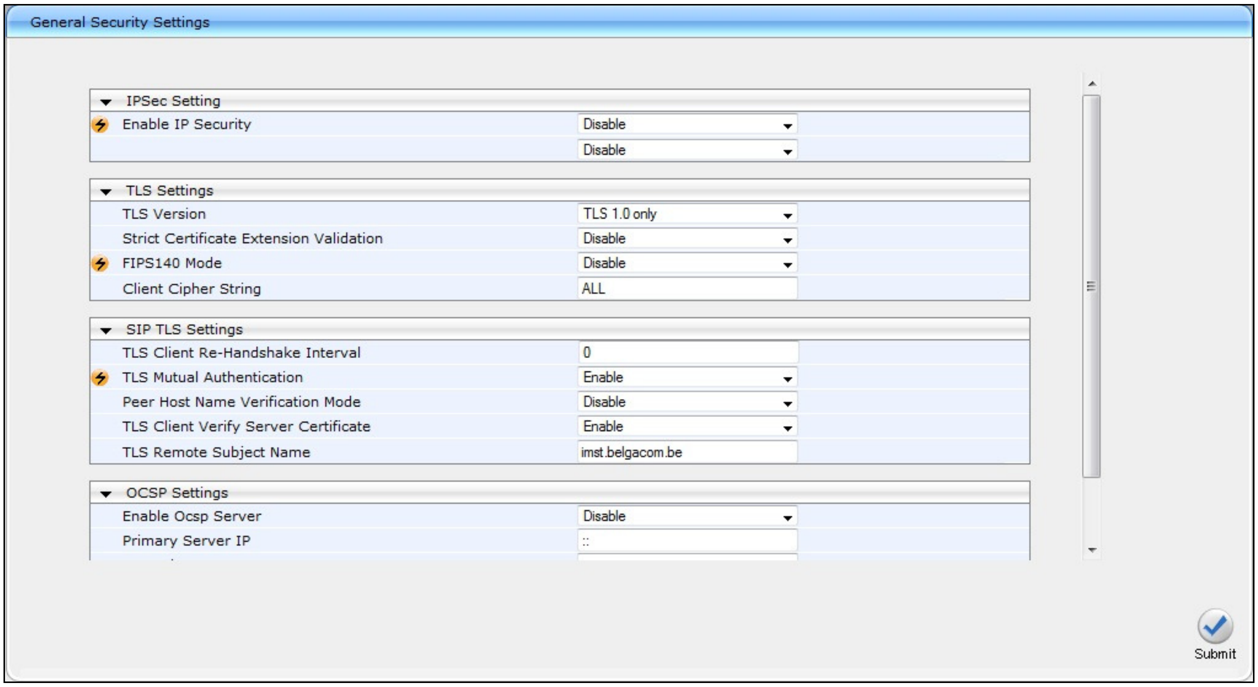
- Click on the **Device Actions** drop down box
- Select **Reset**
- Select **Yes** from the **Burn To FLASH** drop down button
- Click on the **Reset** button next to **Reset Board**
- Click the **OK** button (Not Shown)



Note: It will take up to 60 seconds for the Gateway to reset.

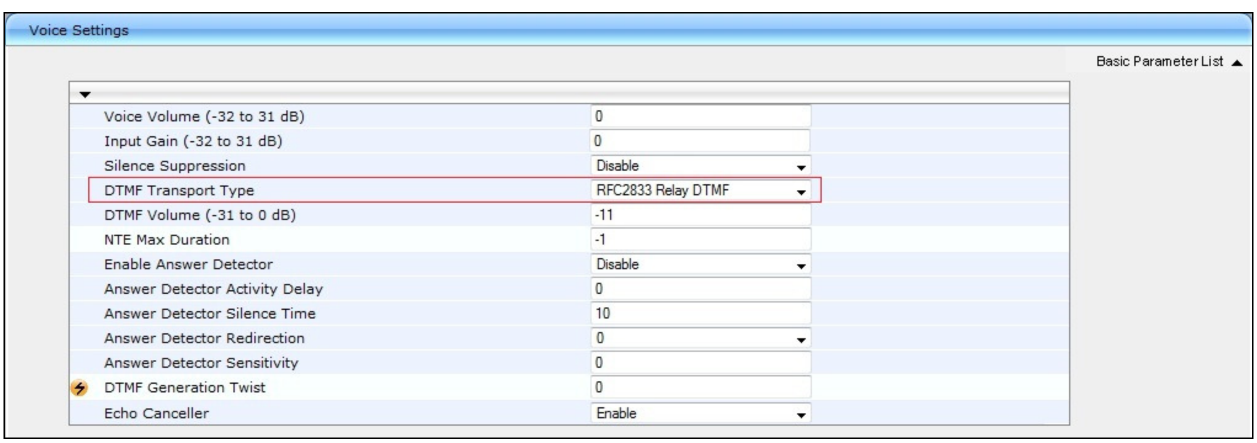
7.3. Configure Security Settings for TLS

The MP-118 was configured to connect to the session manager using TCP during test. Security settings are shown here, however, if a connection is required using TLS. Navigate to **VoIP → Security → General Security Settings** (not shown). Enable **TLS Mutual Authentication** and define the **TLS Remote Subject Name**. During test **imst.belgacom.be** was used:



7.4. Configure Voice Settings

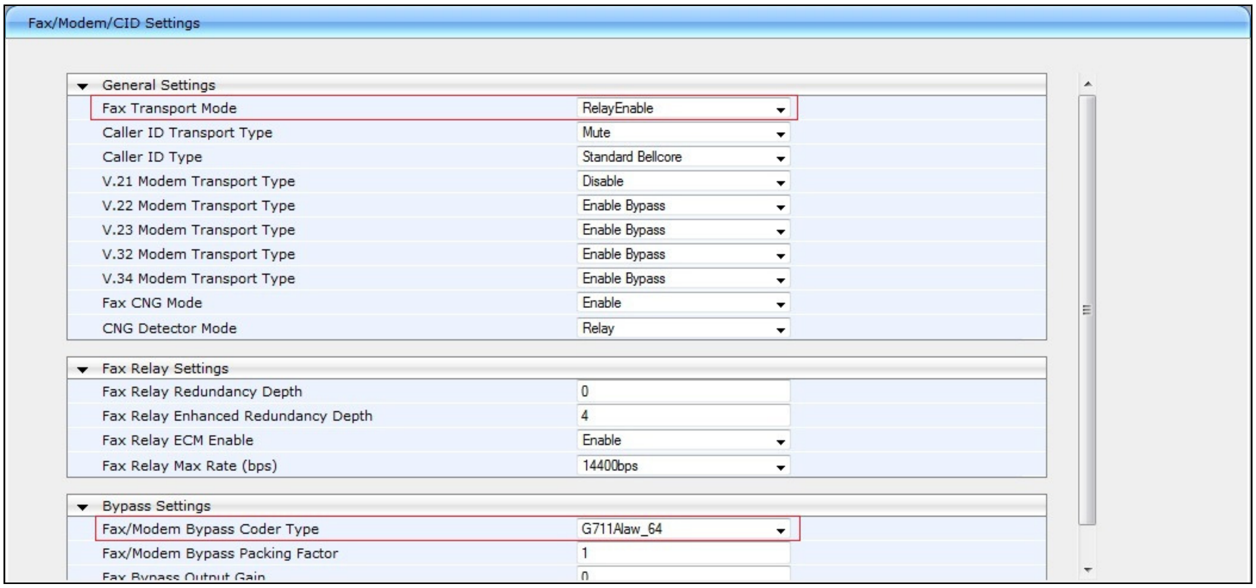
Navigate to **VoIP → Media → Voice Setting** (not shown). The following steps are required:
From the **DTMF Transport Type** drop down box select **RFC2833 Relay DTMF**
Click on the **Submit** button (not shown) to save.



7.5. Configure Fax/Modem/CID Settings

During compliance testing the T.38 Fax configuration was as follows: Navigate to **VoIP → Media → Fax/Modem/CID Settings** (not shown). The following steps are required:

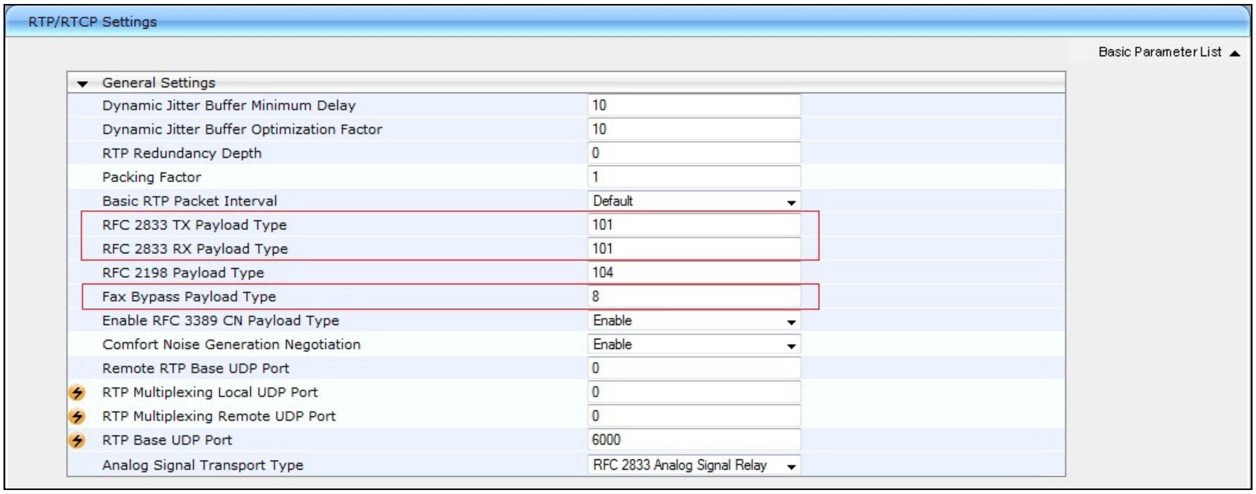
- From the **Fax Transport Mode** drop down box in the General Settings window select **RelayEnable**
- From the **Fax/Modem Bypass Coder Type** drop down box in the Bypass Settings window select **G711Alaw_64**
- Click on the **Submit** button (not shown) to save.



7.6. Configure RTP/RTCP Settings

The configuration of the RTP settings allows setting of the Payload Type for DTMF and Fax Bypass. When negotiation of T.38 fails, the system will fall back to G.711 Alaw. This uses payload Type 8 as standard. Navigate to **VoIP → Media → RTP/RTCP Settings** (not shown). The following steps are required:

- In the **RFC 2833 TX Payload Type** field enter **101** which is the Payload Type used by Belgacom for receiving DTMF
- In the **RFC 2833 RX Payload Type** field enter **101** which is the Payload Type used by Belgacom for transmitting DTMF
- In the **Fax Bypass Payload Type** field enter **8** which is the standard Payload Type allocated to G.711Alaw
- Click on the **Submit** button (not shown) to save.

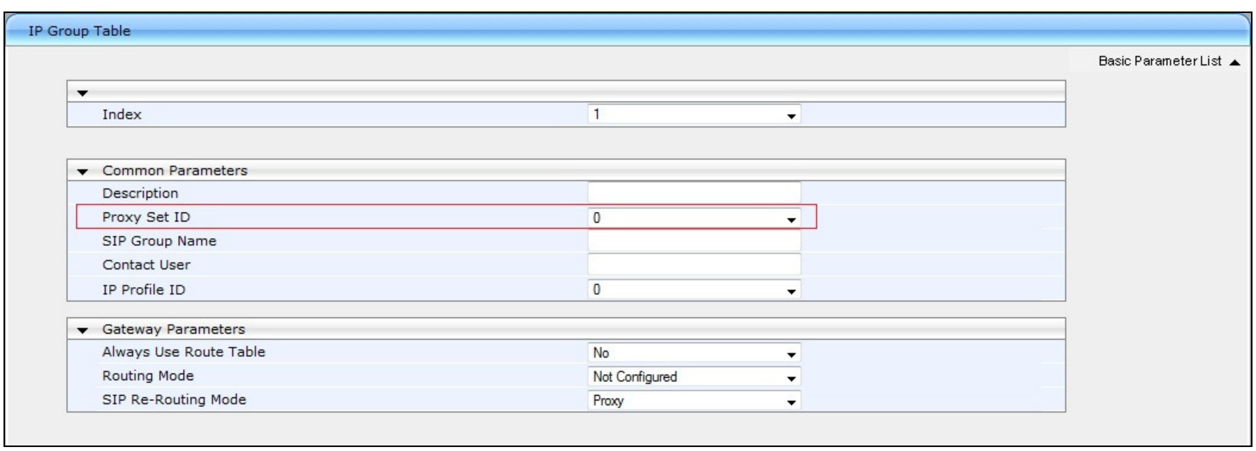


Note: The **Fax Bypass Payload Type** setting of **8** is critical as any other setting will not correctly identify the codec used for bypass as G.711A in the RTP header. The actual codec used for the media is defined by the **Fax/Modem Bypass Coder Type** described in **section 7.5**.

7.7. Configure IP Group Table

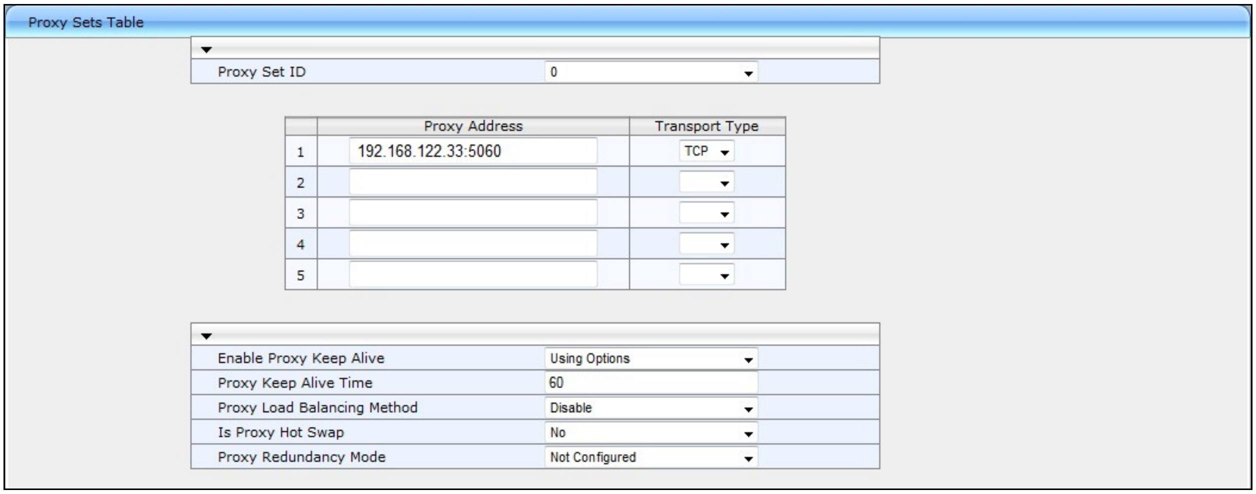
Configure the IP group Table for connection to the Session manager. To do this, navigate to **VoIP → Control network → IP Group Table** (not shown). The following steps are required:

- Select a free index from the **Index** drop down box. i.e., **1**
- Enter a description in the Description field if required (none was entered for the test configuration)
- Select 0 from the **Proxy Set ID** drop down box – this is the Proxy Sets Table to be used to define the IP address of the Session Manager
- Click on the **Submit** button (not shown) to save.



7.8. Configure Proxy Sets Table

Proxy Set ID 0 was configured with the IP address of the Session manager. Navigate to **VoIP → Control network → Proxy Sets Table** (not shown). From the **Proxy Set ID** drop down box select **0**.

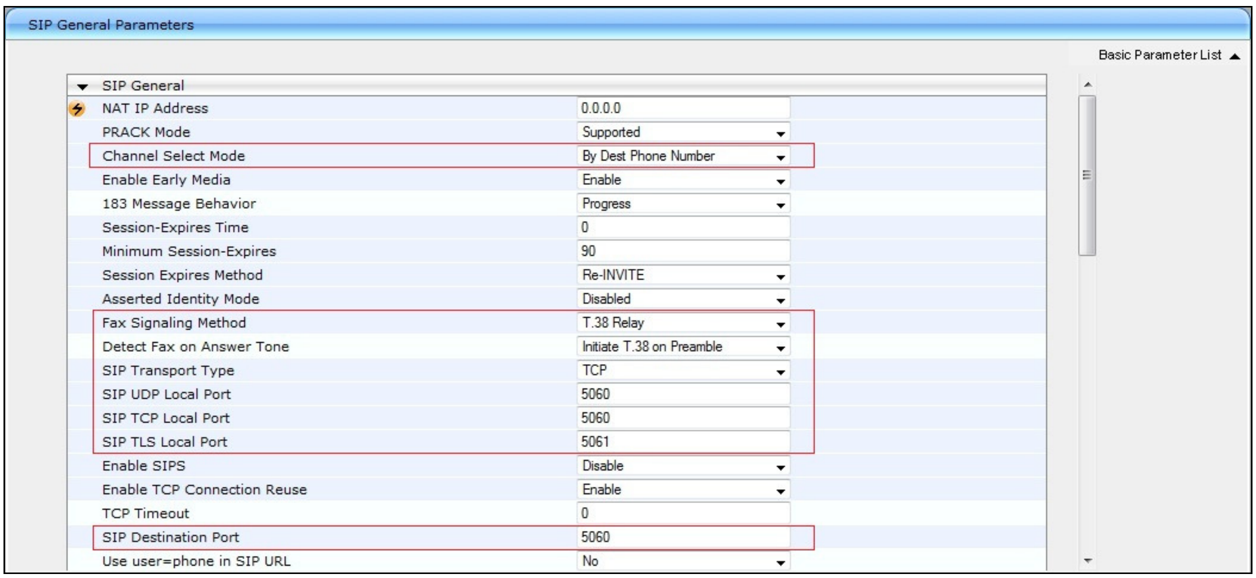


Note: During test an OPTIONS keep-alive was configured for 60 seconds.

7.9. Configure SIP General Parameters

Navigate to **VoIP → SIP Definitions → General Parameters** (not shown). The following steps are required:

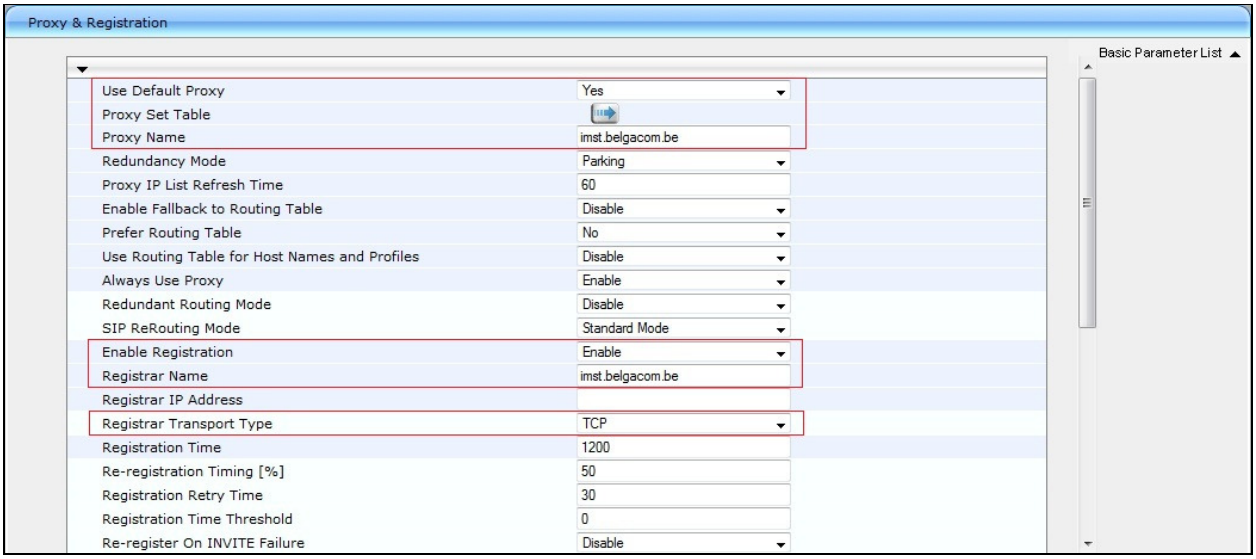
- Select **By Dest Phone Number** from the **Channel Select Mode** drop down box
- Select **T.38 Relay** from the **Fax Signaling Method** dropdown box
- Select **Initiate T.38 on Preamble** from the **Detect Fax on Answer Tone** drop down box
- Select **TCP** from the **SIP Transport Type** drop down box
- Enter **5060** in the **SIP UDP** Local Port field
- Enter **5060** in the **SIP TCP** Local Port field
- Enter **5061** in the **SIP TLS** Local Port field
- Enter **5060** in the **SIP Destination Port** field



7.10. Configure Proxy & Registration

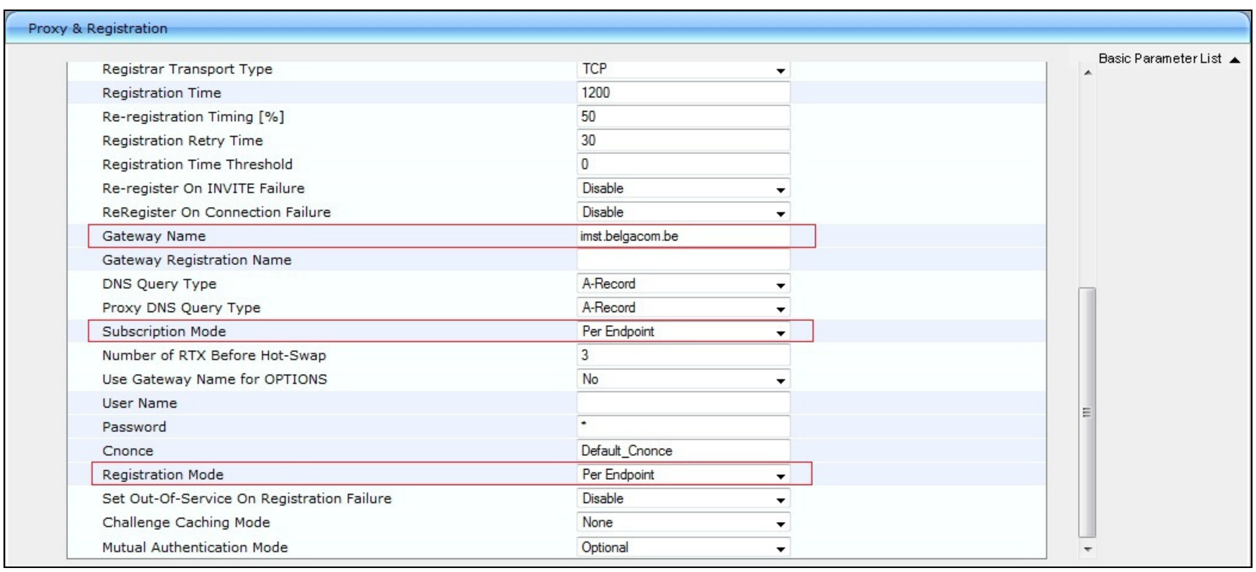
Navigate to **VoIP → SIP Definitions → Proxy & Registration** (not shown). The following steps are required:

- Select a **Yes** from the **Use Default Proxy** drop down box
- Enter the Domain of the Belgacom network in the **Proxy Name** field. i.e., **imst.belgacom.be**
- Select **Enable** from the **Enable Registration** drop down box
- Enter the Domain of the Belgacom network in the **Registrar Name** field. i.e., **imst.belgacom.ie**
- Select **TCP** from the **Registrar Transport Type** drop down box



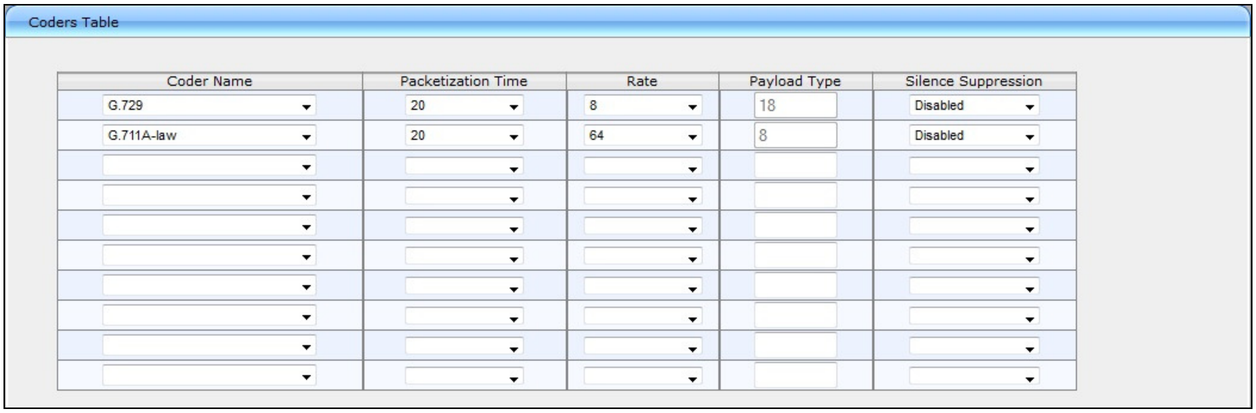
Scroll down using the scroll bar as shown in the screen shot.

- Enter the Domain of the Belgacom network in the **Gateway Name** field. i.e., **imst.belgacom.ie**
- Select **Per Endpoint** from the **Subscription Mode** type dropdown box
- Select **Per Endpoint** from the **Registration Mode** type dropdown box
- Click on the **Submit** (not shown) button to save.



7.11. Configure Coders

During compliance testing the both Codec **G.711A-law** and **G.729** were used. Navigate to **VoIP → Coders and Profiles → Coders**. The following section shows both configurations.

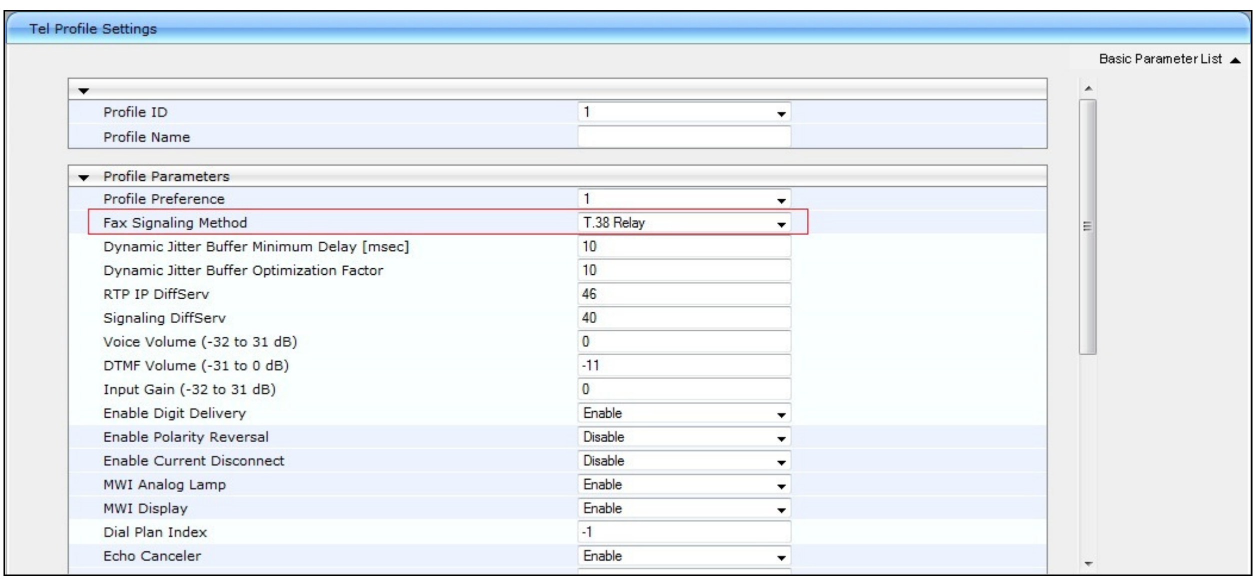


Note: Both Codecs were tested exclusively.

7.12. Configure Tel Profile T.38 for Fax

Navigate to **VoIP → Coders and Profiles → Tel Profile Settings** (not shown). The following steps are required:

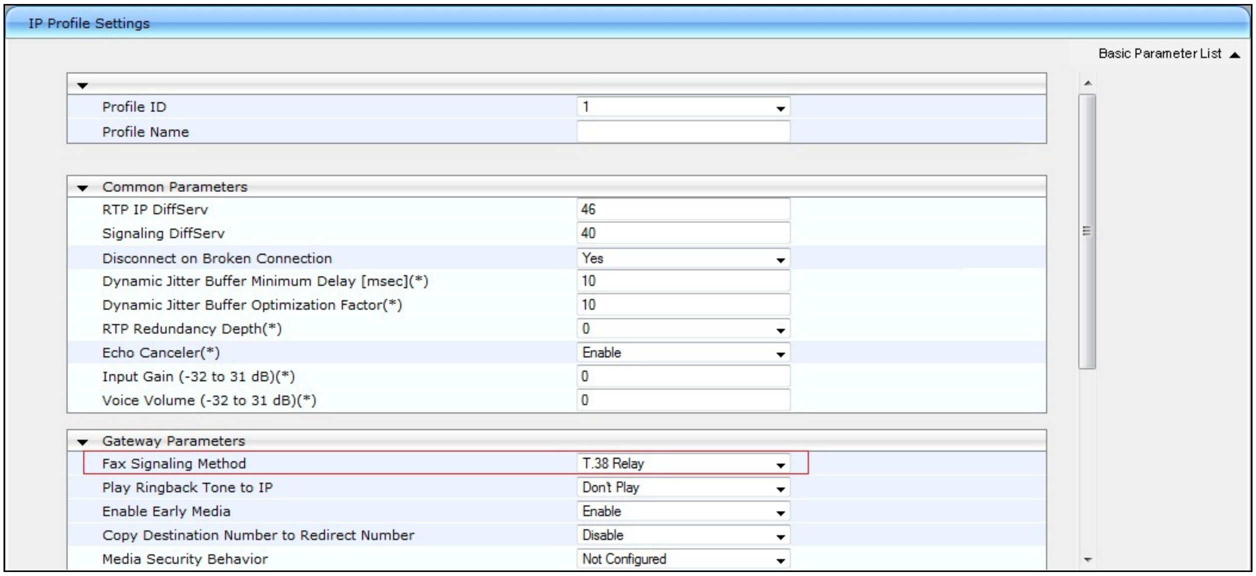
- Select **1** from the **Profile ID** drop down box
- Select **T.38** Relay from the **Fax Signaling Method** drop down box
- Click on the **Submit** button (not shown) to save.



7.13. Configure IP Profile T.38 for Fax

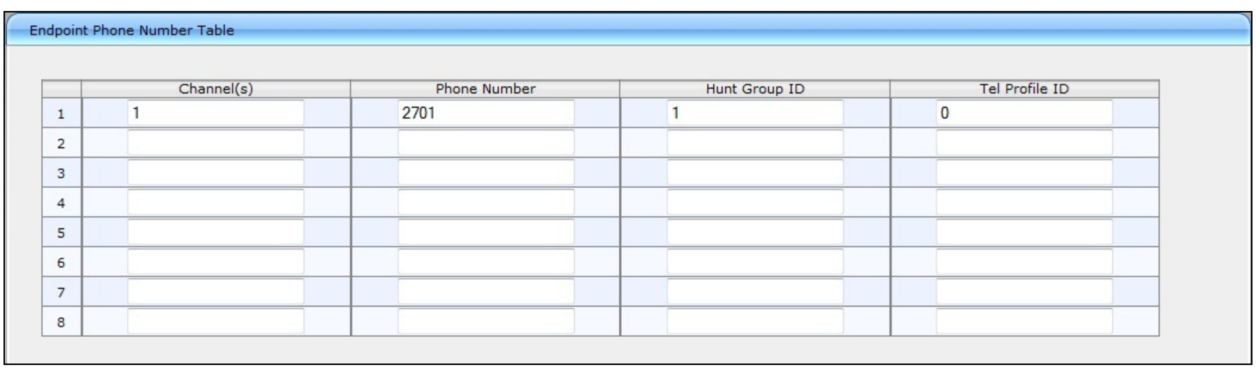
Navigate to **VoIP → Coders and Profiles → IP Profile Settings** (not shown). The following steps are required:

- Select **1** from the Profile ID drop down box
- Select **T.38** Relay from the **Fax Signaling Method** drop down box
- Click on the **Submit** button to save.



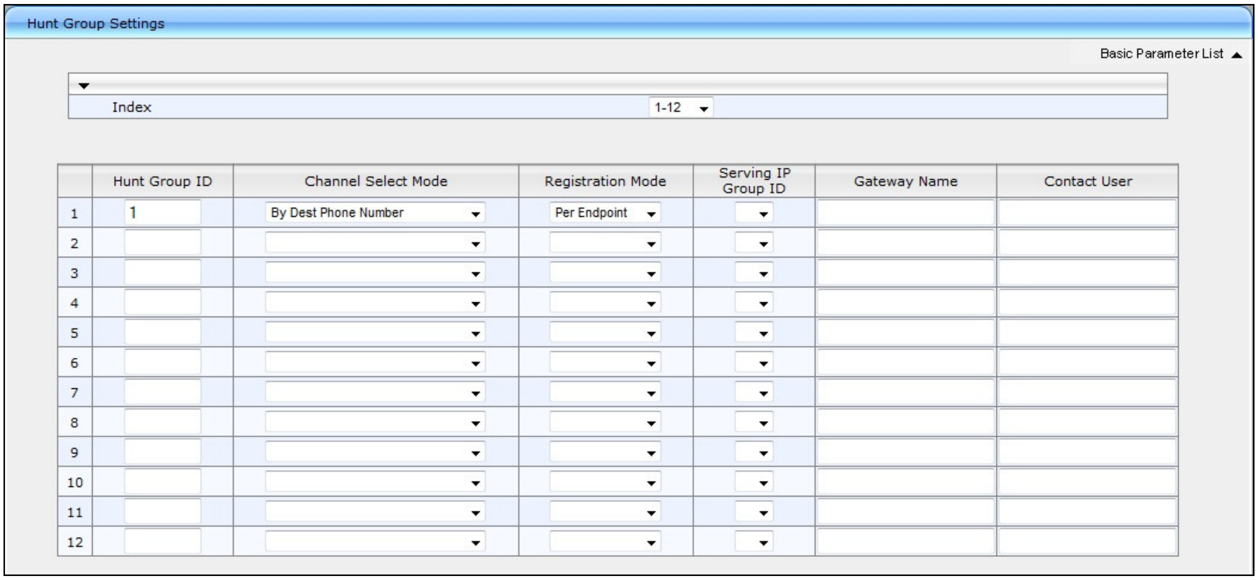
7.14. Configure Endpoint Phone numbers

During compliance testing, only one number was used for fax. The number was defined on channel 1 and uses hunt group 1. Navigate to **VoIP → GW and IP to IP → Hunt Group → Endpoint Phone Number** (not shown). Define the number as shown:



To define the hunt group, navigate to **VoIP → GW and IP to IP → Hunt Group → Hunt Group Settings** (not shown). The following steps are required:

- For **Hunt Group ID 1** select **By Dest Phone Number** from the **Channel Select Mode** drop down box and select **Per Endpoint** from the **Registration Mode** drop down box.
- Click on the **Submit** button (not shown) to save.



Hunt Group Settings

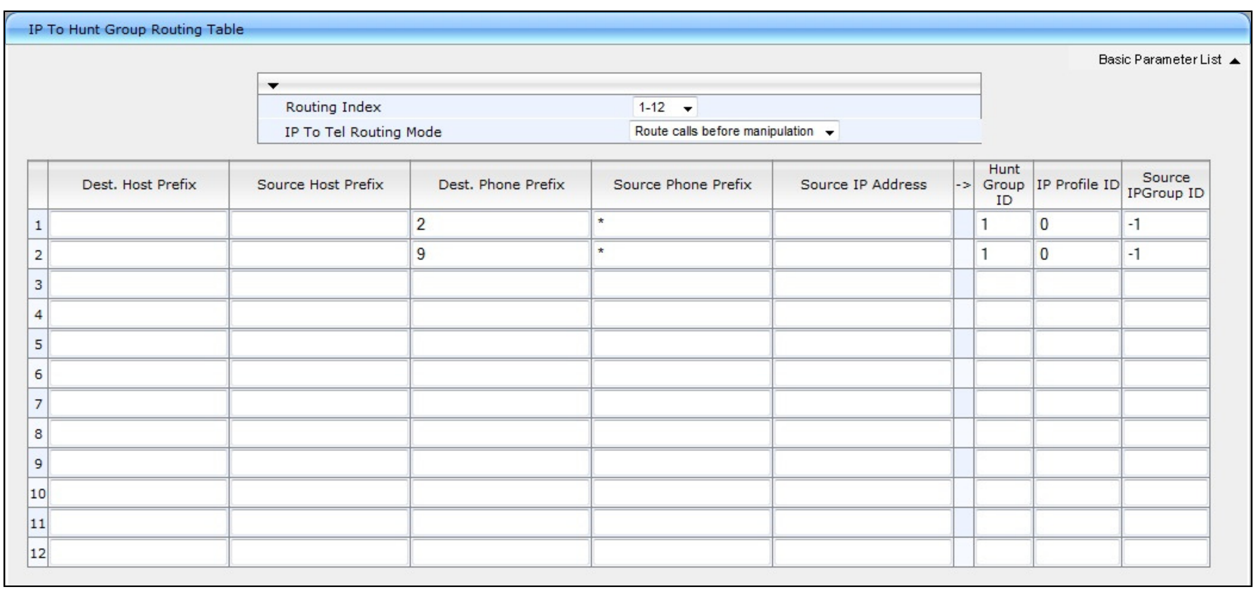
Basic Parameter List

Index: 1-12

	Hunt Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	By Dest Phone Number	Per Endpoint			
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

7.15. Configure IP to Trunk Group Routing

Navigate to **VoIP → GW and IP to IP → Routing → IP to Trunk Group Routing** (not shown). The extension on the MP-118 starts with the digit 2 and digit 9 is dialled to route out to the Session Manager. Enter the values shown in the screenshot below and click **Submit** (not shown):



IP To Hunt Group Routing Table

Basic Parameter List

Routing Index: 1-12

IP To Tel Routing Mode: Route calls before manipulation

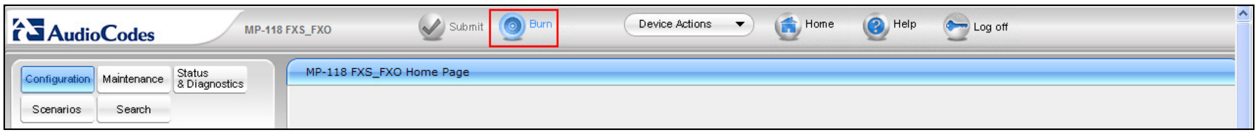
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Hunt Group ID	IP Profile ID	Source IPGroup ID
1			2	*			1	0	-1
2			9	*			1	0	-1
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

Note: where there are no values in a field leave it blank. A "*" indicates that the field can be any value.

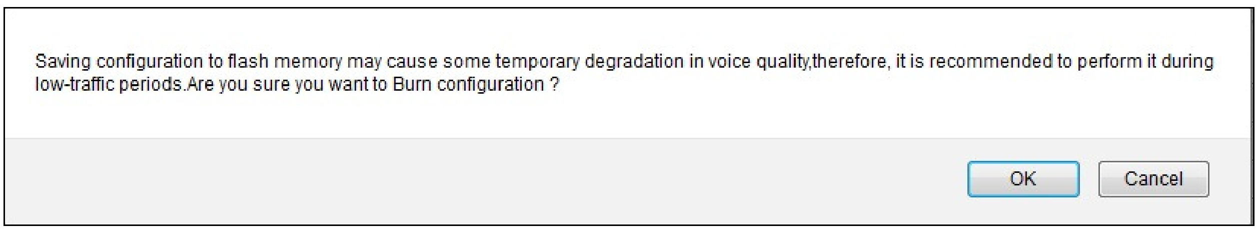
7.16. Save all Configurations to Flash Memory

Configuration changes must be saved to Flash Memory. The following step is required:

- Click on the **Burn** button.



- When the Message from webpage appears click on the **OK** button



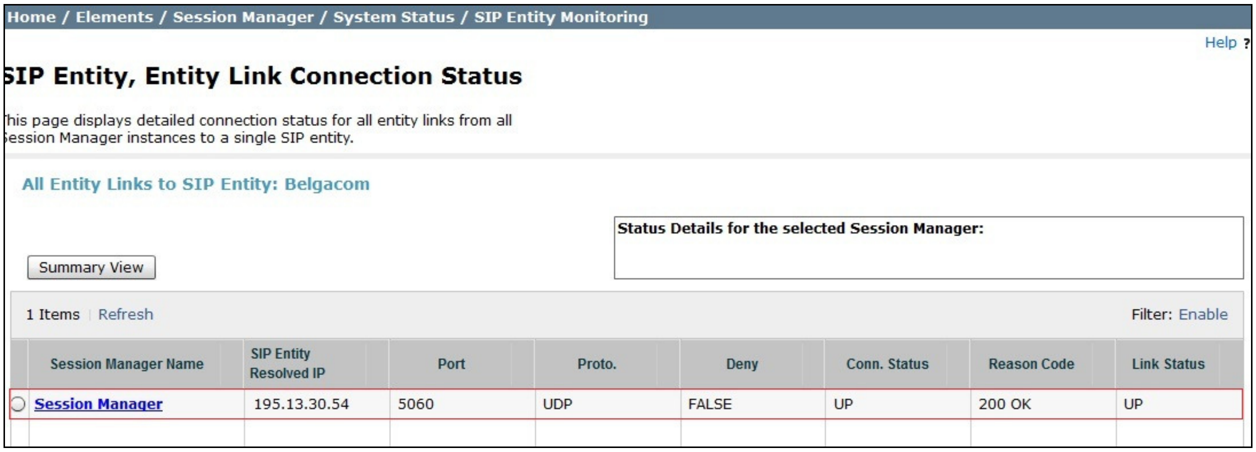
8. Configure Belgacom Network Equipment

The configuration of the Belgacom equipment used to support the Belgacom SIP Trunk service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Belgacom equipment and system configuration please contact an authorised Belgacom representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.



2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

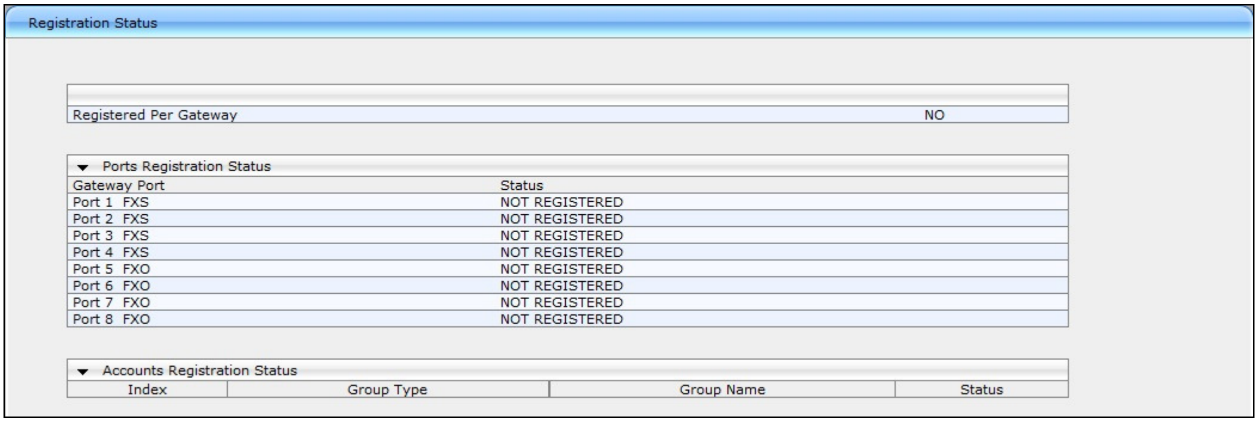
```
status trunk 1

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Check the status of the MP-118 SIP Endpoint used for Fax. Click on the **Status & Diagnostics** button and check the Full radio button (not shown) and navigate to **VoIP Status → Registration Status**



Note: The screenshot was taken after the Session Manager had been reconfigured and the MP-118 was no longer registered on the Session Manager. During test when fax was being successfully transmitted and received, port 1 was shown as "Registered".

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.3 and AudioCodes MP-118 VoIP Gateway to the Belgacom SIP Trunk service. Belgacom SIP Trunk service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a observations listed in **Section 2.2**.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.2, December 2012.

[2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, December 2012.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, December 2012, Document Number 555-245-205.

[5] *Implementing Avaya Aura® System Manager* Release 6.3, December 2012

[6] *Upgrading Avaya Aura® System Manager to 6.3*, January 2013.

[7] *Administering Avaya Aura® System Manager* Release 6.3, December 2012

[8] *Implementing Avaya Aura® Session Manager* Release 6.3, December 2012

[9] *Upgrading Avaya Aura® Session Manager* Release 6.3, December 2012

[10] *Administering Avaya Aura® Session Manager* Release 6.3, December 2012,

[11] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

[12] *Application Notes for Configuring Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 to Support Belgacom SIP Trunk Service* https://downloads.avaya.com/css/P8/documents/100162831

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.