



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Session Manager and Avaya Aura® Communication Manager with AudioCodes Mediant 3000 Gateway for T1 access – Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunking along with T1 access to a simulated PSTN.

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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	5
3.	Reference Configuration.....	6
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager.....	7
5.1.	Verify Avaya Aura® Communication Manager License.....	8
5.2.	Administer System Parameters Features.....	9
5.3.	Administer IP Node Names.....	10
5.4.	Administer IP Network Region and Codec Set.....	11
5.5.	Administer SIP Trunks with Avaya Aura® Session Manager	13
5.5.1.	Add SIP Signaling Group.....	13
5.5.2.	Add Trunk Group.....	14
5.6.	Configure Route Patterns	15
5.6.1.	Route Pattern for reaching Session Manager and Simulated PSTN Endpoints.....	15
5.7.	Administer Private Numbering	16
5.8.	Administer Dial Plan and AAR analysis	17
5.9.	Administer AAR Analysis	17
5.10.	Administer Feature Access Code.....	18
5.11.	Save Changes.....	18
6.	Configure Avaya Aura® Session Manager.....	19
6.1.	Specify SIP Domain	20
6.2.	Add Locations	21
6.3.	Add SIP Entities and SIP Entity Links	22
6.3.1.	Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link	22
6.3.2.	Adding AudioCodes Mediant 3000 Gateway SIP Entity.....	24
6.4.	Add Routing Policies.....	25
6.5.	Add Dial Patterns	27
7.	AudioCodes Mediant 3000 Configuration.....	29
7.1.	Log Into Mediant 3000.....	29
7.2.	Configure Media Gateway IP Network Parameters	31
7.3.	Saving Configuration and Resetting Mediant 3000	32
7.4.	Saving Configuration	32
7.5.	Configure SIP Interface to Avaya Aura® Session Manager	34
7.5.1.	Configure SIP Interface Table	34
7.5.2.	Configure Proxy Sets Table.....	35
7.5.3.	Configure IP Group Table.....	36
7.5.4.	Configure General Parameters.....	37
7.5.5.	Configure Proxy & Registration	38
7.5.6.	Configure the Voice parameters	38

7.5.7.	Configure Media Security	39
7.5.8.	Configure Coders	40
7.6.	Configure T1 Interface to Simulated PSTN	41
7.6.1.	Configure Trunk Settings.....	41
7.6.2.	Configure TDM Bus.....	42
7.6.3.	Configure Digital PCM Settings	42
7.6.4.	Configure Trunk Group Table.....	43
7.6.5.	Configure Trunk Group Settings	44
7.7.	Configure Routing.....	45
7.7.1.	Configure IP to Trunk Group Routing Rules	45
7.7.2.	Configure Outbound IP Routing Rules.....	47
7.8.	Configure Supplementary Services Parameters	48
7.9.	Configure Syslog Parameters for Debug Assistance.....	49
7.10.	Configure Certificates.....	50
8.	Verification Steps	54
8.1.	Verify Avaya Aura® Communication Manager Trunk Status.....	54
8.2.	SIP Monitoring on Avaya Aura® Session Manager.....	55
8.3.	Utilizing Mediant 3000 Web Interface to Observe Status	56
8.3.1.	Device Status	56
8.3.2.	Device Information	57
8.3.3.	Trunks and Channels Status	58
8.3.4.	Proxy Sets Status.....	58
9.	Conclusion	59
10.	Additional References.....	59
11.	Appendix.....	60

1. Introduction

These Application Notes describe the procedure for configuring the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager) using SIP trunking along with T1 access to a simulated PSTN.

These Application Notes present a sample configuration for an enterprise network consisting of Session Manager and Communication Manager, integrated with an AudioCodes Mediant 3000 Gateway using SIP and providing T1 access to a simulated PSTN. The AudioCodes Mediant 3000 is a feature-rich, highly available VoIP gateway supporting low to medium channel densities. The AudioCodes Mediant 3000 compact footprint (2U) allows high capacity and High Availability (HA) when business critical contact centers require such resilience. The AudioCodes Mediant 3000 has comprehensive PSTN access capabilities as well as SIP to SIP interworking features that enable the interconnection between enterprises and service providers. In addition to E1/T1 interfaces, the AudioCodes Mediant 3000 supports high-density PSTN interfaces, such as T3, STM-1 and OC3 to provide the enterprise with lower PSTN lease costs. The proven interoperability of the AudioCodes Mediant 3000 with different PBXs and PSTN switches facilitates smooth deployment. Even though the Mediant 3000 supports a variety of different protocols and features, only SIP and T1 access were verified in this compliance test. Note that AudioCodes Media 3000, at places, is referred as M3K in this document.

2. General Test Approach and Test Results

The general test approach was to make calls, verify codecs, and exercise common PBX features, between endpoints located in the enterprise and the simulated PSTN.

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 Mediant 3000 used TLS and SRTP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability. The feature testing focused on verifying the following:

- Simulated PSTN calls from and to Avaya endpoints
- Calling with various Avaya Deskphone models
- Support for G.711A, G.711MU and G.729 codecs
- SIP transport using UDP and TCP
- Codec negotiation
- Telephony supplementary features, such as Hold, Call Transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval
- Direct IP-to-IP Media (also known as “Shuffling”) over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the AudioCodes Mediant 3000 Gateway and release media processing resources on the Avaya Media Gateway

2.2. Test Results

The AudioCodes Mediant 3000 passed compliance testing.

2.3. Support

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

3. Reference Configuration

As shown in **Figure 1**, the Avaya enterprise network uses SIP trunking for call signaling internally, and with the Mediant 3000 Gateway in order to access the simulated PSTN. The Mediant 3000 is managed by using the web interface. Session Manager, with its SM-100 (Security Module) network interface, routes calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. Session Manager supports flexible inter-system call routing based on the dialed number, the calling number and the system location; it can also provide protocol adaptation to allow multi-vendor systems to interoperate. Session Manager is managed by Avaya Aura® System Manager via the management network interface.

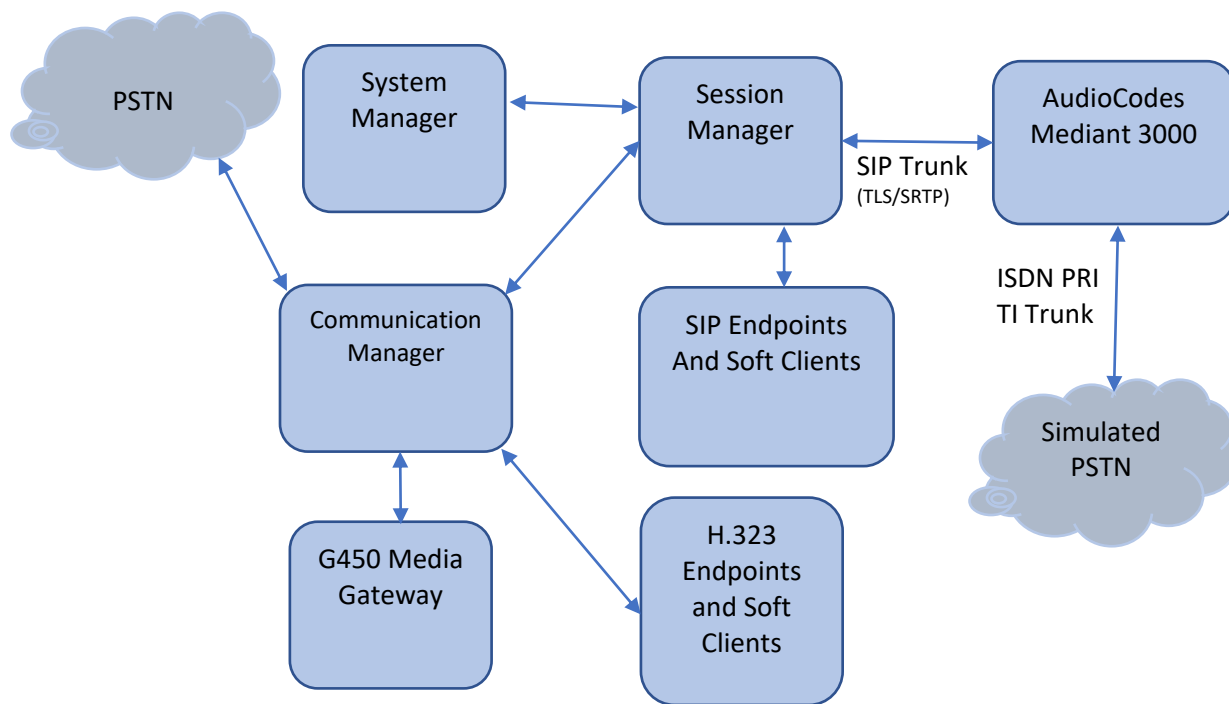


Figure 1: Compliance Test Reference Configuration

For the sample configuration shown in **Figure 1**, Session Manager, System Manager, Communication Manager, and Media Server all run in a virtual environment. These Application Notes focus on the configuration of the SIP trunks and call routing.

4. Equipment and Software Validated

The following equipment and software/firmware 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 3000	7.00A.132

5. Configure Avaya Aura® Communication Manager

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with **Reference [1]**. The procedures include the following areas:

- Verify Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Administer ARS analysis
- Administer Feature Access Codes
- Save Changes

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to verify, on **Page 2**, whether the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

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:	18000	6	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	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:	18000	2	
Maximum Administered SIP Trunks:	12000	10	
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	522	0	

5.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

5.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, the processor Ethernet interface **procr** and **10.64.110.131** are entered as **Name** and **IP Address** for the signaling in Communication Manager running in a virtual environment. In addition, **sm8** and **10.64.110.135** are entered for Session Manager.

```
change node-names ip
```

		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
aes8	10.64.110.132			
ams8	10.64.110.136			
default	0.0.0.0			
procr	10.64.110.131			
procr6	::			
sm8	10.64.110.135			

```
( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number, to configure the network region being used. In the sample network ip-network-region **1** is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1          NR Group: 1
    Location: 1        Authoritative Domain: avaya.com
    Name:              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? 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
    Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The codecs used in the compliance test are shown here. Configure the IP Codec Set as shown in the screen below. Note that in order to configure SRTP, “Media Encryption” will need to be enabled. Please refer to documentation in **Section 10** for additional information.

Retain the default values for the remaining fields.

```
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:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: 3-srtp-aescm128-hmac80-unauth
4: 4-srtp-aescm128-hmac32-unauth
```

5.5. Administer SIP Trunks with Avaya Aura® Session Manager

In the test configuration, a SIP trunk was configured between Communication Manager and Session Manager for enterprise calling between Communication Manager and Session Manager registered endpoints. Additionally, a SIP trunk was configured between Session Manager and the Mediant 3000 in order to communicate between the enterprise and the simulated PSTN. To administer a SIP Trunk on Communication Manager, two steps are required: the creation of a signaling group and a trunk group.

5.5.1. Add SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** sip
- **Transport Method:** tls
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **Section 5.3**
i.e., sm8
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Network Region:** 1
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

```
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? y
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? 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:
                                     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): 65                IP Audio Hairpinning? n
Enable Layer 3 Test? y                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                Alternate Route Timer(sec): 6
```

5.5.2. Add Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** **sip**
- **Group Name:** A descriptive name (i.e., **sm8**)
- **TAC:** An available trunk access code (i.e., **101**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group associated (i.e., **1**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from license verified in **Section 5.1**)

```
add 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? n
  Dial Access? n                               Night Service:
  Queue Length: 0
  Service Type: tie                             Auth Code? n
                                              Member Assignment Method: auto
                                              Signaling Group: 1
                                              Number of Members: 10
```

Navigate to **Page 3** and change **Numbering Format** to **private**. Use default values for all other fields.

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

  Numbering Format: private
                                              UI Treatment: service-provider
                                              Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n
                                              Hold/Unhold Notifications? Y
  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

5.6. Configure Route Patterns

Configure route patterns to correspond to the newly added SIP trunk group. Use the **change route pattern n** command, where **n** is an available route pattern.

The route pattern, as shown below, was configured to route calls to Session Manager and simulated PSTN endpoints.

5.6.1. Route Pattern for reaching Session Manager and Simulated PSTN Endpoints

When changing the route pattern, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name (i.e., **asm**)
- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive
- **Numbering Format:** This was set to **lev0-pvt** in the tested configuration

change route-pattern 1															Page 1 of 3	
Pattern Number: 1 Pattern Name: asm																
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																
1: 1 0 Dgts Intw																
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																

5.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a **5**-digit extension (**Ext Len**) beginning with **5** (**Ext Code**) and routed through any trunk will result in a **5**-digit calling number (**Total Len**). The calling party number will be in the SIP “From” header.

change private-numbering 0					Page	1 of	2
NUMBERING - PRIVATE FORMAT							
Ext	Ext	Trk	Private	Total			
Len	Code	Grp(s)	Prefix	Len			
5	5			5	Total Administered: 2		

Similarly, add the same entry in public numbering table using **change public-unknown-numbering** command .

5.8. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with **5** to stations registered with Session Manager.

Use the **change aar analysis n** command, where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 5** (Extensions on Session Manager) to use **Route Pattern 1** (defined in Section 5.6). The **Call Type** was set to **lev0**.

change aar analysis 5						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 2	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Req'd	
5	5	5	1	lev0		n	

5.9. Administer AAR Analysis

For simulated calls, call dialed to a 5 digit number starting with 53 was routed to PSTN via AudioCodes Mediant 3000. Use the **change aar analysis 53** command and add an entry to specify how to route calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed digits to match on **53**
- **Total Min:** Minimum number of digits, in this case **5**
- **Total Max:** Maximum number of digits, in this case **5**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e., **1**
- **Call Type:** **aar**

Note: The additional entries may be added for different number destinations.

change aar analysis 53						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	
53	5	5	1	aar		n	

5.10. Administer Feature Access Code

Configure a feature access code to use for AAR and ARS routing. Use the **change feature access code** command to define **Access Code** for **Auto Alternate Routing (AAR)** and for **Auto Route Selection (ARS)**. In the test configuration, **8** and **9** were used respectively.

```
change feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9    Access Code 2:
Automatic Callback Activation:                    Deactivation:
```

5.11. Save Changes

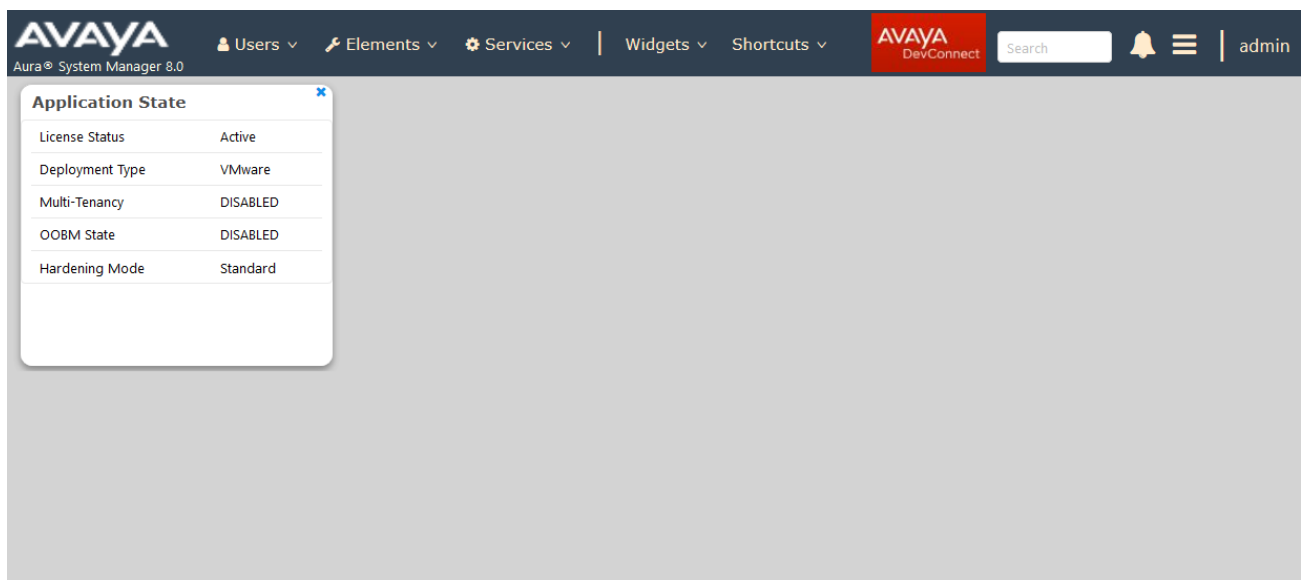
Use the **save translation** command to save all changes.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in **Reference [2]**. The procedures include adding the following items:

- Specify SIP Domain
- Add Locations
- Add Adaptations
- Add SIP Entities and Entity Links
- Add Routing Policies
- Add Dial Patterns
- Add Users for SIP Phones

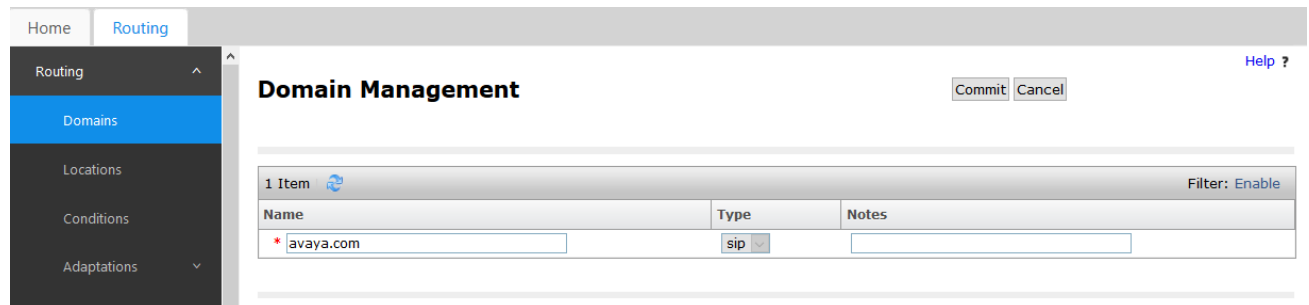
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The home screen as shown below is displayed. Expand the **Routing** Link under **Elements**.



6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Elements** → **Routing** → **Domains** and clicking the **New** button on the right (not shown). The following screen will then be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name (e.g., **avaya.com**)
- **Type** Select **sip**
- **Notes:** Descriptive text (optional)



The screenshot shows a web interface for "Domain Management". On the left is a sidebar with a "Routing" menu expanded, showing "Domains" selected. The main area has a header with "Domain Management", "Commit", "Cancel", and "Help ?" buttons. Below the header is a table with 1 item. The table has columns for Name, Type, and Notes. The first row shows "avaya.com" as the Name, "sip" as the Type, and an empty Notes field.

Name	Type	Notes
* avaya.com	sip	

6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. A single location is added to the configuration for Communication Manager and the Mediant 3000 Gateway. To add a location, select **Locations** on the left and click on the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

Under **General**:

- **Name:** A descriptive name

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location (optional). In these Application Notes, no pattern was defined.

Defaults can be used for the remaining fields. The screen below shows addition of the **DevConnect** location, which includes all the components of the compliance test environment. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The left sidebar shows a tree view with 'Routing' selected, and 'Locations' highlighted under the 'Routing' category. The main content area is titled 'Location Details' and contains two sections: 'General' and 'Location Pattern'. In the 'General' section, the 'Name' field is populated with 'DevConnect', and the 'Notes' field is empty. In the 'Location Pattern' section, there is an 'Add' button and a 'Remove' button. Below these, a table lists the patterns. The table has two columns: 'IP Address Pattern' and 'Notes'. The first row shows a checkbox, the pattern '*10.64.*', and an empty notes field. At the bottom of the table, there is a 'Select : All, None' option. The form has 'Commit' and 'Cancel' buttons at the top right and bottom right.

Location Pattern	
1 Item	
<input type="checkbox"/>	*10.64.*

6.3. Add SIP Entities and SIP Entity Links

A SIP Entity is required for each SIP-based telephony system wishing to communicate with Session Manager for call routing. In the sample configuration, a SIP Entity and SIP Entity Link is added for Communication Manager, and the Mediant 3000.

6.3.1. Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link

Select **SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **cm8**
- **FQDN or IP Address:** IP address of the Communication Manager i.e., **10.64.110.131**
- **Type:** Select **CM**
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity

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
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Communication Manager.

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

AVAYA

DevConnect

Search

adm

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

SIP Entity Details

Commit

Cancel

Help ?

General

* Name:

cm8

* FQDN or IP Address:

10.64.110.131

Type:

CM

Notes:

Adaptation:

Location:

DevConnect

Time Zone:

America/Denver

* SIP Timer B/F (in seconds):

4

Minimum TLS Version:

Use Global Setting

Credential name:

Securable:

Call Detail Recording:

none

Entity Links

Override Port & Transport with DNS SRV:

Add

Remove

1 Item

Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sm8_cm8_5061_TLS	sm8	TLS	* 5061	cm8	* 5061	trusted	<input type="checkbox"/>

Select : All, None

6.3.2. Adding AudioCodes Mediant 3000 Gateway SIP Entity

Select **SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **m3k**
- **FQDN or IP Address:** IP address of the Mediant 3000 i.e., **10.64.50.199**
- **Type:** Select **SIP Trunk**

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
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Mediant 3000.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ AVAYA DevConnect Search 🔍 🔔 ☰ | admin

Home Routing

SIP Entity Details Commit Cancel

General

* Name: m3k

* FQDN or IP Address: 10.64.50.199

Type: SIP Trunk ▾

Notes:

Adaptation: ▾

Location: DevConnect ▾

Time Zone: America/Denver ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: egress ▾

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item 🔁 Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sm8_m3k_5061_TLS	sm8 ▾	TLS ▾	* 5061	m3k ▾	* 5061	trusted ▾	<input type="checkbox"/>

Select : All, None

6.4. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 6.3**. A routing policy must be added for Communication Manager and the Mediant 3000 Gateway. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under **General**

- Enter a descriptive **Name**

Under **SIP Entity as Destination**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day**:

- Click **Add**, and select the time range configured. In these Application Notes, the predefined **24/7 Time Range** is used

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and the Mediant 3000.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a tree view with 'Routing' selected, and 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section has input fields for 'Name' (cm8), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with columns 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The 'Time of Day' section has buttons for 'Add', 'Remove', and 'View Gaps/Overlaps'.

Name	FQDN or IP Address	Type	Notes
cm8	10.64.110.131	CM	

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

AVAYA

DevConnect

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

m3k

Disabled:

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
m3k	10.64.50.199	SIP Trunk	

Time of Day

6.5. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration numbers beginning with **5** with 5-digit length reside in the Enterprise network. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager.

Under **General**:

- **Pattern:** Dialed number or prefix i.e., **5**
- **Min:** Minimum length of dialed number i.e., **5**
- **Max:** Maximum length of dialed number i.e., **5**
- **SIP Domain:** Select **ALL**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

The following screen shows the dial pattern definition for calls within the Enterprise.

AVAYA Aura® System Manager 8.0 | Users | Elements | Services | Widgets | Shortcuts | AVAYA DevConnect | Search | Help ?

Home | **Routing**

Dial Pattern Details [Commit] [Cancel]

General

* **Pattern:** 5

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect		cm8	0	<input type="checkbox"/>	cm8	

Select : All, None

The following screen shows the dial pattern definition for calls destined for the Mediant 3000. Calls starting with 53 and 5 digits long were routed to Mediant 3000.

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

AVAYA

DevConnect

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern:

7

* Min:

5

* Max:

5

Emergency Call:

☐

SIP Domain:

-ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		m3k	0	<input type="checkbox"/>	m3k	

Select : All, None

7. AudioCodes Mediant 3000 Configuration

This section describes the configuration for enabling the Mediant 3000 to interoperate with Session Manager and Simulated PSTN.


The Mediant 3000 can be administered using the Native Web Interface or AudioCodes Element Management System (EMS) as described in **Reference [3]**. Note that this section displays the provisioning that was utilized for this sample configuration, and does not show exhaustive procedures for administering an initial configuration. In these Application Notes, configuration was accomplished with the web interface.

7.1. Log Into Mediant 3000

The configuration of the Mediant 3000 Gateway is done via a Web browser. To access the device, enter the **IP address** of the Mediant 3000 in the **Address** field of the web browser. The IP address was provisioned during initial installation.

Login credentials

The following pop-up window will appear. Log in with the proper credentials.

Mediant 3000

Web Login

Username

Admin

Password

•••••

☐ Remember Me

Login

Mediant 3000 Home Page

The **Mediant 3000 Home Page** will appear as shown below.

The screenshot displays the Audiocodes Mediant 3000 Home Page. The interface includes a top navigation bar with the Audiocodes logo, user information ("Mediant 3000 'Admin'"), and buttons for "Submit", "Burn", "Device Actions", "Home", and "Log off". A "SRD Filter" dropdown is set to "All". On the left, a sidebar contains tabs for "Configuration", "Maintenance", and "Status & Diagnostics", with a "Search" button. Below these are expandable sections for "Basic" and "Advanced" configuration, with "System" and "VoIP" listed under "Basic". The main content area, titled "Mediant 3000 Home Page", features a graphical representation of the device hardware with status indicators (green for OK, red for Critical, orange for Major/Minor, green for Shelf). Below this is a "General Information" table and a "PSTN" status section.

General Information	
IP Address	10.64.50.199
Subnet Mask	255.255.255.0
Default Gateway Address	10.64.50.1
Firmware Version	7.00A.132
Protocol Type	SIP
Gateway Operational State	UNLOCKED
High Availability	Not Operational: RTM Card Error
Active Board Slot Number	1

PSTN	
<input type="radio"/> No Link	
<input checked="" type="radio"/> Working Link	
<input type="radio"/> Protection Link	
<input type="radio"/> Alarm	

7.2. Configure Media Gateway IP Network Parameters

To configure the network parameters, navigate to **VoIP → Network → IP Interfaces Table** and click on the **Add** button to add an index with **Application Type** of **OAMP + Media + Control** and ensure the **Interface Mode** is set to **IPv4 Manual** and that **IP Address** (i.e., **10.64.50.199**), **Prefix Length** (i.e., **24**), and **Default Gateway** (i.e., **10.64.50.1**) are set according to the expected values.

The screenshot displays the Audiocodes Mediant 3000 configuration interface. The left sidebar shows a tree view with 'Basic' and 'Advanced' tabs. Under 'Advanced', the 'Network' section is expanded, showing 'IP Interfaces Table' as the selected item. The main content area is titled 'Interface Table' and contains a table with the following data:

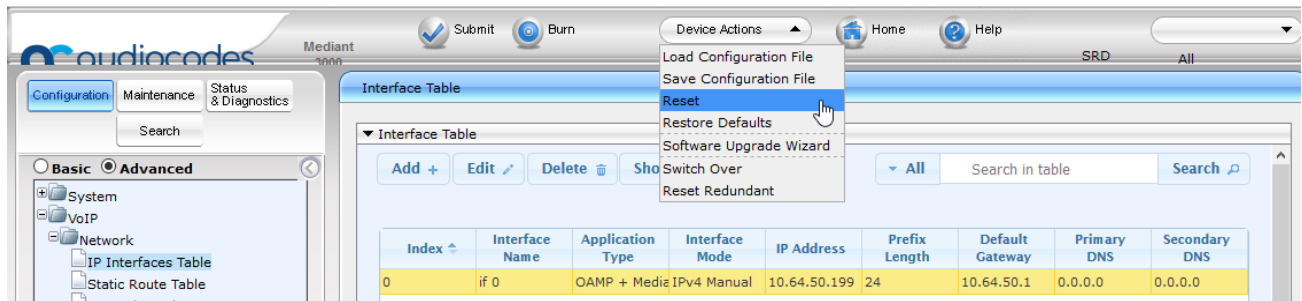
Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS
0	if 0	OAMP + Media	IPv4 Manual	10.64.50.199	24	10.64.50.1	10.64.110.100	75.75.75.75

Below the table, there is a pagination control showing 'Page 1 of 1' and a 'View 1 - 1 of 1' indicator.

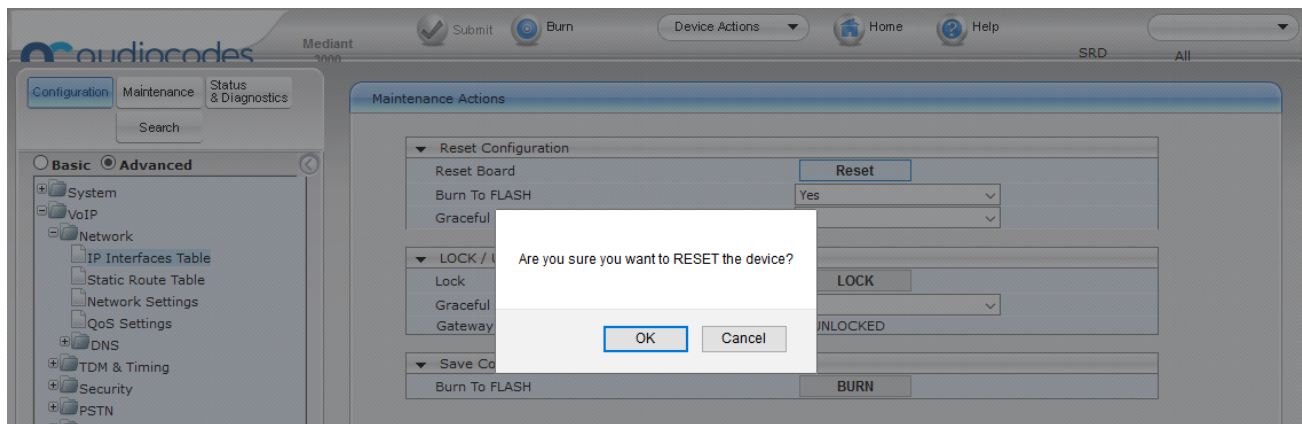
7.3. Saving Configuration and Resetting Mediant 3000

Save settings to the device's flash memory and reset the device by performing the following:

From the **Device Actions** pull-down menu, click **Reset** to display the **Maintenance Actions** screen.



Make sure **Burn To FLASH** is set to **Yes**, and then click the **Reset** button then click **OK** for confirmation. The device's new configuration is saved (burned) to the flash memory and the device resets.



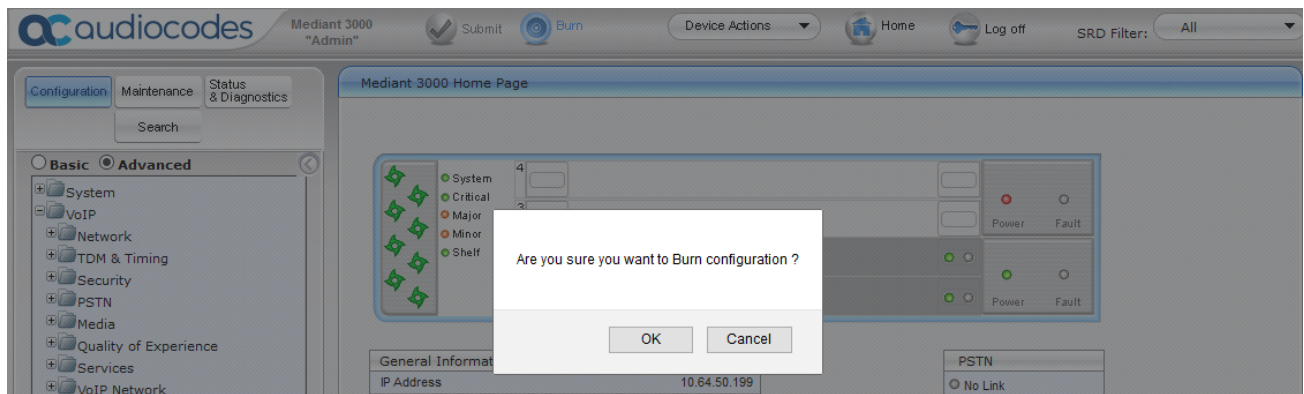
Note: if any parameter with the lightening symbol beside it (see the screenshot is **Section 7.6.1** for example) is changed, a Reset with Burn To Flash is required. The reset does not have to be done until all configuration is completed, and there will be a red reset notification at the top of the page (not shown).

7.4. Saving Configuration

To permanently save settings to the device's flash memory, activate the **Maintenance Actions** page (**Maintenance** tab → **Maintenance** → **Maintenance Actions**) and click the **BURN** button under **Save Configuration** as shown below.



Also note the **Burn** button at the top of the screen. This is the shortest path to do a burn and can be used at any time. When clicked, it will present a pop-up similar to the one shown below.

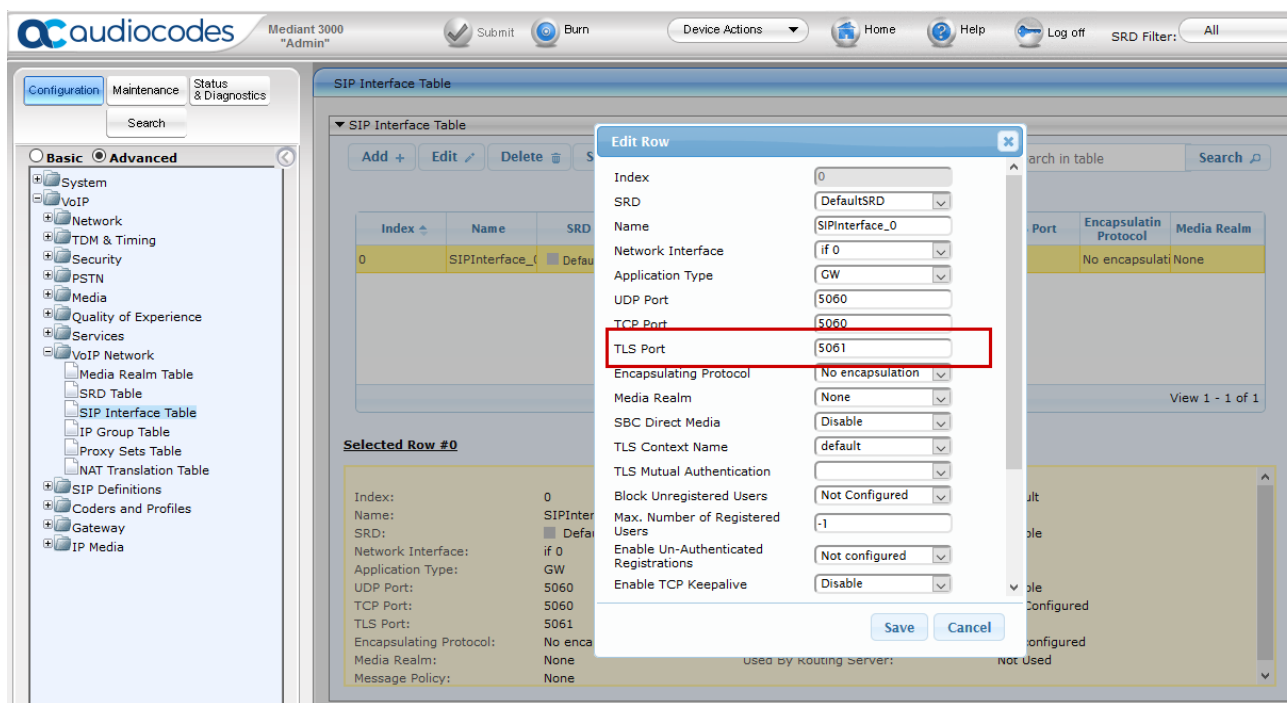


7.5. Configure SIP Interface to Avaya Aura® Session Manager

This section provides instructions to configure SIP Interface to Session Manager

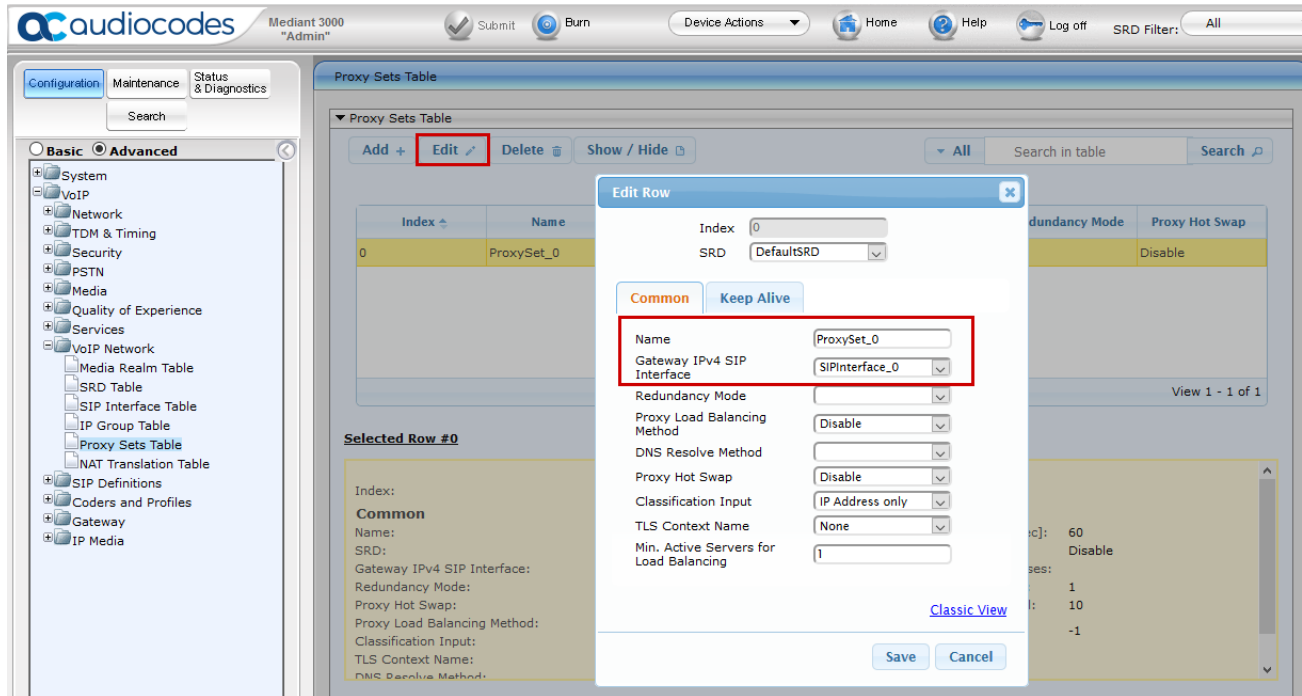
7.5.1. Configure SIP Interface Table

Configure the TLS port **5061**, which will be used to send SIP/TLS signaling between Session Manager and Mediant M3K. To configure SIP Interface Table, on the left pane navigate to **VoIP** → **VoIP Network** → **SIP Interface Table**. Edit the existing table, and set **TLS Port** to **5061**.

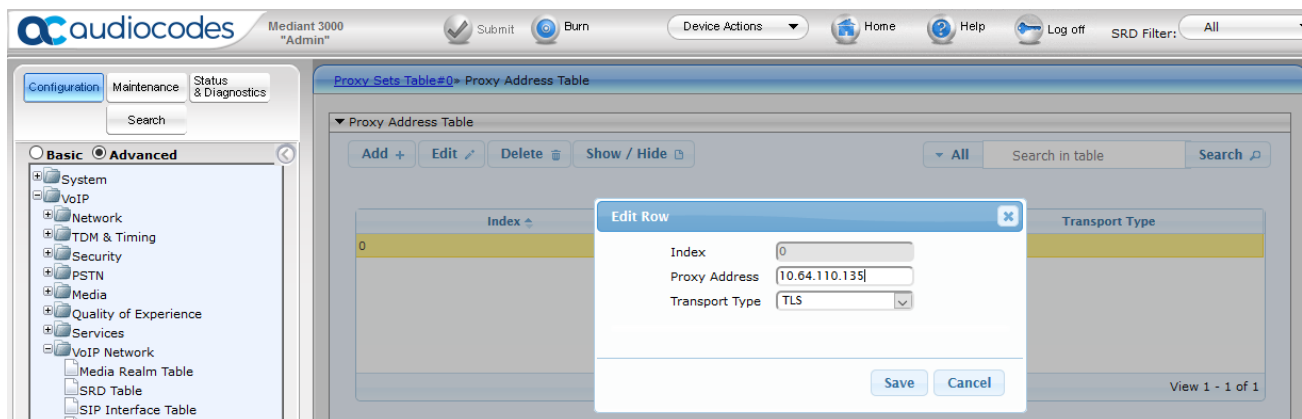


7.5.2. Configure Proxy Sets Table

Configure an Proxy Sets Table for Session Manager. To configure Proxy Sets Table, on the left pane navigate to **VoIP → VoIP Network → Proxy Sets Table**. Click **Edit**, provide a and select the SIP Interface from previous section for **Gateway IPv4 SIP Interface**.



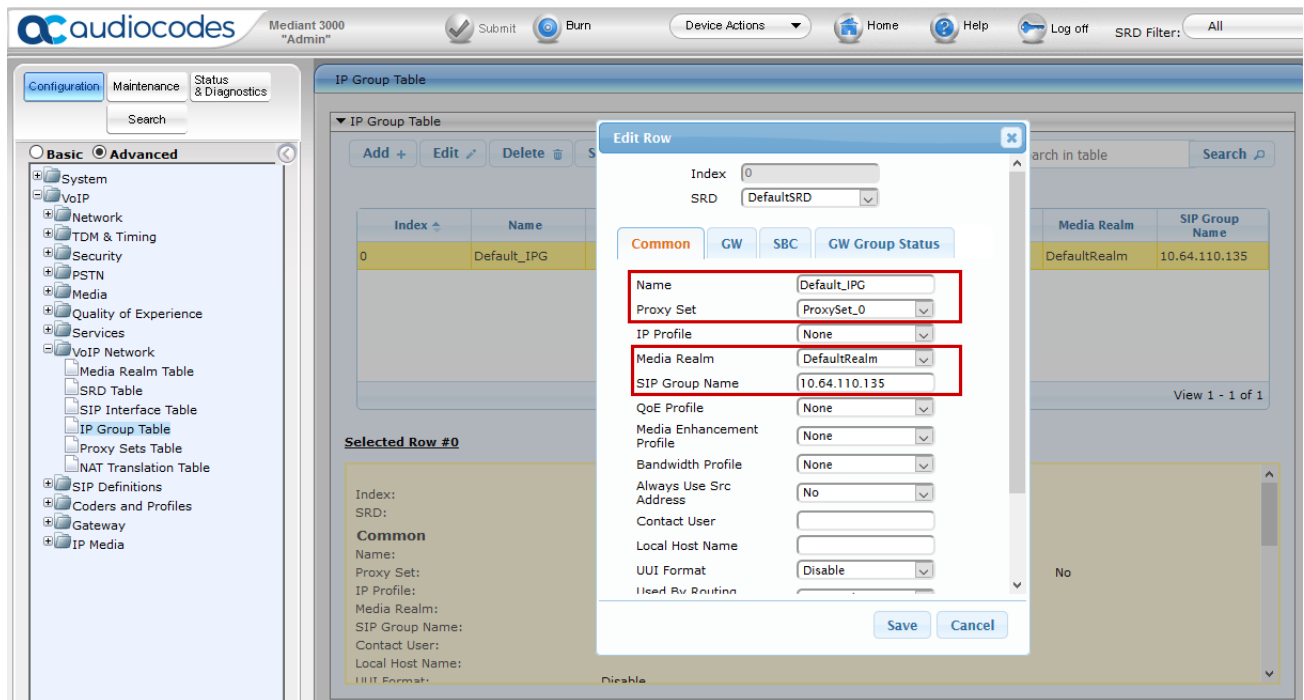
At the bottom of the page select **Proxy Address Table** (not shown). Select **Add** an entry for Session Manager. Configure **Proxy Address** to the SIP Signaling IP Address of Session Manager and **Transport Type** to **TLS**.



7.5.3. Configure IP Group Table

Configure an IP Group Table for Session Manager. To configure SIP Interface Table, on the left pane navigate to **VoIP → VoIP Network → IP Group Table**. Edit the existing group and configure as follows:

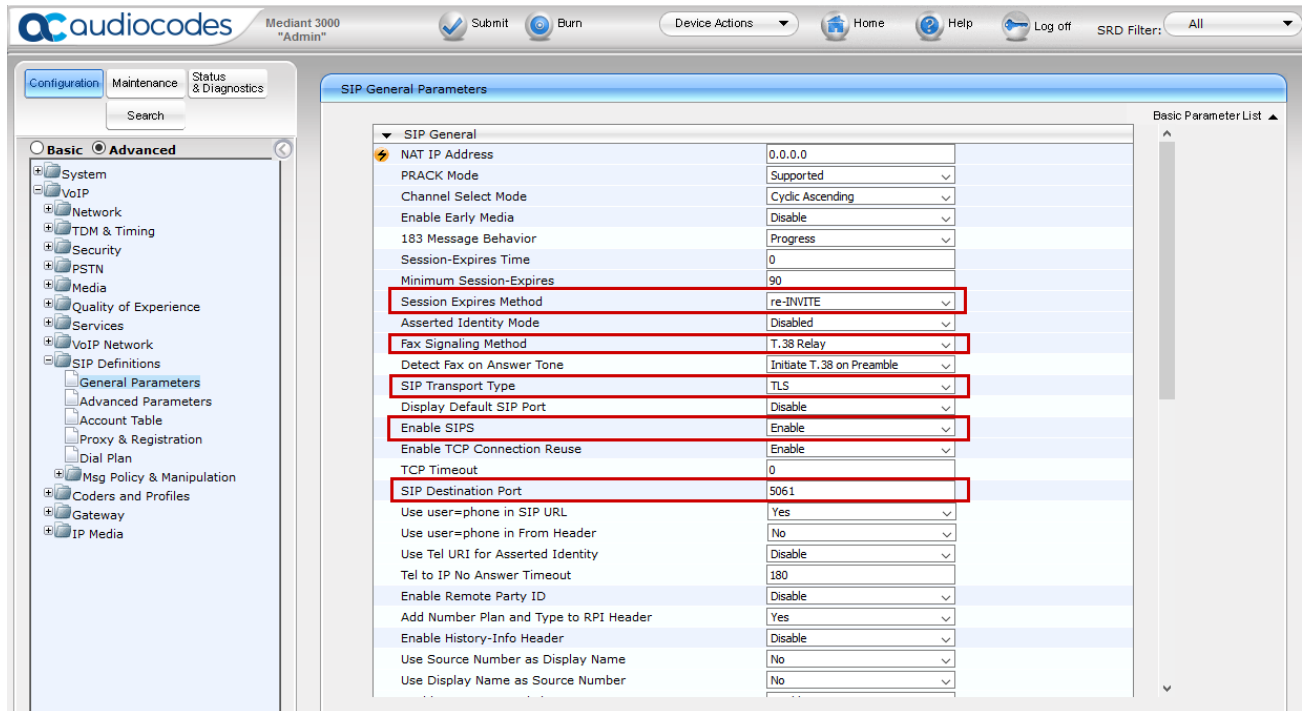
- **Proxy Set:** Proxy Set configured in previous section
- **Media Realm:** **DefaultRealm**
- **SIP Group Name:** SIP Signaling IP Address of Session Manager



7.5.4. Configure General Parameters

To configure SIP General Parameters, navigate to **VoIP → SIP Definitions → General Parameters**. Configure as follows:

- **Session Expires Method:** re-INVITE
- **Fax Signaling Method:** T-38 Relay
- **SIP Transport Type:** TLS
- **Enable SIPs:** Enable
- **SIP Destination Port:** 5061



7.5.5. Configure Proxy & Registration

To configure Proxy and Registrations Parameters, navigate to **VoIP → SIP Definitions → Proxy & Registration**. Configure as follows:

- **User Default Proxy:** No
- **Gateway Name:** Domain configured in **Section 6.1**.

The screenshot shows the Audiocodes Mediant 3000 'Admin' interface. The left sidebar contains a tree view with categories like System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Quality of Experience, Services, VoIP Network, SIP Definitions, General Parameters, Advanced Parameters, Account Table, Proxy & Registration (selected), Dial Plan, Msg Policy & Manipulation, Coders and Profiles, Gateway, and IP Media. The main content area is titled 'Proxy & Registration' and contains a list of parameters. The 'Use Default Proxy' parameter is set to 'No' and is highlighted with a red box. The 'Gateway Name' parameter is set to 'avaya.com' and is also highlighted with a red box. Other parameters include Proxy Name, Redundancy Mode, Proxy IP List Refresh Time, Enable Fallback to Routing Table, Prefer Routing Table, Always Use Proxy, Redundant Routing Mode, SIP ReRouting Mode, Gateway Registration Name, DNS Query Type, Proxy DNS Query Type, Number of RTX Before Hot-Swap, Use Gateway Name for OPTIONS, User Name, Password, Cnonce, Authentication Mode, Challenge Caching Mode, Mutual Authentication Mode, Use Proxy IP as Host, Max Generated Register Rate, and Enable Registration.

7.5.6. Configure the Voice parameters

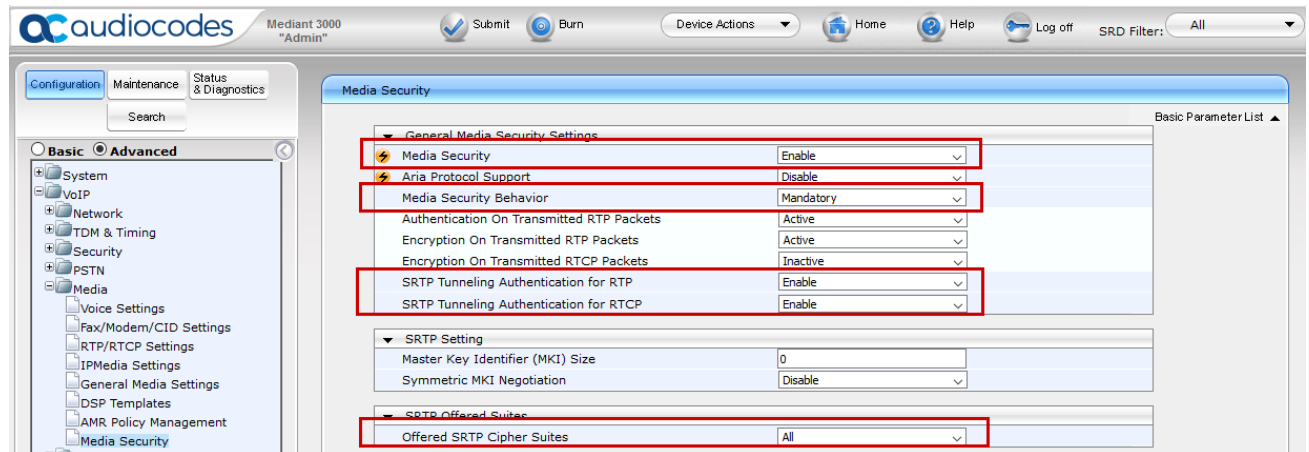
To configure the Voice Settings, navigate to **VoIP → Media → Voice Settings**. Set **DTMF Transport Type** to **RFC2833 Relay DTMF** as shown below, and click the **Submit** button to save changes.

The screenshot shows the Audiocodes Mediant 3000 'Admin' interface. The left sidebar is the same as in the previous screenshot, with 'Voice Settings' selected under the 'SIP Definitions' category. The main content area is titled 'Voice Settings' and contains a list of parameters. The 'DTMF Transport Type' parameter is set to 'RFC2833 Relay DTMF' and is highlighted with a red box. Other parameters include Voice Volume (-32 to 31 dB), Input Gain (-32 to 31 dB), Silence Suppression, DTMF Volume (-31 to 0 dB), and NTE Max Duration.

7.5.7. Configure Media Security

To configure SRTP, navigate to **VoIP → Media → Media Security**. Configure as follows:

- **Media Security:** **Enable**
- **Media Security Behavior:** **Mandatory**
- **Offered SRTP Cipher Suites:** **All**
- **SRTP Tunneling Authentication for RTP:** **Enable**
- **SRTP Tunneling Authentication for RTCP:** **Enable**



7.5.8. Configure Coders

To configure Codecs, navigate to **VoIP → Coders and Profiles → Coders**. Configure as follows:

- From the **Coder Name** drop-down list, select the required coder
- From the **Packetization Time** drop-down list, select the packetization time (in msec) for the selected coder. The packetization time determines how many coder payloads are combined into a single RTP packet
- From the **Rate** drop-down list, select the bit rate (in kbps) for the selected coder
- In the **Payload Type** field, if the payload type (i.e., format of the RTP payload) for the selected coder is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified)
- From the **Silence Suppression** drop-down list, enable or disable the silence suppression option for the selected coder

The screenshot shows the Audiocodes Mediant 3000 configuration interface. The left sidebar contains a tree view with categories like System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Quality of Experience, Services, VoIP Network, SIP Definitions, and Coders and Profiles. The 'Coders' option under 'Coders and Profiles' is selected. The main area displays the 'Coders Table' with the following columns: Coder Name, Packetization Time, Rate, Payload Type, Silence Suppression, and Coder Specific. Three rows are highlighted with a red border:

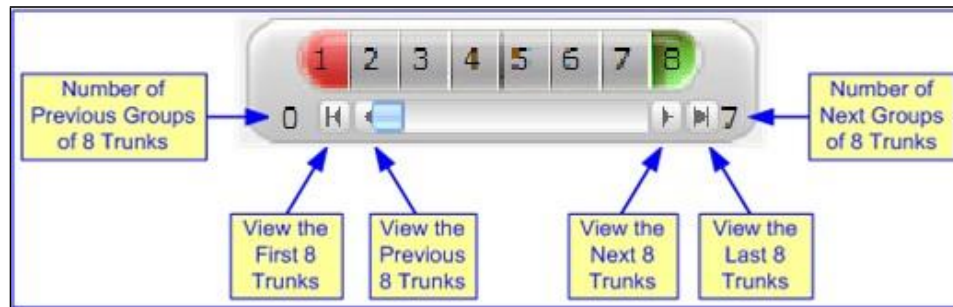
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711U-law	20	64	0	Disabled	
G.711A-law	20	64	8	Disabled	
G.729	20	8	18	Disabled	



7.6. Configure T1 Interface to Simulated PSTN

This section provides information to configure T1 interface to Simulated PSTN.

7.6.1. Configure Trunk Settings

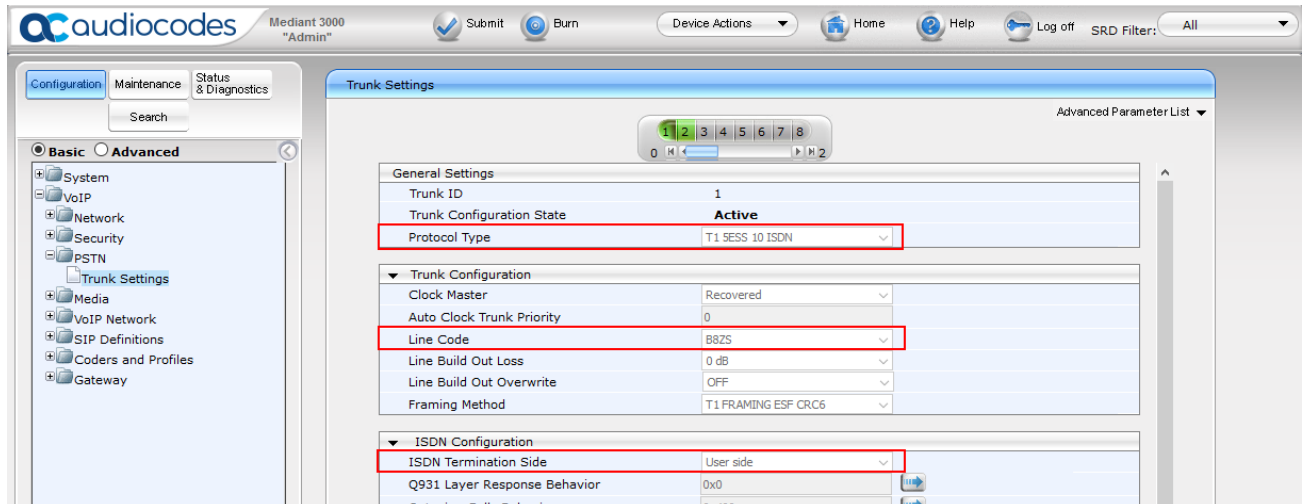
To configure Trunk Settings, navigate to **VoIP → PSTN → Trunk Settings**. Select the trunk to be configured, by clicking the desired Trunk number icon in the right pane. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), refer to the figure below:



Click the **Stop Trunk**  button (located at the bottom of the page) to take the trunk out of service to allow configuration of the currently grayed out (unavailable) parameters. (Skip this step to configure parameters that are available when the trunk is active). The stopped trunk is indicated by the **Trunk Configuration State** field displaying **Inactive**. The **Stop Trunk** button is replaced by the **Apply Trunk Settings**  button.

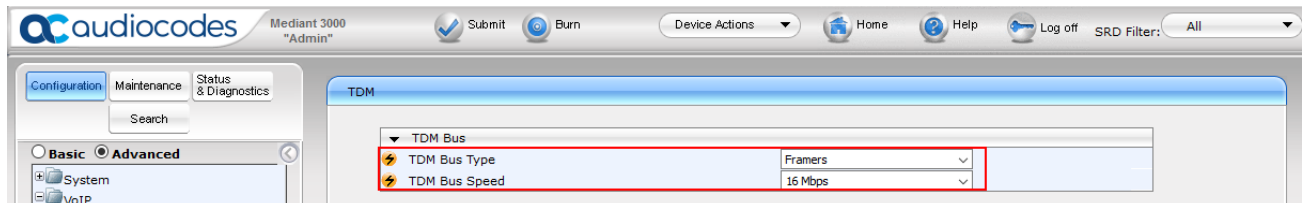
In these Application Notes the PSTN interface was configured as follows:

- **Protocol Type:** **T1 5ESS 10 ISDN**
- **Line Code:** **B8ZS**
- **Framing Method:** **T1 FRAMINIG ESF CRC6**
- **ISDN Termination Side:** **User side**



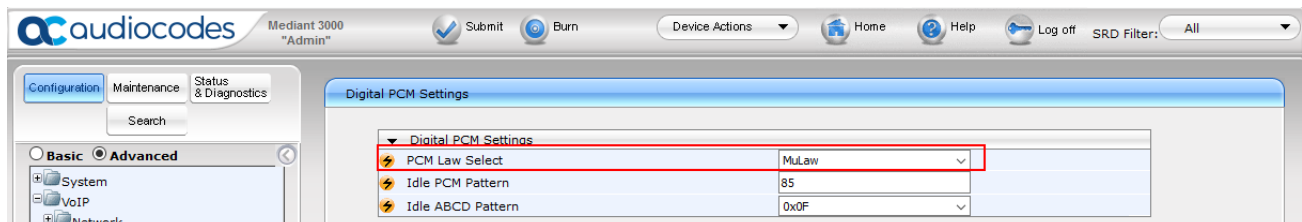
7.6.2. Configure TDM Bus

To configure the TDM Bus settings, navigate to **VoIP → TDM & Timing → TDM**, configure **TDM Bus Type** and **TDM Bus Speed** parameters as required. For T1 set **TDM Bus Type** to **Framers** and **TDM Bus speed** to **16Mbps**.



7.6.3. Configure Digital PCM Settings

To configure the digital PCM settings, navigate to **VoIP → TDM & Timing → Digital PCM Settings**. Configure the parameters as required, i.e., **MuLaw** for **PCM Law Select** for T1.



7.6.4. Configure Trunk Group Table

To configure Trunk Group, navigate to **VoIP → Gateway → Trunk Group → Trunk Group**. Select the appropriate **Group Index**, and set the appropriate parameters in the table, i.e., **From /To Trunk, Channels, Phone Number, Trunk Group ID, Tel Profile ID**. For detailed information refer to [3]. The screen below illustrates setting used for the compliance test.

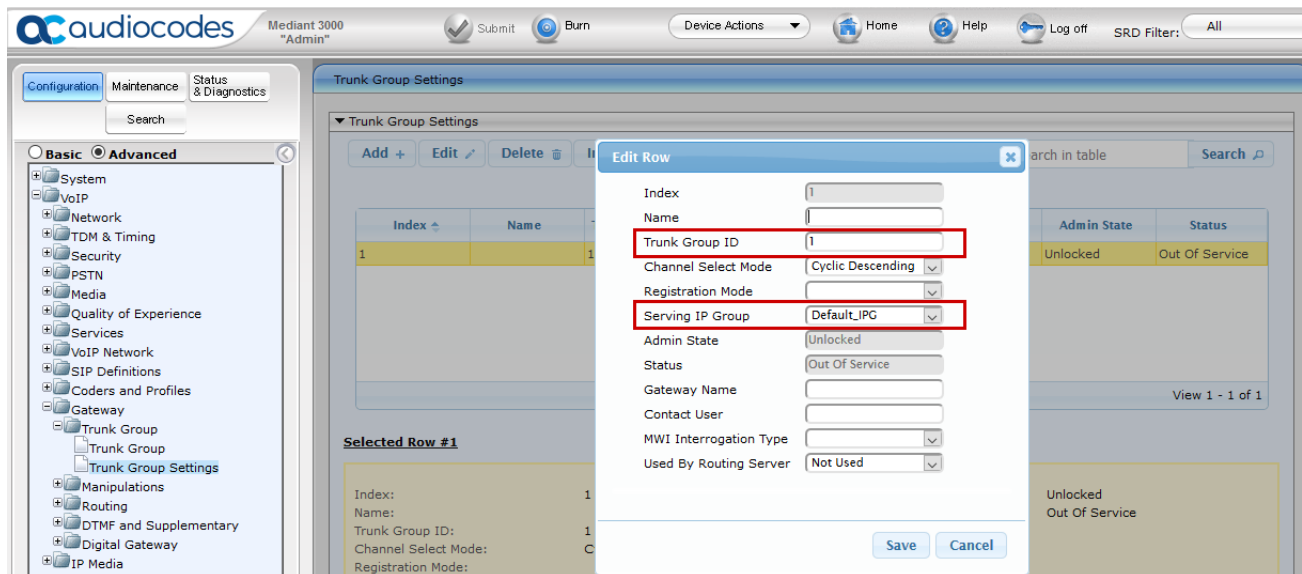
The screenshot shows the Audiocodes Mediant 3000 'Admin' web interface. The left sidebar contains a navigation tree with 'Basic' and 'Advanced' tabs. The 'Advanced' tab is selected, and the 'VoIP' section is expanded. The main content area is titled 'Trunk Group Table' and contains a configuration form. The form has two sections: 'Add Phone Context As Prefix' (set to 'Disable') and 'Trunk Group Index' (set to '1-10'). Below these is a table with the following columns: 'Group Index', 'From Trunk', 'To Trunk', 'Channels', 'Phone Number', 'Trunk Group ID', and 'Tel Profile Name'. The table has three rows, with the first row (Group Index 1) highlighted in red. The first row contains the values: '1', '1', '1', '1-24', an empty field, '1', and 'None'.

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	1	1	1-24		1	None
2						None
3						None

7.6.5. Configure Trunk Group Settings

To configure Trunk Group Settings, navigate to **VoIP → Gateway → Trunk Group → Trunk Group Settings**. Select **Add** to add settings for the trunk group created in previous section. Configure as follows:

- **Trunk Group ID:** Trunk Group ID from previous section
- **Channel Select Mode:** **Cyclic Descending**
- **Serving IP Group:** From Section 7.5.3.



7.7. Configure Routing

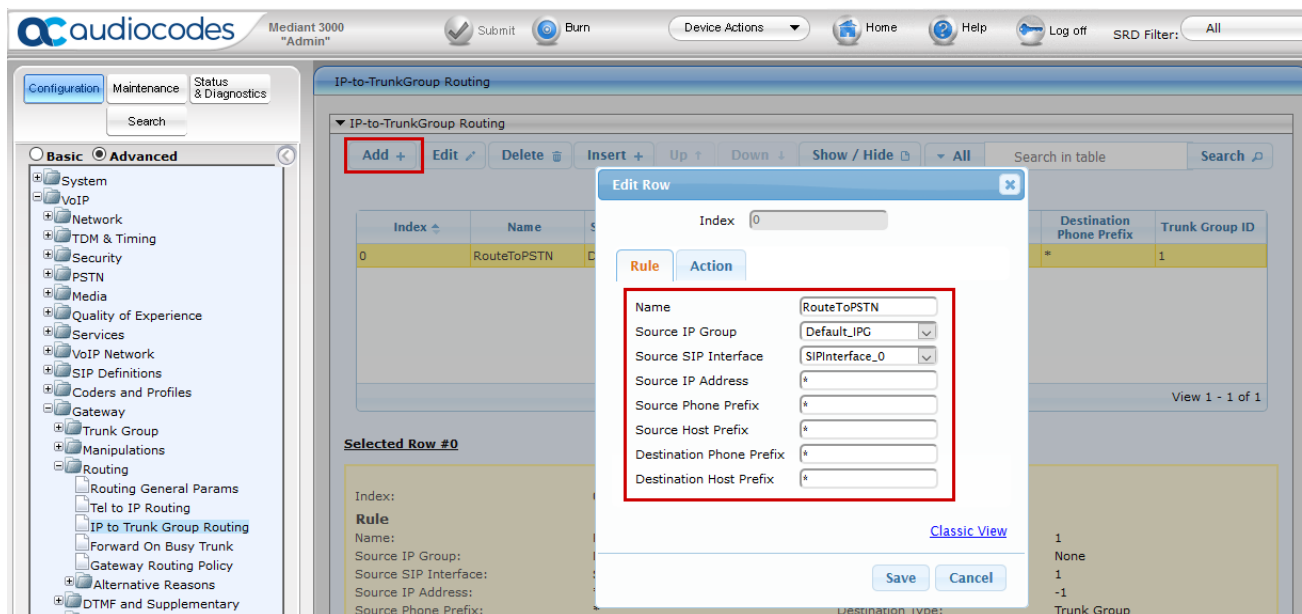
This section provides information to configure routing between Session Manager and Simulated PSTN via Mediant 3000.

7.7.1. Configure IP to Trunk Group Routing Rules

To configure route to Simulated PSTN, navigate to **VoIP → Gateway → Routing → IP to Trunk Group Routing**. To **Add** an entry, select **Add** and configure as follows:

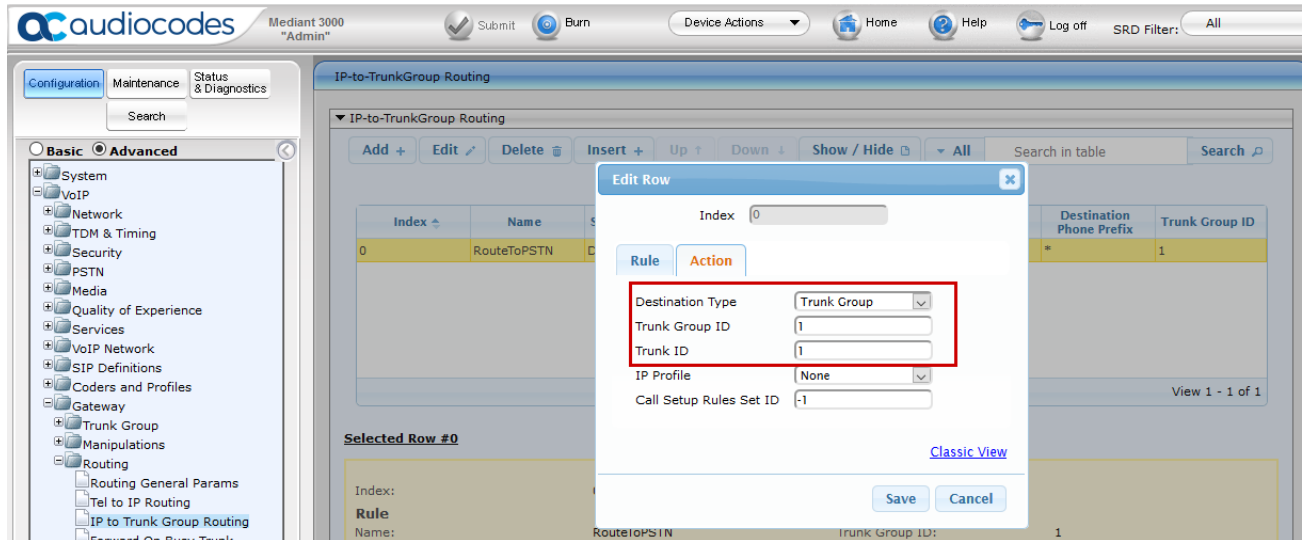
- **Rule tab:**
 - **Name:** Desired name
 - **Source IP Group:** From **Section 7.5.3**
 - **Source SIP Interface:** From **Section 7.5.2**
 - **Source IP Address:** *
 - **Source Phone Prefix** *
 - **Source Host Prefix** *
 - **Destination Phone Prefix** *
 - **Destination Host Prefix** *

Continue to **Action** tab.



- **Action Tab:**

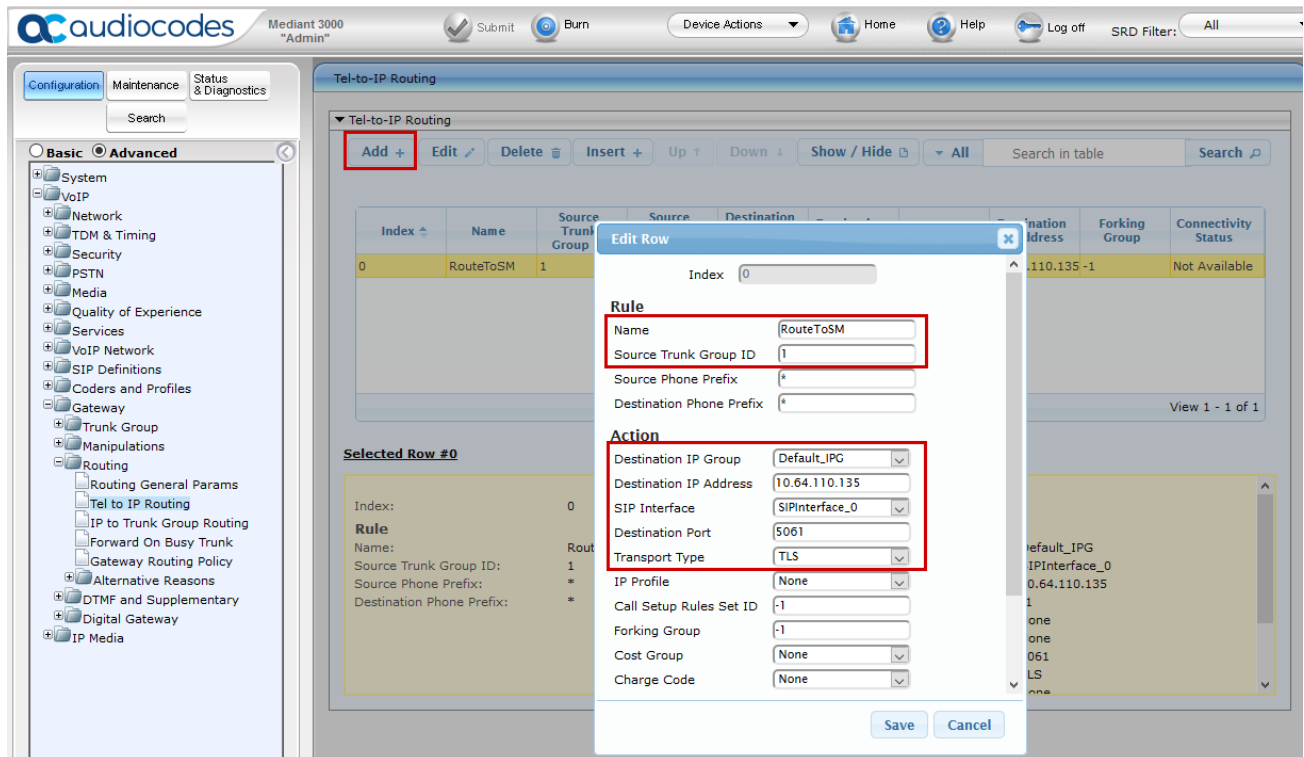
- **Destination Type:** **Trunk Group**
- **Trunk Group ID:** **From Section 7.6.4**
- **Trunk ID:** **From Section 7.6.1**



7.7.2. Configure Outbound IP Routing Rules

To configure routing to Session Manager, navigate to **VoIP → Gateway → Routing → Tel to IP Routing**. Click the **Add** to add an entry and configure as follows:

- **Name:** Desired Name
- **Source Trunk Group ID:** From Section 7.6.4
- **Destination IP Group:** From Section 7.5.3
- **Destination IP Address:** SIP Signaling IP Address of Session Manager
- **Destination Port:** 5061
- **Transport Type:** TLS



7.8. Configure Supplementary Services Parameters

Navigate to **VoIP → Gateway → DTMF and Supplementary → Supplementary Services**. Set the following parameters:

- **Enable Hold:** **Enable**
- **Enable Transfer:** **Enable**
- **Enable Call Forward:** **Enable**
- **Enable Call Waiting:** **Enable**

The screen below illustrates the **Supplementary Services** page.

Supplementary Services	
Enable Hold	Enable
Answer Supervision	No
Enable Hold to ISDN	Disable
Hold Format	0.0.0.0
Held Timeout	-1
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Number of Call Waiting Indications	2
Time Between Call Waiting Indications	10
Time Before Waiting Indications	0
Waiting Beep Duration	300
Enable Caller ID	Disable
Hook-Flash Code	
Enable NRT Subscription	Disable
AS Subscribe IPGroupID	-1
NRT Subscribe Retry Time	120
Call Forward Ring Tone ID	1
Send All Coders on Retrieve	Disable
Generate Metering Tones	Disable
AoC Support	Disable

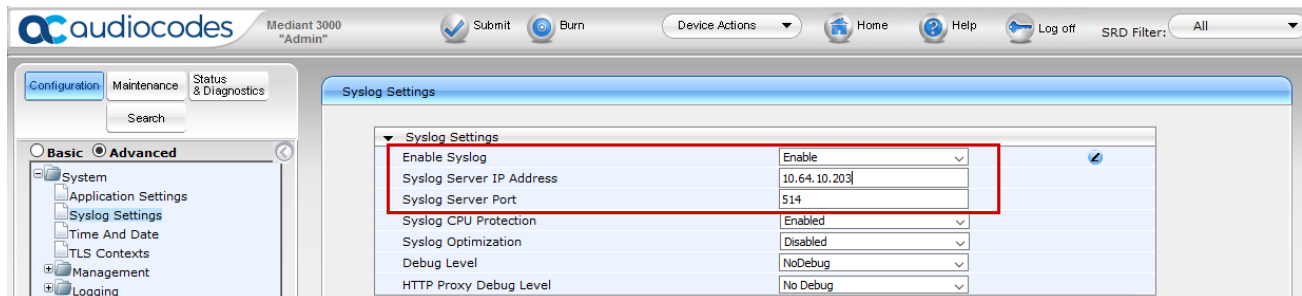
7.9. Configure Syslog Parameters for Debug Assistance

The Mediant 3000 Media Gateway can be configured to output logs to an external Syslog Server for debug assistance. To configure Syslog facility, open the **Syslog Settings** page (**Configuration** tab → **System** → **Syslog Settings**). Configure the following settings:

- **Enable Syslog:** Set to **Enable**
- **Syslog Server IP Address:** Set to IP address of device running a Syslog Server
- **Syslog Server Port:** Set to port utilized on the Syslog Server listening device (i.e., **514**)
- **Debug Level:** Set to **Detailed** to capture proper level of debug information

Click the **Submit** button to save changes. The screen below illustrates settings used during compliance testing.

Note: The Syslog facility should be used only for Debugging purposes. **Enable** the Syslog service as needed and revert to **Disable** once troubleshooting is completed.



Note: Once configuration of the Mediant 3000 is complete refer to Section 7.4 to save the configuration.

7.10. Configure Certificates

In order for TLS to successfully work, TLS contexts need to be configured. During the compliance testing, System Manager was used as the Certificate Authority for AudioCodes M3K. To configure the certificates, navigate to **System → TLS Contexts → TLS Context Certificates**. Below is an example of the fields configured for generating a CSR during the compliance testing.

audiocodes Mediant 3000 "Admin"

Configuration Maintenance Status & Diagnostics

Search

Basic Advanced

System

Application Settings

Syslog Settings

Time And Date

TLS Contexts

Management

Logging

Call Detail Record

Test Call

VoIP

Network

TDM & Timing

Security

Firewall Settings

General Security Settings

TLS Context#0 -> Context Certificates

Certificate Signing Request

Subject Name [CN] m3k

1st Subject Alternative Name [SAN] EMAIL test@avaya.com

2nd Subject Alternative Name [SAN] EMAIL

3rd Subject Alternative Name [SAN] EMAIL

4th Subject Alternative Name [SAN] EMAIL

5th Subject Alternative Name [SAN] EMAIL

Organizational Unit [OU] (optional) DevConnect

Company name [O] (optional) Avaya

Locality or city name [L] (optional) Thornton

State [ST] (optional) CO

Country code [C] (optional) US

Create CSR

Select **Create CSR** and copy/paste the CSR on a notepad; save it on local PC.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQMwYDEMMAoGA1UEAwDbTNrMRMwEQYDVQQQLDApZEXZDb25uZWNO
MQ4wDAYDVQQKDAVBdmF5TERMA8GA1UEBwwIVGhvcm50b24xCzAJBgNVBAGMAkNP
MQswCQYDVQQGEwJVUzCBnzANBQkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6onNEsJ
Qd+yx008hGUHKEAwKHZErl1mwn24awgtCjX4Ttn7VOQOu1N7AgpnE691nFwNB0tB
96Oat0t/chOKpPybzr1F37sVYNySd6VBsmj9tNyu0upVoGfVumLT3cgHk5XSTnSY
FsSb8tBLf1s+fwgoQmEdoq70Exhp3SciIfMCAwEAAaAaMCoGCSqGSIb3DQEJDbEd
MBswCQYDVORBBBIwEIEOdGVzdEBhdmF5YS5jb20wDQYJKoZIhvcNAQEFBQADgYEA
XoeKsxcnTnCSk2RfVzqcOhfBetqKd6x2aK/oRxcMbcXfvFYMU/kV3aDeoiL/lHkS
ZigKbH83QhE01ahaavUYrAlpboVdTf1ZrPlkousZxJQBj6QDV9MpCF7+YrHJx51s
PlyjakK1Z9roX5+MvhVHTLfr21dwyaRHAiPnmZKOFQ=
-----END CERTIFICATE REQUEST-----
```


Via a browser, open the System Manager configuration utility and navigate to **Services → Security → Certificates → Authority → Add End Entity**. Below is an example of the fields configured during compliance testing. Select **Add** once done.

Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS ▾	Required
Username	audiocodesm3k	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	••••	<input checked="" type="checkbox"/>
Confirm Password	••••	
E-mail address	test @ avaya.com	<input type="checkbox"/>
Subject DN Attributes		
CN, Common name	audiocodesm3k	<input checked="" type="checkbox"/>
CN, Common name		<input type="checkbox"/>
O, Organization	Avaya	<input type="checkbox"/>
C, Country (ISO 3166)	US	<input type="checkbox"/>
OU, Organizational Unit	DevConnect	<input type="checkbox"/>
L, Locality	Thornton	<input type="checkbox"/>
ST, State or Province	CO	<input type="checkbox"/>
Other subject attributes		
Subject Alternative Name		
DNS Name		<input type="checkbox"/>
DNS Name		<input type="checkbox"/>
IP Address		<input type="checkbox"/>
Main certificate data		
Certificate Profile	ID_CLIENT_SERVER ▾	<input checked="" type="checkbox"/>
CA	tmdefaultca ▾	<input checked="" type="checkbox"/>
Token	User Generated ▾	<input checked="" type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

Made by PrimeKey Solutions AB, 2002–2014.

One the left pane select **Public Web (not shown)**. A new browser tab will open. On the left pane select **Generate Certificate from CSR**. Type in the **Username** and **Enrollment Code** from previous page, and browse to the CSR for AudioCodes M3K. Click **OK** and save the certificate to local PC (not shown).

**EJBCA**
PKI BY PRIMEKEY

Enroll

[Create Browser Certificate](#)
[Create Certificate from CSR](#)
[Create Keystore](#)
[Create CV certificate](#)
Register

[Request Registration](#)
Retrieve

[Fetch CA Certificates](#)
[Fetch CA CRLs](#)
[List User's Certificates](#)
[Fetch User's Latest Certificate](#)
Inspect

[Inspect certificate/CSR](#)
[Check Certificate Status](#)
Miscellaneous

[Administration](#)
[Documentation](#)

Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) for upload, or paste a PEM-formatted request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with
-----BEGIN CERTIFICATE REQUEST-----
and ending with
-----END CERTIFICATE REQUEST-----

Enroll

Username

audiocodesm3k

Enrollment code

....

Request file

Browse...

m3k.csr

or pasted request

Result type

PKCS#7 certificate

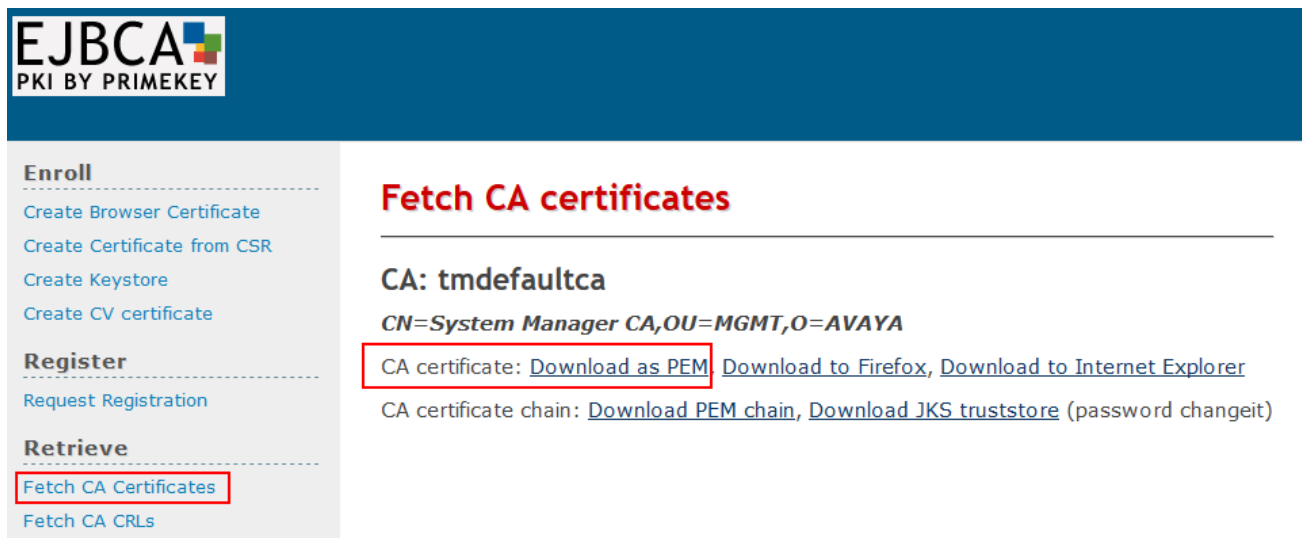
OK

KJA; Reviewed:
SPOC 2/27/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

52 of 70
ACM3KT1CMSM80

On the left pane select **Fetch CA Certificates** and download the **CA Certificate** by selecting **Download as PEM**.



EJBCA
PKI BY PRIMEKEY

Enroll

- Create Browser Certificate
- Create Certificate from CSR
- Create Keystore
- Create CV certificate

Register

- Request Registration

Retrieve

- Fetch CA Certificates**
- Fetch CA CRLs

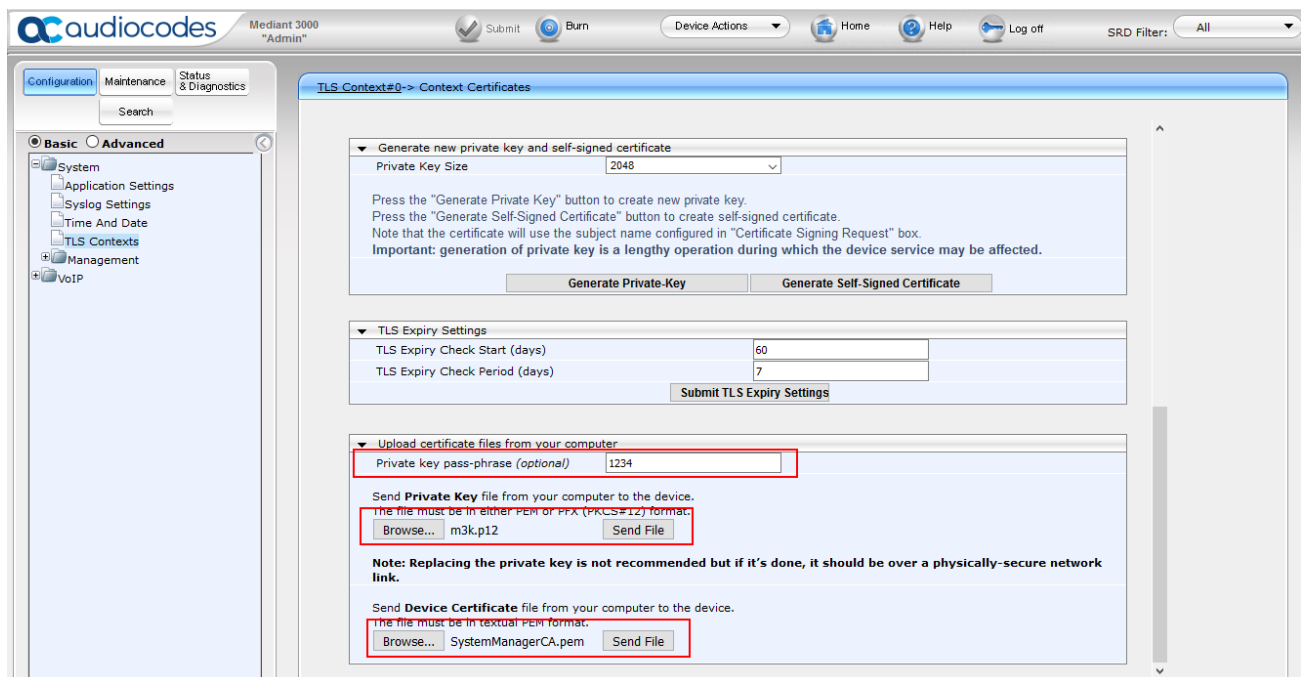
Fetch CA certificates

CA: tmdefaultca
CN=System Manager CA,OU=MGMT,O=AVAYA

CA certificate: [Download as PEM](#) [Download to Firefox](#) [Download to Internet Explorer](#)

CA certificate chain: [Download PEM chain](#) [Download JKS truststore](#) (password changeit)

Return to the AudioCodes M3K webconsole and navigate to **System → TLS Contexts → TLS Context Certificate**. Scroll down to the bottom and select the generate p12 certificate file for AudioCodes M3K and Select the System Manager CA certificate. Type in the **Private key pass-phrase** (Enrollment code used during adding the Enmity on System Manager). Select **Send File** for each certificate.



audiocodes Mediant 3000 "Admin"

Configuration Maintenance Status & Diagnostics

Search

Basic ☐ **Advanced**

- System
 - Application Settings
 - Syslog Settings
 - Time And Date
 - TLS Contexts**
 - Management
 - VoIP

TLS Context#0 -> Context Certificates

Generate new private key and self-signed certificate

Private Key Size: 2048

Press the "Generate Private Key" button to create new private key.
Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
Note that the certificate will use the subject name configured in "Certificate Signing Request" box.
Important: generation of private key is a lengthy operation during which the device service may be affected.

[Generate Private-Key](#) [Generate Self-Signed Certificate](#)

TLS Expiry Settings

TLS Expiry Check Start (days): 60

TLS Expiry Check Period (days): 7

[Submit TLS Expiry Settings](#)

Upload certificate files from your computer

Private key pass-phrase (optional): 1234

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PKCS#12 format.

[Browse...](#) m3k.p12 [Send File](#)

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

[Browse...](#) SystemManagerCA.pem [Send File](#)

8. Verification Steps

This section provides the verification steps that may be performed to verify the configuration.

8.1. Verify Avaya Aura® Communication Manager Trunk Status

On Communication Manager, ensure that all the signaling groups are in service by issuing the command status **signaling-group n** where **n** is the signaling group number.

```
status signaling-group 1
                        STATUS
SIGNALING GROUP
    Group ID: 1
    Group Type: sip
    Group State: in-service
```

8.2. SIP Monitoring on Avaya Aura® Session Manager

From System Manager's Home screen, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. The screen below shows the link status between Session Manager and the Mediant 3000.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Session Manager' selected. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a description: 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' Below this, there is a section for 'All Entity Links to SIP Entity: m3k' with a 'Summary View' button. A table shows the connection status for one item, 'sm8', with columns for Session Manager Name, IP Address Family, SIP Entity Resolved IP, Port, Proto, Deny, Conn. Status, Reason Code, and Link Status. The table indicates a successful connection with a status of 'UP'.

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
sm8	IPv4	10.64.50.199	5061	TLS	FALSE	UP	200 OK	UP

8.3. Utilizing Mediant 3000 Web Interface to Observe Status

The **Status & Diagnostics** menu is used to view and monitor the device's channels, Syslog messages, hardware and software product information, and to assess the device's statistics and IP connectivity information.

8.3.1. Device Status

To view the status of the device's hardware components, open the **Components Status** page (**Status & Diagnostics** tab → **System Status** → **Components Status**). The screen below illustrates the **Component Status** page for the gateway where the TP8410 board in slot 1 is active.

The screenshot displays the Mediant 3000 Web Interface. The top navigation bar includes the Audiocodes logo, user information (Mediant 3000, "Admin"), and buttons for Submit, Burn, Device Actions, Home, Help, and Log off. A search filter (SRD Filter) is set to All. The left sidebar shows a tree view with tabs for Configuration, Maintenance, and Status & Diagnostics. Under Status & Diagnostics, the Components Status page is selected. The main content area shows the following data:

Slots	
Slot #1	TP8410, StandAlone, Temperature(Celsius)=29
Slot #2	SAT 2, StandAlone
Slot #3	Not Occupied
Slot #4	Not Occupied

Fan Status	
Tray	Fan Tray ID : 3, Version 0
1 Bottom Front Fan	Speed = 13440 (RPM)
2 Bottom Middle Fan	Speed = 13440 (RPM)
3 Bottom Middle Fan	Speed = 13560 (RPM)
4 Bottom Rear Fan	Speed = 11520 (RPM)
5 Top Front Fan	Speed = 13560 (RPM)
6 Top Middle Fan	Speed = 13560 (RPM)
7 Top Middle Fan	Speed = 13560 (RPM)
8 Top Rear Fan	Speed = 11400 (RPM)

Alarm Severity of Power Supply	
Top	Major
Bottom	No Alarm

PEM	
Top	PEM 2 Tray ID : 2, Version : 6, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3, Disconnected
Bottom	PEM 1 Tray ID : 2, Version : 6, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3

8.3.2. Device Information

Open the **Device Information** page (**Status & Diagnostics** tab → **System Status** → **Device Information**).

The screenshot displays the Audiocodes Mediant 3000 'Admin' web interface. The top navigation bar includes the Audiocodes logo, the device name 'Mediant 3000 "Admin"', and buttons for 'Submit', 'Burn', 'Device Actions', 'Home', 'Help', 'Log off', and an 'SRD Filter' dropdown set to 'All'. On the left, a sidebar menu shows 'Configuration', 'Maintenance', and 'Status & Diagnostics' tabs, with a 'Search' button below them. Under 'Status & Diagnostics', the 'Advanced' section is expanded, showing a tree view with 'System Status' selected, containing sub-items like 'Message Log', 'Activity Log', 'Device Information', 'Ethernet Port Information', 'Components Status', 'Carrier-Grade Alarms', 'Performance Monitoring', and 'VoIP Status'. The main content area is titled 'Device Information' and contains three expandable sections: 'General Settings', 'Versions', and 'Loaded Files'. The 'General Settings' section lists various device parameters. The 'Versions' section shows software and flash versions. The 'Loaded Files' section shows a loaded call progress tones file and a default coder table.

General Settings	
MAC Address:	00908f3c7ea2
Serial Number:	3964578
Product Key:	
Board Type:	49
Device Up Time:	41d:1h:40m:29s:71th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [Mbytes]:	32
RAM Size [Mbytes]:	512
CPU Speed [MHz]:	450

Versions	
Version ID:	7.00A.132
DSP Type:	2
DSP Software Version:	70041
DSP Software Name:	491096AE3
Flash Version:	220

Loaded Files	
Call Progress Tones File Name:	M2K_usa_tones.dat Delete
Loaded Coder Table :	Default CODERTABLE

8.3.3. Trunks and Channels Status

To view the status of the device's trunks and the trunks' channels (Simulated PSTN), open the **Trunks & Channels Status** page (**Status & Diagnostics** tab → **VoIP Status** → **Trunks & Channels Status**). The following screen illustrates the **Trunks and Channel Status** page, where the symbols of the port in green represent channels engaged with a call.

The screenshot shows the Audiocodes Mediant 3000 'Admin' interface. The left sidebar contains a navigation menu with 'Basic' and 'Advanced' tabs. Under 'Advanced', the 'VoIP Status' section is expanded, showing 'Trunks & Channels Status' as the selected item. The main content area is titled 'Trunks & Channels Status' and includes a 'Page Number' selector (1, 2, 3) and a 'Go To Page' input field. Below this is a table with columns for 'Trunks' and 'Channels'. The table lists 8 trunks, each with 24 channels. Trunk 1 and Trunk 2 are highlighted in green, indicating they are engaged with a call. The status of each channel is represented by a small icon: a green icon for channels engaged with a call and a blue icon for channels not engaged.

8.3.4. Proxy Sets Status

To view the status of the SIP trunk to Session Manager, open the **Proxy Sets Status** page (**Status & Diagnostics** tab → **VoIP Status** → **Proxy Sets Status**). The following screen illustrates the **Proxy Sets Status** page; note the Status of ONLINE for Proxy Set ID 1.

The screenshot shows the Audiocodes Mediant 3000 'Admin' interface. The left sidebar contains a navigation menu with 'Basic' and 'Advanced' tabs. Under 'Advanced', the 'VoIP Status' section is expanded, showing 'Proxy Sets Status' as the selected item. The main content area is titled 'Proxy Sets Status' and includes a message 'This page refreshes every 60 seconds'. Below this is a table with columns for 'Proxy Set ID', 'Mode', 'Keep Alive', 'Address', 'Priority', 'Weight', 'Success Count', 'Failure Count', and 'Status'. The table lists two proxy sets, ID 0 and ID 1. Both are in 'Parking' mode and have 'Keep Alive' enabled. Proxy Set ID 1 is highlighted in green, indicating it is ONLINE.

Proxy Set ID	Mode	Keep Alive	Address	Priority	Weight	Success Count	Failure Count	Status
0	Parking	Enabled	10.64.110.12:5061(*)	-	-	64646	265	ONLINE
1	Parking	Enabled	10.64.110.12:5061(*)	-	-	32344	265	ONLINE

9. Conclusion

These Application Notes describe the procedures required to configure the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The AudioCodes Mediant 3000 Gateway successfully passed compliance testing.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Document 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Document 03-603324
- [3] *User's Manual Mediant™ 3000 Gateway & E-SBC* Version 7.0

Product documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for AudioCodes products may be found at <http://www.audiocodes.com>.

11. Appendix

The AudioCodes M3000 .ini file was generated after completing the compliance test. Its contents were copied below. Please use it only for reference purposes.

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

;Board: Mediant 3000
;HW Board Type: 63  FK Board Type: 49
;M3K Board Type: TrunkPack 8410
;Serial Number: 3964578
;Slot Number: 1
;Software Version: 7.00A.125.004
;DSP Software Version: 491096AE3=> 700.40
;Board IP Address: 10.64.50.199
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.50.1
;Ram size: 512M  Flash size: 32M
;Num of DSP Cores: 36  Num DSP Channels: 504
;Profile: NONE
;;;Key features;;Board Type: Mediant 3000 ;PSTN STM1\SONET Interface Not
Supported ;E1Trunks=16 ;T1Trunks=21 ;IP Media: VXML CALEA ;PSTN
Protocols: ISDN IUA=84 CAS V5.2 ;Channel Type: RTP DspCh=504 ;HA ;Coders:
G723 G729 GSM-FR G727 ILBC ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;DSP Voice features: IpmDetector
AMRPolicyManagement ;Control Protocols: MSFT MGCP MEGACO SIP ;Default
features;;Coders: G711 G726;
;-----

[SYSTEM Params]

;PM_gwSBCRegisteredUsers is hidden but has non-default value
SyslogServerIP = 10.64.10.202
EnableSyslog = 1
;VpFileLastUpdateTime is hidden but has non-default value
TLSPkeySize = 2048
NTPServerIP = '0.0.0.0'
;LastConfigChangeTime is hidden but has non-default value
;RootFileLastUpdateTime is hidden but has non-default value
;PkeyFileLastUpdateTime is hidden but has non-default value
```

[BSP Params]

PCMLawSelect = 3
TDMBusClockSource = 4
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[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

[PSTN Params]

ProtocolType_0 = 13
ProtocolType_1 = 13
ProtocolType_2 = 0
ProtocolType_3 = 0
ProtocolType_4 = 0
ProtocolType_5 = 0
ProtocolType_6 = 0
ProtocolType_7 = 0
ProtocolType_8 = 0
ProtocolType_9 = 0
ProtocolType_10 = 0
ProtocolType_11 = 0
ProtocolType_12 = 0
ProtocolType_13 = 0
ProtocolType_14 = 0
ProtocolType_15 = 0
ProtocolType_16 = 0
ProtocolType_17 = 0
ProtocolType_18 = 0
ProtocolType_19 = 0
ProtocolType_20 = 0

```
FramingMethod_0 = D
FramingMethod_1 = D
FramingMethod_2 = 0
FramingMethod_3 = 0
FramingMethod_4 = 0
FramingMethod_5 = 0
FramingMethod_6 = 0
FramingMethod_7 = 0
FramingMethod_8 = 0
FramingMethod_9 = 0
FramingMethod_10 = 0
FramingMethod_11 = 0
FramingMethod_12 = 0
FramingMethod_13 = 0
FramingMethod_14 = 0
FramingMethod_15 = 0
FramingMethod_16 = 0
FramingMethod_17 = 0
FramingMethod_18 = 0
FramingMethod_19 = 0
FramingMethod_20 = 0
```

[SS7 Params]

[Voice Engine Params]

```
CallProgressTonesFilename = 'M2K_usa_tones.dat'
IdlePCMPattern = 85
AnswerDetectorSilenceTime = 0
AnswerDetectorSensitivity = 0
EnergyDetectorQualityFactor = 0
EnergyDetectorThreshold = 0
ENABLEMEDIASECURITY = 1
RTCPEncryptionDisableTx = 1
```

[WEB Params]

;HTTPSPkeyFileName is hidden but has non-default value

[SIP Params]

```
SIPDESTINATIONPORT = 5061
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SIPGATEWAYNAME = 'avaya.com'
```

```
USEGATEWAYNAMEFOROPTIONS = 1
ISFAXUSED = 1
SIPTRANSPORTTYPE = 2
ENABLESIPS = 1
MEDIASECURITYBEHAVIOUR = 1
ENABLETCPCONNECTIONREUSE = 0
MSLDAPPRIMARYKEY = 'telephoneNumber'
FIRSTTXDTMFOPTION = 4
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value
```

[SCTP Params]

[VXML Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

;ContextEngineID is hidden but has non-default value

[Video 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, 10.64.50.199, 24, 10.64.50.1, 1, "if 0",
0.0.0.0, 0.0.0.0;
```

[\InterfaceTable]

[DspTemplates]

```

FORMAT DspTemplates_Index = DspTemplates_DspTemplateName,
DspTemplates_DspResourcesPercentage;
DspTemplates 0 = 0, 100;

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$YQVaVldWB1JaD1pcXwkKDEAUQUpHFkVCQE9DQ09JGk21t7rlsbyysr256+66u03tqaX0q
qT0866hrPur/qmoqcU=", 1, 0, 5, 15, 60, 200,
"39ea427ac3a5abe249eb8e0e3bb18e26";
WebUsers 1 = "User",
"$1$Wj44aG9rbVFTV1IHVVVTXgxZWfUMWAwUF0UREhAXThlKtK4YRBhI5eK2s+Hhsb+6vem8t
bjqvvgJo6eg8fei+fo=", 1, 0, 2, 15, 60, 50,
"bb9a70129d690ca6545321ae6d4e1999";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_OcspEnable,
TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary,
TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse,
TLSContexts_DHKeySize;
TLSContexts 0 = "default", 4, 2, "RC4:AES128", "DEFAULT", 0, 0.0.0.0,
0.0.0.0, 2560, 0, 2048;

[ \TLSContexts ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;

```



```

CpMediaRealm 0 = "DefaultRealm", "if 0", "", 6000, 2016, 26159, 1, "",
"";

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]

[ SRD ]

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

[ \SRD ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "SIPInterface_0", "if 0", 0, 5060, 5060, 5061,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "DefaultRealm", 0, -1, -
1, -1, 0;

[ \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_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 1, 60, 0, 0, "DefaultSRD", 0, "default", -1, -
1, "", "SIPInterface_0", "", "", "", "", "", 1, 1, 10, -1;
ProxySet 1 = "AvayaSM", 1, 120, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"SIPInterface_0", "", "", "", "", "", 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_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_SBCDialPlanName;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
"", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, "";
```

```
IPGroup 1 = 0, "SM", "AvayaSM", "10.64.110.12", "", -1, 0, "DefaultSRD",
"DefaultRealm", 1, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, "";
```

```
[ \IPGroup ]
```

```
[ 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 0 = "RouteToSM", "*", "10.64.110.12", "*", "", "", 5061, "SM", 2,
1, "SIPInterface_0", "", -1, -1, "Not Available";
```

```
[ \PREFIX ]
```

```
[ TrunkGroup ]
```

```
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel,
TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber,
TrunkGroup_ProfileName, TrunkGroup_LastTrunkId, TrunkGroup_Module;
TrunkGroup 0 = 1, 0, 1, 24, "", "", 0, 255;
```

```
[ \TrunkGroup ]
```

```
[ PstnPrefix ]
```

```
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 0 = "RouteToPSTN", "*", 1, "*", "*", "", "SM", "*", "*",
"SIPInterface_0", 1, -1, 0;
```

```
[ \PstnPrefix ]
```

[ProxyIp]

```
FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,  
ProxyIp_IpAddress, ProxyIp_TransportType;  
ProxyIp 0 = "0", 0, "10.64.110.12", 2;  
ProxyIp 1 = "1", 0, "10.64.110.12", -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 1 = 1, 3, 5, "", "", "SM", 255, "", 0, 0;
```

[\TrunkGroupSettings]

[CodersGroup0]

```
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,  
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,  
CodersGroup0_CoderSpecific;  
CodersGroup0 0 = "g729", 20, 0, -1, 0, "";  
CodersGroup0 1 = "g711Alaw64k", 20, 0, -1, 0, "";  
CodersGroup0 2 = "g711Ulaw64k", 20, 0, -1, 0, "";  
CodersGroup0 3 = "t38fax", 255, 255, -1, 255, "";
```

[\CodersGroup0]

[GwRoutingPolicy]

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

[\GwRoutingPolicy]

```
[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

©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.