Avaya Solution & Interoperability Test Lab

Application Notes for AudioCodes Mediant 1000 Gateway with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.1

Abstract

This Application Notes contain interoperability instructions for configuring AudioCodes Mediant 1000 Gateway with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Compliance testing was conducted to verify the interoperability.

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

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

©2019 Avaya Inc. All Rights Reserved.

Table of Contents

©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

AudioCodes Mediant 1000 (M1K) gateways provide voice technology to connect analog phones, fax machines and modems (FXS) or landlines (FXO) to IP based PBX systems. AudioCodes M1K was configured to communicate with Avaya Aura® Session Manager using SIP (Users).

These Application Notes present a sample configuration for an enterprise network consisting of Session Manager and Communication Manager, integrated with an AudioCodes M1K Gateway using FXS (SIP) and providing simulated PSTN (FXO).

2. General Test Approach and Test Results

Interoperability compliance testing focused on verifying various inbound and outbound call flows between AudioCodes M1K, 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and AudioCodes M1K made use of TLS/SRTP for Session Manager connectivity.

2.1. Interoperability Compliance Testing

Analog lines on AudioCodes M1K were configured as SIP users on Session Manager. Each configured analog line user registered with Session Manager. SIP TLS and SRTP were utilized during this test effort. Following features and functionalities were covered during compliance testing:

- Incoming calls to AudioCodes M1K
- Outgoing calls from AudioCodes M1K
- Voice codecs G.711u, G.711A and G.729 using SRTP
- Incoming and outgoing faxes using T.38
- DTMF tone transmission with RFC2833

©2019 Avaya Inc. All Rights Reserved.

- Calls using various Analog, H.323 and SIP endpoints supported by Avaya IP telephony solution

Note: Configuration instructions in this document are primarily geared towards FXS lines on AudioCodes M1K. Configuration for FXO lines is clearly noted and is only necessary if configuring FXO lines on AudioCodes M1K.

2.2. Test Results

The AudioCodes Mediant 1000 passed compliance testing.

2.3. Support

For technical support, contact AudioCodes via the support link at www.audiocodes.com.

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Sample configuration that was used during compliance testing consisted of following components:

- Avaya G430 Media Gateway with Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya IP Phones: SIP and H.323
- AudioCodes Mediant 1000

Calls and faxes were routed to/from AudioCodes M1K via Communication Manager and Session Manager.

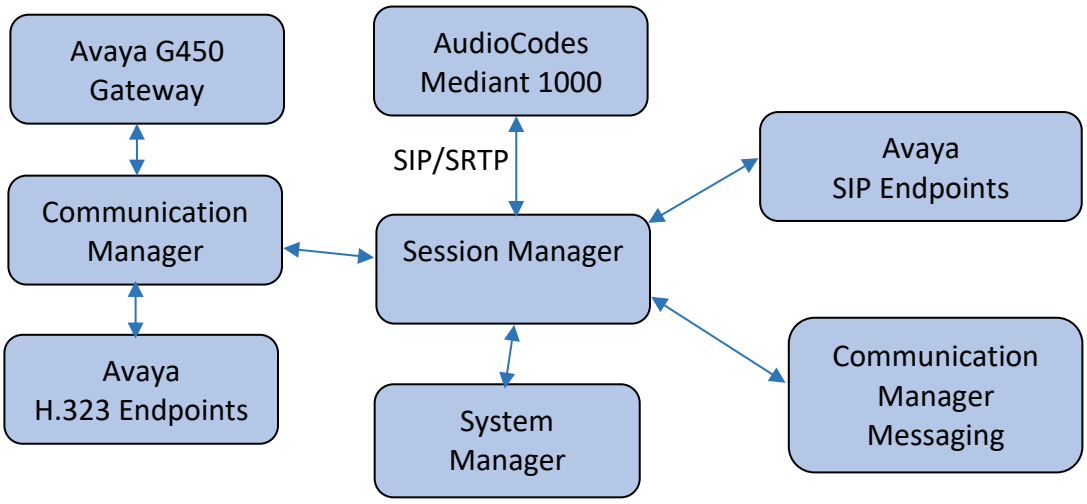


Figure 1: AudioCodes Mediant 1000 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

©2019 Avaya Inc. All Rights Reserved.

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 in a Virtual Environment	8.0.1.0.0-FP1
Avaya Aura® Session Manager in a Virtual Environment	8.0.1.0.801007
Avaya Aura® System Manager in a Virtual Environment	8.0.1.0
Avaya Aura® Media Server in a Virtual Environment	8.0.0.173
Avaya 96x1 Deskphone	SIP 7.1.4.0, H.323 6.7.1
Analog Phone and Fax Machine	-
AudioCodes Mediant 1000	7.20A.204.222

©2019 Avaya Inc. All Rights Reserved.

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 enough 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: 12000 0
          Maximum Concurrently Registered IP Stations: 2400  2
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 2400  0
             Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 36000 0
                  Maximum Video Capable IP Softphones: 2400  0
                      Maximum Administered SIP Trunks: 12000 10
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 688   0
```

On **Page 5,** verify **Media Encryption Over IP** fields are set to **y**.

```
display system-parameters customer-options                      Page   5 of  12
                              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
```


©2019 Avaya Inc. All Rights Reserved.

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.

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 and **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:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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
```


©2019 Avaya Inc. All Rights Reserved.

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.

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

- Set **Audio Codec 1, 2 and 3** to **G.711MU, G.711A, G.729AB** respectively
- Set **Media Encryption** as shown below.

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

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

                        IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.711A            n         2        20
 3: G.729AB             n         2        20
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: enforce-enc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: 3-srtp-aescm128-hmac80-unauth
 4: 4-srtp-aescm128-hmac32-unauth
 5: none
```

On **Page 2**:

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

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

                        IP MEDIA PARAMETERS

                            Allow Direct-IP Multimedia? y
             Maximum Call Rate for Direct-IP Multimedia:  1024:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  1024:Kbits

                                      Redun-                        Packet
                        Mode          dancy                         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
```


©2019 Avaya Inc. All Rights Reserved.

5.4. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm8** and **10.64.110.135** entry was added.

```
change node-names ip                                          Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
aes8                10.64.110.132
ams8                10.64.110.136
cms18               10.64.110.20
default             0.0.0.0
procr               10.64.110.131
procr6              ::
sm8                 10.64.110.135
```

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.

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Transport Type** to **tls**
- Set **Enforce SIPS URI for SRTP** to **y**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.4**, i.e. sm8
- Set **Far-end Network region** to the configured region in **Section 5.2**, i.e. 1
- Enter a **Far-end Domain,** e.g. avaya.com

```
change 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? y
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sm8
 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): 120                IP Audio Hairpinning? y
         Enable Layer 3 Test? y                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```


©2019 Avaya Inc. All Rights Reserved.

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.

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

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. sm8
- Enter a valid **TAC**, e.g. 101
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.5**, i.e. 1
- Enter a desired number in **Number of Member** field

```
change trunk-group 1                                          Page   1 of   5
                               TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: sm8                         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   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                            UUI Treatment: shared
                                           Maximum Size of UUI Contents: 128
                                              Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n
```


©2019 Avaya Inc. All Rights Reserved.

5.7. Administer Route Pattern

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

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**, i.e. 1
- For line 1, set **FRL** to **0**
- Set **Number Format** to **lev0-pvt**

```
change route-pattern 1                                          Page   1 of   4
                  Pattern Number: 1      Pattern Name:
   SCCAN? n    Secure SIP? n     Used for SIP stations? n

   Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
   No          Mrk Lmt List Del  Digits                          QSIG
                                 Dgts                            Intw
 1: 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 Sub  Numbering LAR
   0 1 2 M 4 W     Request                                Dgts Format
 1: y y y y y n  n            rest                             lev0-pvt  none
 2: y y y y y n  n            rest                                       none
 3: y y y y y n  n            rest                                       none
 4: y y y y y n  n            rest                                       none
 5: y y y y y n  n            rest                                       none
 6: y y y y y n  n            rest                                       none
```


©2019 Avaya Inc. All Rights Reserved.

5.8. Administer Private Numbering

Use the **change private-numbering 0** command to define the calling party number to send to Session Manager.

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

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

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  5              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*** on Session Manager. Extensions starting with 5 were used.

- Set **Dialed String** to starting digits of extensions that will be used, e.g. 5
- 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 **aar**

```
change aar analysis 5                                         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
    5                     5    5    1         aar          n
    5                     7    7    999       aar          n
    53                    5    5    1         aar          n
    59998                 5    5    1         aar          n
    6                     7    7    999       aar          n
    7                     5    5    1         aar          n
    8                     7    7    999       aar          n
    9                     5    5    5         aar          n
```


©2019 Avaya Inc. All Rights Reserved.

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 M1K. 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 M1K.

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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    303                   10   10    1        hnpa         n
    4                     7    7     2        hnpa         n
    411                   3    3     deny     svcl         n
    555                   7    7     deny     hnpa         n
    6                     7    7     2        hnpa         n
    611                   3    3     1        svcl         n
    7                     7    7     2        hnpa         n
    8                     7    7     2        hnpa         n
```

5.11. Administer Stations

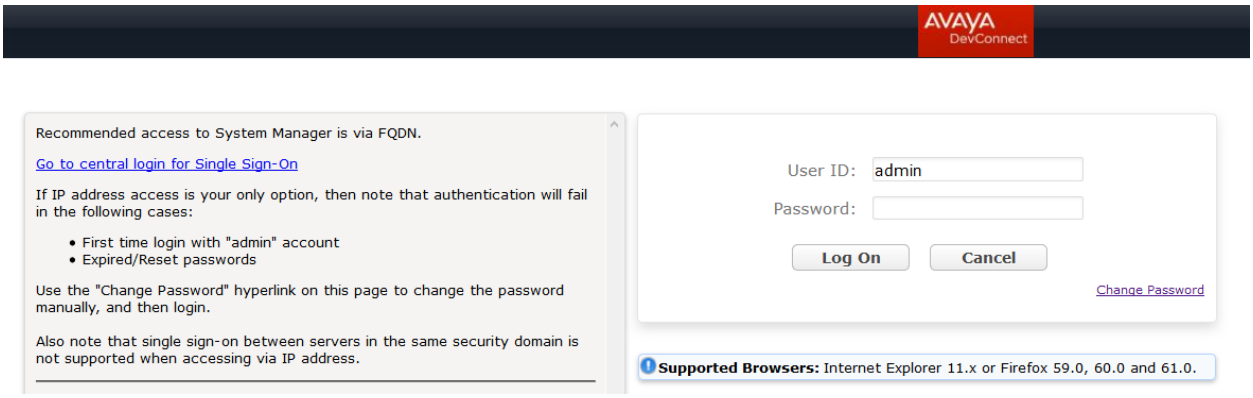
Administration of Avaya Stations/Extensions in Communication Manager and Session Manager is not shown in this document. Please refer to document [1] and/or [2] in reference section of this document.

Note: Please ensure that SRTP encryption is turned on for SIP stations connected to Session Manager. SRTP encryption can be turned on by modifying the 46xxsettings.txt file; change **MEDIAENCRYTION** parameter to **1,9;** 1 is encryption of **aescm128-hmac80** and **9** is **none**.

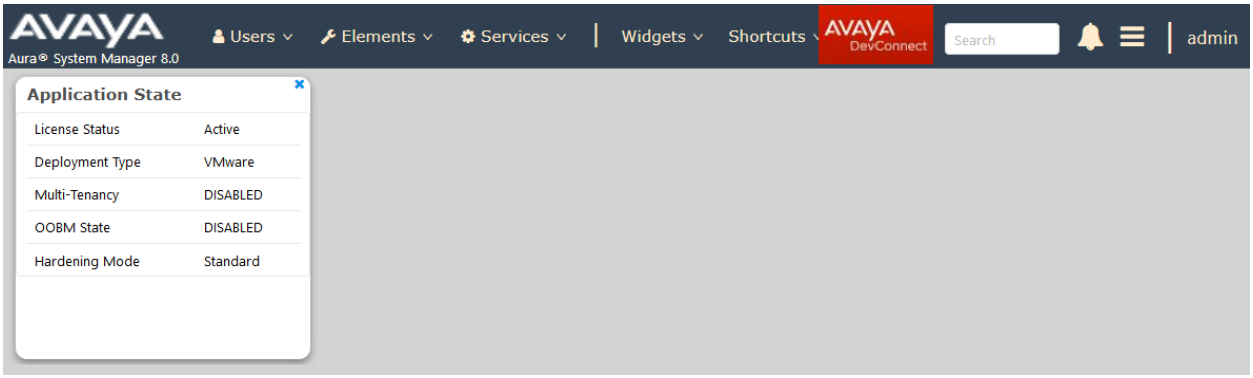
©2019 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager

Configuration of Avaya Aura® Session Manager is performed via Avaya Aura® System Manager. Access the System 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.



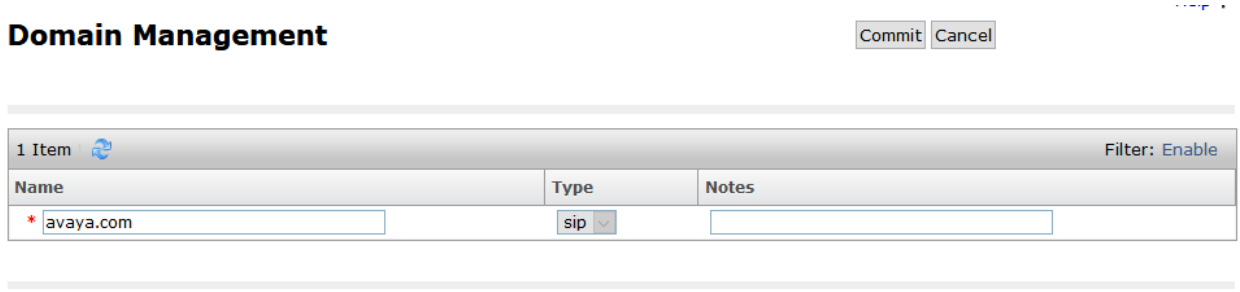
©2019 Avaya Inc. All Rights Reserved.

6.1. Add SIP Domain

Navigate to **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**) i.e. avaya.com
- Set **Type** to **sip**

Click **Commit** to save changes.



6.2. Add Location

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

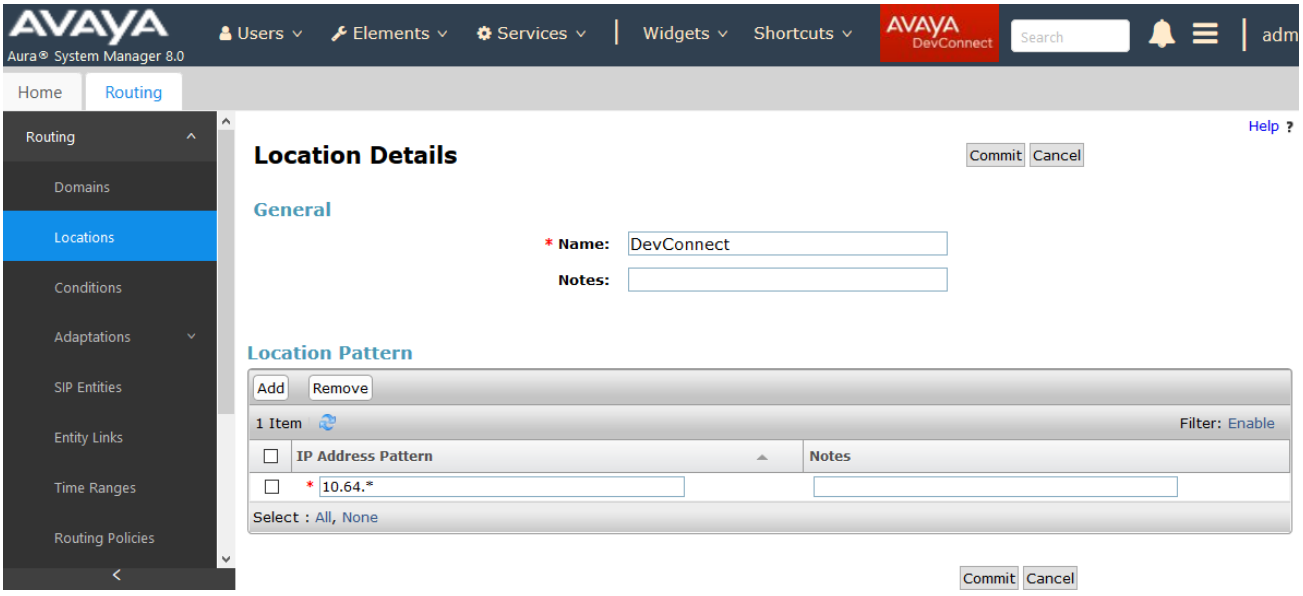
Under **General**:

- Type in a descriptive **Name**

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

- Type in an **IP Address Pattern**, e.g. 10.64.*

Click **Commit** to save changes. Screen shot shown on next page.



©2019 Avaya Inc. All Rights Reserved.

6.3. Add SIP Entity

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

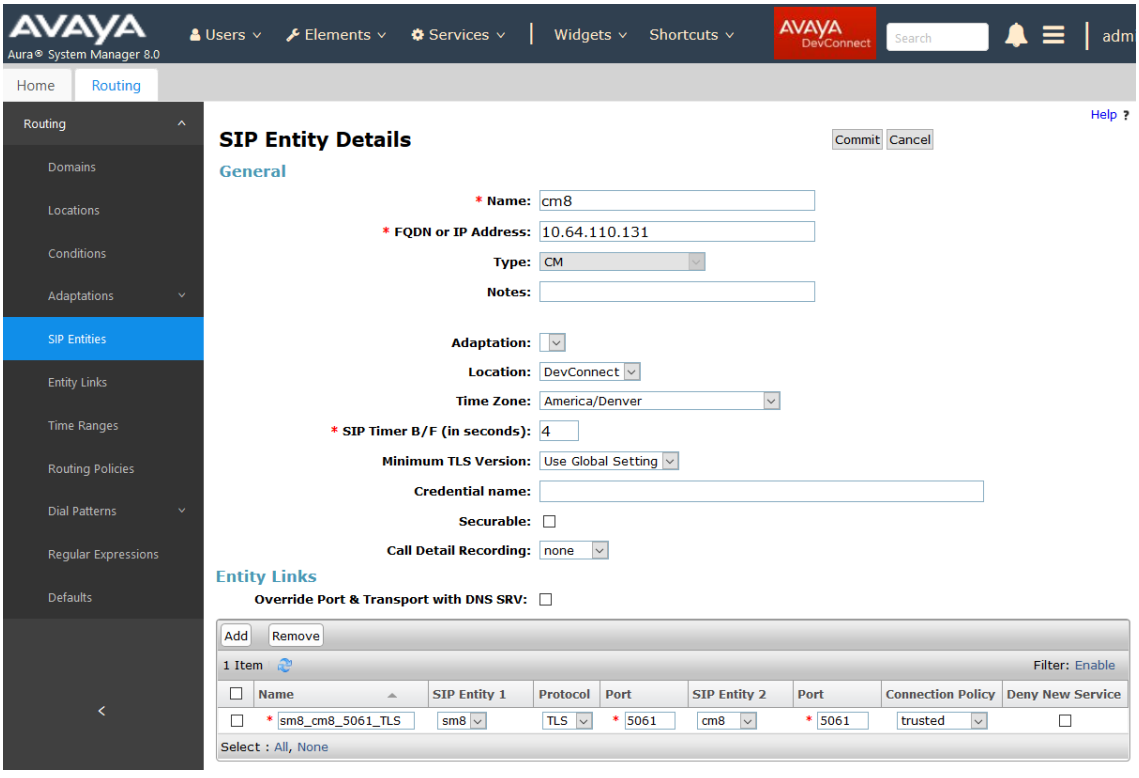
- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**

Add Entity Links. Under **Entity Links**, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Name:** Will be populated automatically
- **SIP Entity 2:** Will be populated automatically with the name of this SIP Entity.
- **SIP Entity 1:** Select Session Manager from the pull down box
- **Protocol:** Select the desired Protocol from the pull down box
- **Port:** Enter the desired port number for the Entity Link

Click **Commit** to save changes.

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



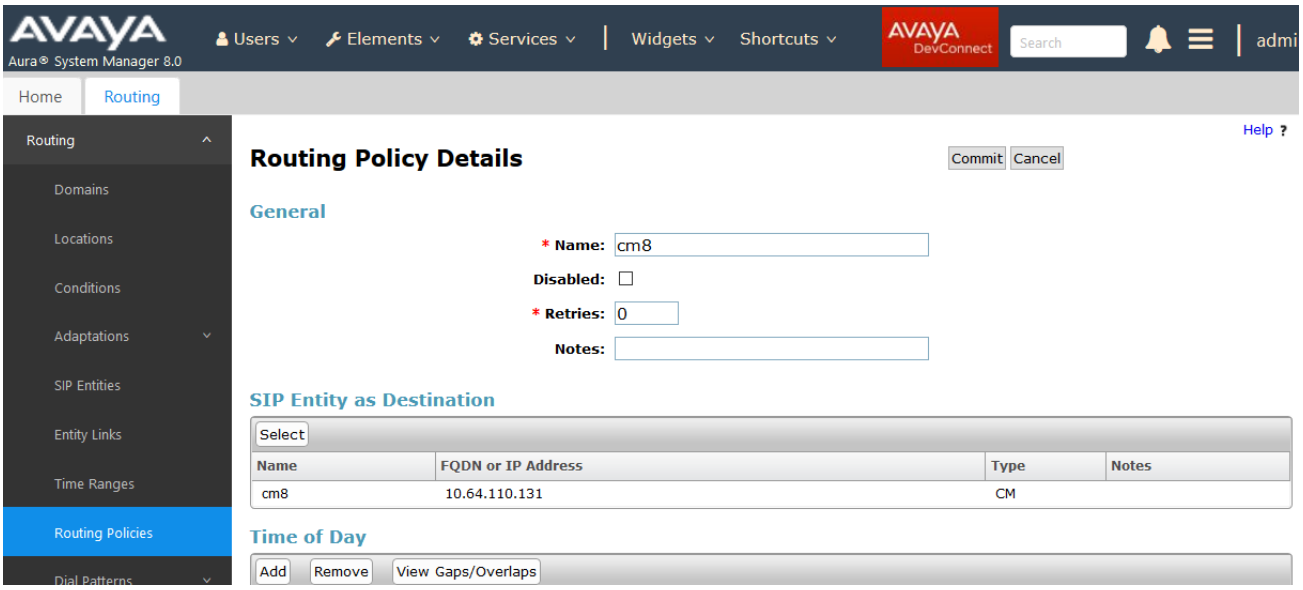
©2019 Avaya Inc. All Rights Reserved.

6.4. 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** (not shown):
  - Select Communication Manager SIP entity added in **Section 6.3**
- Under **Time of Day**, click on **Add** (not shown):
  - Select time range added in previous step

Click **Commit** to save changes.



©2019 Avaya Inc. All Rights Reserved.

6.5. Add Dial Patterns

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

Under **General:**

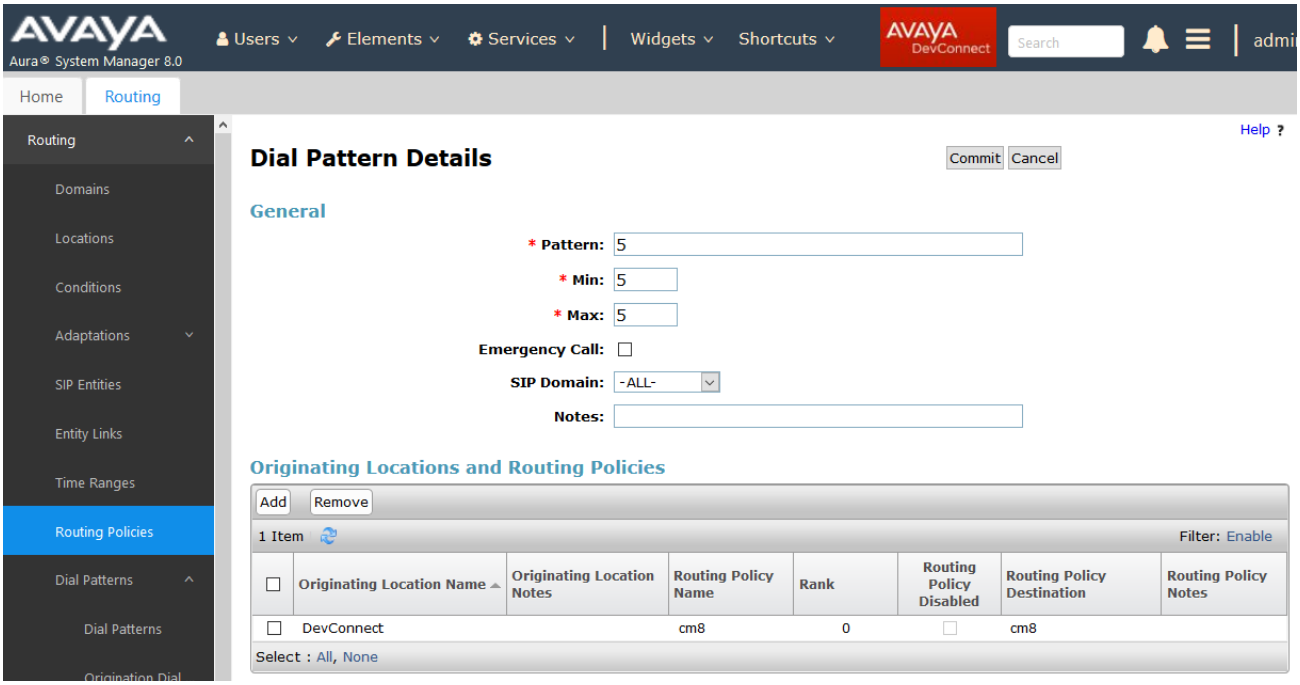
- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number
- Set **Domain** to domain configured on **Section 6.1**

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and Communication Manager routing policy as configured in **Section 6.2** and **Section 6.4** respectively

Click **Commit** to save changes.

Note: For Compliance testing, dialed number of 5xxxx were used. Thus, pattern, min and max values were all set to 5.



©2019 Avaya Inc. All Rights Reserved.

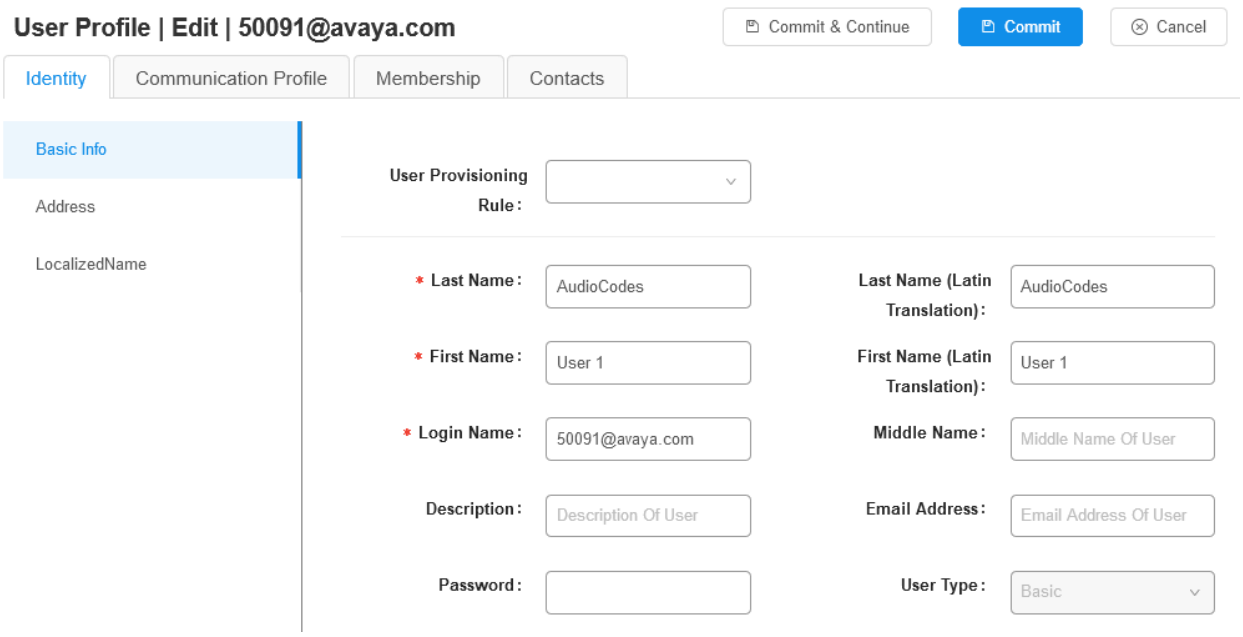
6.6. Add User

For each analog line on AudioCodes M1K, a user needs to be added on Session Manager. Information in this section will be used by AudioCodes M1K 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:

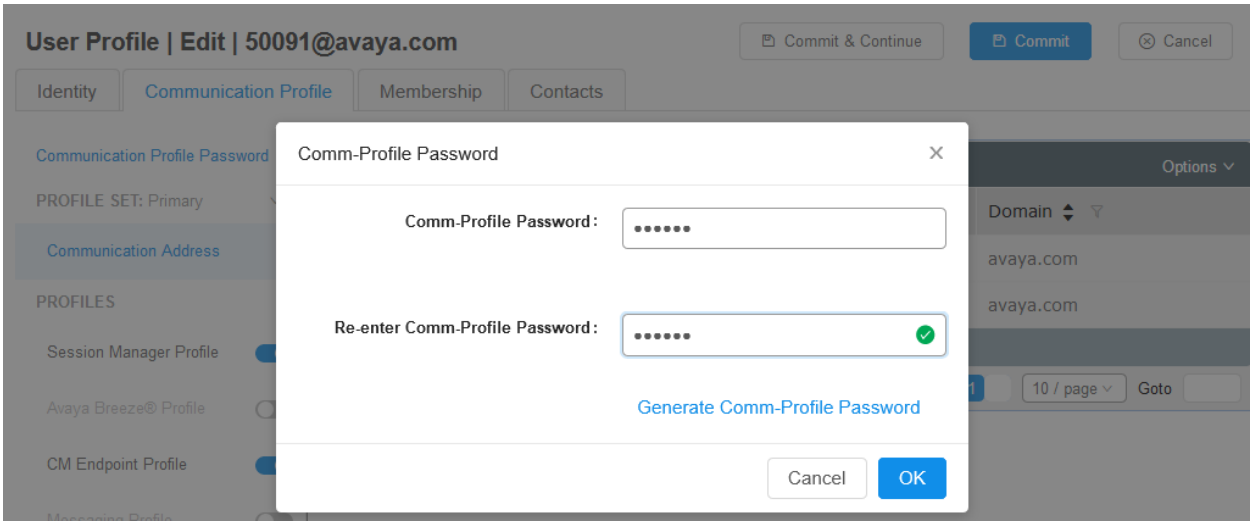
- Type in **Last Name** and **First Name**
- In **Login Name** field type in <extension>@<domain>. <Extension> is an extension which will be configured on AudioCodes M1K to receive and make calls. <domain> is as configured in **Section 6.1**



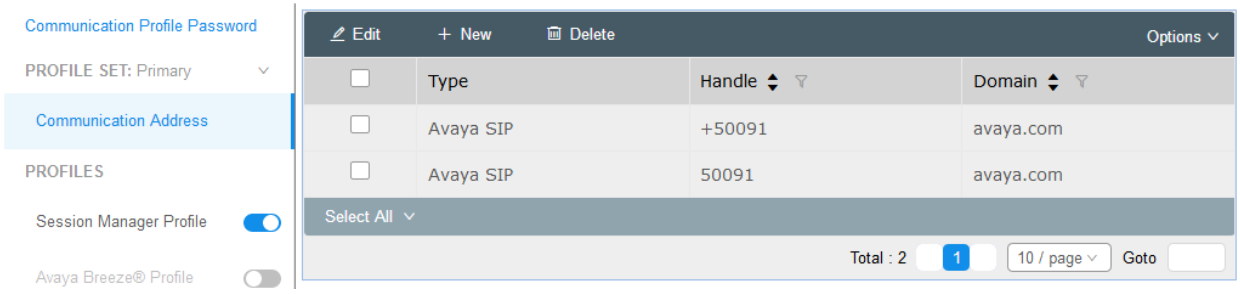
©2019 Avaya Inc. All Rights Reserved.

Under **Communication Profile** tab:

- Under **Communication Profile**, select **Communication Profile Password** and type in the passwords.

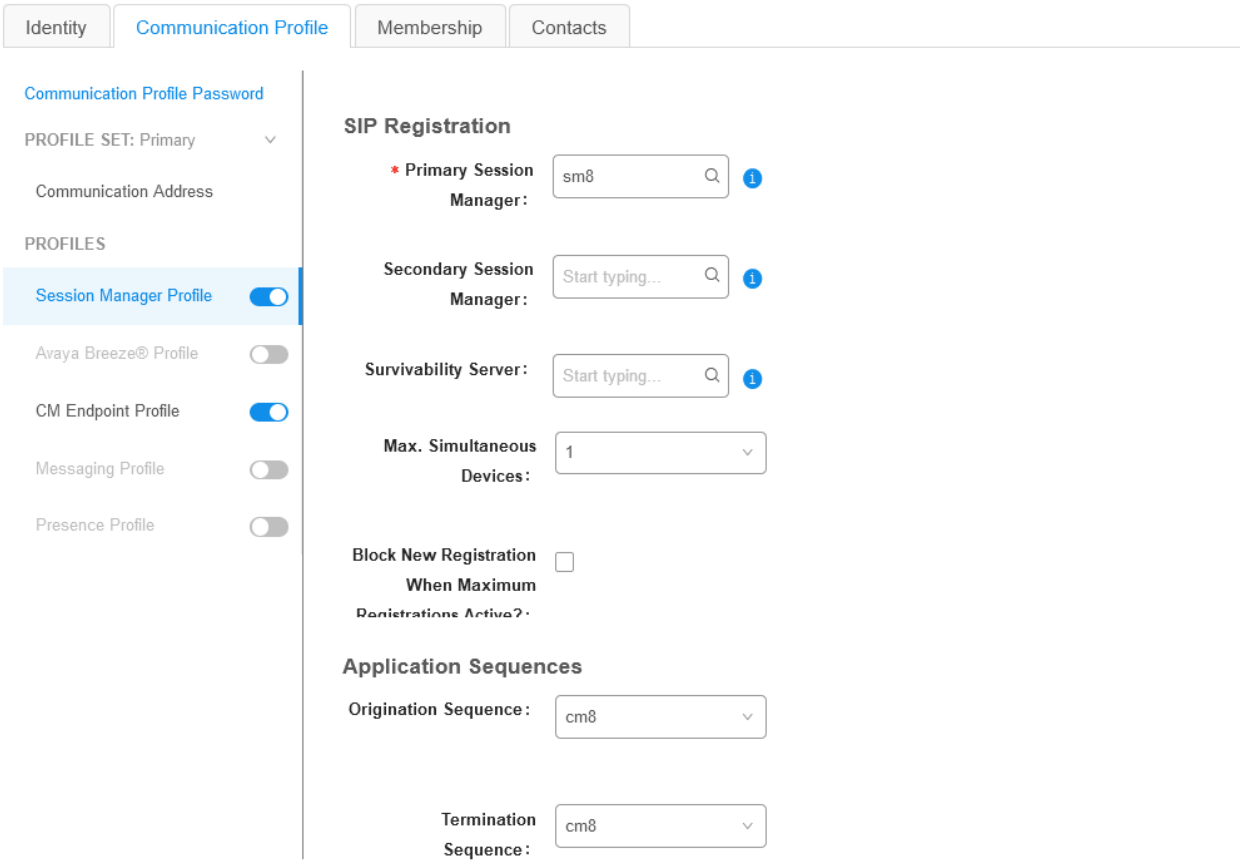


- Under **Communication Address**, click on **New** (not shown)
  - Type in <extension> in the text field, select domain configured in **Section 6.1** for **Fully Qualified Address**. <Extension> is the same extension configured for login name under Identity tab. Click on **Add**. Please note that AudioCodes M1K will use this information has login name to register to Session Manager.



©2019 Avaya Inc. All Rights Reserved.

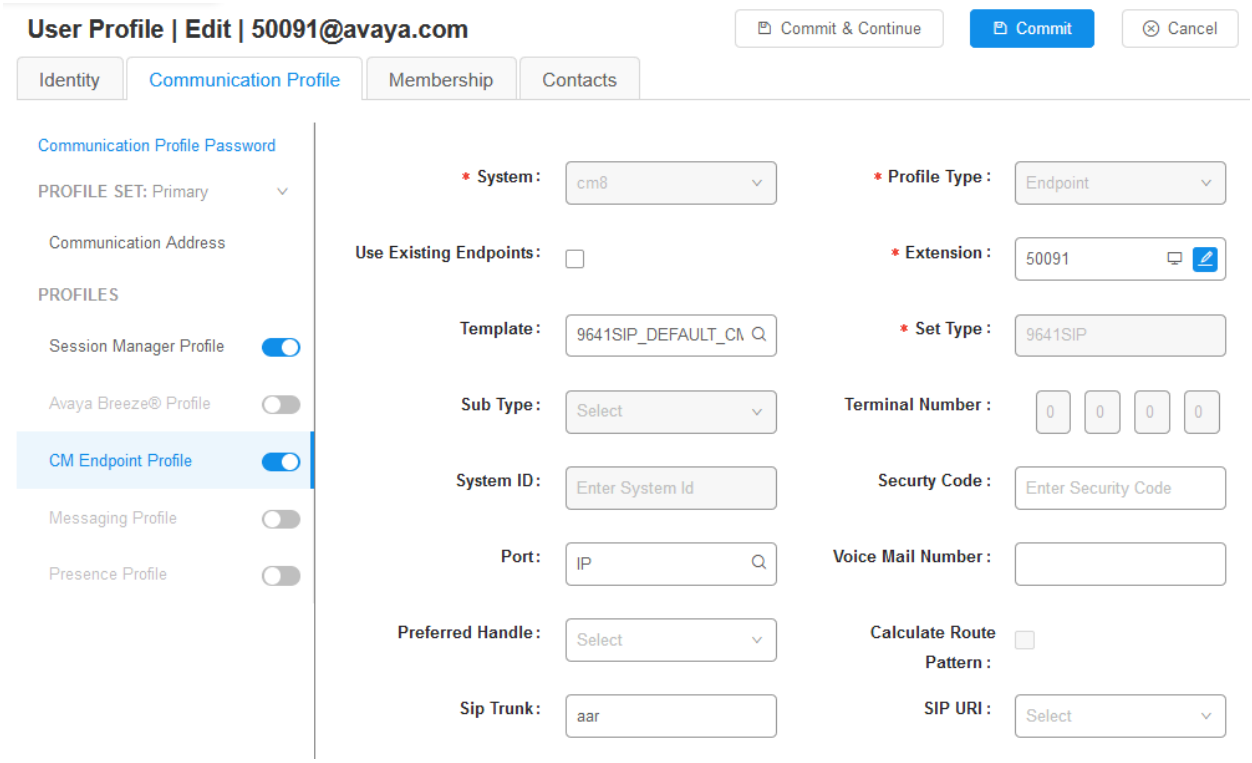
- Check the **Session Manager Profile** box:
  - Set **Primary Session Manager** to Session Manager. i.e. sm8.
  - Set **Origination Application Sequence** and **Termination Application Sequence** to Communication Manager. Please note that configuration for Application Sequence is not shown in this document. Please refer to document [2] in reference section of this document for further details.
  - Set **Home Location.**



©2019 Avaya Inc. All Rights Reserved.

- Check the **CM Endpoint Profile** box:
  - Set **System** to Communication Manager.
  - Set **Profile Type** to **Endpoint.**
  - Type in extension number used in this section for **Extension** field.
  - Set **Template** to **9641SIP_DEFAULT_CM_8_0**
  - Set **Security Code** to a desired value. Please note that AudioCodes M1K will use this security code as password to register to Session Manager.

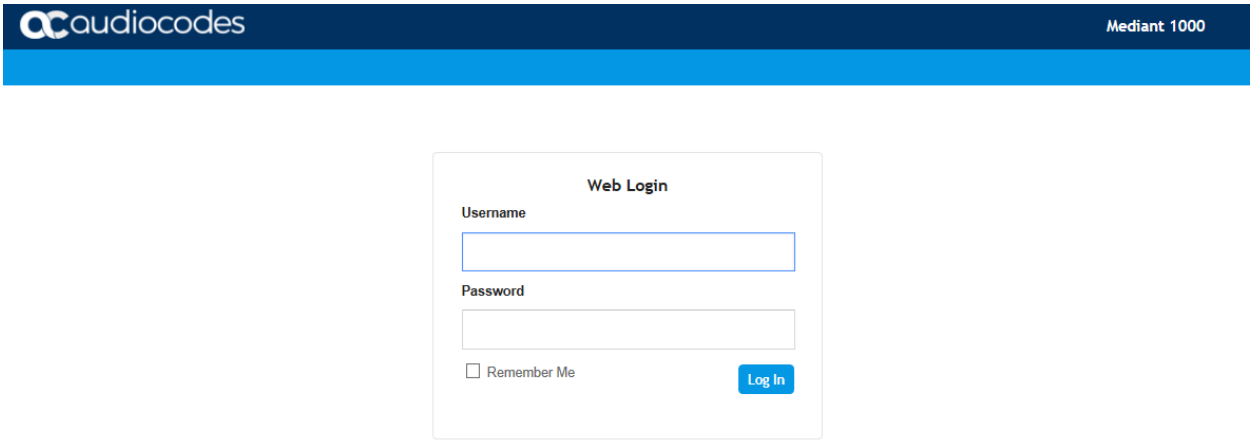
Click **Commit** to save changes.



©2019 Avaya Inc. All Rights Reserved.

7. Configure AudioCodes Mediant 1000

Administration for AudioCodes M1K series is done via the administrative console. Type in http://<ip-address> URL in a web browser, where <ip-address> is the IP Address of AudioCodes M1K. Log on to the administrative console using appropriate credentials.

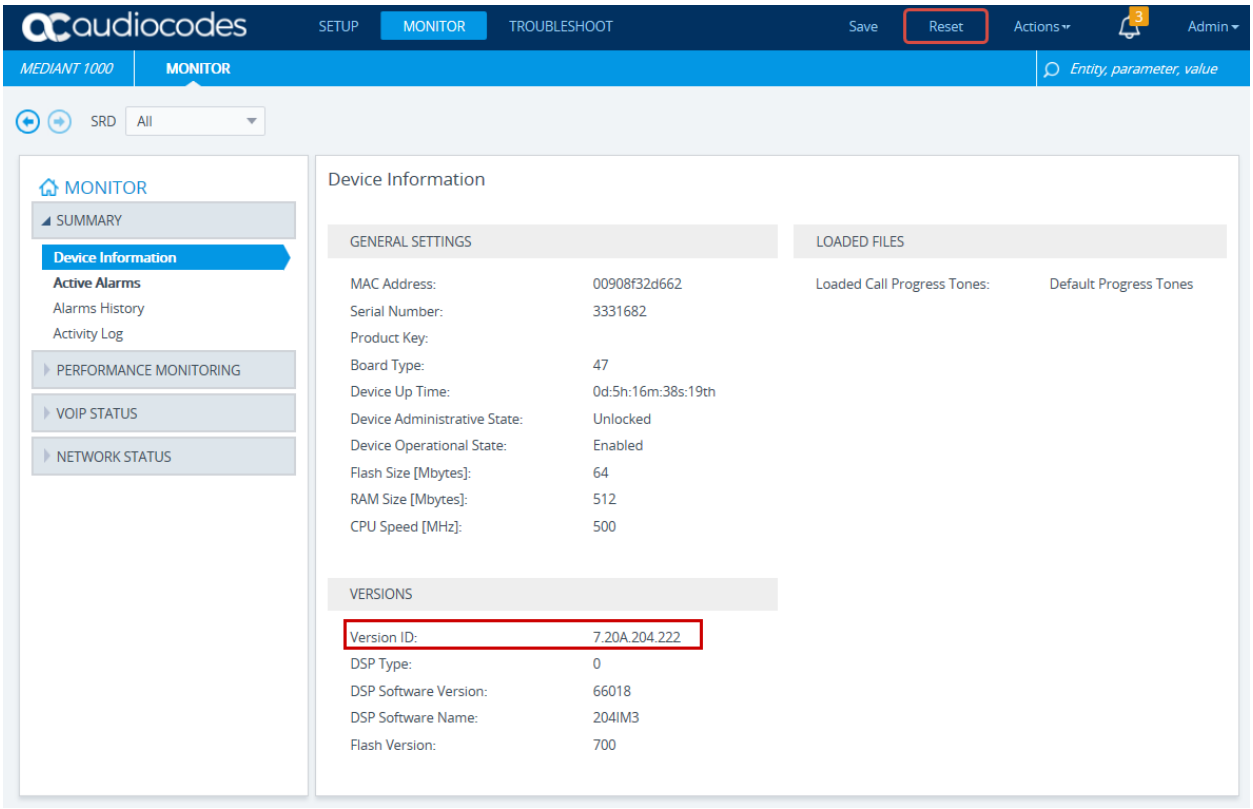


Note: Configuration mentioned in the section is performed for AudioCodes M1K. A sample .ini file generated after configuring AudioCodes M1K can be found in **Appendix A**.

©2019 Avaya Inc. All Rights Reserved.

7.1. Verify Firmware Version

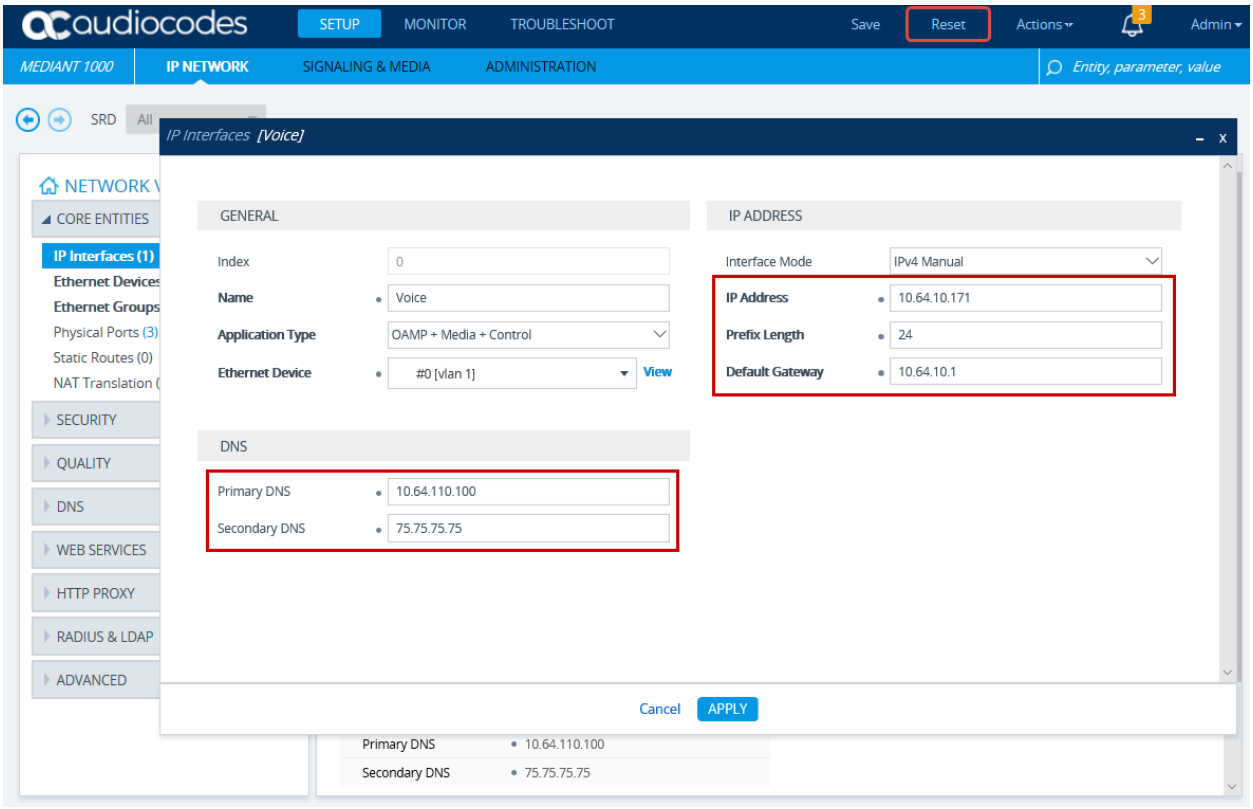
Once logged in, the firmware version can be found under **Monitor → Device Information** box. The firmware version should be **7.20A.204.222** or higher.



©2019 Avaya Inc. All Rights Reserved.

7.2. Administer IP Interface

Navigate to **SETUP → IP NETWORK → CORE ENTITIES → IP Interface** and edit an available interface. Configure the network information.



©2019 Avaya Inc. All Rights Reserved.

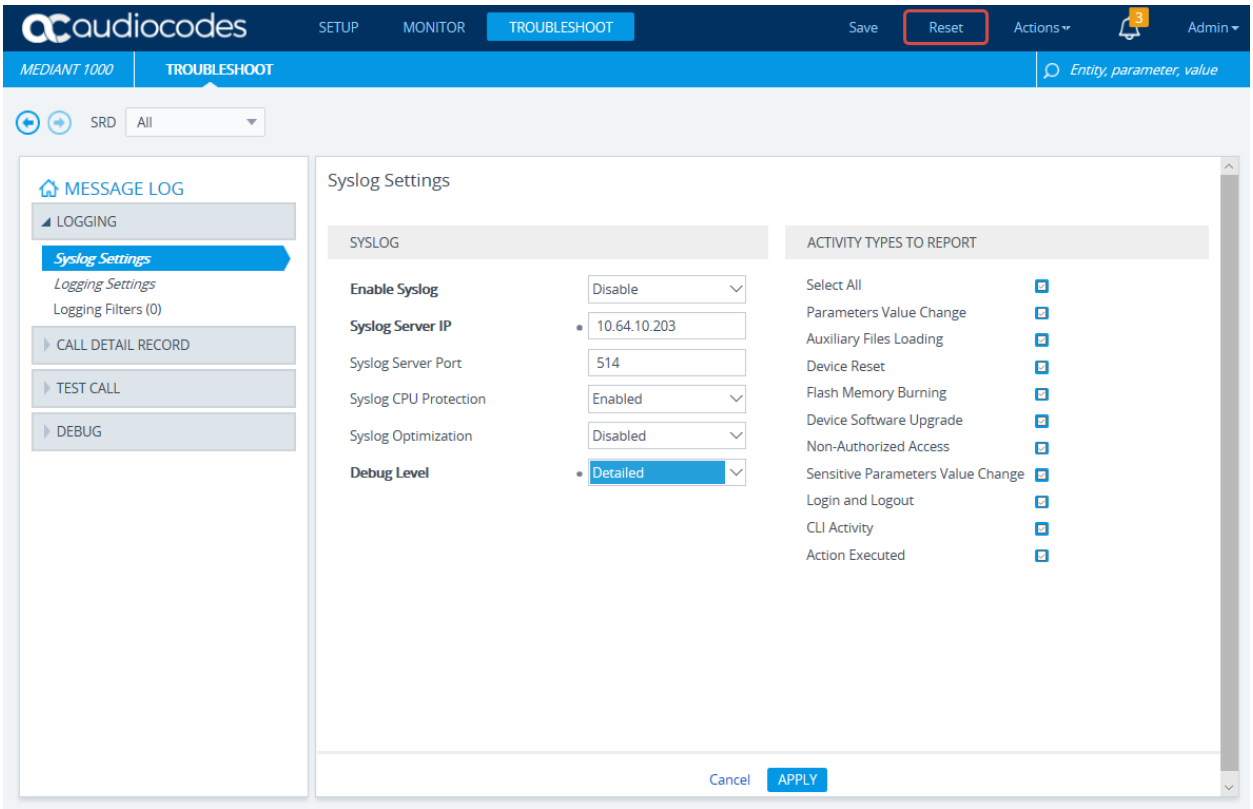
7.3. Administer Syslog Settings

To troubleshoot any issues, Syslog can be enabled. Navigate to **TROUBLESHOOT → LOGGING → 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 **Detailed**
- Under **ACTIVITY TYPES TO REPORT**, check all boxes

Please note that, Syslog does not need to be enabled to successfully interoperate Session Manager with AudioCodes M1K. However, AudioCodes recommends it to be turned on for troubleshooting purposes. Turning Syslog on does not impact performance of AudioCodes M1K.

Click **Submit** to save changes (not shown).
Reset the device to save changes to flash memory of AudioCodes M1K.



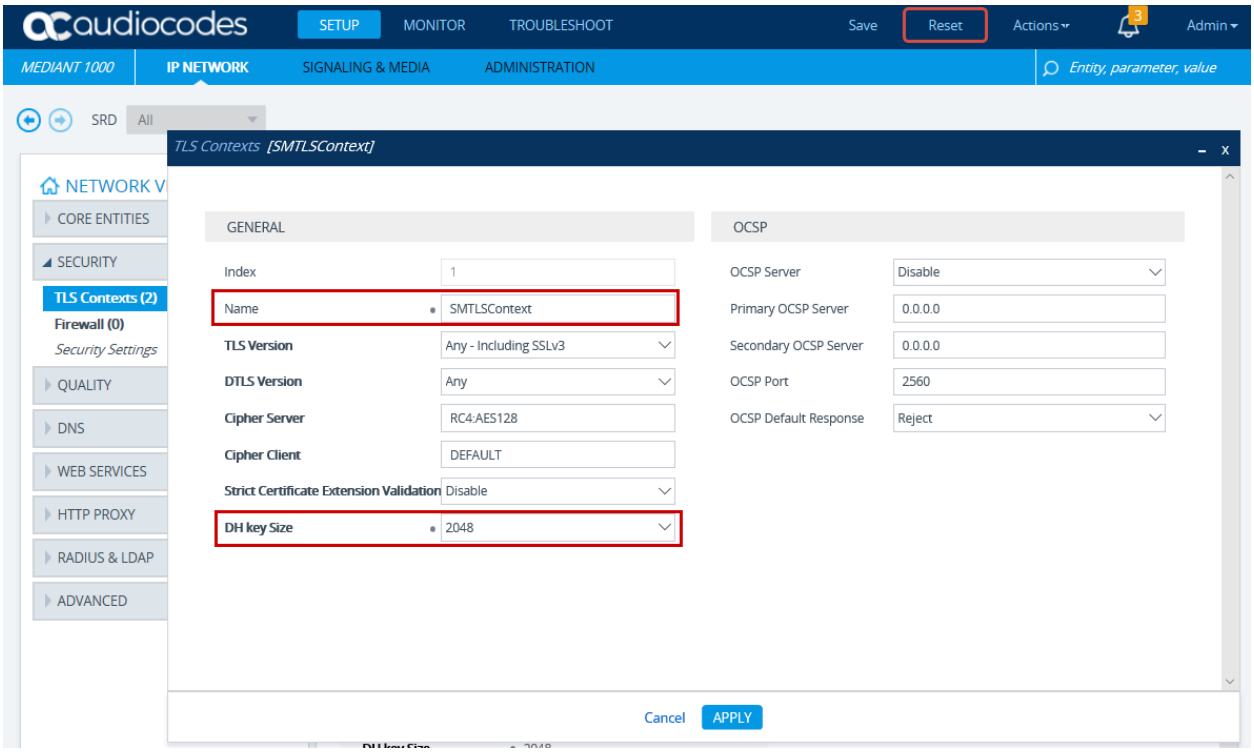
©2019 Avaya Inc. All Rights Reserved.

7.4. Administer TLS Context

Navigate to **SETUP → IP NETWORK → SECURITY → TLS Contexts** and select **New** (not shown) to create a new TLS Context that will be used for Session Manager.

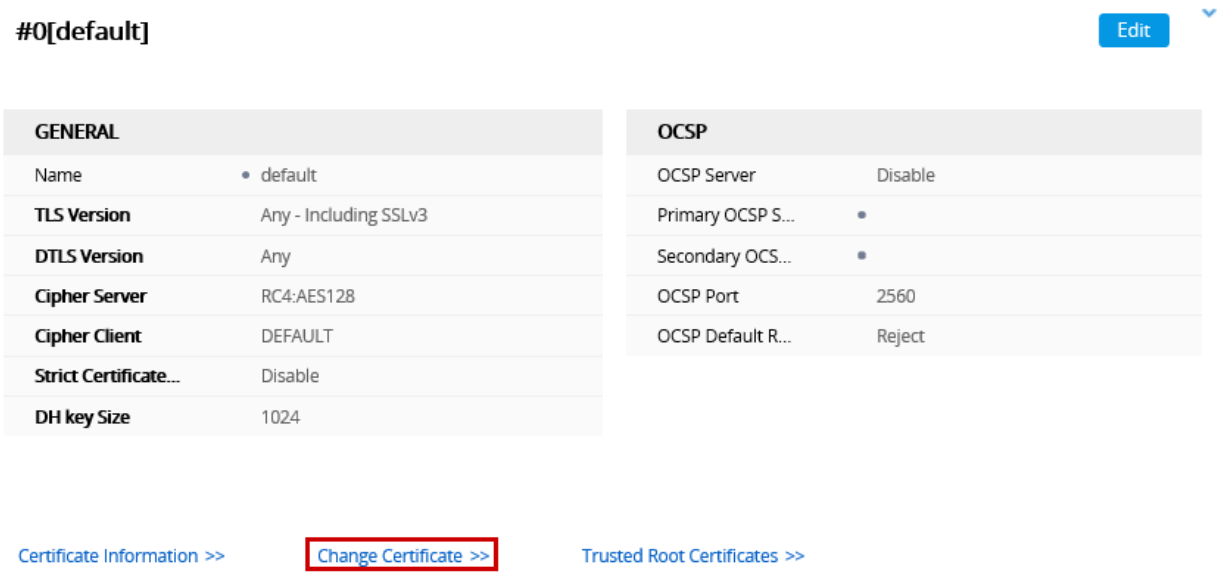
- Type in a **Name**
- Set **DH Key Size** to **2048**

Select **Apply** once done.

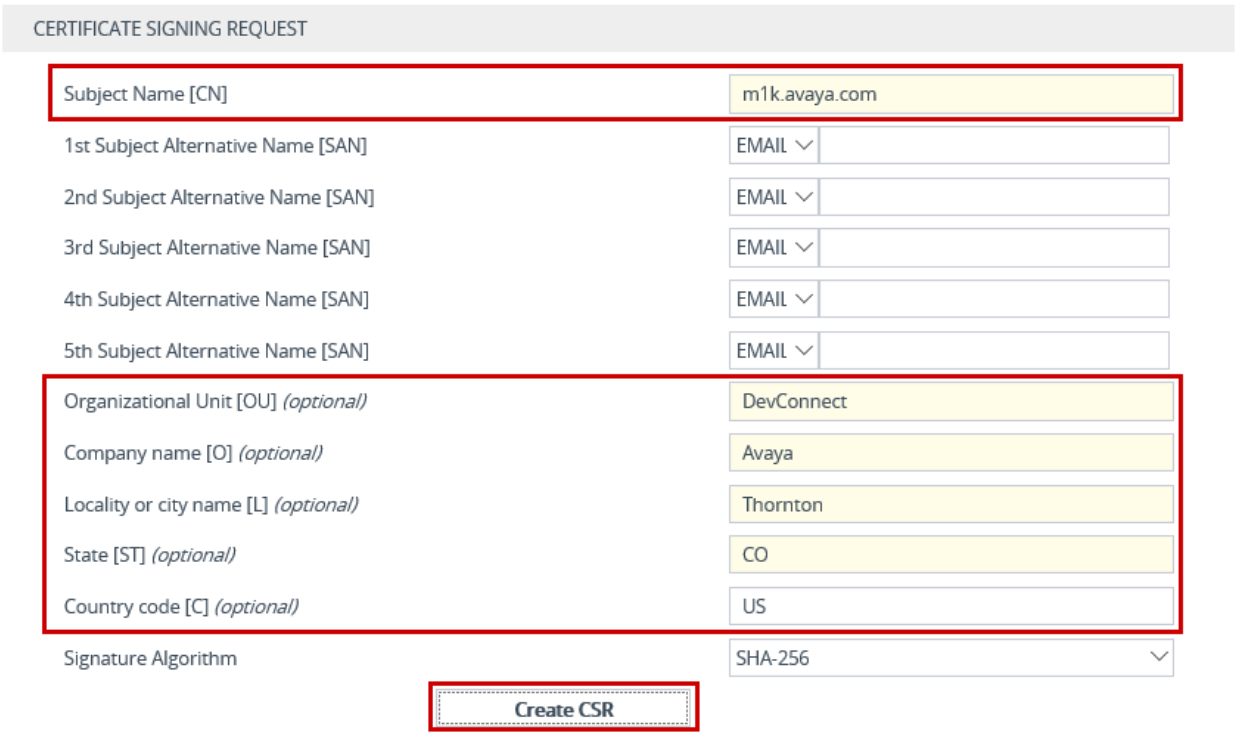


©2019 Avaya Inc. All Rights Reserved.

Select **Change Certificate** at the bottom of the page.

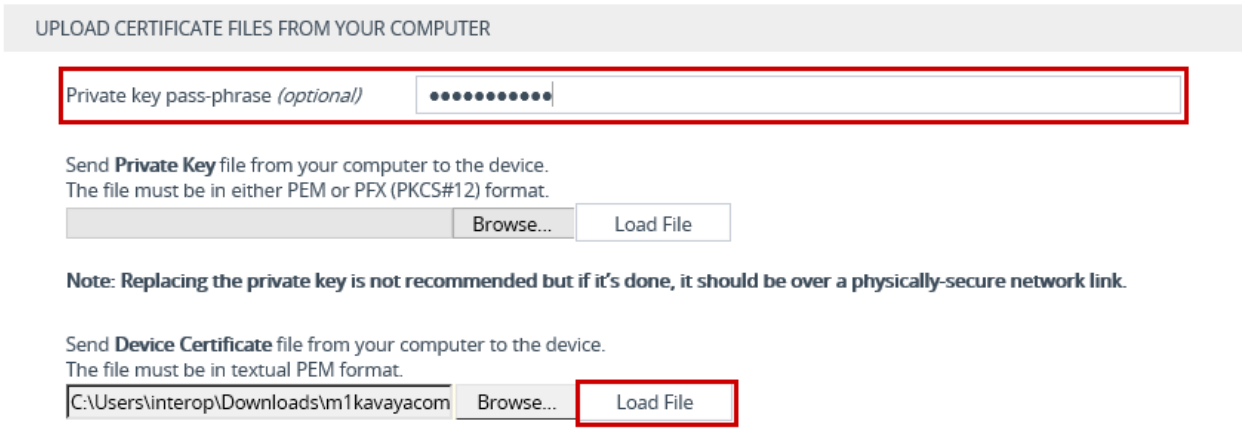


Fill in the highlighted information below and select **Create CSR.** Copy the CSR and use it to generate a device certificate from System Manager.



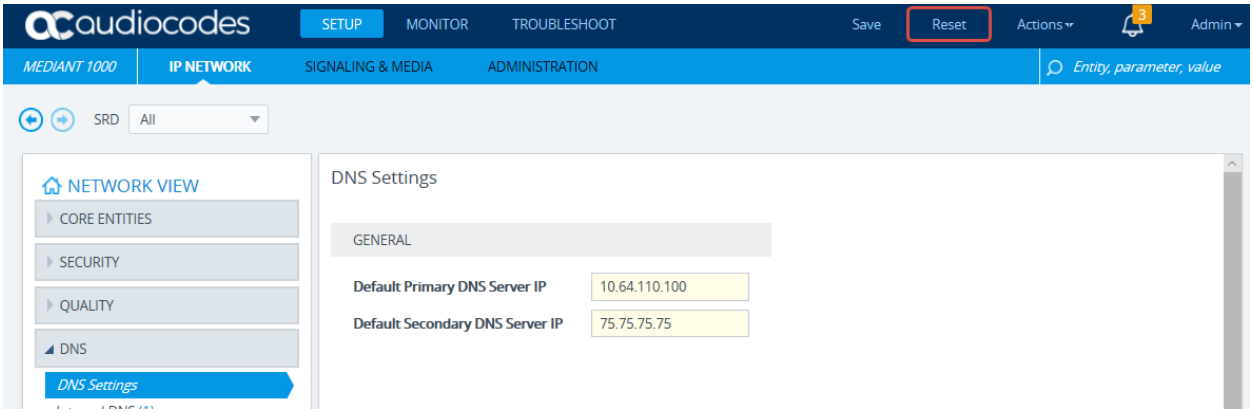
©2019 Avaya Inc. All Rights Reserved.

Once the device certificate is generated from System Manager, at the bottom of the page, **Browse** to the **Device Certificate.** Type in the pass-phrase used and select **Load File**.

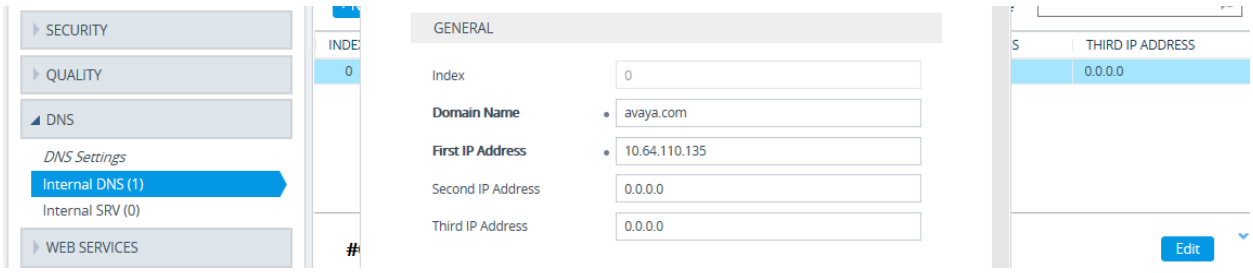


7.5. Administer DNS Setting

On the left pane, navigate to **SETUP → IP NETWORK → DNS → DNS Setting**. If DNS Servers are used, type in their IP Address. For compliance testing, following was configured.



Continuing from above, select **Internal DNS** on the left and add a **New** entry for the **Domain Name** from **Section 6.1**. Type in Session Manager SIP Entity IP in **First IP Address.**



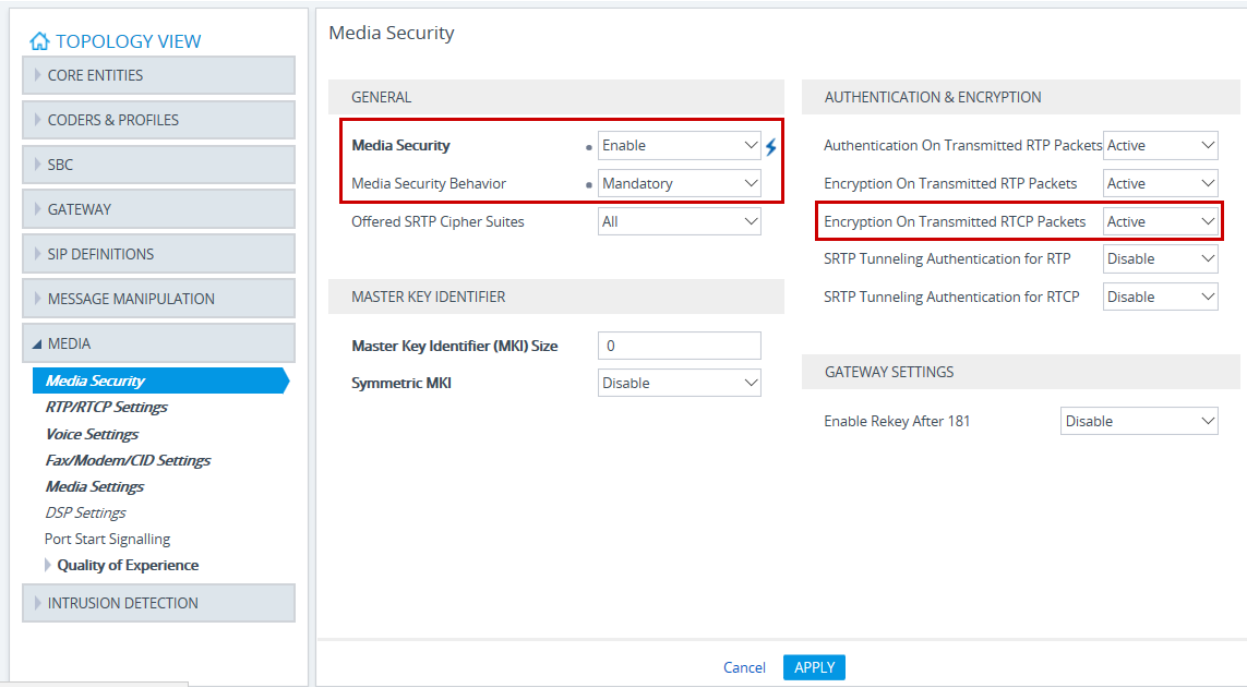
©2019 Avaya Inc. All Rights Reserved.

7.6. Administer Media Security

On the left pane, navigate to **SETUP → SIGNALING & MEDIA → Media → Media Security**

- Set **Media Security** to **Enable**
- Set **Media Security Behavior** to **Mandatory**
- Set **Encryption on Transmitted RTCP Packets** to **Active**

Click **Apply** to save changes.



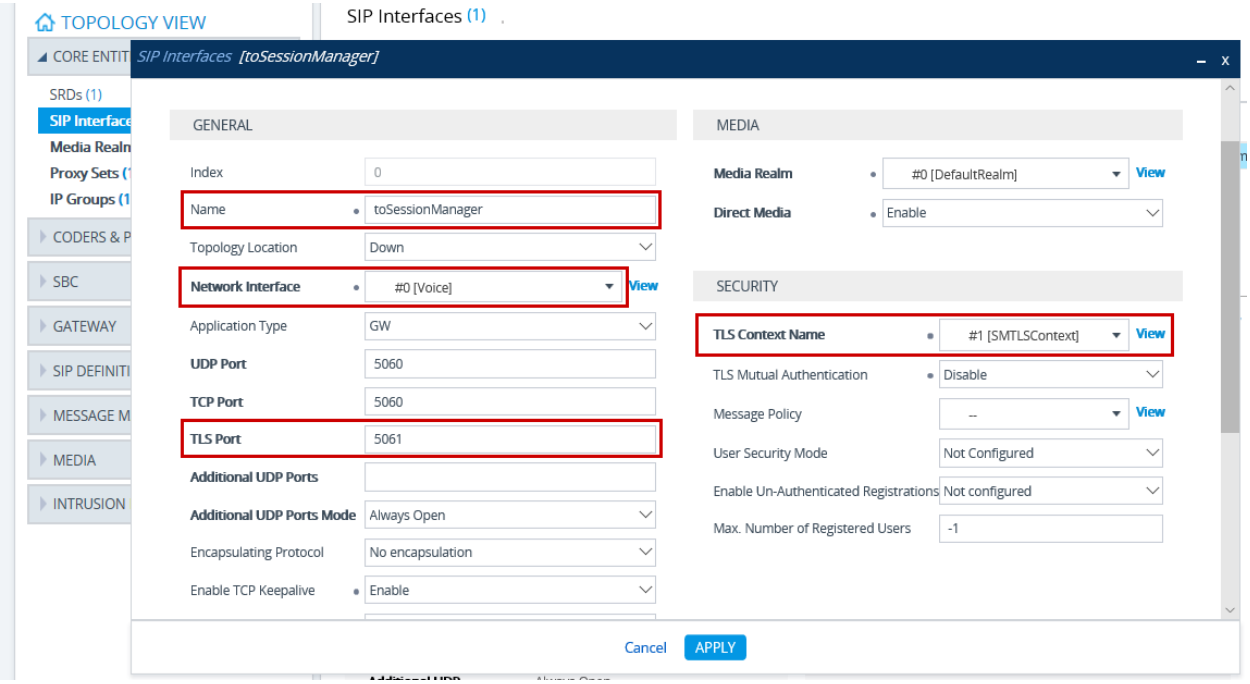
Note: This change requires a reset of AudioCodes M1K. Please burn the changes and reset the device before performing any further configuration.

©2019 Avaya Inc. All Rights Reserved.

7.7. Administer SIP Interface

To configure SIP Interface to Session Manager, navigate to **SETUP → SIGNALING & MEDIA → CORE ENTITIES → SIP Interface** and select **New** (not shown).

- Type in a **Name.**
- Set **Network Interface** to the IP Interface from **Section 7.2.**
- Verify **TLS Port** is configured as **5061.**
- Set **TLS Context Name** to the TLS Context from **Section 7.4.**



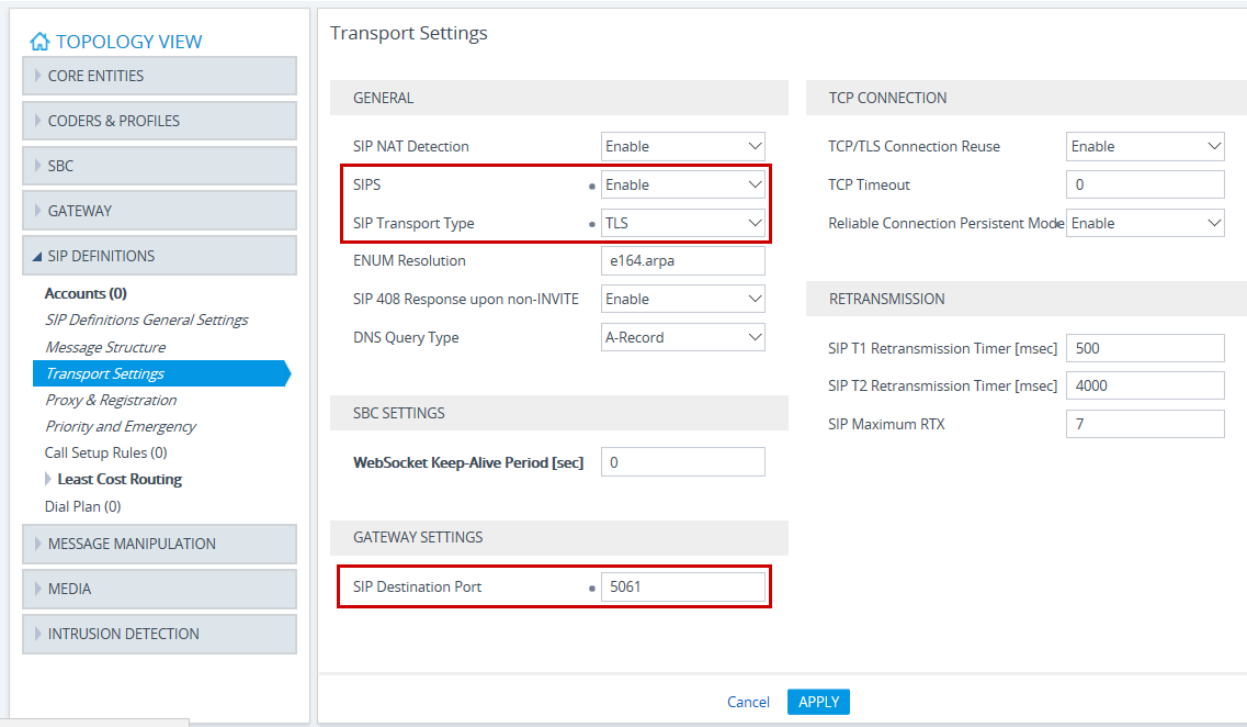
©2019 Avaya Inc. All Rights Reserved.

7.8. Administer Transport Settings

On the left pane, navigate to **SIP DEFINITIONS → Transport Settings**

- Set **SIP Transport Type** to **TLS**
- Set **Enable SIPS** to **Enable**
- Set **SIP Destination Port** to **5061**

Click **Submit** to save changes (not shown).



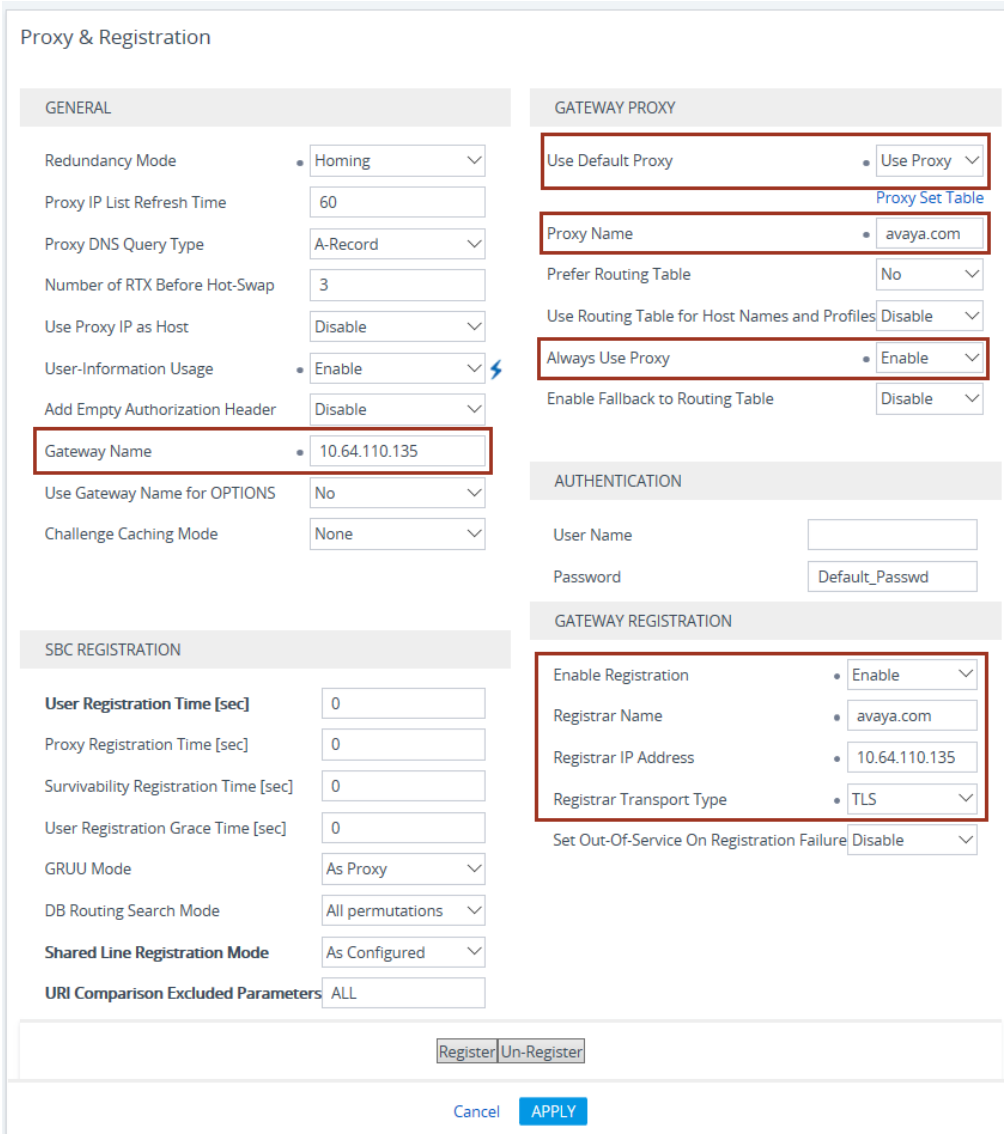
©2019 Avaya Inc. All Rights Reserved.

7.9. Administer Proxy and Registration

On the left name, select **SIP DEFINITIONS → Proxy & Registration**

- Set **Use Default Proxy** to **Use Proxy**
- Set **Proxy Name** from **Section 6.1**
- Set **Always Use Proxy** to **Enable**
- Set **Enable Registration** to **Enable**
  Set **Registrar Name** from **Section 6.1**
- Set **Registrar IP Address** to the SIP Entity IP Address of Session Manager
- Set **Registrar Transport Type** to **TLS**
- Fill in **Registration Time** to a desired value, in seconds

Click **Apply** to save changes. Screen capture below.

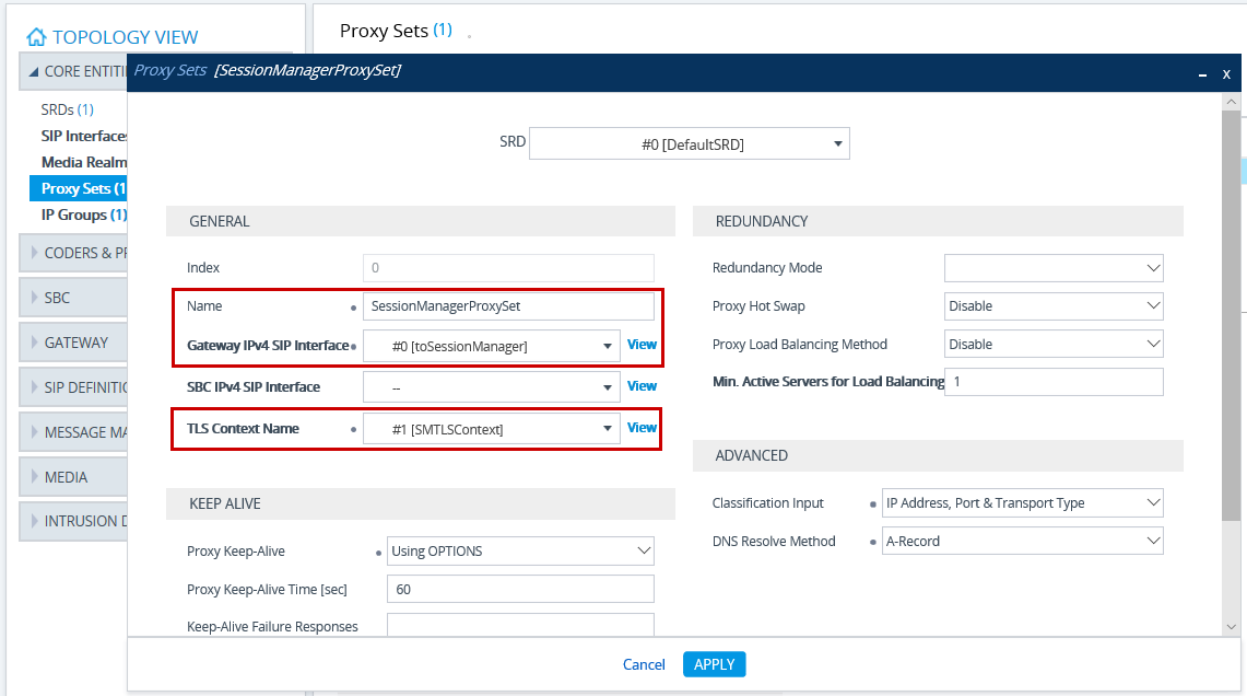


©2019 Avaya Inc. All Rights Reserved.

On the same page, **Proxy Table Set** and select **New** to add a new proxy set (not shown).

- Type in a **Name**
- Set **Gateway IPv4 SIP Interface** from **Section 7.7**
- Set **TLS Context Name** to the TLS Context from **Section 7.4**

Click **Apply** to save changes.



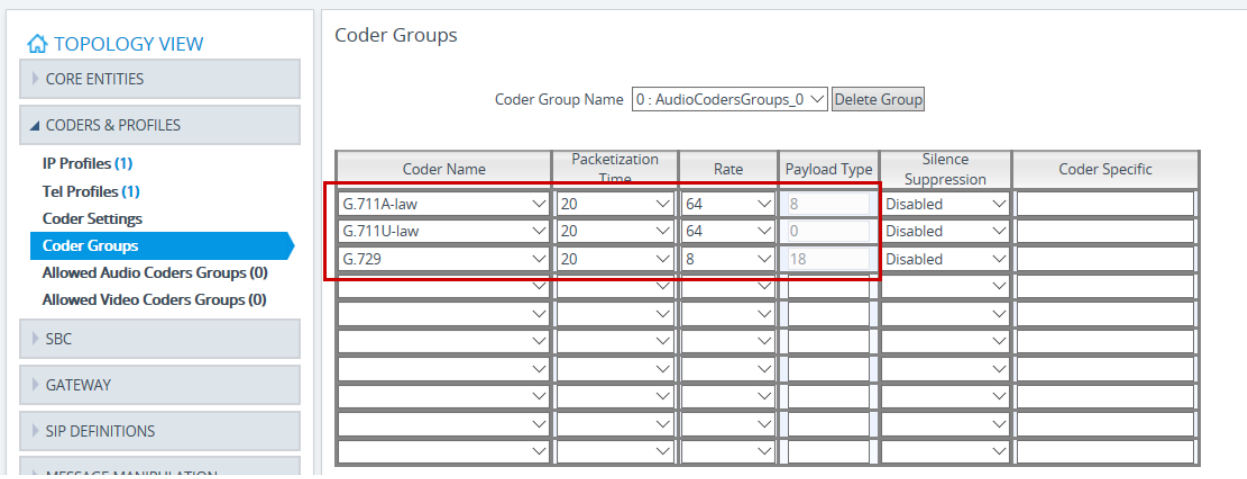
©2019 Avaya Inc. All Rights Reserved.

7.10. Administer Coders

On the left pane, Select **CODERS & PROFILES → Coders**

- Set coders as shown in the screen capture below

Note: Default value of **Packetization Time** is 20. When adding a coder, verify that **Packetization Time** value is **20**. Also, **Packetization Time** must match **Packet Size(ms)** value in **Section 5.3, 20**.



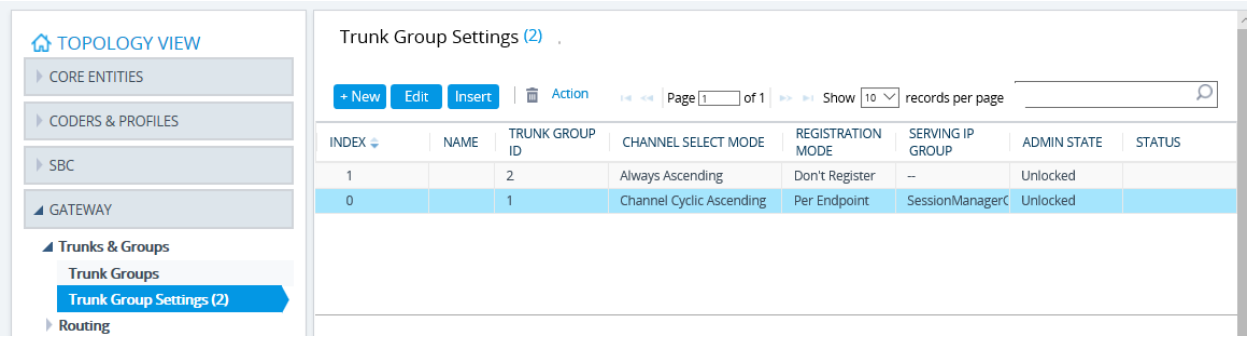
©2019 Avaya Inc. All Rights Reserved.

7.11. Administer Trunk Group Settings

On the left pane, select **Trunk Group Settings** and select **New.**

- Set **Trunk Group ID** to an available ID.
- 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.** If configuring FXO port, set to **Don't Register.**

Click **Apply** to save changes (not shown). Following was configured during the compliance test.



©2019 Avaya Inc. All Rights Reserved.

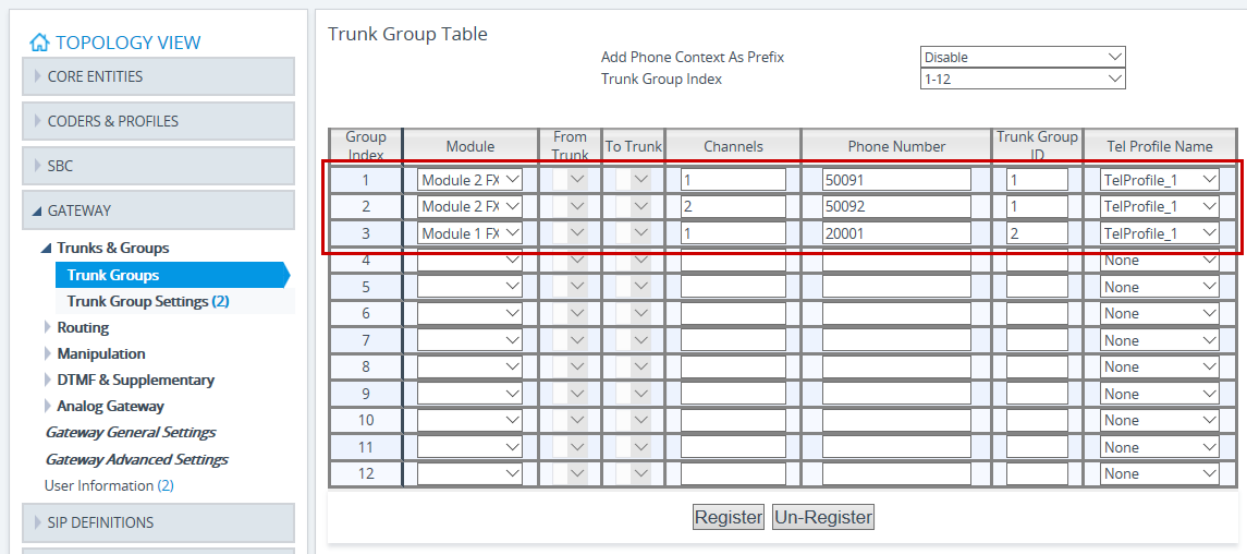
7.12. Administer Trunk Groups

On the left pane, navigate to **GATEWAY → Trunks & Groups → Trunk Groups**; for each line:

- Set **Channel** to a channel number, e.g. 1.
- Set **Phone Number** to the extension configured is Session Manager, **Section 6.6.**
- Set **Trunk Group ID** from previous section.
- Set **Tel Profile ID** to 0 for default Tel Profile.

Click **Submit** to save changes (not shown).
Note: All extension numbers entered in this screen for FXS 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 M1K DSP capacity is reduced by 25%.

Click on **Register** at the bottom of the screen (not shown) to register with Session Manager.



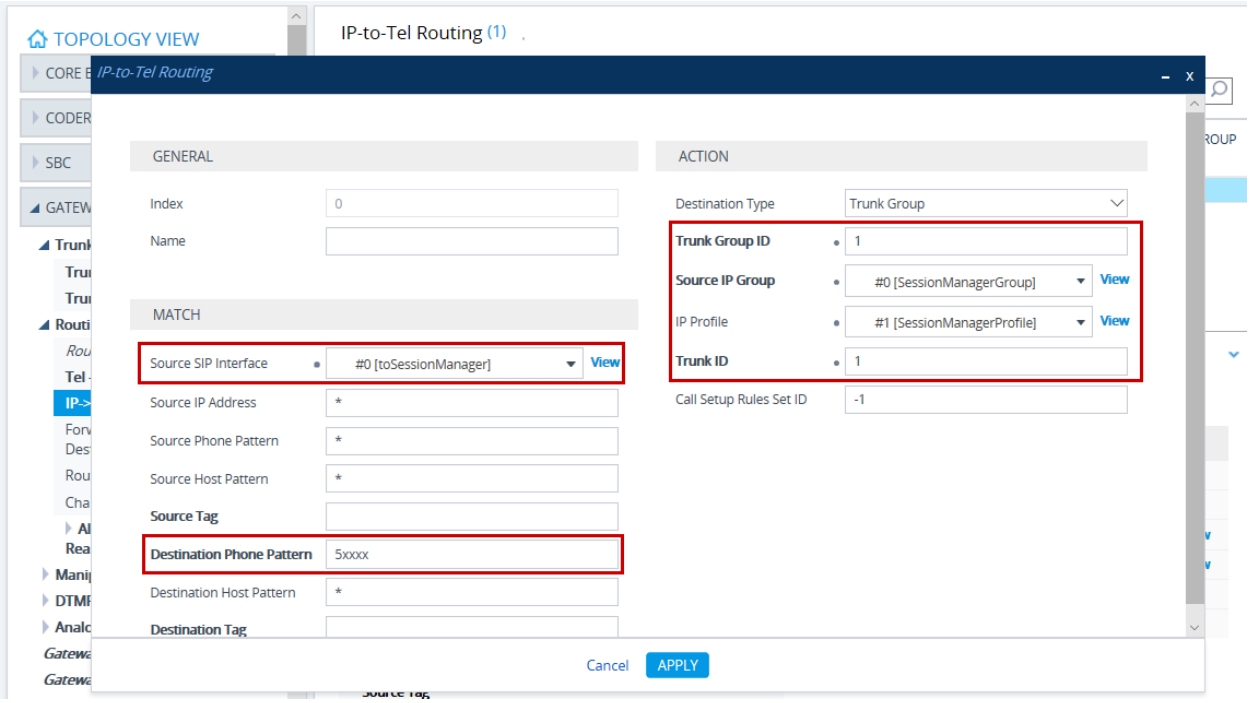
©2019 Avaya Inc. All Rights Reserved.

7.13. Administer IP to Tel Routing

On the left pane, select **GATEWAY → Routing → IP -> Tel Routing** and select **New** to add a new entry (not shown)

- Set **Source SIP Interface** from **Section 7.7**
- Set **Dest. Host Pattern, Source Host Pattern, Source Phone Pattern** and **Source IP Address** to *
- Set **Destination Phone Pattern** to the prefix of extensions, e.g. 5xxxx.
- Set **Trunk Group ID** and **Trunk ID** to ID configured in previous step for FXS, i.e. 1.
- Set **Source IP Group** and **IP Profile** to the ones configured for Session Manager.

Click **Submit** to save changes (not shown).



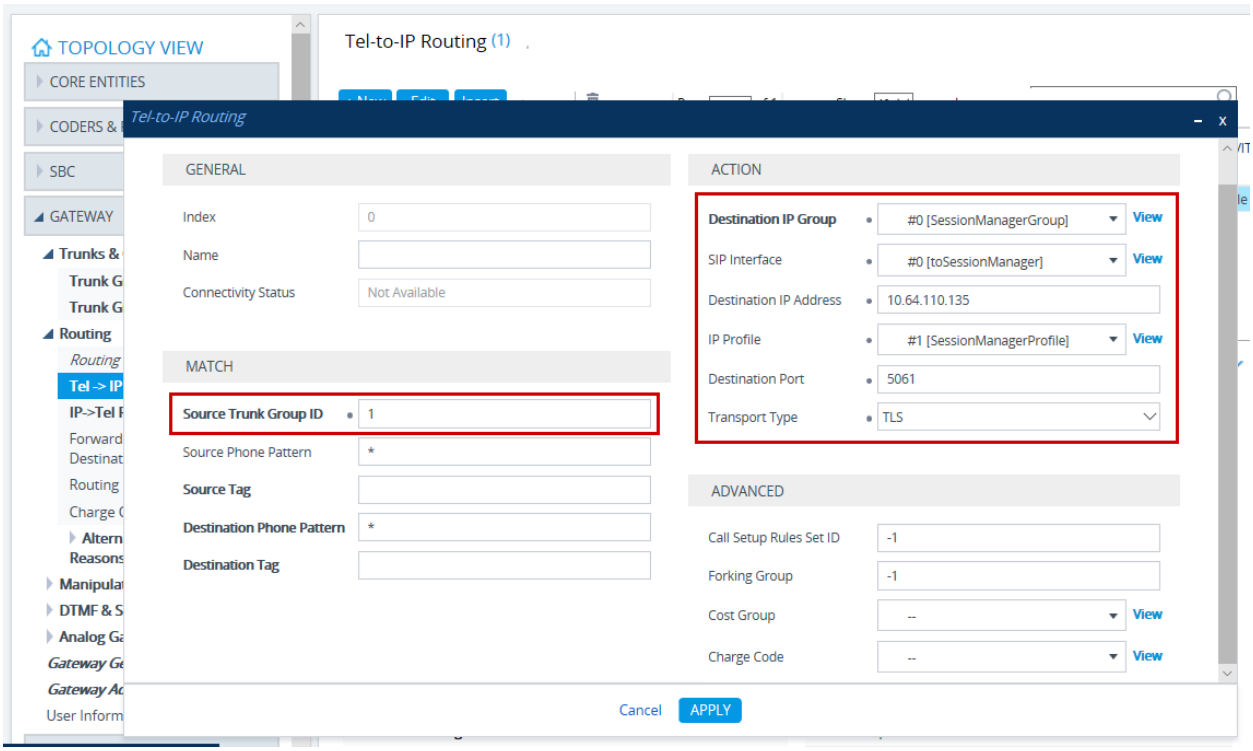
©2019 Avaya Inc. All Rights Reserved.

7.14. Administer TEL to IP Routing

On the left pane, select **GATEWAY → Routing → Tel -> IP Routing** and select **New** to add a new entry (not shown)

- Set **Source Trunk Group ID** from **Section 7.11** for FXS ports.
- Set **Source Phone Pattern** and **Destination Phone Pattern** to *
- Set **Destination IP Group, SIP Interface** and **IP Profile** that were configured for Session Manager.
- Set **Destination IP Address** to the SIP Entity IP Address of Session Manager
- Set **Destination Port** to **5061**
- Set **Transport Type** to **TLS**

Click **Apply** to save changes (not shown).



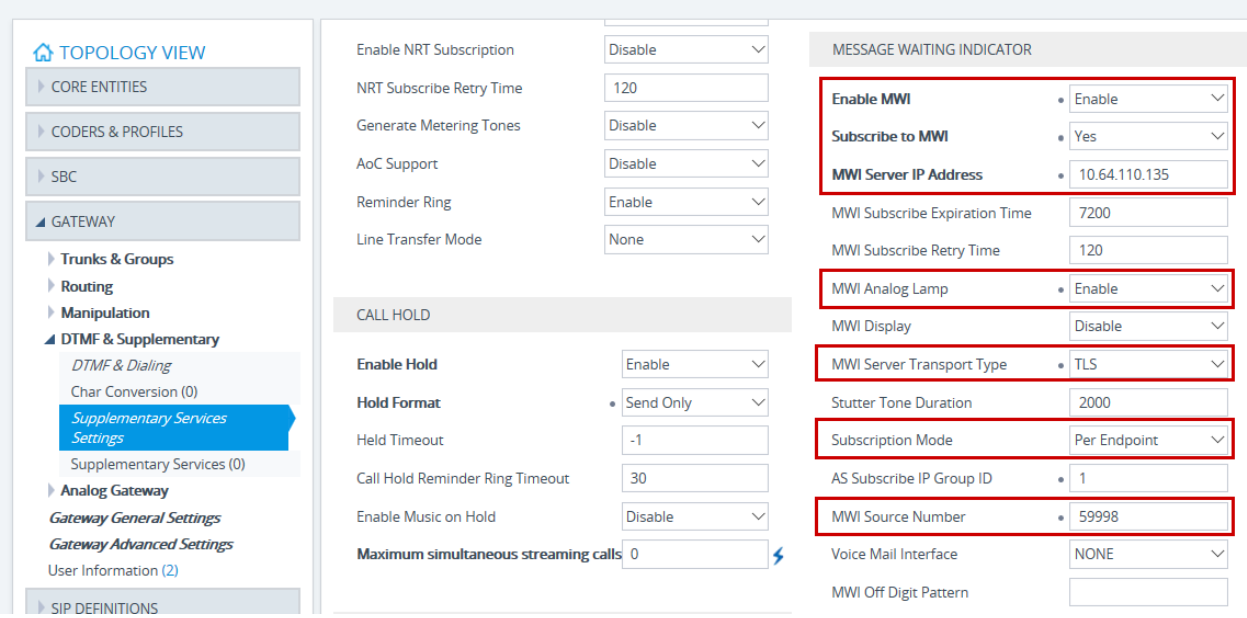
©2019 Avaya Inc. All Rights Reserved.

7.15. Administer Supplementary Services

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

- Under **MESSAGE WAITING INDICATOR:**
  - Set **Enable MWI** to **Enable**
  - Set **Subscribe to MWI** to **Yes**
  - For **MWI Server IP Address**, type in SIP Entity IP Address of Session Manager
  - Set **MWI Analog Lamp** to **Enable**
  - Set **MWI Server Transport Type** to **TLS**
  - Set **Subscription Mode** to **Per Endpoint**
  - Set **MWI Source Number** to the pilot number of the Voicemail system.

Click **Submit** to save changes



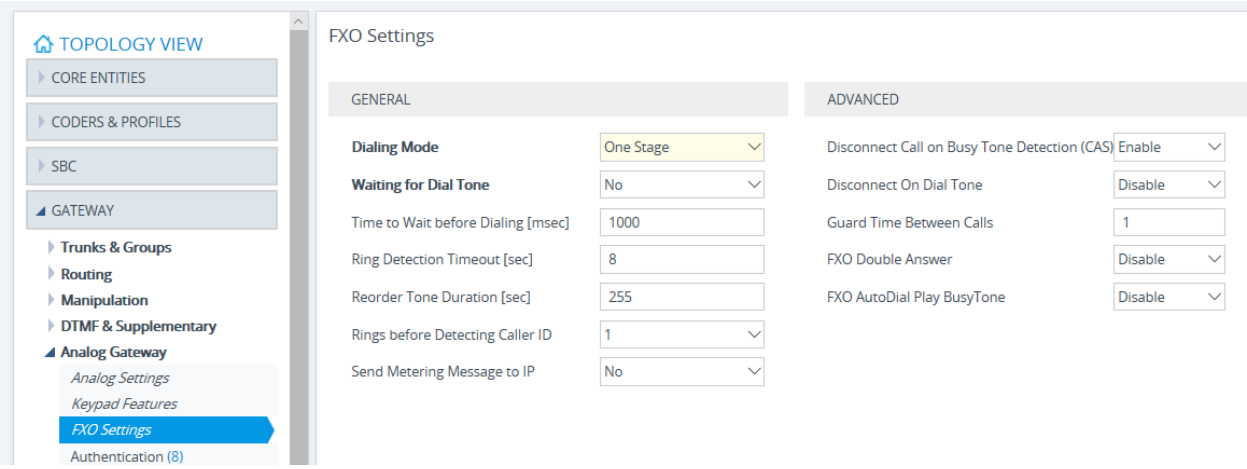
©2019 Avaya Inc. All Rights Reserved.

7.16. Administer FXO

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

- Set **Dialing Mode** to **One Stage**

Click **Apply** to save changes. Also, click **Save** at the top of the screen to save changes to the flash memory of AudioCodes M1K.



©2019 Avaya Inc. All Rights Reserved.

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 5.6**. Service State column should show **in-service/idle.**

```
status trunk 1                                                    Page   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
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
0001/013 T00013   in-service/idle    no
0001/014 T00014   in-service/idle    no
```


©2019 Avaya Inc. All Rights Reserved.

- Verify registration from AudioCodes M1K to Session Manager via the System Manager console, http://<ip-address/SMGR
- Navigate to **Elements → Session Manager → System Status → User Registration.** Verify the Users configured in **Section 6.6** for AudioCodes are Registered.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

Customize

View | Default | Export | Force Unregister | AST Device Notifications: | Reboot | Reload | Failback | As of 3:29 PM | Advanced Search

7 Items | Show All | Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
☐	Show	---	User 2	Polycom	---	---	☐	☐	0/1	☐	☐	☐	☐
☐	Show	---	User 1	Polycom	---	---	☐	☐	0/1	☐	☐	☐	☐
☐	Show	---	MP11x	User 1	---	---	☐	☐	0/1	☐	☐	☐	☐
☐	Show	50091@avaya.com	User 1	AudioCodes	DevConnect	10.64.10.171	☐	☐	1/1	☐	☑	☐	☐
☐	Show	50092@avaya.com	User 2	AudioCodes	DevConnect	10.64.10.171	☐	☐	1/1	☐	☑	☐	☐
☐	Show	51001@avaya.com	User 1	SIP	DevConnect	10.64.10.215	☐	☐	1/1	☑	☑ (AC)	☐	☐
☐	Show	51002@avaya.com	User 2	SIP	DevConnect	10.64.10.202	☐	☐	1/1	☑	☑ (AC)	☐	☐

Select : All, None

©2019 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for AudioCodes Mediant 1000 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 8.0.1, Issue 3, December 2018

[2] Administering Avaya Aura® Session Manager, Release 7.13, July 2018

Documentation related to AudioCodes Mediant 1000 can be obtained directly from AudioCodes.

©2019 Avaya Inc. All Rights Reserved.

A. Appendix

AudioCodes M1K .ini file generated after following the above instruction is as follows: Please use it only for reference purposes.

Note: Please note that password for registration will need to be changed if this ini file is loaded on an AudioCodes M1K device.

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

;Board: Mediant 1000
;Board Type: 47
;Serial Number: 3331682
;Slot Number: 1
;Software Version: 7.20A.204.222
;DSP Software Version: 204IM3=> 660.18
;Board IP Address: 10.64.10.171
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.10.1
;Ram size: 512M   Flash size: 64M
;Num of DSP Cores: 2  Num DSP Channels: 8
;Num of physical LAN ports: 3
;Profile: NONE
;;;Key features:;Board Type: Mediant 1000 ;PSTN Protocols: IUA=4
CAS ;E1Trunks=2 ;T1Trunks=2 ;FXSPorts=4 ;FXOPorts=4 ;Coders: G723 G729 GSM-FR
G727 ILBC SPEEX_WB OPUS_NB ;IP Media: VXML VoicePromptAnnounc(H248.9) ;Eth-
Port=3 ;DATA features: ;Channel Type: DspCh=240 IPMediaDspCh=240 ;DSP Voice
features: ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Control Protocols: MGCP MEGACO SIP SASurvivability
SBC=120 MSFT EMS SBC-SIGNALING=120 WebRTC ;Default features:;Coders: G711
G726;

;-----  HW components -----
;
; Slot # : Module type : # of ports : # of DSPs
;----------------------------------------------
;      1 : DAA_O       :          4 :         1
;      2 : FXS         :          4 :         1
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.64.10.203
EnableSyslog = 0
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'cli', 'ae'
```


©2019 Avaya Inc. All Rights Reserved.

```
DebugRecordingDestIP = 10.64.10.203
;VpFileLastUpdateTime is hidden but has non-default value
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '0.0.0.0'
OAMPDEFAULTNETWORKSOURCE = 1
;LastConfigChangeTime is hidden but has non-default value
DefaultPrimaryDnsServerIp = 10.64.110.100
DefaultSecondaryDnsServerIp = 75.75.75.75
SingleNetworkMode = 0
;TLSPkeyPassphrases is hidden but has non-default value
;LocalTimeZoneName is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
DisableICMPRedirects = 1
DisableICMPUnreachable = 1
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

RFC2833TxPayloadType = 101
EnableAnswerDetector = 1
EnableDSPIPMDetectors = 1
ENABLEMEDIASECURITY = 1
FarEndDisconnectSilenceMethod = 0

[WEB Params]

HTTPSCipherString = 'RC4:EXP'
Languages = 'en-US', '', '', '', '', '', '', '', '', ''

[SIP Params]

ENABLECALLERID = 1
MAXDIGITS = 5
ISPROXYUSED = 1
ISREGISTERNEEDED = 1
SIPDESTINATIONPORT = 5061
ISTWOSTAGEDIAL = 0
SECURECALLSFROMIP = 2
GWDEBUGLEVEL = 5
```


©2019 Avaya Inc. All Rights Reserved.

```
ENABLEEARLYMEDIA = 1
DEFAULTNUMBER = ''
PROXYNAME = 'avaya.com'
REGISTRARIP = '10.64.110.135'
SIPGATEWAYNAME = '10.64.110.135'
ALWAYSSENDTOPROXY = 1
PROXYREDUNDANCYMODE = 1
ENABLEDIGITDELIVERY = 1
ENABLEMWISUBSCRIPTION = 1
MWISERVERIP = '10.64.110.135'
MWIANALOGLAMP = 1
ENABLEMWI = 1
ENABLEDIGITDELIVERY2IP = 1
ISFAXUSED = 1
DigitPatternInternalCall = '51*'
DigitPatternExternalCall = '20*'
HOLDFORMAT = 1
SIPTRANSPORTTYPE = 2
REGISTRARNAME = 'avaya.com'
ENABLESIPS = 1
ENABLEUSERINFOUSAGE = 1
USESIPTGRP = 2
MEDIASECURITYBEHAVIOUR = 1
ENABLEHISTORYINFO = 1
ENABLEREASONHEADER = 0
ENABLE3WAYCONFERENCE = 1
ENABLESIPREMOTERESET = 1
MWISOURCENUMBER = '59998'
REGISTRARTRANSPORTTYPE = 2
MWISERVERTRANSPORTTYPE = 2
SOURCEIPADDRESSINPUT = 0
RELIABLECONNECTIONPERSISTENTMODE = 1
NOTIFICATIONIPGROUPID = 1
ASSUBSCRIBEIPGROUPID = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SIPT38VERSION = 0
TESTCALLID = '51002'
SendRejectOnOverload = 0
DISPLAYDEFAULTSIPPORT = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 2157969408
SBCSendTryingToSubscribe = 1
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_0_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
```


©2019 Avaya Inc. All Rights Reserved.

```
PhysicalPortsTable 2 = "GE_0_3", 1, 4, "User Port #2", "GROUP_2", "Active";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_0_1", "GE_0_2";
EtherGroupTable 1 = "GROUP_2", 1, "GE_0_3", "";
EtherGroupTable 2 = "GROUP_3", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName, DeviceTable_Tagging,
DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 1, 1500;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.64.10.171, 24, 10.64.10.1, "Voice",
10.64.110.100, 75.75.75.75, "vlan 1";

[ \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 ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
```


©2019 Avaya Inc. All Rights Reserved.

```
WebUsers 0 = "Admin",
"$1$NVYBUV1cDw9ZDgYOeHNxeyd9ciQtK3lzKH9/LmE0YDE1bG40aj1oOmxtaT1RVANXUFwFVA4NX
VxeXA9aExdKRUw=", 1, 0, 2, -1, 15, 60, 200,
"29a378d22a8c93b87bbc9a0d850e1b99", "";
WebUsers 1 = "User",
"$1$kKjw96alpvWkrq/+q6n//aaXxcDHkZTAnsuZkpvOyZfL1tWCgoXUjtbdgImIi9yMjvmg+vKi9
vai8fyr8/Wpr60=", 1, 0, 2, -1, 15, 60, 50,
"a82f7eab00082faa8732eed959b2212b", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 0, 0, "RC4:AES128", "DEFAULT", 0, 0, , , 2560, 0,
1024;
TLSContexts 1 = "SMTLSContext", 0, 0, "RC4:AES128", "DEFAULT", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 2048;

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode, IpProfile_VxxTransportType,
IpProfile_NSEMode, IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption, IpProfile_EnableHold,
IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName, IpProfile_MediaIPVersionPreference,
IpProfile_TranscodingMode, IpProfile_SBCAllowedMediaTypes,
IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
```


©2019 Avaya Inc. All Rights Reserved.

```
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior,
IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection, IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute, IpProfile_SBCRemoveCryptoLifetimeInSDP,
IpProfile_SBCIceMode, IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW, IpProfile_CreatedByRoutingServer,
IpProfile_SBCFaxReroutingMode, IpProfile_SBCMaxCallDuration,
IpProfile_SBCGenerateRTP, IpProfile_SBCISUPBodyHandling,
IpProfile_SBCISUPVariant, IpProfile_SBCVoiceQualityEnhancement,
IpProfile_SBCMaxOpusBW, IpProfile_SBCEnhancedPlc,
IpProfile_LocalRingbackTone, IpProfile_LocalHeldTone,
IpProfile_SBCGenerateNoOp, IpProfile_SBCRemoveUnKnownCrypto;
IpProfile 1 = "SessionManagerProfile", 1, "AudioCodersGroups_0", 1, 10, 10,
46, 24, 0, 0, 2, 0, 0, 1, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 1, 3, 0, 0, 0, 0, 0, 8, 300, 400, 0,
0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 250, -1, -1, 0, 0, 0, 0, 0,
0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_RemoteIPv4IF, CpMediaRealm_RemoteIPv6IF,
CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
```


©2019 Avaya Inc. All Rights Reserved.

```
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile,
CpMediaRealm_BWProfile, CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "DefaultRealm", "Voice", "", "", "", 6000, 330, 9299, 1, "",
"", 0;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 1, "";

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName, SRD_AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "", "";

[ \SRD ]


[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -1, 1,
"", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_AdditionalUDPPortsMode,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
```


©2019 Avaya Inc. All Rights Reserved.

```
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName, SIPInterface_AdmissionProfile,
SIPInterface_CallSetupRulesSetId;
SIPInterface 0 = "toSessionManager", "Voice", 0, 5060, 5060, 5061, "", 0,
"DefaultSRD", "", "SMTLSContext", 0, 1, 500, -1, 0, "DefaultRealm", 1, -1, -
1, -1, 1, 0, "", "", -1;

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName, ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRDName, ProxySet_ClassificationInput,
ProxySet_TLSContextName, ProxySet_ProxyRedundancyMode,
ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp,
ProxySet_GWIPv4SIPInterfaceName, ProxySet_SBCIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_MinActiveServersLB, ProxySet_SuccessDetectionRetries,
ProxySet_SuccessDetectionInterval, ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "SessionManagerProxySet", 1, 60, 0, 0, "DefaultSRD", 1,
"SMTLSContext", -1, 0, "", "toSessionManager", "", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput, IPGroup_DestUriInput,
IPGroup_ContactName, IPGroup_Username, IPGroup_Password, IPGroup_UUIFormat,
IPGroup_QOEProfile, IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr,
IPGroup_MsgManUserDef1, IPGroup_MsgManUserDef2, IPGroup_SIPConnect,
IPGroup_SBCPSAPMode, IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment, IPGroup_AdmissionProfile,
IPGroup_ProxyKeepAliveUsingIPG;
IPGroup 0 = 0, "SessionManagerGroup", "SessionManagerProxySet", "avaya.com",
"", -1, 0, "DefaultSRD", "DefaultRealm", 1, "SessionManagerProfile", -1, -1,
-1, 0, 0, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0,
0, "", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 1;

[ \IPGroup ]
```


©2019 Avaya Inc. All Rights Reserved.

```
[ PREFIX ]

FORMAT PREFIX_Index = PREFIX_RouteName, PREFIX_DestinationPrefix,
PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileName,
PREFIX_MeteringCodeName, PREFIX_DestPort, PREFIX_DestIPGroupName,
PREFIX_TransportType, PREFIX_SrcTrunkGroupID, PREFIX_DestSIPInterfaceName,
PREFIX_CostGroup, PREFIX_ForkingGroup, PREFIX_CallSetupRulesSetId,
PREFIX_ConnectivityStatus, PREFIX_DestTags, PREFIX_SrcTags;
PREFIX 0 = "", "5xxxx", "10.64.110.135", "*", "SessionManagerProfile", "",
5061, "SessionManagerGroup", 2, 1, "toSessionManager", "", -1, -1, "Not
Available", "", "";

[ \PREFIX ]


[ TelProfile ]

FORMAT TelProfile_Index = TelProfile_ProfileName, TelProfile_TelPreference,
TelProfile_CodersGroupName, TelProfile_IsFaxUsed,
TelProfile_JitterBufMinDelay, TelProfile_JitterBufOptFactor,
TelProfile_IPDiffServ, TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC, TelProfile_MWIAnalog,
TelProfile_MWIDisplay, TelProfile_FlashHookPeriod,
TelProfile_EnableEarlyMedia, TelProfile_ProgressIndicator2IP,
TelProfile_TimeForReorderTone, TelProfile_EnableDIDWink,
TelProfile_IsTwoStageDial, TelProfile_DisconnectOnBusyTone,
TelProfile_EnableVoiceMailDelay, TelProfile_DialPlanIndex,
TelProfile_Enable911PSAP, TelProfile_SwapTelToIpPhoneNumbers,
TelProfile_EnableAGC, TelProfile_ECNlpMode, TelProfile_DigitalCutThrough,
TelProfile_EnableFXODoubleAnswer, TelProfile_CallPriorityMode,
TelProfile_FXORingTimeout, TelProfile_JitterBufMaxDelay,
TelProfile_IP2TelCutThroughCallBehavior, TelProfile_PlayBusyTone2Isdn,
TelProfile_MWINotificationTimeout;
TelProfile 1 = "TelProfile_1", 1, "AudioCodersGroups_0", 1, 10, 10, 46, 24, -
11, 0, 0, 0, 0, 0, 1, 1, 1, 700, 0, -1, 255, 0, 1, 1, 1, -1, 0, 0, 0, 0, 0,
0, 0, 0, 250, 0, 0, 0;

[ \TelProfile ]


[ TrunkGroup ]

FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileName, TrunkGroup_LastTrunkId,
TrunkGroup_Module;
TrunkGroup 0 = 1, 255, 1, 1, "50091", "TelProfile_1", 255, 2;
TrunkGroup 1 = 1, 255, 2, 2, "50092", "TelProfile_1", 255, 2;
TrunkGroup 2 = 2, 255, 1, 1, "20001", "TelProfile_1", 255, 1;

[ \TrunkGroup ]


[ PstnPrefix ]
```


©2019 Avaya Inc. All Rights Reserved.

```
FORMAT PstnPrefix_Index = PstnPrefix_RouteName, PstnPrefix_DestPrefix,
PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress,
PstnPrefix_ProfileName, PstnPrefix_SrcIPGroupName, PstnPrefix_DestHostPrefix,
PstnPrefix_SrcHostPrefix, PstnPrefix_SrcSIPInterfaceName, PstnPrefix_TrunkId,
PstnPrefix_CallSetupRulesSetId, PstnPrefix_DestType, PstnPrefix_DestTags,
PstnPrefix_SrcTags;
PstnPrefix 0 = "", "5*", 1, "*", "*", "SessionManagerProfile",
"SessionManagerGroup", "*", "*", "toSessionManager", 1, -1, 0, "", "";

[ \PstnPrefix ]


[ Dns2Ip ]

FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress,
Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress;
Dns2Ip 0 = "avaya.com", 10.64.110.135, 0.0.0.0, 0.0.0.0;

[ \Dns2Ip ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_Priority, ProxyIp_Weight;
ProxyIp 0 = "0", 0, "10.64.110.135", 2, 1, 1;

[ \ProxyIp ]


[ TrunkGroupSettings ]

FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,
TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode,
TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser,
TrunkGroupSettings_ServingIPGroupName,
TrunkGroupSettings_MWIInterrogationType, TrunkGroupSettings_TrunkGroupName,
TrunkGroupSettings_UsedByRoutingServer, TrunkGroupSettings_AdminState;
TrunkGroupSettings 0 = 1, 1, 0, "avaya.com", "", "SessionManagerGroup", 3,
"", 0, 0;
TrunkGroupSettings 1 = 2, 2, 4, "", "20001", "", 255, "", 0, 0;

[ \TrunkGroupSettings ]


[ EnableCallerId ]

FORMAT EnableCallerId_Index = EnableCallerId_IsEnabled,
EnableCallerId_Module, EnableCallerId_Port, EnableCallerId_PortType;
EnableCallerId 4 = 1, 2, 1, "FXS";
EnableCallerId 5 = 1, 2, 2, "FXS";

[ \EnableCallerId ]
```


©2019 Avaya Inc. All Rights Reserved.

```
[ Authentication ]

FORMAT Authentication_Index = Authentication_UserId,
Authentication_UserPassword, Authentication_Module, Authentication_Port,
Authentication_PortType;
Authentication 4 = "50091", "$1$tIWHhYONjw==", 2, 1, "FXS";
Authentication 5 = "50092", "$1$tIWHhYONjw==", 2, 2, "FXS";

[ \Authentication ]


[ CodersGroup0 ]

;
;  *** TABLE CodersGroup0 ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \CodersGroup0 ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 1, "";

[ \GwRoutingPolicy ]


[ 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 ]
```


©2019 Avaya Inc. All Rights Reserved.

```
[ GWUserInfoTable ]

FORMAT GWUserInfoTable_Index = GWUserInfoTable_PBXExtension,
GWUserInfoTable_GlobalPhoneNumber, GWUserInfoTable_DisplayName,
GWUserInfoTable_Username, GWUserInfoTable_Password;
GWUserInfoTable 0 = "50091", "50091", "AudioCodes User 1", "50091",
"$1$tIWHhYONjw==";
GWUserInfoTable 1 = "50092", "50092", "AudioCodes User 2", "50092",
"$1$tIWHhYONjw==";

[ \GWUserInfoTable ]


[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix 'sip-
scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix 'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix 'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix 'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix 'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content prefix
'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content prefix
'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content prefix
'siparmyknife'";

[ \MaliciousSignatureDB ]


[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 2, 2, 90, -1, 0, "";
AudioCoders 2 = "AudioCodersGroups_0", 2, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]
```


©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.