Avaya Solution & Interoperability Test Lab

Application Notes for AudioCodes MediaPack 11x with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Session Manager 7.0 – Issue 1.0

Abstract

These Application Notes contain interoperability instructions for configuring AudioCodes MediaPack 11x with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Compliance testing was conducted to verify interoperability.

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 in Thornton, CO.

Table of Contents

1. Introduction

AudioCodes MediaPack (MP) 11x Analog VoIP gateways implement voice technology that connect analog telephones, fax machines (FXS) and landlines (FXO) to IP based PBX systems. In the compliance test, AudioCodes MP-118 VoIP gateway was used to verify interoperability within an Avaya Aura® IP Telephony Environment.

2. General Test Approach and Test Results

Interoperability compliance testing focused on verifying various inbound and outbound call flows between AudioCodes MP-11x, Communication Manager and Session Manager.

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

Analog lines on AudioCodes MP-11x were configured to register as SIP users on Session Manager. SIP TLS and SRTP were utilized during this test effort. The following features and functionalities were covered during compliance testing:

- Incoming calls to AudioCodes MP-11x
- Outgoing calls from AudioCodes MP-11x
- Voice codecs G.711U, G.711A and G.729 using SRTP
- Incoming and outgoing faxes using T.38
- DTMF tone transmission with RFC2833
- Calls using various Avaya endpoints, including analog, H.323 and SIP.
- Basic features including Hold/Resume, DTMF transmission, Voicemail with Message Waiting Indicator (MWI).

2.2. Test Results

All test cases were executed and passed with the following exception/observations:

MWI was tested by sending MWI indication to the MP-11x and verifying that stutter tone was heard on the analog phone.

2.3. Support

Technical support for AudioCodes MP-11x can be obtained through the following:

- Phone:
  - Americas: +1-732-652-1085 or 1-800-735-4588
  - Rest of the World: 800-44422444 or 972-3-9764343
- Web:crm.audiocodes.com
- E-Mail: support@audiocodes.com

3. Reference Configuration

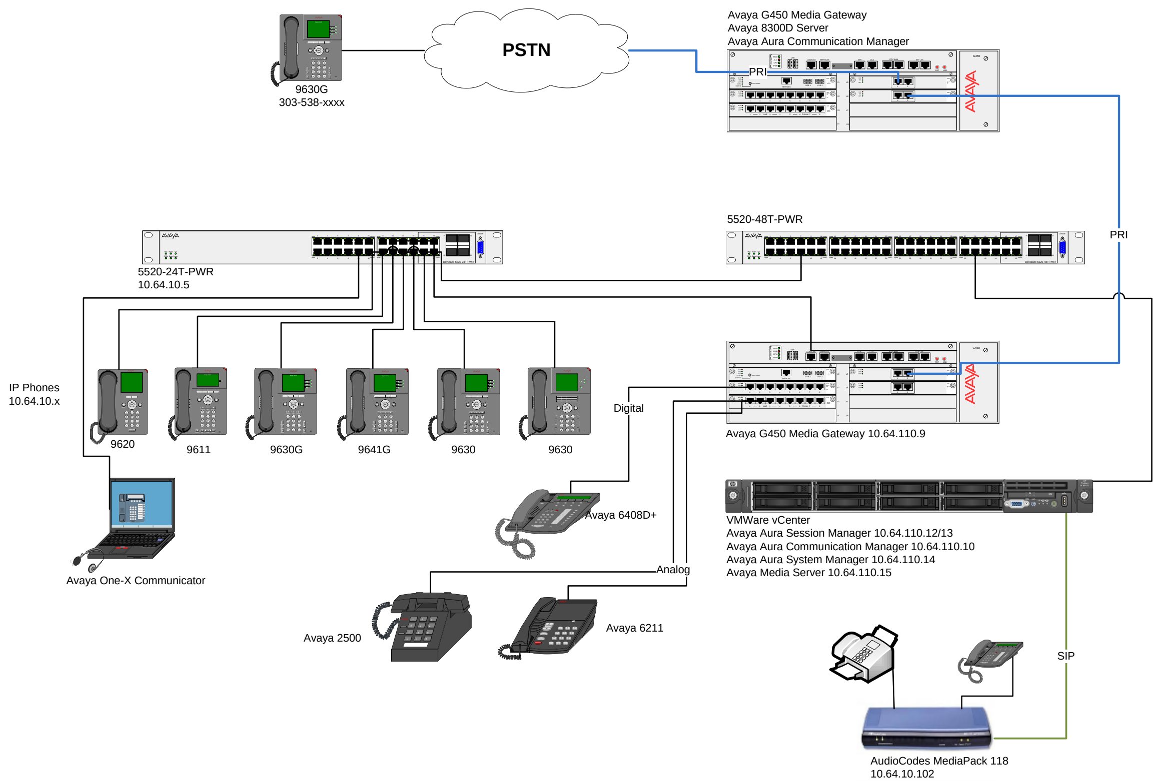


Figure 1: AudioCodes MP-118 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8300D Server	7.0.1.1.1.441.23384
Avaya Aura® Session Manager	7.0.1.1.701114
Avaya Aura® System Manager	7.0.1.1.065378
Avaya 9600 Series IP Deskphones	H.323 3.2.7
	SIP 7.0.1.2, H.323 6.6.3
Avaya 6408D+ Digital Deskphone	-
Avaya 2500 and 6221 Analog Phone	-
AudioCodes MediaPack 118	6.60A.328.004

5. Configure Avaya Aura® Communication Manager

This section provides steps for configuring Communication Manager. All configuration for Communication Manager is done through System Access Terminal (SAT).

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameters customer-options** command to verify options.

On **Page 2,** verify that there is sufficient capacity for SIP trunks by comparing **Maximum Administered SIP Trunks** field with corresponding **USED** column field.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  20
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  15
                       Maximum Administered SIP Trunks: 4000  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
        (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 5,** verify **ISDN/PRI** and **Media Encryption Over IP** fields are 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 Network Region

Use the **change ip-network-region *n*** command to configure a network region, where ***n*** is an existing network region.

5.2.1. IP Network Region for Voice and Fax Calls

Configure this network region as follows:

- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter an **Authoritative Domain**, e.g. **avaya.com**

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main                  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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
```

5.3. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where ***n*** is an existing codec set number

5.3.1. IP Codec set for Voice and Fax Calls

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1, 2 and 3** to **G.711MU, G.729AB, G.711A** respectively
- Set **Media Encryption 1** to **1-srtp-aescm128-hmac80**

Note: G.711MU, G.711A and G.729AB were tested during compliance testing

```
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.711MU          n          2        20
 2: G.729AB          n          2        20
 3: G.711A           n          2        20
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
 5:
```

On **Page 2**:

- Set **Fax Mode** to **t.38-standard**

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  2048:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  2048:Kbits

                                                                  Packet
                          Mode                 Redundancy         Size(ms)
    FAX                   t.38-standard         0            ECM: y
    Modem                 off                   0
    TDD/TTY               US                    3
    H.323 Clear-channel   n                     0
    SIP 64K Data          n                     0                 20
```

5.4. Administer IP Node Names

Use the **change node-names ip** command to add and entry for Session Manager. For compliance testing, **asm** and **10.64.110.13** entry was added.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
acms                10.64.110.18
aes                 10.64.110.15
ams                 10.64.110.16
asm                 10.64.110.13
biscom              10.64.101.152
cms17               10.64.10.85
default             0.0.0.0
egw1                10.64.110.200
egw2                10.64.110.201
hospitality         10.64.10.47
kpc                 10.64.10.47
mx                  10.64.10.22
procr               10.64.110.10
procr6              ::
```

5.5. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number.

5.5.1. Signaling Group for Voice and Fax Calls

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **TLS**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.4**, i.e. **asm**
- Set **Far-end Network region** to the configured region in **Section 5.2.1**, i.e. **1**
- Enter a **Far-end Domain,** e.g. **avaya.com**

```
add signaling-group 1                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? y
   Near-end Node Name: procr                Far-end Node Name: asm
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: avaya.com
                                             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? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Note: Signaling Group, Trunk Group and Route Pattern for PSTN calls via PRI was pre-configured and is not shown in this document.

5.6. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where ***n*** is an available trunk group number.

5.6.1. Trunk Group for Voice and Fax Calls

Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. **asm**
- Enter a valid **TAC**, e.g. **101**
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 0**, i.e. **1**
- Enter a desired number in **Number of Member** field

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

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

On **Page 3**:

- Set **Number Format** to **private**

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



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

5.7. Administer Route Pattern

Use the **change route-pattern** ***n*** command to configure a route pattern, where ***n*** is an available route patterns

5.7.1. Route Pattern for Voice and Fax Calls

Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 5.6.1**, i.e. **1**
- For line 1, set **FRL** to **0**

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Voice and Fax
                             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
```

5.8. Administer Private Numbering

Use the **change private-numbering 1** command to define the calling party number to send to Session Manager and configure private numbering as follows:

- Add entries for trunk group configured in **Section 5.6**

Note: For compliance testing, 5-digit extensions beginning with 1 routed over trunk group 1 which resulted in a 5-digit calling party number.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  1                1                           5     Total Administered: 1
                                                         Maximum Entries: 540
```

5.9. Administer AAR Analysis

Use the **change aar analysis *n*** command to configure routing for extensions starting with ***n***. Add two entries, one for voice and fax calls and another one for modem calls. For compliance testing, extensions starting with **111** were used for voice and fax calls.

- Set **Dialed String** to starting digits of extensions that will be used, e.g. **111**
- Set **Min** and **Max** to **5** for 5 digit extensions
- Set **Route Pattern** to pattern configured in **Section 5.7**, i.e. **1**
- Set **Call Type** to **lev0**

Note: An entry to dial plan will need to be added for extension range used in this step.

```
change aar analysis 11                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 0

          Dialed           Total     Route     Call   Node  ANI
          String         Min  Max  Pattern    Type   Num   Reqd
    111                  5    5     1         lev0         n
```

5.10. Administer ARS Analysis

Use the **change ars analysis *n*** command to configure routing for calling to PSTN, where n is an NPA or starting digit of PSTN numbers. This configuration is used to route PSTN calls to an FXO line on AudioCodes MP-11x. For compliance testing, PSTN calls were placed to phones with NPA of 303.

- Set **Dialed String** to **303**
- Set **Total Min** and **Total Max** to **10**
- Set **Route Pattern** to pattern configured in **Section 5.7**, i.e. **1**
- Set **Call Type** to **hnpa**

Note: This administration is only required if FXO line is being configured on AudioCodes MP-11x

```
change ars analysis 3                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 3

          Dialed            Total     Route    Call   Node  ANI
          String           Min  Max  Pattern   Type   Num   Reqd
    303                    10   10     1       hnpa         n
    4                      7    7      deny    hnpa         n
    411                    3    3      deny    svcl         n
    444                    10   10     2       fnpa         n
    5                      7    7      deny    hnpa         n
    555                    7    7      deny    hnpa         n
    6                      7    7      deny    hnpa         n
    611                    3    3      1       svcl         n
```

5.11. Administer Stations

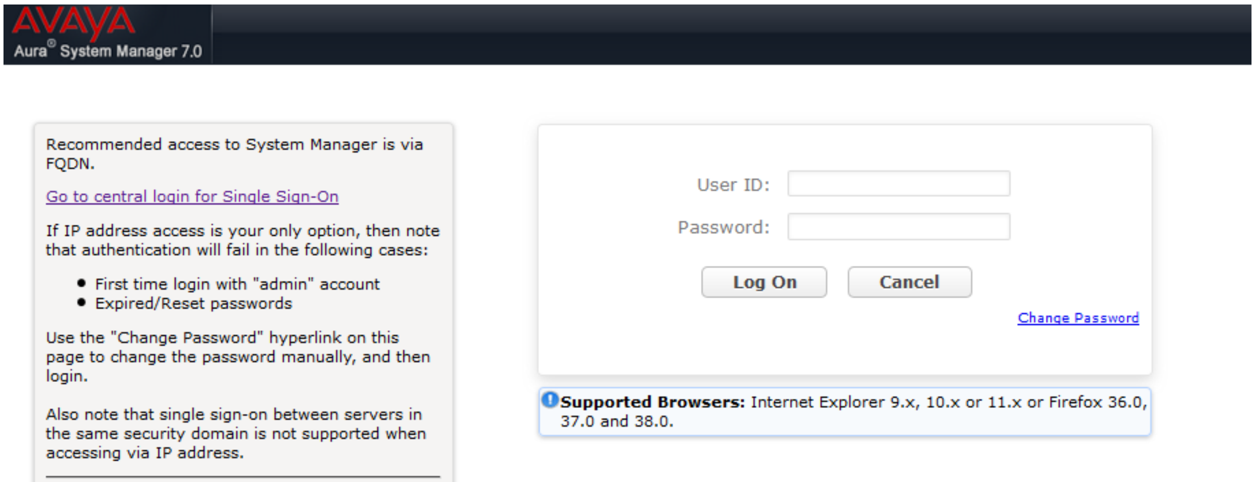
Administration of Avaya Stations/Extensions in Communication Manager and Session Manager is not shown in this document. Please refer to document [1] and/or [2] in reference section of this document.

Note: During compliance testing, Media Encryption settings were modified in the 46xxsettings.txt to enable SRTP for the Avaya SIP Deskphones. TLS registration for Avaya Deskphones is required for SRTP and is enabled by default.

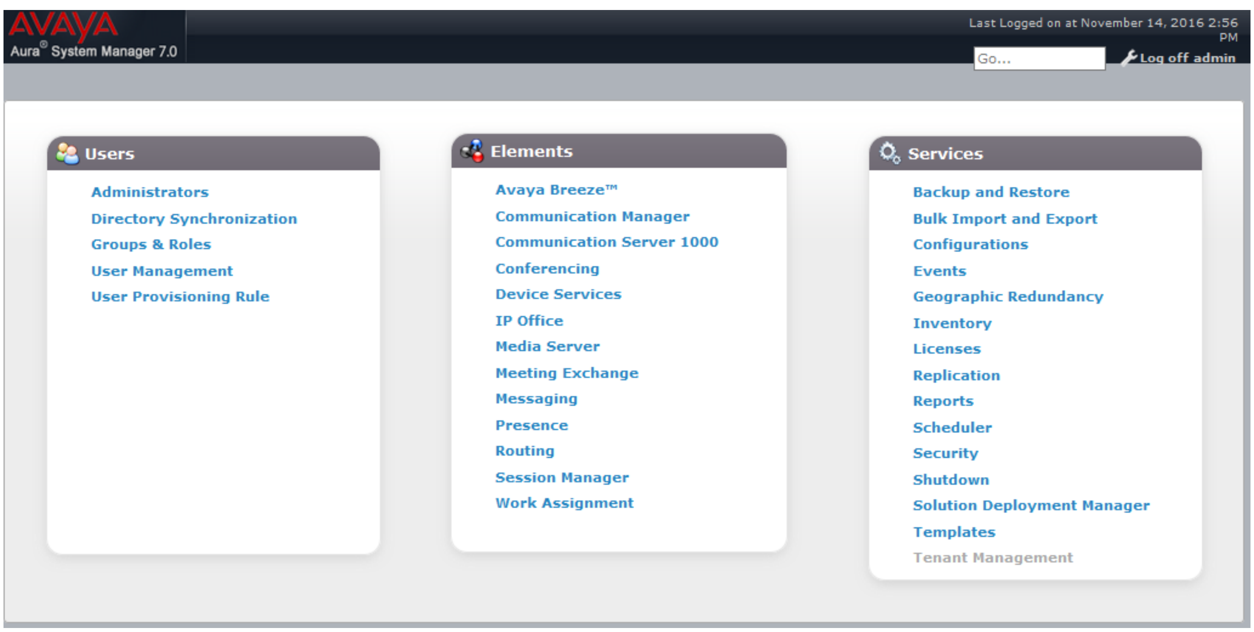
```
## Media Encryption Support
##   Specifies media encryption (SRTP) options supported by
##   phone. Up to 2 options may be selected. Values are in
##   comma-separated list. Options should match those
##   specified in CM IP-codec-set form.
##     1 = aescm128-hmac80
##     2 = aescm128-hmac32
##     3 = aescm128-hmac80-unauth
##     4 = aescm128-hmac32-unauth
##     5 = aescm128-hmac80-unenc
##     6 = aescm128-hmac32-unenc
##     7 = aescm128-hmac80-unenc-unauth
##     8 = aescm128-hmac32-unenc-unauth
##     9 = none (default)
SET MEDIAENCRYPTION "1"
```

6. Configure Avaya Aura® Session Manager

Access the Session Manager Administration web interface by entering https://<ip-address>/SMGR URL in a web browser, where <ip-address> is the IP address of System Manager.



Log in using appropriate credentials

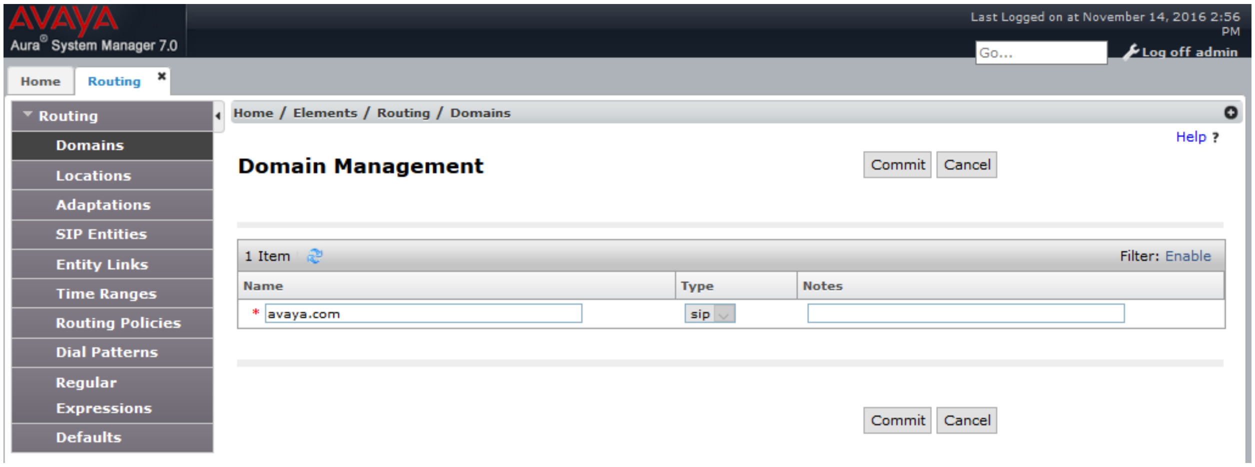


6.1. Add SIP Domain

Navigate to **Home → Elements → Routing → Domains**, click on **New** button (not shown) and configure as follows:

- In **Name** field type in a domain (authoritative domain used in **Section 5.2**) i.e. **avaya.com**
- Set **Type** to **sip**

Click **Commit** to save changes.



6.2. Add Location

Navigate to **Home → Elements → Routing → Location**, click on **New** button (not shown) and configure as follows:

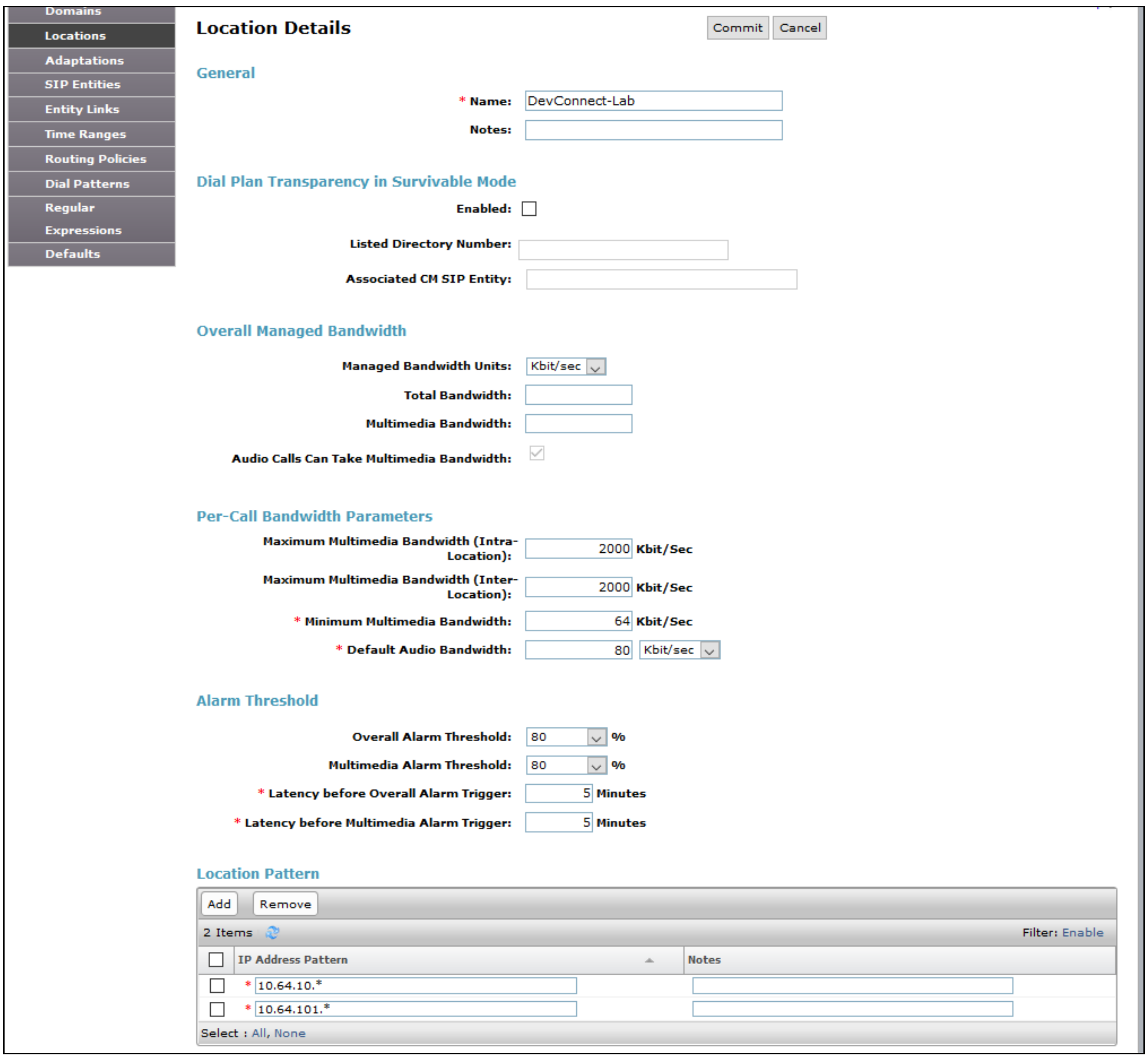
Under **General**:

- Type in a descriptive **Name**

Under **Location Pattern** click on **New** (not shown):

- Type in **IP Address Pattern** for applicable subnets, e.g. **10.64.10.***

Click **Commit** to save changes.



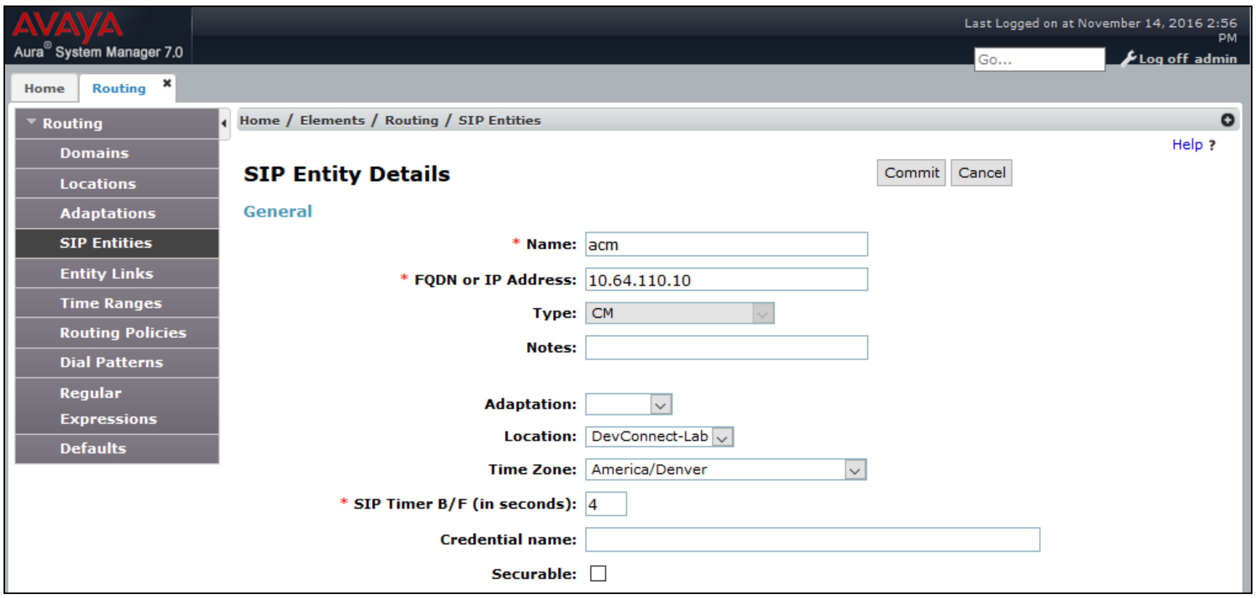
6.3. Add SIP Entity

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address of FQDN of Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes

Note: It is assumed that SIP Entity for Session Manager has been already configured.

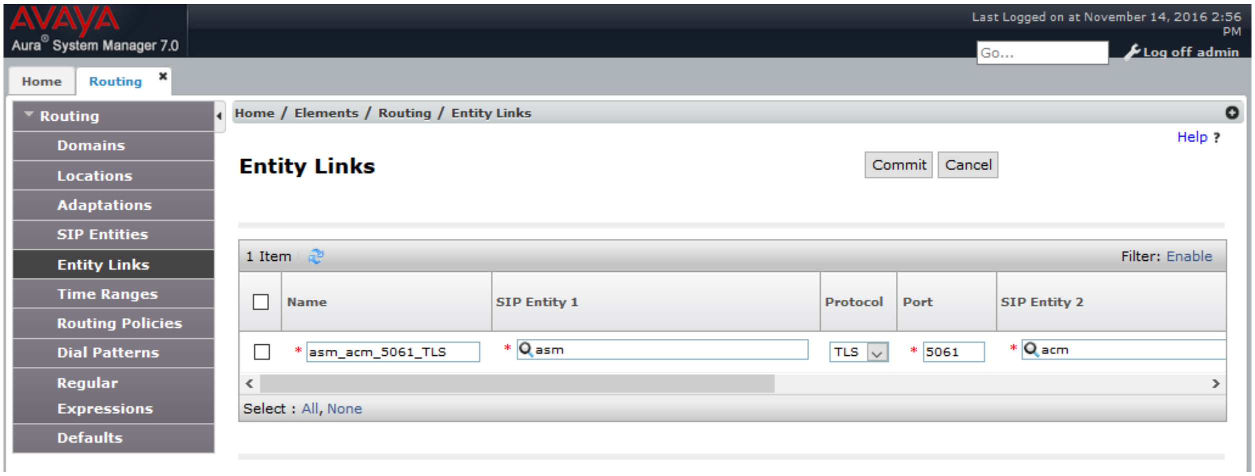


6.4. Add Entity Link

Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.3**

Click **Commit** to save changes.

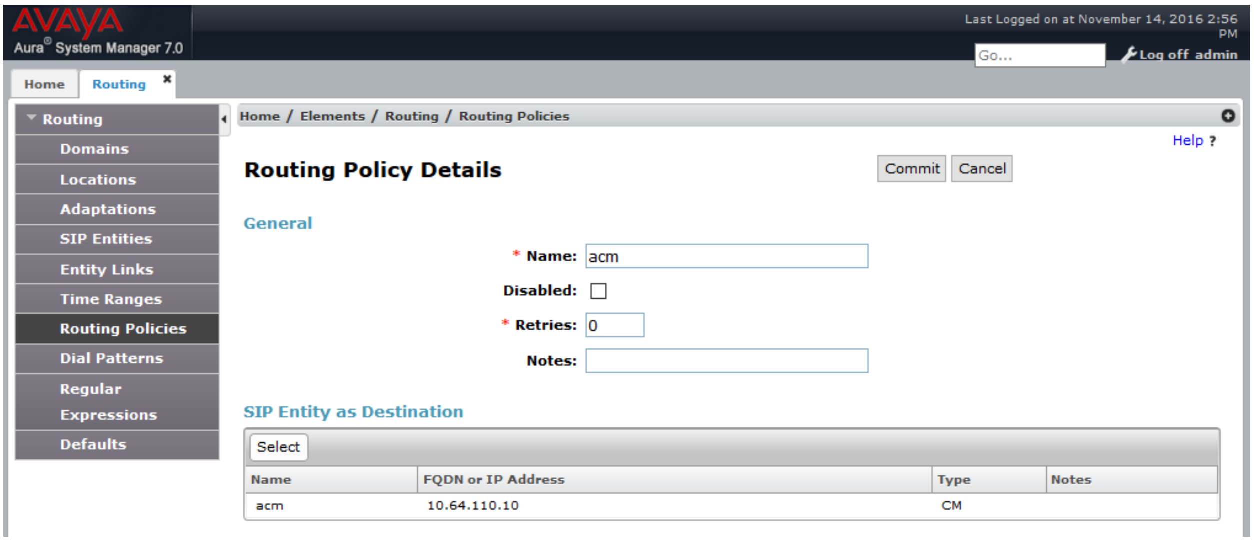


6.5. Add Routing Policy

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select**
  - Select Communication Manager SIP entity added in **Section 6.3**

Click **Commit** to save changes.



6.6. Add Dial Patterns

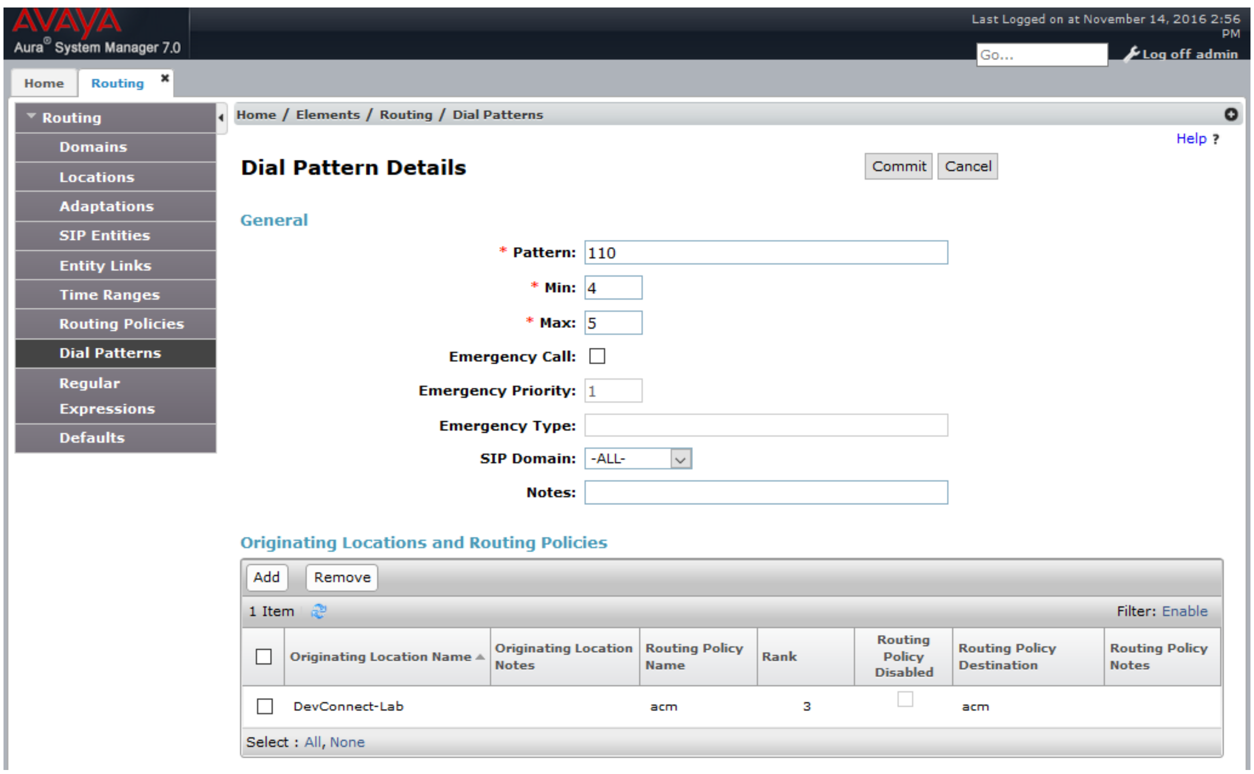
Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General:**

- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number

Under **Originating Locations and Routing Policies:**
Click **Add** and select originating location and Communication Manager routing policy.
Click **Commit** to save changes.

Note: For Compliance testing, dialed number of 110xx were used.



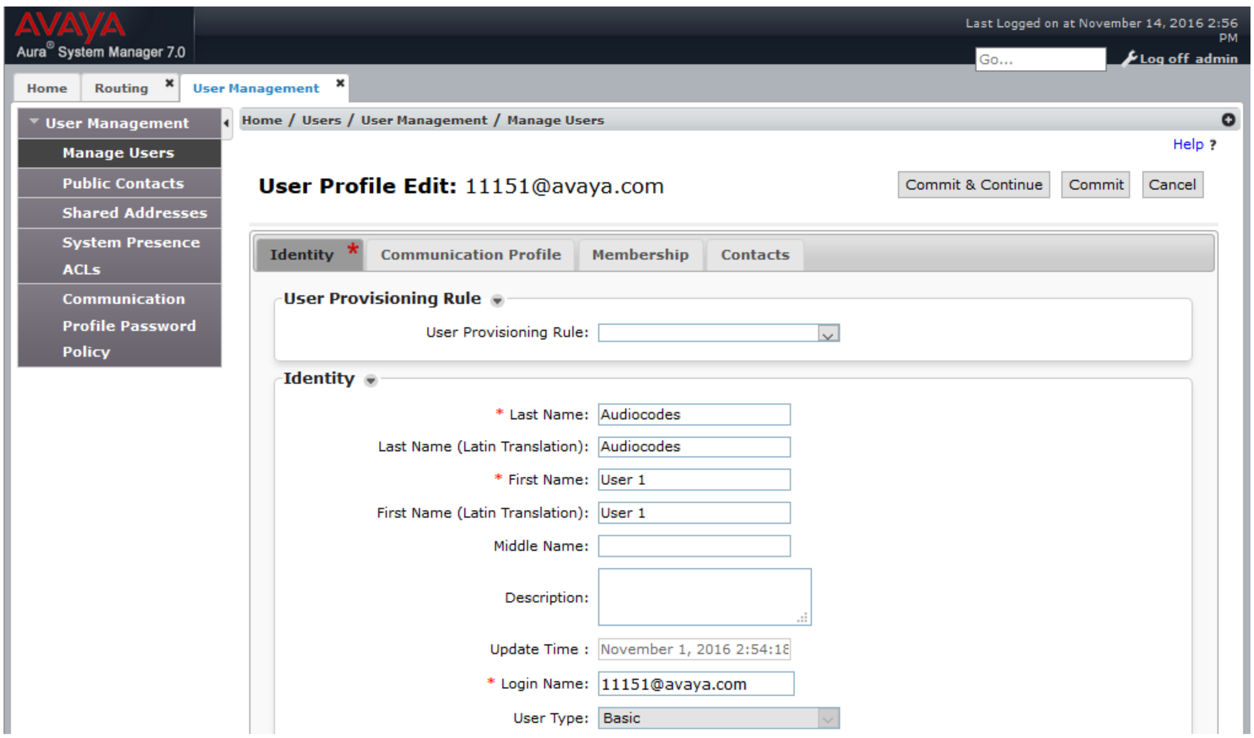
6.7. Add User

For each analog line on AudioCodes MP-11x, a user needs to be added on Session Manager. Information in this section will be used by AudioCodes MP-11x for registering to Session Manager.

Navigate to **Home → Users → User Management → Manage User**, click on **New** (not shown) and configure as follows:

Under **Identity** tab:

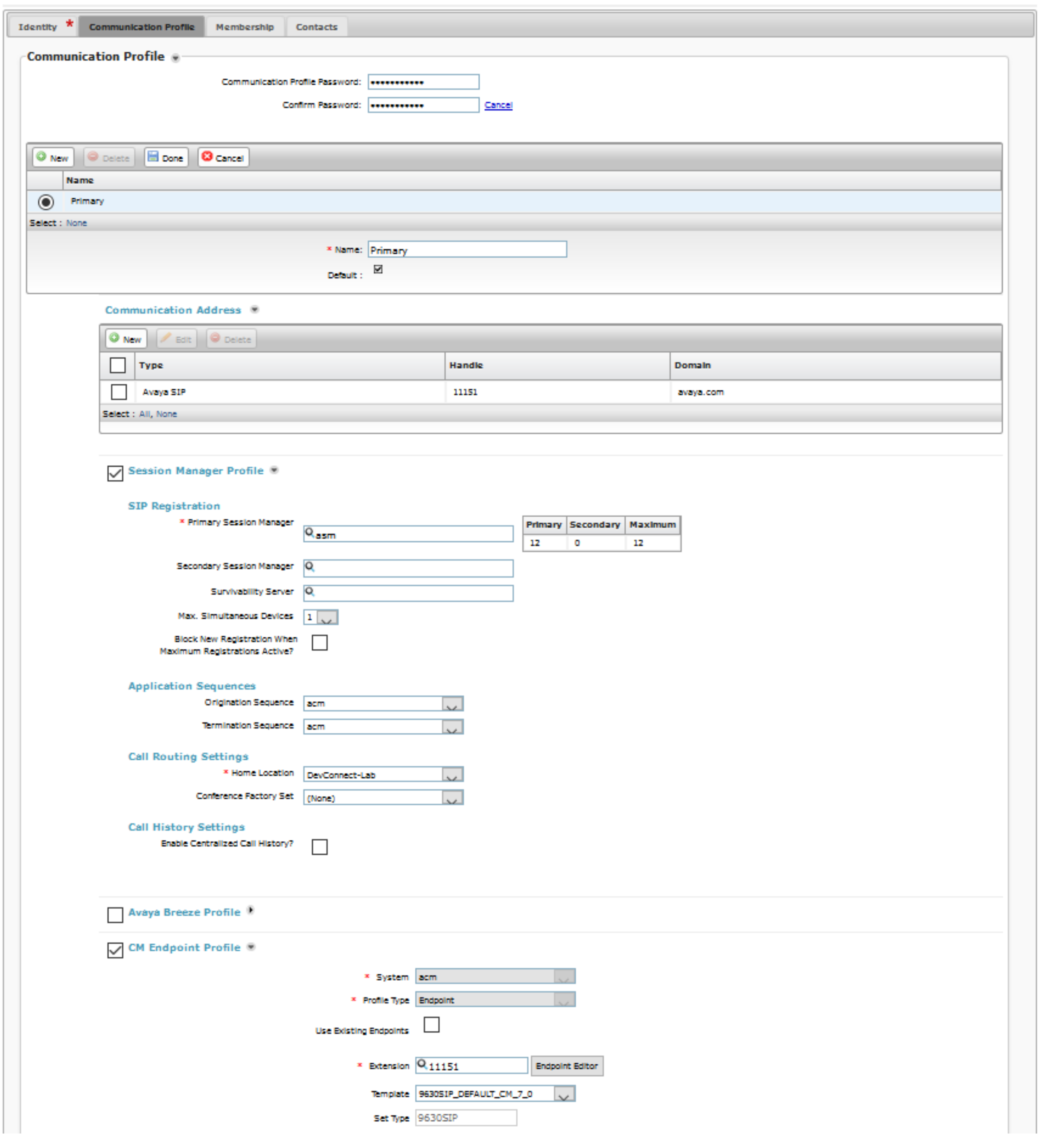
- Type in **Last Name** and **First Name**
- In **Login Name** field type in <extension>@<domain>. <Extension> is an extension which will be configured on AudioCodes MP-11x to receive and make calls. <domain> is as configured in **Section 6.1**



Under **Communication Profile** tab:

- Under **Communication Profile,** type in desired **Communication Profile Password** and **Confirm Password**
- Under **Communication Address**, click on **New** (now shown)
    - Type in <extension> in the text field, select domain configured in **Section 6.1** for **Fully Qualified Address**. <Extension> is the same extension configured for login name under Identity tab. Click on **Add**. Please note that AudioCodes MP-11x will use this information has login name to register to Session Manager
- Check the **Session Manager Profile** box:
    - Set **Primary Session Manager** to Session Manager. i.e. acm
    - Set **Origination Application Sequence** and **Termination Application Sequence** to Communication Manager entity. Please note that configuration for Application Sequence is not shown in this document. Please refer to document [2] in reference section of this document for further details.
    - Set **Home Location**
- Check the **CM Endpoint Profile** box:
    - Set **System** to Communication Manager entity
    - Set **Profile Type** to **Endpoint**
    - Type in extension number used in this section for **Extension** field
    - Set **Template** to **9630SIP_ DEFAULT_CM_7_0**
    - Set **Security Code** to a desired value. Please note that AudioCodes MP-11x will use this security code as password to register to Session Manager

Click **Commit** to save changes.


Identity
Communication Profile
Membership
Contacts
Communication Profile
Communication Profile Password:
Confirm Password:
Cancel
New
Delete
Done
Cancel
Name
Primary
Select : None
* Name:
Primary
Default :
Communication Address
New
Edit
Delete
Type
Handle
Domain
Avaya SIP
11151
avaya.com
Select : All, None
Session Manager Profile
SIP Registration
* Primary Session Manager
asm
Primary
Secondary
Maximum
12
0
12
Secondary Session Manager
Survivability Server
Max. Simultaneous Devices
1
Block New Registration When Maximum Registrations Active?
Application Sequences
Origination Sequence
acm
Termination Sequence
acm
Call Routing Settings
* Home Location
DevConnect-Lab
Conference Factory Set
(None)
Call History Settings
Enable Centralized Call History?
Avaya Breeze Profile
CM Endpoint Profile
* System
acm
* Profile Type
Endpoint
Use Existing Endpoints
* Extension
11151
Endpoint Editor
Template
9630SIP_DEFAULT_CM_7_0
Set Type
9630SIP

7. Configure AudioCodes MediaPack 11x

Administration for AudioCodes MP-11x series is done via administrative console. Type in http://<ip-address> URL in a web browser, where <ip-address> is the IP Address of AudioCodes MP-11x.

Note: It is assumed that AudioCodes MP-11x has been assigned an IP address. If AudioCodes MP-11x is using the factory defaults, change the computer IP address to 10.1.10.1 with a subnet of 255.255.0.0 so that it can communicate with the device using its factory default IP address of 10.1.10.10. For further details, please see document [5] in additional references section of this document.

Note: Configuration mentioned in the section is performed for AudioCodes MP-118. AudioCodes MP-11x series devices' administrative console is similar to the one that is configured in this section.

Log on to administrative console using appropriate credentials.

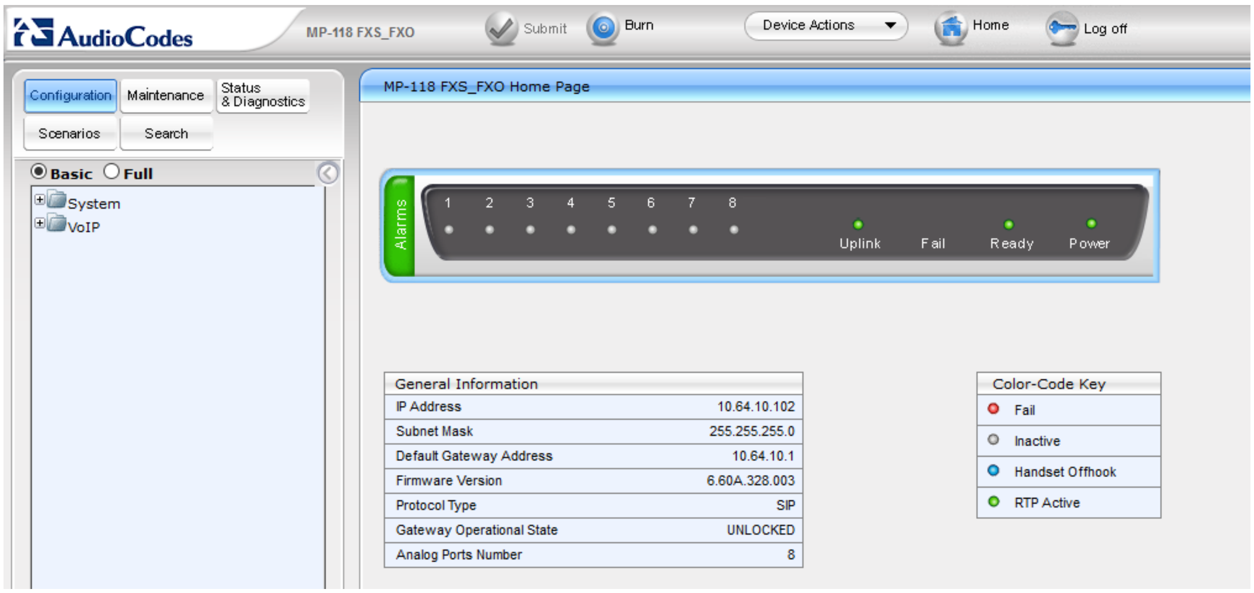
7.1. Verify/Upgrade Firmware Version

Once logged in, the firmware version can be found on the Home page under **General Information** box. The firmware version should be **6.60A**or higher.

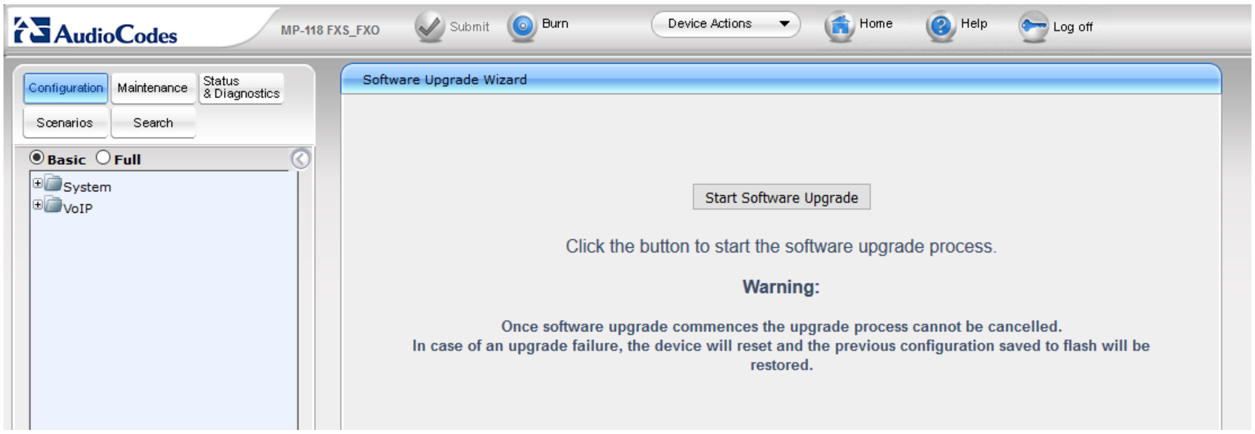
Please note that during the compliance testing, the version of AudioCodes MP-11x used, was **6.60A.328.003**.

If the version is different, contact AudioCodes support and get the correct version firmware. Once it has been obtained:

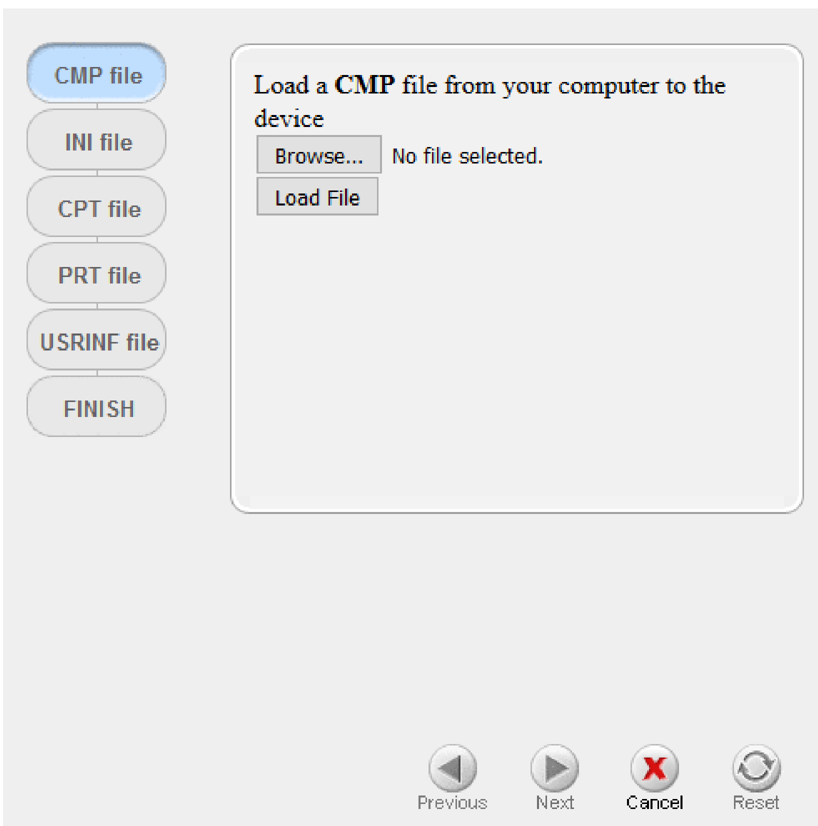
- Click on the drop down menu as shown and select **Software Upgrade Wizard**



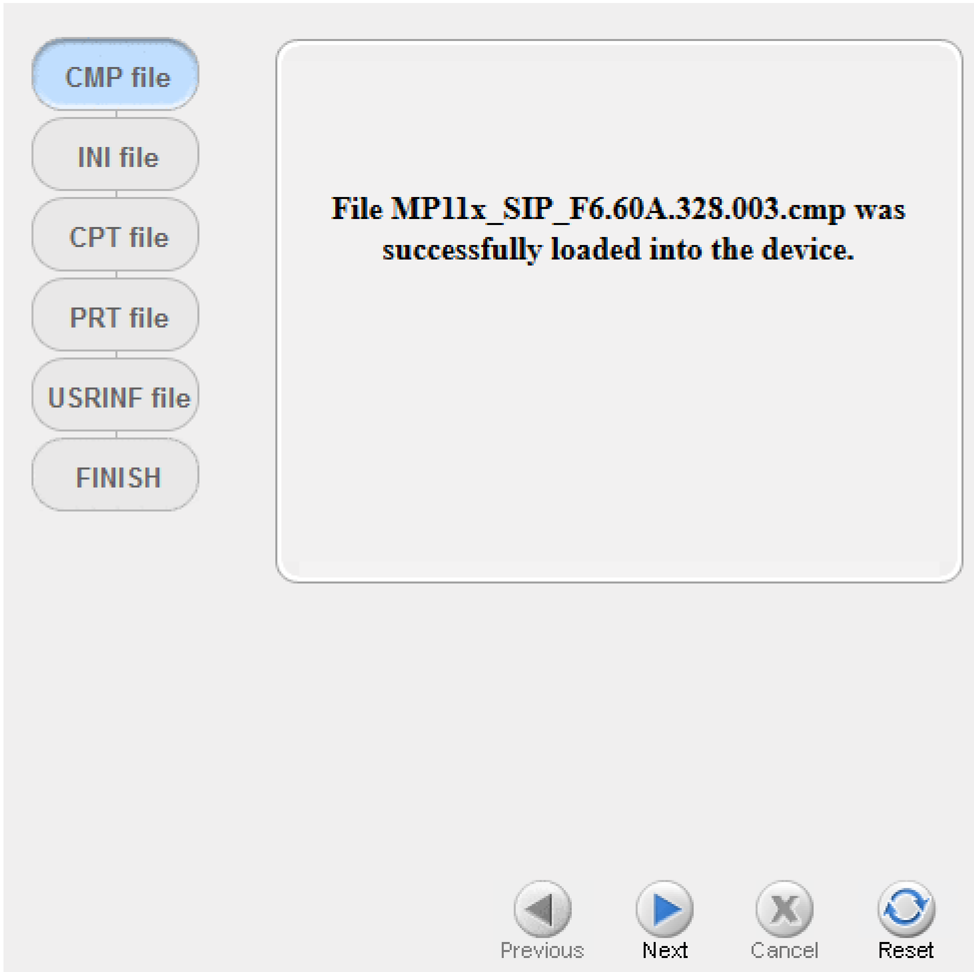
- Click on **Start Software Upgrade**



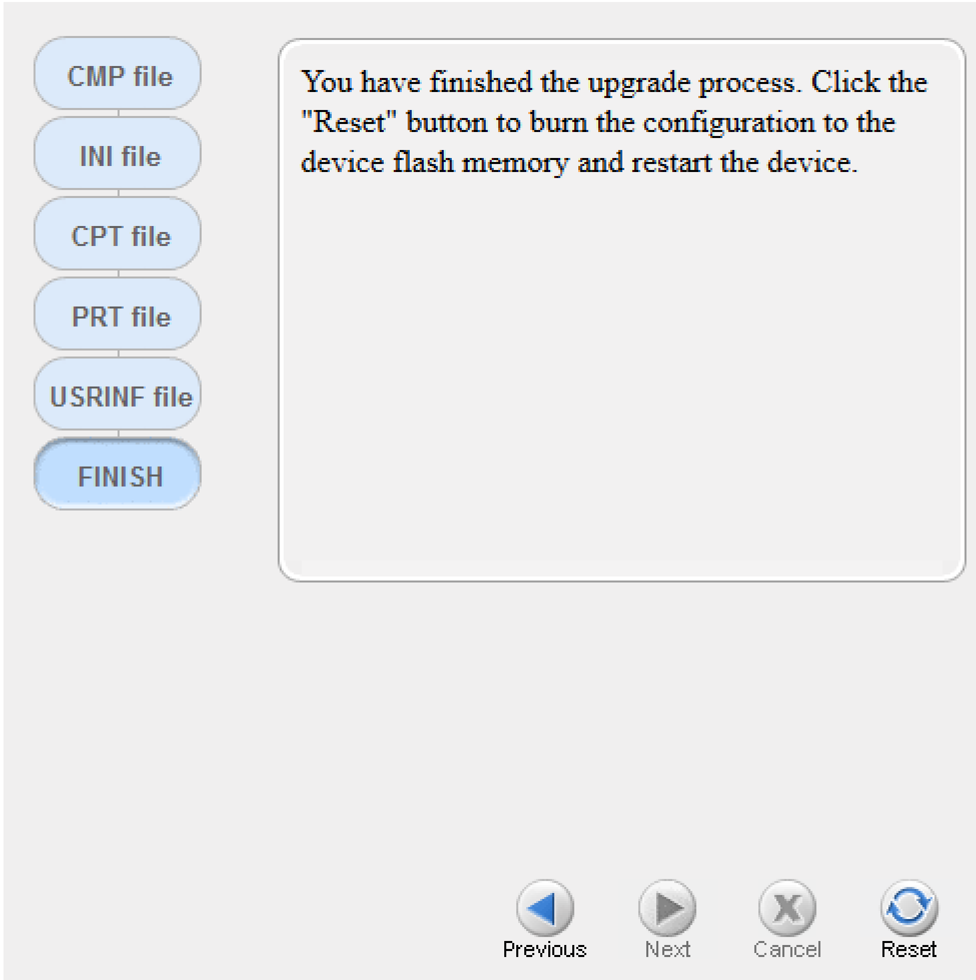
- A pop-up window will open, click on **CMP File**. Select **Browse** and locate the firmware (not shown)
- Click on **Load File**



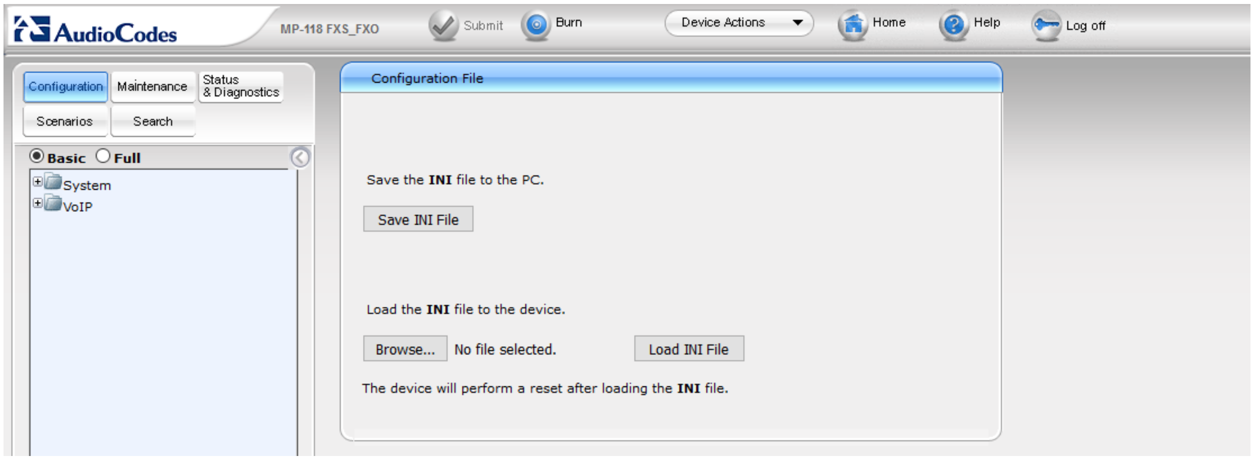
- Once the file is loaded on the device, following text will be displayed



- Click **Reset** to upgrade the device.



- Verify the version once the upgrade process is complete as mentioned earlier in this section
- To ensure that the configuration is default, in a case where the box was previously used, upload an **ini** file that is empty:
- Open Notepad on a Windows machine, and save as **empty.ini**
- From AudioCodes MP-11x console, click on the drop down menu **Device Actions** in the top center of the screen, and select **Load Configuration File** (not shown)
- Click on **Choose File** and navigate to the location of recently created **empty.ini** and select it.
- Click on **Send INI File**
- Click **OK** to confirm (not shown)

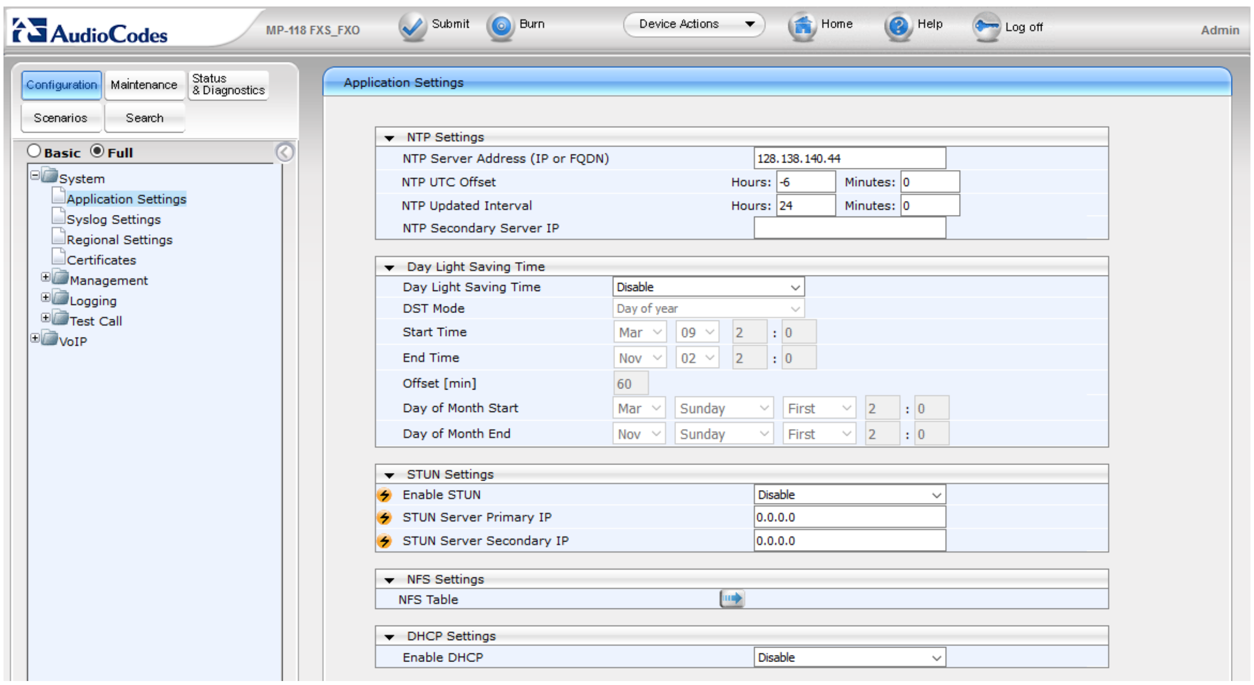


7.2. Administer Application Settings

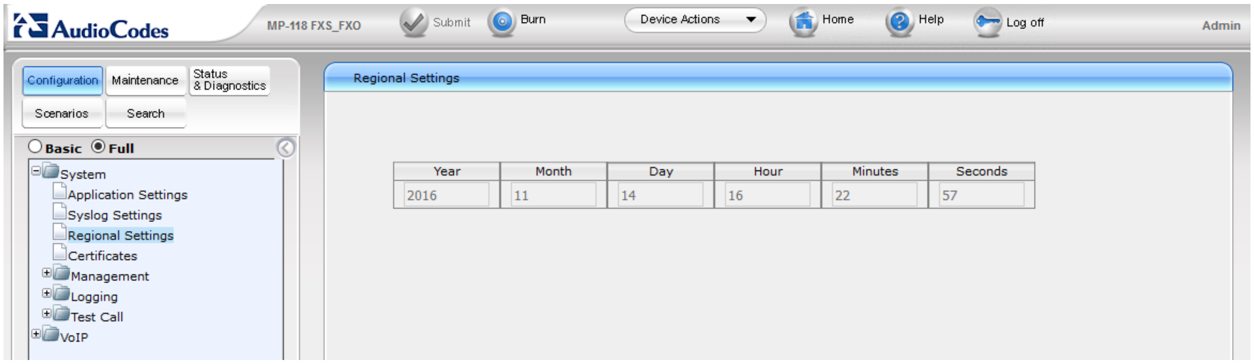
All administration is done via the left pane on administrative console.

- Click on **Full** as shown on the screen shot
- Expand **System** folder and click on **Application Settings**
- Fill in **NTP Server IP Address**
- Fill in **NTP UTC Offset** for the local time zone
- Under **DHCP Setting**, ensure that **Enable DHCP** is set to **Disable** (not shown)

Note: For compliance testing a local NTP server was provided and an offset of -6 was used
Click on **Submit** to save changes.



- Click on **Regional Setting** on the left pane. It should now display the correct local time

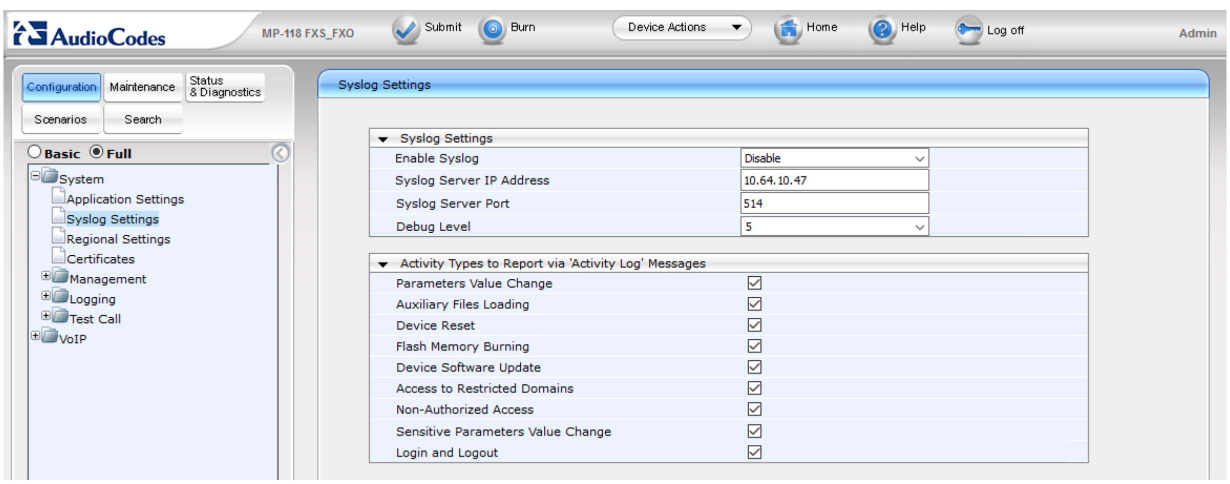


7.3. Administer Syslog Settings

If Syslog needs to be enabled, navigate to **System → Syslog Settings**

- Set **Enable Syslog** to **Enable**
- For **Syslog Server IP** Address, type in the IP address of a workstation that is running a syslog application, e.g. **ACSyslog**
- Set **Debug Level** to **5**
- Under **Activity Types to Report via 'Activity Log' Messages**, check all boxes

Click **Submit** to save changes.
Reset the device to save changes to flash memory of AudioCodes MP-11x.



7.4. Administer Certificates

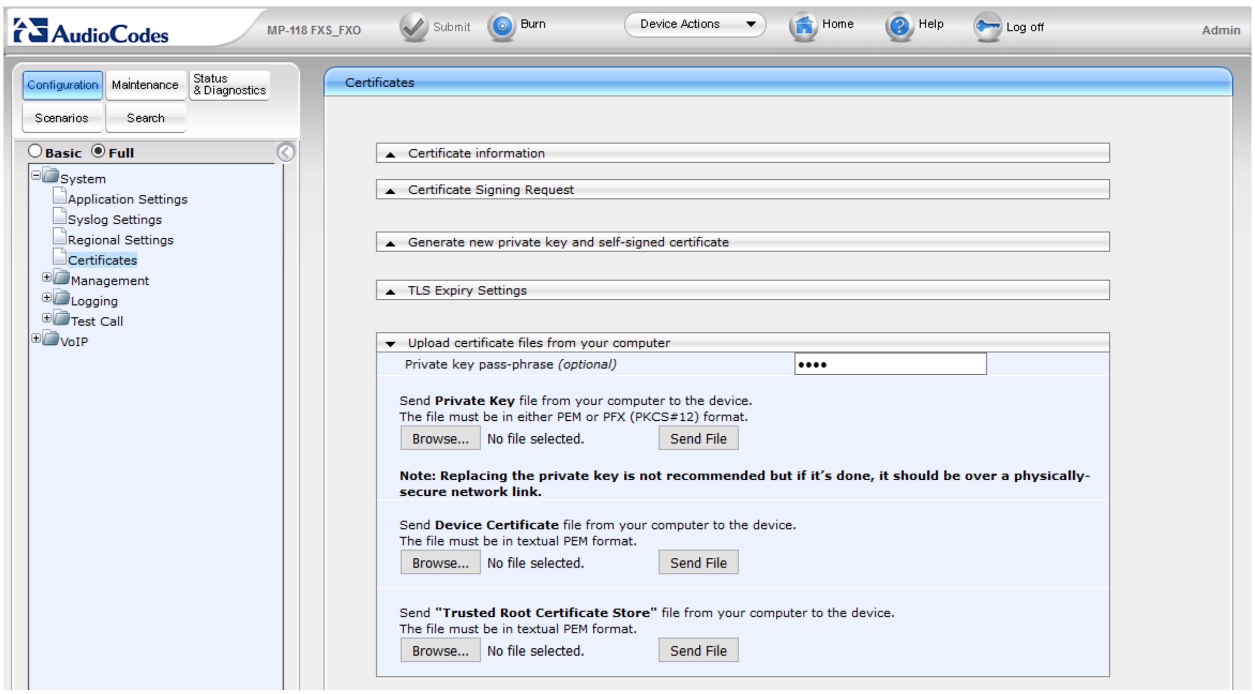
In order for TLS/SRTP to work, three certificates are needed

1. Private Key Certificate
2. Trusted Root Certificate
3. Server Certificate

Please note that without these certificates, TLS/SRTP will not work. Certificates were generated using System Manager as the Certificate Authority.

Once certificates have been obtained, configure as follows:

- Navigate to **System → Certificates** on the left pane
- For each certificate, click on **Upload certificate files from your computer, next click Browse** and locate the file. Click on **Send File**



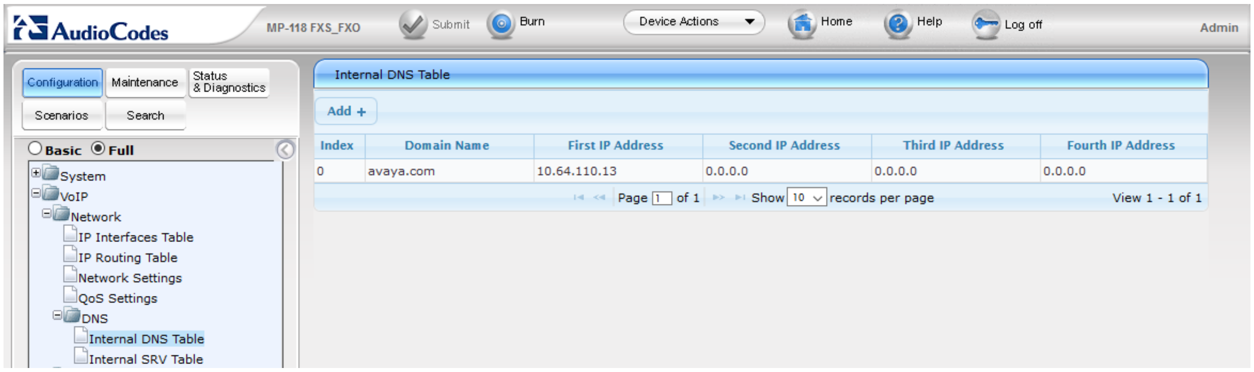
7.5. Administer DNS Setting

DNS entries can be entered manually by navigating to **VoIP → Network → DNS → Internal DNS Table**

- Fill in the information for **Domain** and **First IP Address i.e. SIP Domain and IP Address of Session Manager.**

Click **Submit** to save changes.

Note: It is good practice to click **Burn** on top of the page, after each change is made, to burn changes into flash memory of AudioCodes MP-11x.

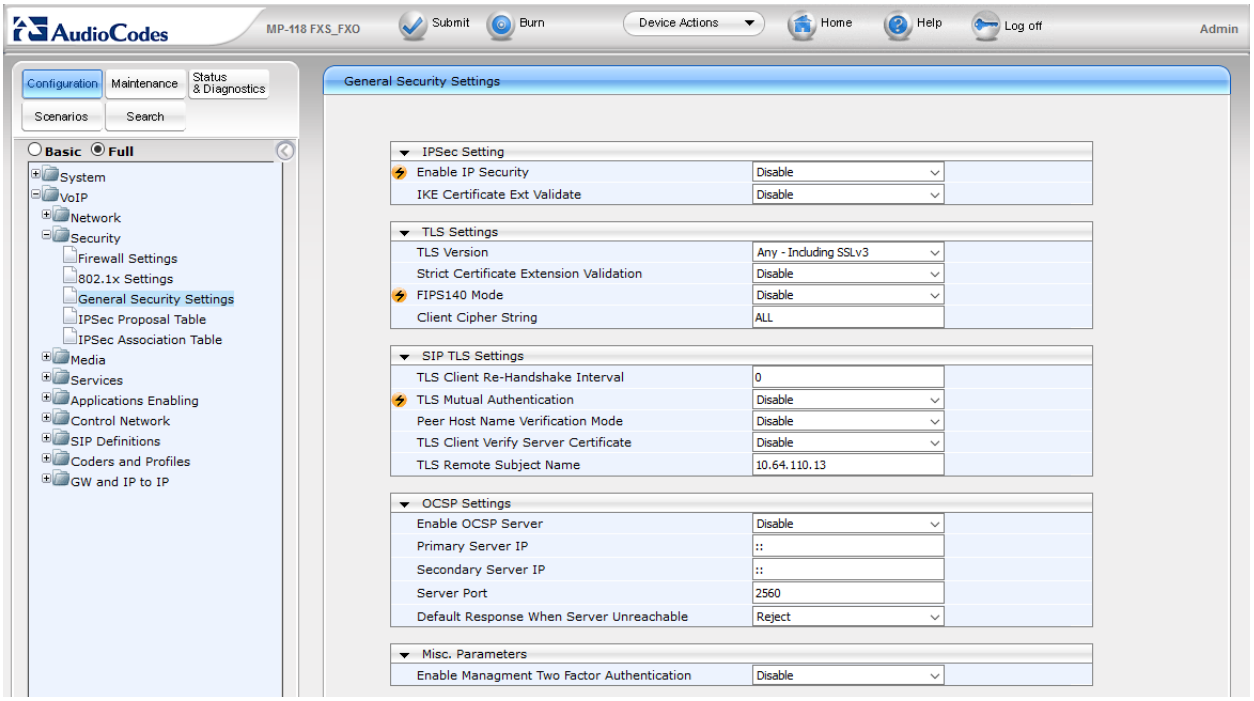


7.6. Administer General Security

On the left pane, navigate to **VoIP → Security → General Security Settings**

- Set **TLS Version** to **Any – Including SSLv3**
- Set **TLS Remote Subject Name** to IP Address of Session Manager

Click **Submit** to save changes.

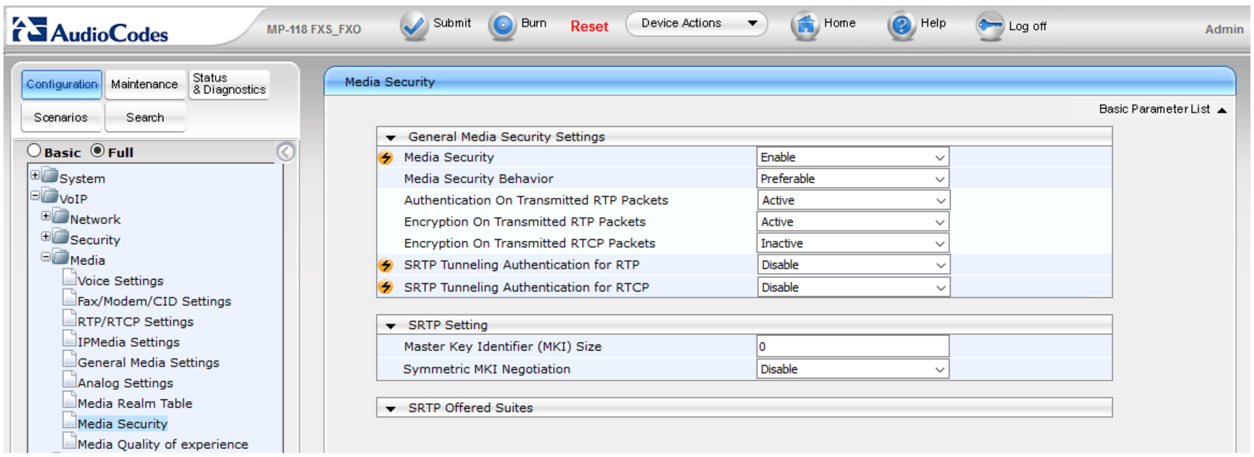


7.7. Administer Media Security

On the left pane, navigate to **VoIP → Media → Media Security**

- Set **Media Security** to **Enable**
- Set **Media Security Behavior** to **Preferable**
- Set **Encryption on Transmitted RTCP Packets** to **Inactive**

Click **Submit** to save changes.



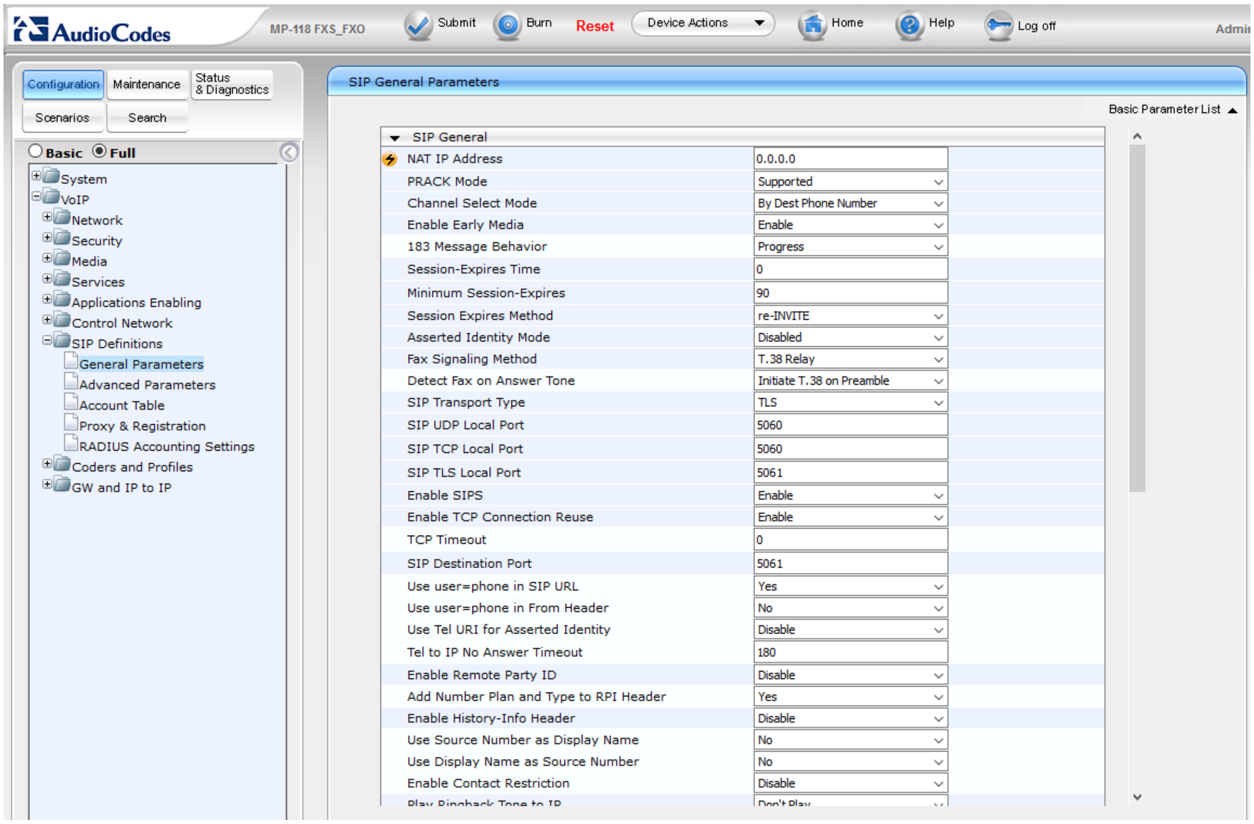
Note: This change requires a reset of AudioCodes MP-11x. Please burn the changes and reset the device before performing any further configuration.

7.8. Administer General Parameters

On the left pane, navigate to **VoIP → SIP Definitions → General Parameters**

- Set **Enable Early Media** to **Enable**
- Set **Fax Signaling Method** to **T.38 Relay**
- Set **SIP Transport Type** to **TLS**
- Set **Enable SIPS** to **Enable**
- Set **SIP Destination Port** to **5061**

Click **Submit** to save changes.

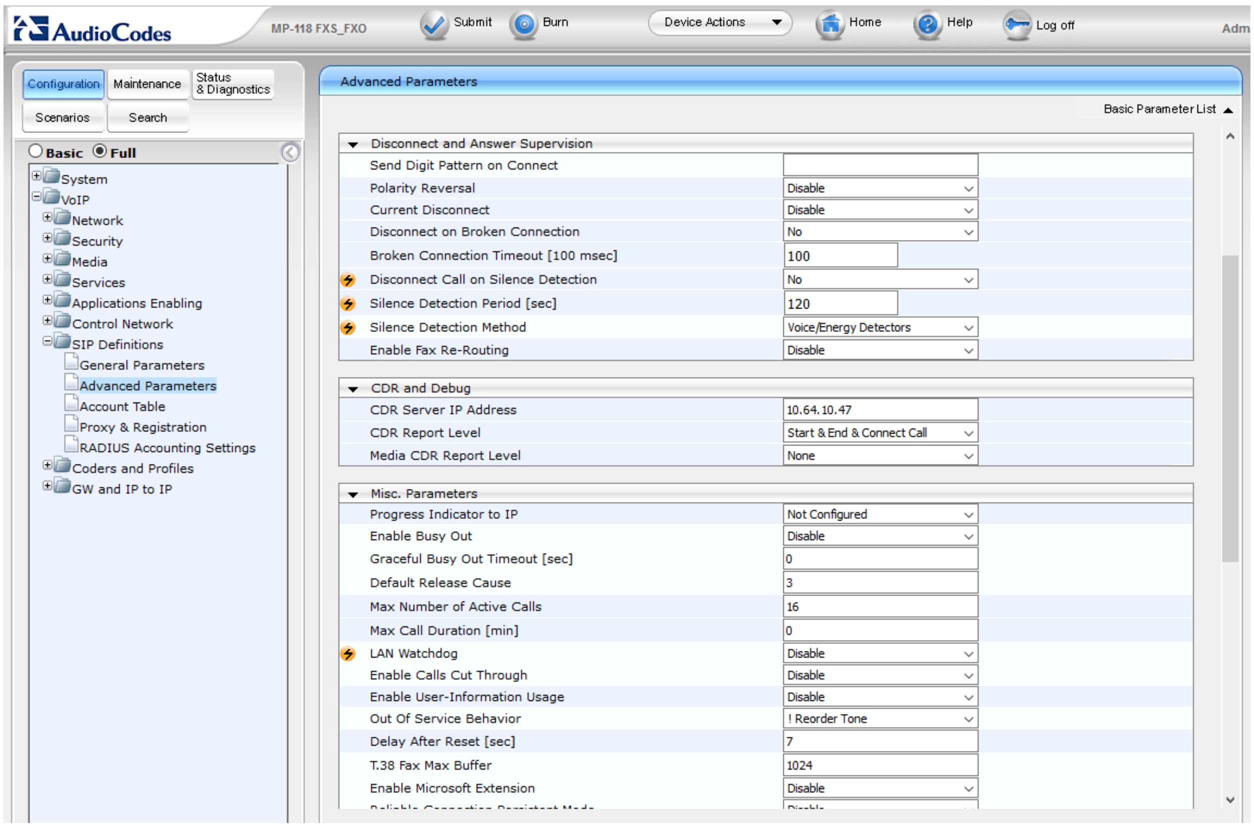


7.9. Administer Advanced Parameter

On the left pane, navigate to **VoIP → SIP Definitions → Advanced Parameter**

- Set **Disconnect on Broken Connection** to **No**
- Set **CDR Server IP Address** to the same ip address configured for syslog ip address
- Set **CDR Report Level** to **Start & End & Connect Call**

Click **Submit** to save changes.

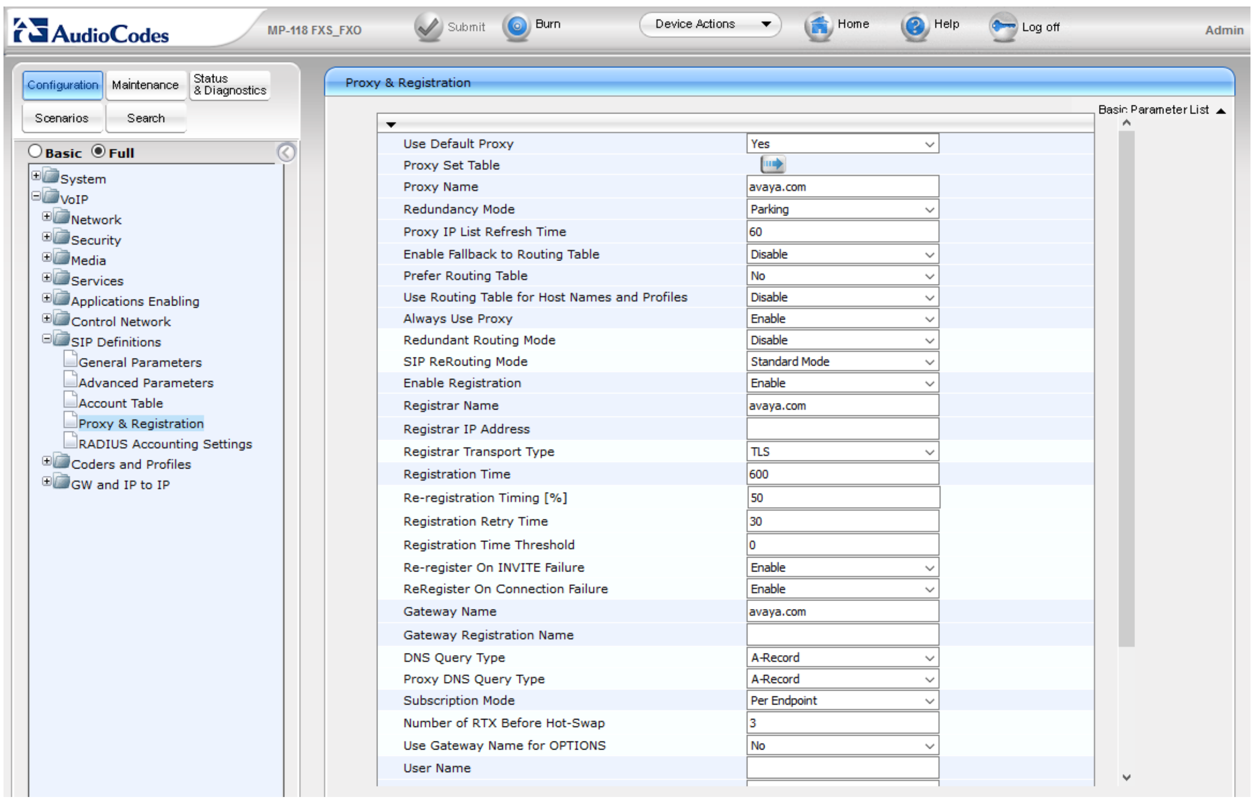


7.10. Administer Proxy and Registration

On the left name, navigate to **VoIP → SIP Definitions → Proxy & Registration**

- Set **Use Default Proxy** to **Yes**
- Set **Proxy Name** to **avaya.com**
- Set **Always Use Proxy** to **Enable**
- Set **Redundant Routing Mode** to **Disable**
- Set **Enable Registration** to **Enable**
- Set **Registrar Name** to the domain name used for registration, e.g. **avaya.com**
- Set **Registrar Transport Type** to **TLS**
- Fill in **Registration Time** to a desired value, in seconds
- Set **Re-register On INVITE Failure** to **Enable**
- Set **ReRegister On Connection Failure** to **Enable**
- Fill in **Gateway Name**, e.g. **avaya.com**

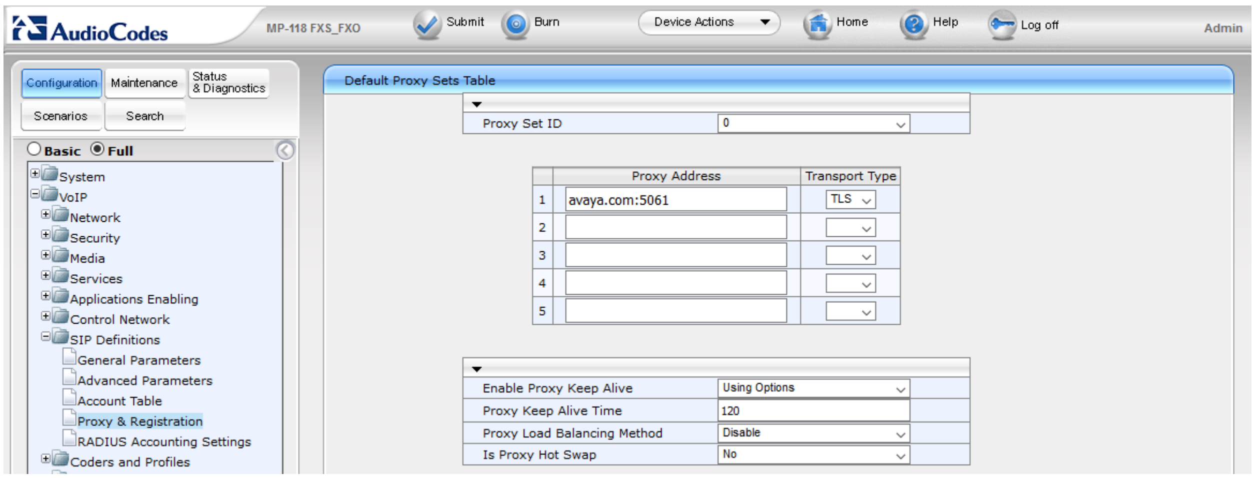
Click **Submit** to save changes. Screen capture on next page.



On the **Proxy & Registration** page, shown in **Section 7.10** click on the Arrow icon, , next to **Proxy Set Table**

- Type in the **Proxy Address,** e.g. avaya.com:5061
- Set **Transport Type** to **TLS**
- Set **Enable Proxy Keep Alive** to **Using Options**
- Set **Proxy Keep Alive Time** to a desired value, in seconds.

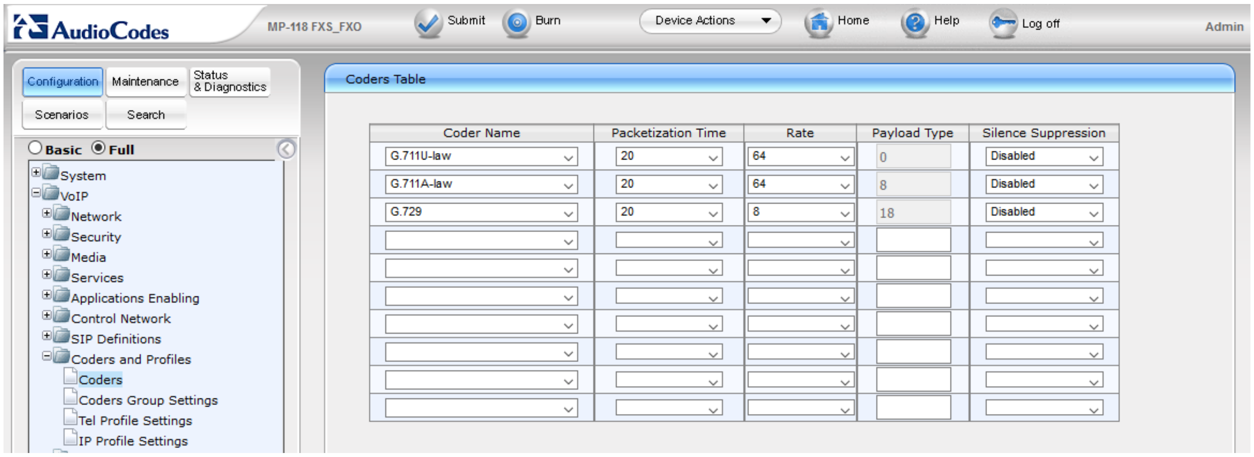
Click **Submit** to save changes.



7.11. Administer Coders

On the left pane, navigate to **VoIP → Coders and Profiles → Coders**

- Set coders as shown in the screen capture below



7.12. Administer End Point Phone Number

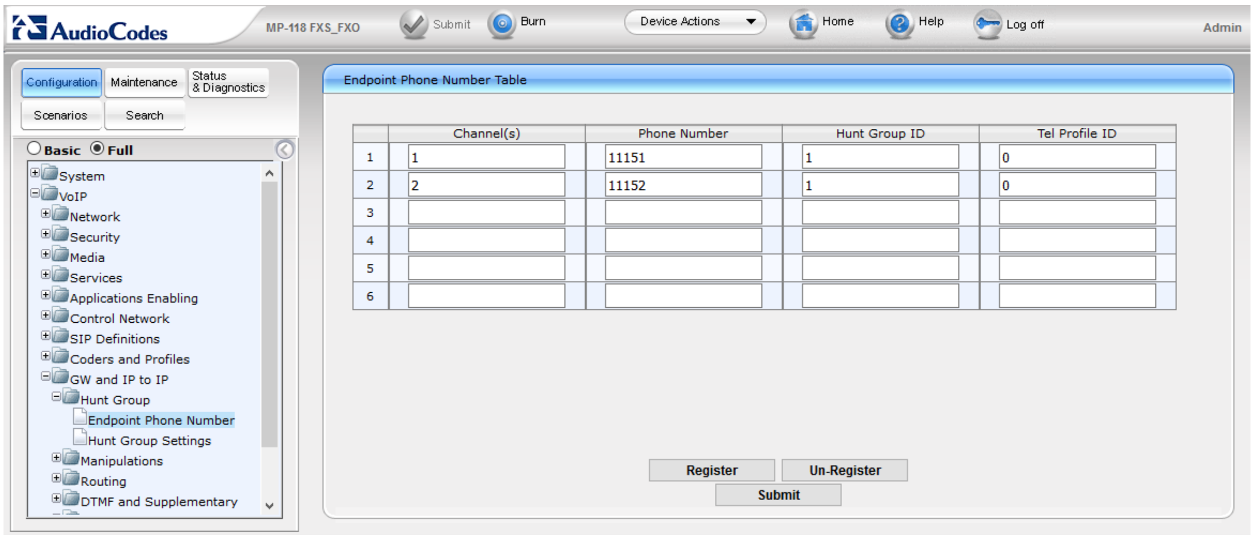
On the left pane, navigate to **VoIP → GW and IP to IP → Hunt Group → Endpoint Phone Number**, for each line

- Set **Channel** to a channel number, e.g. 1
- Set **Phone Number** to the extension configured is Session Manager, e.g. **11151**
- Set **Hunt Group ID** to a hunt group value (configured in next section), e.g. **1**
- Set **Tel Profile ID** to 0 for global

Click **Submit** to save changes.

Note: All phone numbers entered in this screen must be configured as users in Session Manager

Note: Channel 1 and 2 are FXS lines, Channel 3 is FXO line. When SRTP is configured, AudioCodes MP-11x DSP capacity is reduced by 25%. In this case, there are 8 analog ports on AudioCodes MP-118, but since SRTP is enabled, only 6 ports can be used.
Click on **Register** at the bottom of the screen to register with Session Manager.

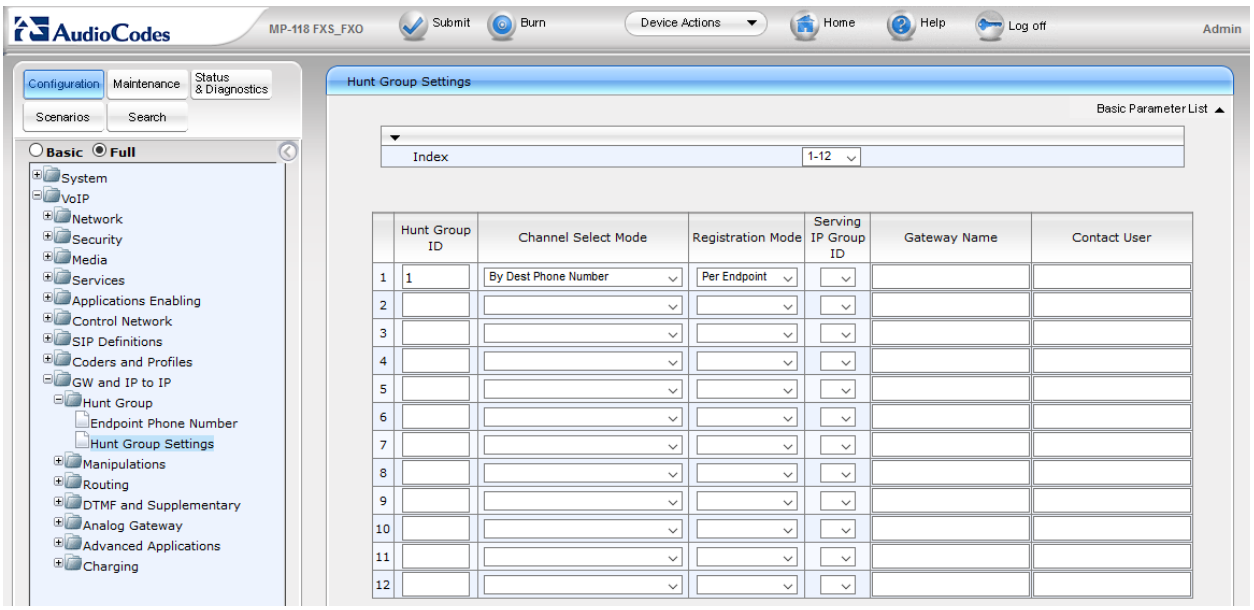


7.13. Administer Hunt Group Settings

On the left pane, navigate to **VoIP → GW and IP to IP → Hunt Group → Hunt Group Settings**

- Set **Hunt Group ID** to the ID used in previous step, i.e. **1**
- Set **Channel Select Mode** to **By Dest Phone Number** for FXS ports. If configuring FXO port, set it to **Cyclic Ascending**
- Set **Registration Mode** to **Per Endpoint**

Click **Submit** to save changes.

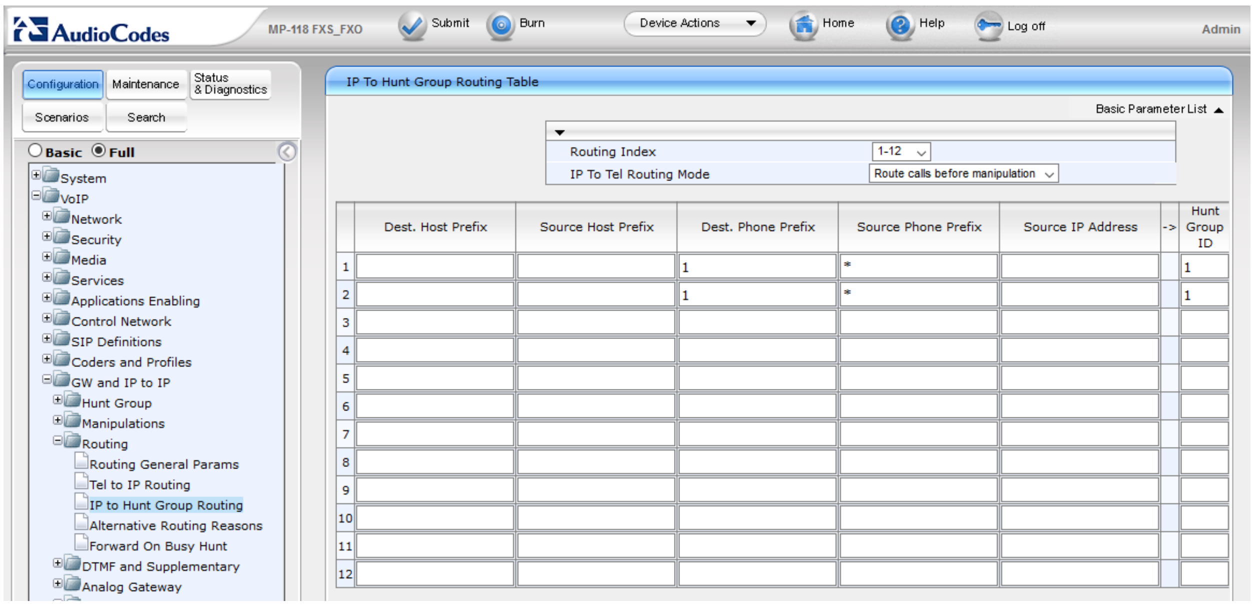


7.14. Administer IP to Trunk Group Routing

On the left pane, navigate to **VoIP → GW and IP to IP → Routing → IP to Hunt Group Routing**, for each extension

- Set **Source Phone Prefix** to *
- Set **Dest. Phone Prefix** to the prefix of extensions, e.g. **1**
- Set **Hunt Group ID** to ID configured in previous step, i.e. **1**
- Set **IP Profile ID** to **0**

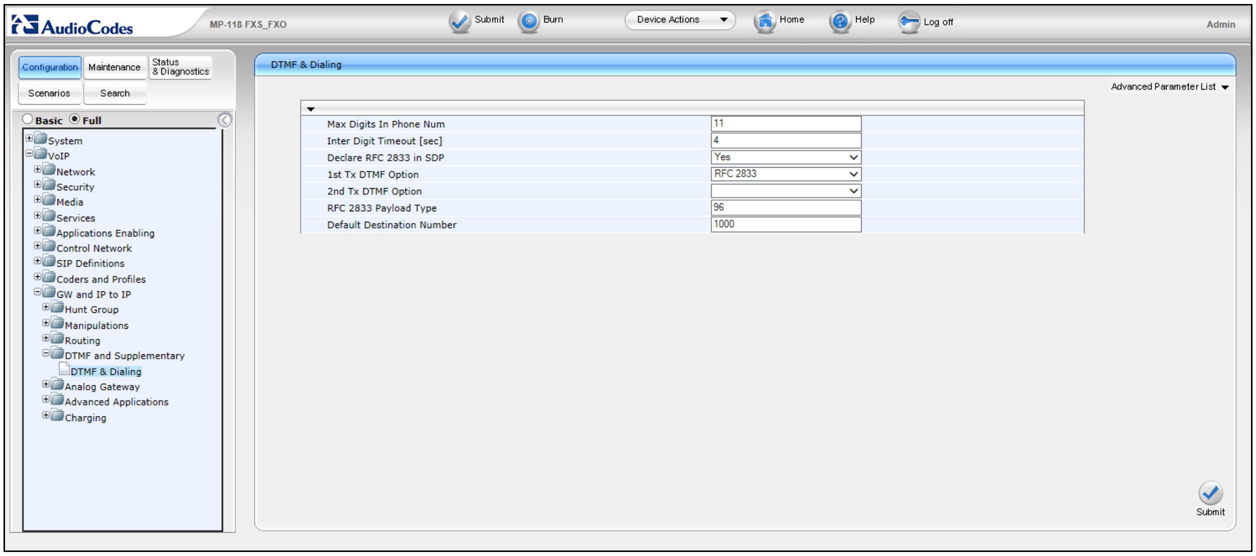
Click **Submit** to save changes



7.15. Administer DTMF and Dialing

On the left pane, navigate to **VoIP → GW and IP to IP → DTMF and Supplementary → DTMF & Dialing**

- Set **Max Digits In Phone Num** to **11**

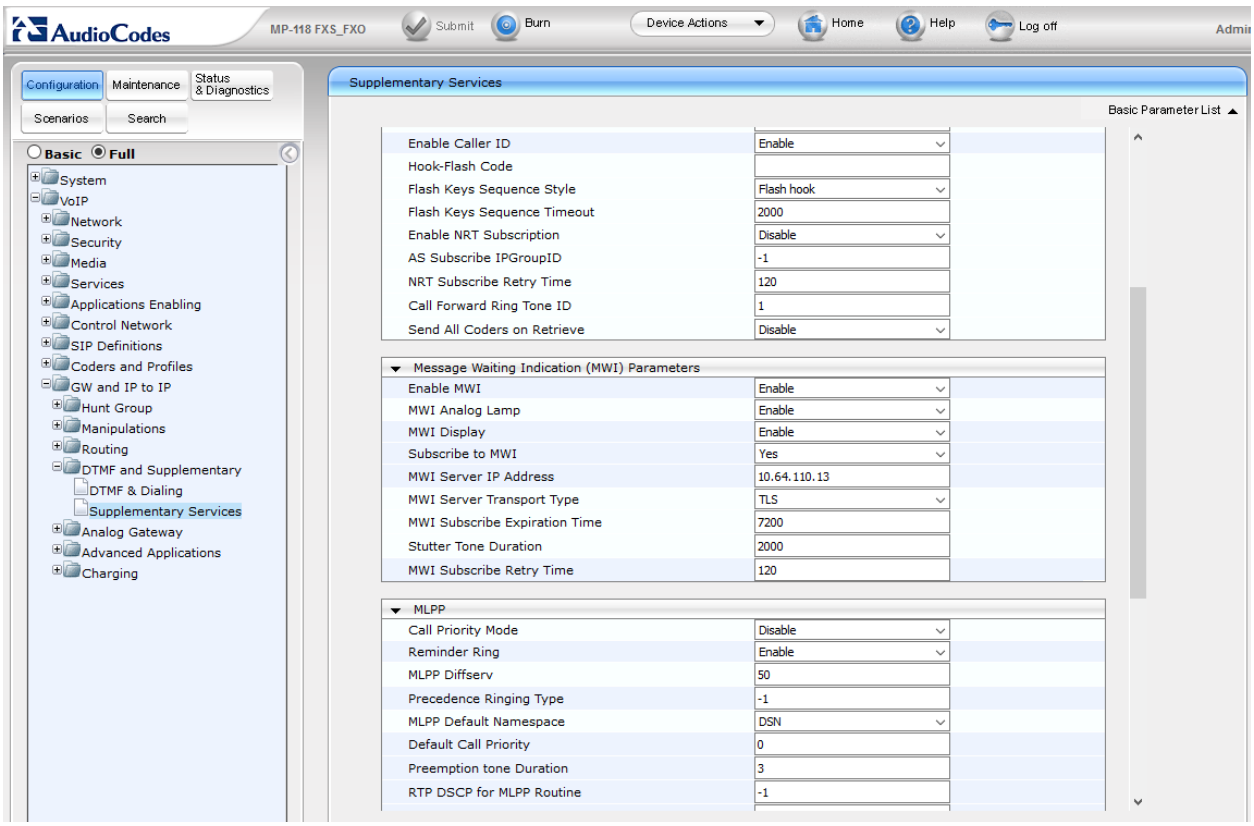


7.16. Administer Supplementary Services

On the left pane, navigate to **VoIP → GW and IP to IP → DTMF and Supplementary → Supplementary Services**

- Set **Enable Caller ID** to **Enable**
- Under **Message Waiting Indication (MWI) Parameters:**
  - Set **Enable MWI** to **Enable**
  - Set **MWI Analog Lamp** to **Enable**
  - Set **MWI Display** to **Enable**
  - Set **Subscribe to MWI** to **Yes**
  - For **MWI Server IP Address**, type in Session Manager's IP Address
  - Set **MWI Server Transport Type** to **TLS**

Click **Submit** to save changes

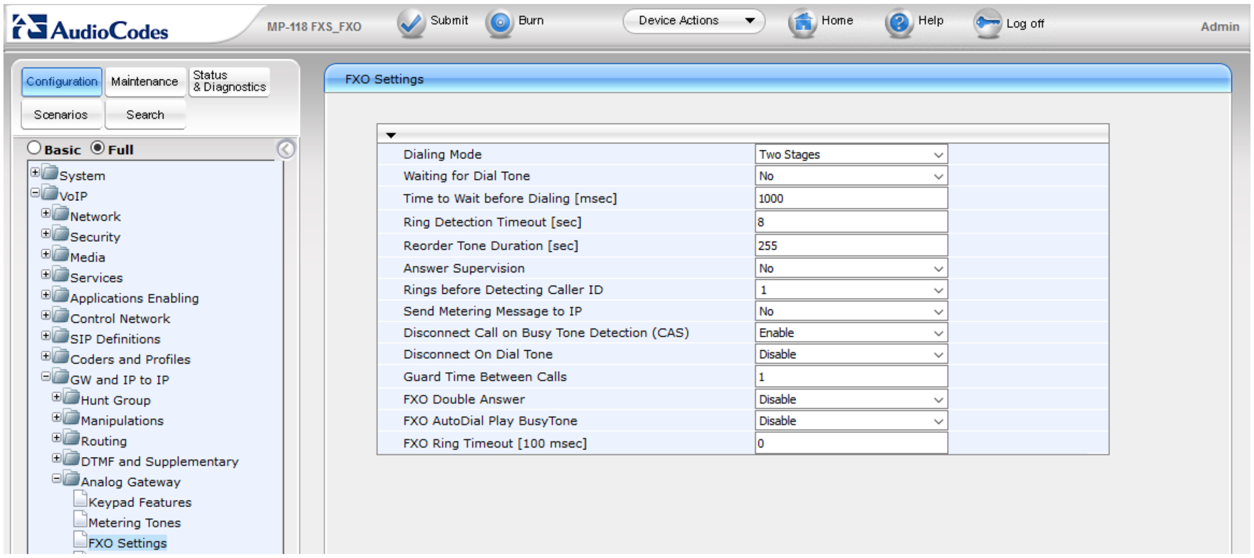


7.17. Administer FXO

On the left pane, navigate to **VoIP → GW and IP to IP → Analog Gateway → FXO Settings**

- Set **Dialing Mode** to **Two Stages**

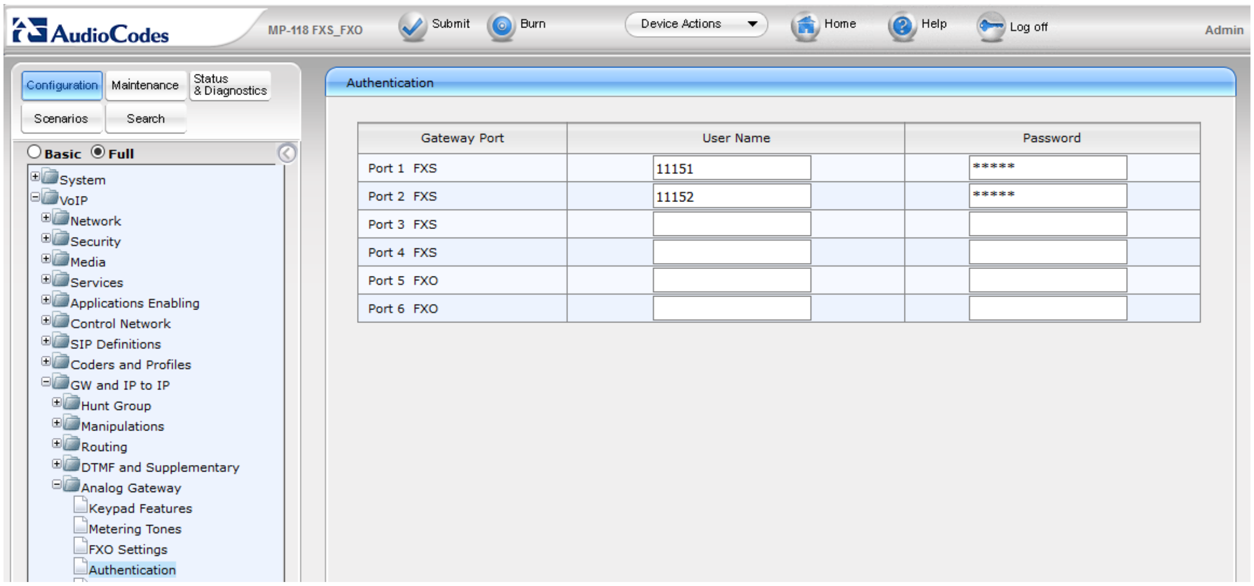
Click **Submit** to save changes. Also, click **Burn** to save changes to the flash memory of AudioCodes MP-11x.



7.18. Administer Authentication for FXS Lines

On the left pane, navigate to **VoIP → GW and IP to IP → Analog Gateway → Authentication**

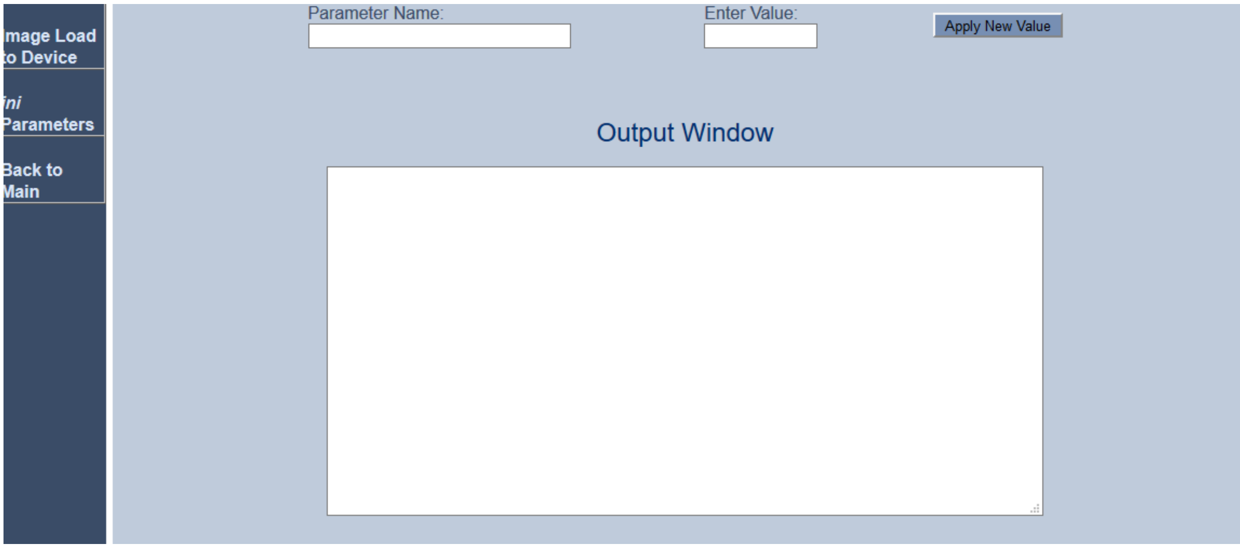
- Add the **User Name** and **Password** for the users configured on Session Manager**.**



Click **Submit** to save changes. Also, click **Burn** to save changes to the flash memory of AudioCodes MP-11x.

7.19. Administer other parameters

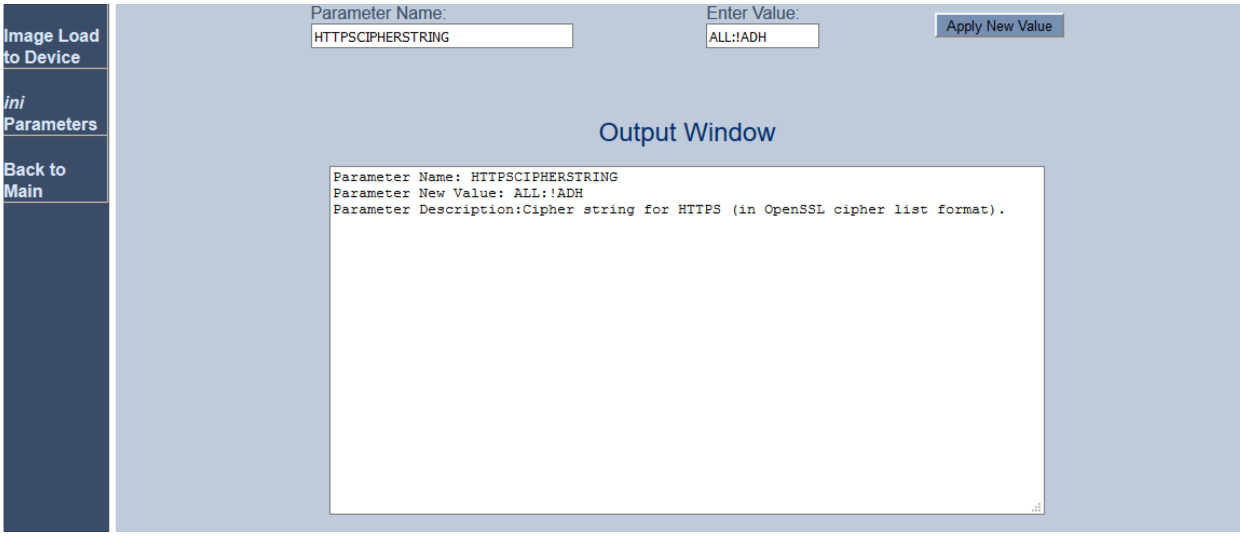
Type in http://<ip-address>/AdminPage URL in a web browser, where <ip-address> in the ip address of AudioCodes MP-11x, click on **ini Parameters** on the left pane



- In the table below type in each parameter and associated value, click **Apply New Value**
- Verify the output shows updated value

Parameter Name	Value
HTTPSCIPHERSTRING	ALL:!ADH
RTCPENCRYPTIONDISABLERX	1

The screen capture below shows output after applying a new value of **HTTPSCIPHERSTRING**.



8. Verification Steps

8.1. Avaya Aura® Communication Manager and Avaya Aura® Session Manager

- Verify SIP trunks to Session Manager are in service via SAT, using **status trunk *n***, where n is the number of the trunk configured in **Section 6**. Service State column should show **in-service/idle.**

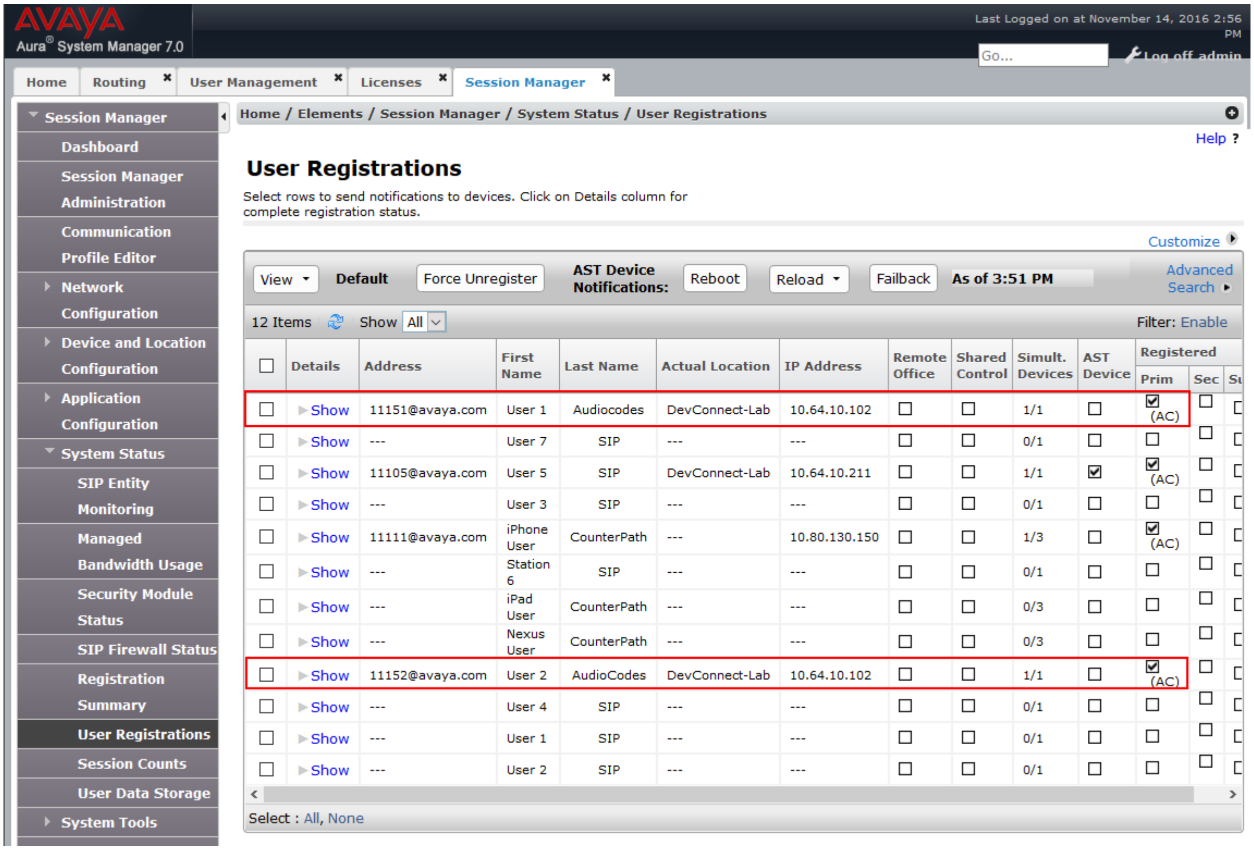
```
status trunk 1

                             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
```

- Verify registration from AudioCodes MP-11x to Session Manager via System Manager console, http://<ip-address/
- Navigate to **Home → Session Manager → System Status → User Registration**



9. Conclusion

These Application Notes describe the configuration steps required for AudioCodes MP-11x to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature and serviceability test cases completed and pass with observations/exceptions noted in **Section 2.2**

10. Additional References

This section references the product documentation relevant for these Application Notes.

[1] Administering Avaya Aura® Communication Manager, Release 7.0

[2] Administering Avaya Aura® Session Manager, Release 7.0

[3] AudioCodes Transport Layer Security Note, Document LTRT-31600, January 2012

[4] MP-11x and MP-124 SIP User's Manual, Version 6.6, Document LTRT-65422, January 2014

[5] MP-11x and MP-124 SIP Installation Manual, Version 6.6, Document LTRT-59820, December 2014

[6] SIP CPE Release Notes, Version 6.6, Document LTRT-26916

A. Appendix

AudioCodes MP-118 .ini file generated after following the instruction is as follows: Please use it only for reference purposes.

Note: Please note that the password for registration will need to be changed if this ini file is loaded on an AudioCodes MP-11x device.

```
;**************
;** Ini File **
;**************

;Board: MP-118 FXS_FXO
;Board Type: 56
;Serial Number: 547031
;Slot Number: 1
;Software Version: 6.60A.328.003
;DSP Software Version: 204IM3=> 660.14
;Board IP Address: 10.64.10.102
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.10.1
;Ram size: 32M   Flash size: 8M
;Num of DSP Cores: 2  Num DSP Channels: 8
;Profile: NONE
;License Key limits aren't active full features capabilities are available !;
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.64.10.47
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = -21600
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc',
'll'
;VpFileLastUpdateTime is hidden but has non-default value
DayLightSavingTimeStart = '03:09:02:00'
DayLightSavingTimeEnd = '11:02:02:00'
TLSClientCipherString = 'ALL'
TLSPkeySize = 2048
NTPServerIP = '128.138.140.44'
LDAPSEARCHDNSINPARALLEL = 0

[BSP Params]

PCMLawSelect = 3

[Analog Params]


[ControlProtocols Params]
```

```
AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
DIGITMAPPING = '1xxxx|91xxxxxxxxxx'

[Voice Engine Params]

CallProgressTonesFilename = 'usa_tones_13.dat'
RTCPEncryptionDisableTx = 1

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'ALL:!ADH'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value

[SIP Params]

ENABLECALLERID = 1
MAXDIGITS = 19
REGISTRATIONTIME = 600
ISPROXYUSED = 1
ISREGISTERNEEDED = 1
CDRREPORTLEVEL = 4
;ENABLECDR is hidden but has non-default value
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLEEARLYMEDIA = 1
PROXYNAME = 'avaya.com'
SIPGATEWAYNAME = 'avaya.com'
ALWAYSSENDTOPROXY = 1
;SHOULDREGISTER is hidden but has non-default value
DISCONNECTONBROKENCONNECTION = 0
CDRSYSLOGSERVERIP = 10.64.10.47
ENABLEMWISUBSCRIPTION = 1
MWISERVERIP = '10.64.110.13'
;SHOULDSUBSCRIBE is hidden but has non-default value
MWIANALOGLAMP = 1
MWIDISPLAY = 1
ENABLEMWI = 1
ISFAXUSED = 1
SIPTRANSPORTTYPE = 1
REGISTRARNAME = 'avaya.com'
ENABLE3WAYCONFERENCE = 1
REGISTERONINVITEFAILURE = 1
REGISTRARTRANSPORTTYPE = 2
```

```
MWISERVERTRANSPORTTYPE = 1
TLSREMOTESUBJECTNAME = '10.64.50.31'
REREGISTERONCONNECTIONFAILURE = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'

[IPsec Params]


[SNMP Params]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
InterfaceTable 0 = 6, 10, 10.64.10.102, 24, 10.64.10.1, 1, "O+M+C",
75.75.75.75, 0.0.0.0;

[ \InterfaceTable ]


[ DspTemplates ]

;
;  *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]


[ TrunkGroup ]

FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId,
TrunkGroup_Module;
TrunkGroup 0 = 1, 255, 1, 1, "11151", 0, 255, 255;
TrunkGroup 1 = 1, 255, 2, 2, "11152", 0, 255, 255;

[ \TrunkGroup ]


[ PstnPrefix ]

; ** NOTE: Changes were made to active configuration.
; **       The data below is different from current values.
FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId,
PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId,
PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix,
PstnPrefix_SrcSRDID, PstnPrefix_TrunkId, PstnPrefix_CallSetupRulesSetId;
PstnPrefix 0 = "1", 1, "*", "", 0, -1, "", "", , -1, -1;
```

```
PstnPrefix 1 = "1", 1, "*", "", 0, -1, "", "", , -1, -1;

[ \PstnPrefix ]


[ Dns2Ip ]

FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress,
Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress;
Dns2Ip 0 = "avaya.com", 10.64.110.13, 0.0.0.0, 0.0.0.0, 0.0.0.0;

[ \Dns2Ip ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "avaya.com:5061", 2, 0;

[ \ProxyIp ]


[ TxDtmfOption ]

FORMAT TxDtmfOption_Index = TxDtmfOption_Type;
TxDtmfOption 0 = 4;

[ \TxDtmfOption ]


[ TrunkGroupSettings ]

FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,
TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode,
TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser,
TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType,
TrunkGroupSettings_TrunkGroupName;
TrunkGroupSettings 0 = 1, 0, 0, "", "", -1, 255, "";

[ \TrunkGroupSettings ]


[ Authentication ]

FORMAT Authentication_Index = Authentication_UserId,
Authentication_UserPassword, Authentication_Port, Authentication_PortType;
Authentication 0 = "11151", *, 1, "FXS";
Authentication 1 = "11152", *, 2, "FXS";

[ \Authentication ]


[ ProxySet ]
```

```
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput,
ProxySet_ProxyRedundancyMode, ProxySet_KeepAliveFailureResp;
ProxySet 0 = 1, 120, 0, 0, 0, 0, -1, "";

[ \ProxySet ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Ulaw64k", 20, 0, -1, 0;

[ \CodersGroup0 ]


[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

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.