Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the AudioCodes Mediant 1000 Multi Service Business Router / Media Gateway / Session Border Controller with Stand Alone Survivability with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the AudioCodes Mediant 1000 Multi Service Business Router with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The AudioCodes Multi Service Business Routers serve several functions, primarily for branch locations. First, as a bridge, offering connectivity between legacy analog endpoints at a branch location and a VoIP infrastructure at the Enterprise Core using the Session Initiation Protocol (SIP). Second, as a Stand Alone Survivable media gateway providing PSTN access for SIP endpoints when connectivity to the Enterprise Core is lost. Third, as a PSTN Gateway used for least cost routing for the enterprise when connectivity with the Enterprise Core is available.

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

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

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedure for configuring AudioCodes Mediant 1000 Multi Service Business Routers (MSBR) with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The AudioCodes Mediant Multi Service Business Routers serve several functions, primarily for branch locations. The MSBR used during testing had 4 FXS (analog endpoint) ports and 4 FXO (POTS trunk) ports. The Mediant 1000 series can be expanded by adding additional modules. Using the FXO ports, PSTN trunks were configured allowing the gateway to connect calls to and from external parties. During normal conditions, calls to the analog trunk were routed to Session Manager as SIP messages, and Session Manager used routing rules to determine where to route the call. Analog endpoints were connected to FXS ports and the MSBR acted as a SIP proxy to register these endpoints with Session Manager, enabling the analog endpoints to make and receive calls through Session Manager and the Enterprise Core.

As a Stand Alone Survivable media gateway, the MSBR provided PSTN access for analog and SIP endpoints when connectivity to the Enterprise Core was lost. The SIP endpoints simultaneously registered to both Session Manager and the local MSBR. When the phones detected the loss of connectivity with Session Manager, they performed a soft reset enabling them to use the Audio Codes MSBR as a SIP proxy. The soft reset generally occurred within a minute of loss of WAN, and the reset would also initiate when a user attempted to initiate a call while WAN connectivity was out of service. Upon restoration of the WAN, all phones re-established communications and used Session Manager for call processing, typically within a minute of the link being restored.

In this tested configuration, while WAN connectivity to the Enterprise Core was in service, calls to PSTN endpoints in the local calling area of the branch were routed by Session Manager to the Audio Codes MSRB. The MSRB in turn routed the calls to the PSTN using the FXO ports.

2. General Test Approach and Test Results

The general test approach was to make calls to/from telephones at the branch site using various codec settings and exercising common PBX features.

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.

©2015 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

The testing included both analog telephones, and Avaya SIP telephones. Calls were made to/from Enterprise users located in the branch as well as in the central Enterprise Core location, to and from the PSTN and within the branch site. The same test cases, where applicable, were repeated with a simulated data WAN outage using the local analog trunks to access the PSTN.

The following features and functionality were verified using analog telephones as well as a variety of Avaya SIP endpoints when the data WAN was available.

- Calls to/from endpoints registered to the Enterprise Core
- Calls to/from the PSTN (routed by Session Manager through the local gateway FXO ports)
- Intra-branch calls
- Distributed Call Routing for calls to/from local branch endpoints
- Distributed Call Routing for calls to/from Enterprise endpoints (users in other locations)
- G.711mu, G.711A and G.729 codec support
- Proper recognition of DTMF transmissions
- Hold, Transfer, Call Waiting, and Conferencing
- Proper system recovery after a restart

The following features and functionality were verified when a simulated data WAN failure was introduced.

- Automatic routing to the POTS line to complete calls to the Enterprise Core. Incoming calls to the branch were limited to the single POTS number assigned to the branch.
- Local device support for Hold, Transfer, Conference and Call Waiting
- Survivability of active calls
- Failover of branch SIP endpoints to local branch MSBR.

2.2. Test Results

The AudioCodes Mediant 1000 Multi Service Business Router successfully passed compliance testing.

2.3. Support

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

©2015 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The lab test environment used for compliance testing the AudioCodes Mediant 1000 Multi Service Business Router solution is shown in **Figure 1.** This test bed included the following components:

- Branch
  - AudioCodes M1000 Multi Service Business Router with analog FXS stations and analog FXO PSTN trunks
  - 9600 and 96x1 SIP phones
- Headquarters
  - Communication Manager
  - Session Manager (configured from Avaya Aura® System Manager)
  - G450 Media Gateway
  - HTTP Phone Configuration Server (not shown)
  - Avaya analog, digital, and IP Phones (H.323 and SIP)
- PSTN
  - Simulated lab PSTN analog trunks used.

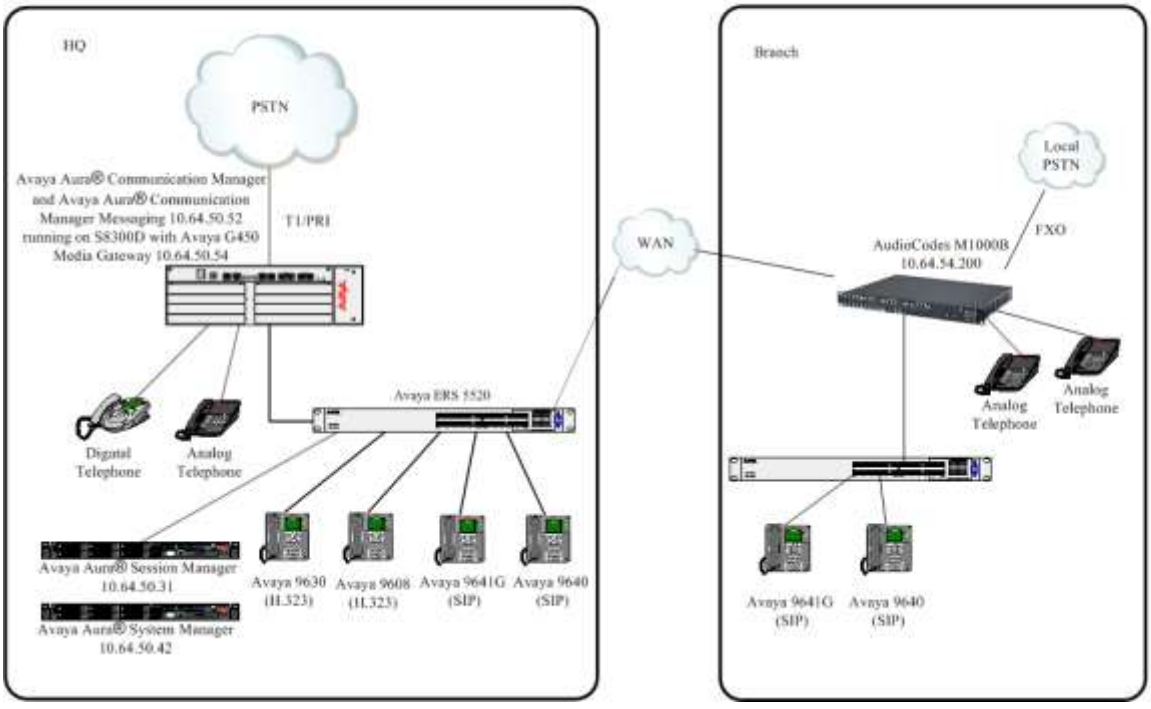


Figure 1: AudioCodes Multi Service Business Router Test Configuration

©2015 Avaya Inc. All Rights Reserved.

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 running on Avaya S8300D Server	6.3 03.0.124.0-21588
Avaya Aura® Session Manager	6.3.10.0.631008
Avaya Aura® System Manager	6.3.10.7.2656
Avaya 96x0 Deskphone	SIP 2.6.12.1, H.323 3.230A
Avaya 96x1 Deskphone	SIP 6.4.1.25, H.323 6.4014
Avaya 6211 and 6221 Analog Phone	-
Avaya 1416 Digital Phone	Rel. 39.0
AudioCodes Mediant 1000B	6.80A.244.006

5. Configure Avaya Aura® Communication Manager

The configuration between Communication Manager and Session Manager was via a SIP trunk group. This configuration was in place prior to this test, and followed standard configuration. Full details of this part of the configuration are not relevant to the tested solution. Only those particular configuration settings that are helpful to understanding the tested solution are provided, primarily relating to call routing.

5.1. Configuration Details for Communication Manager

The following configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

The changes made were:

- Configure IP Network Regions
- Configure IP Codecs
- Configure Signaling Group for Session Manager
- Configure SIP Trunks for Session Manager
- Configure Numbering Format for SIP Calls to Session Manager
- Create a route pattern that will use the SIP trunk to Session Manager
- Map Incoming DID Numbers to Internal Route Points
- Configure the Phone Settings File

©2015 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Configure IP Network Regions** Use the **change ip-network-region *n*** command, where ***n*** is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. In the case of the compliance test, the same IP network region that contains the Avaya S8300D Server and IP Telephones was selected to contain the Session Manager server. By default, the Server and IP telephones are in IP Network Region 1. On the **IP Network Region** form: ▪ The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is ***d4f27.com***. This name will appear in the "From" header of SIP messages originating from this IP region. ▪ By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the G450 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be restricted at the trunk level on the **Signaling Group** form. ▪ The **Codec Set** is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used, then Page 3 of each **IP Network Region** form must be used to specify the codec set for inter-region communications. ▪ The default values can be used for all other fields. **change ip-network-region 1** **Page 1 of 20** IP NETWORK REGION Region: 1 Location: 1 **Authoritative Domain: d4f27.com** Name: CM Local Stub Network Region: n MEDIA PARAMETERS **Intra-region IP-IP Direct Audio: yes** **Codec Set: 1** **Inter-region IP-IP Direct Audio: yes** UDP Port Min: 2048 IP Audio Hairpinning? y UDP Port Max: 65535 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

©2015 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Configure IP Codecs** Use the **change ip-codec-set *n*** command, where ***n*** is the codec set value specified in Step 1, to enter the supported audio codecs for calls routed to Session Manager. Multiple codecs can be listed in priority order to allow codec negotiation during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test.

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

                           IP CODEC SET

   Codec Set: 1

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


    Media Encryption
 1: none
 2:
 3:
```


©2015 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Configure Signaling Group for Session Manager** Use the **add signaling group *n*** command, where ***n*** is the number of an unused signaling group, to create the SIP signaling group as follows: ▪ Set the **Group Type** field to ***sip***. ▪ The **Transport Method** field will default to ***tls*** (Transport Layer Security). ▪ Specify the Avaya S8300D Server (node name ***procr***) and Session Manager (node name ***sm5031***) as the two ends of the signaling group in the **Near-end Node Name** and the **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form (not shown). ▪ Ensure that the TLS port value of ***5061*** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields. ▪ In the **Far-end Network Region** field, enter the IP network region value assigned in the **IP Network Region** form in Step 1. This defines which IP network region contains the Session Manager. If the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions. ▪ Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is ***d4f27.com***. This domain is specified in the Uniform Resource Identifier (URI) of the SIP "To" header in the INVITE message. ▪ The **Direct IP-IP Audio Connections** field is set to ***y***. ▪ The **DTMF over IP** field must be set to the default value of ***rtp-payload*** for a SIP trunk. This value enables Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values for the other fields may be used. **Note:** *Initially the **Peer Server** field will be set to **Others**. After the configuration has been completed and the signaling group is in service this field should display SM when connected to Session Manager.*

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

 Group Number: 2              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: Others
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                Far-end Node Name: sm5031
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                    Far-end Network Region: 1

Far-end Domain: d4f27.com
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate              RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                IP Audio Hairpinning? n
         Enable Layer 3 Test? y                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```


©2015 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Configure SIP Trunks for Session Manager** Add a SIP trunk group by using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. For the compliance test, trunk group number 2 was chosen. On Page 1, set the fields to the following values: ▪ Set the **Group Type** field to ***sip***. ▪ Enter a descriptive **Group Name**. ▪ Specify an available trunk access code (**TAC**) that is consistent with the existing dial plan. ▪ Set the **Service Type** field to ***tie***. ▪ Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in Step 3. ▪ Specify the **Number of Members** supported by this SIP trunk group. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk. In this solution, each analog endpoint at the branch counts as a SIP telephone. ▪ The default values may be retained for the other fields. **add trunk-group 2** **Page 1 of 21** TRUNK GROUP Group Number: 2 **Group Type: sip** CDR Reports: y Group Name: To_sm5031 COR: 1 TN: 1 **TAC: *002** 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: 2** **Number of Members: 10**

©2015 Avaya Inc. All Rights Reserved.

Step	Description
	Configure SIP Trunks for Session Manager (continued) ▪ Verify the **Numbering Format** field is set to ***private***. This field specifies the format of the calling party number sent to the far-end. ▪ The default values may be retained for the other fields. **add trunk-group 2** **Page 3 of 21** TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y **Numbering Format: private** UUI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n
5.	**Configure Numbering Format for SIP Calls to Session Manager** Use the **change private-unknown-numbering 6** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in Step 4. In the example shown below, all calls originating from a 5-digit extension beginning with 3 or 6 and routed across trunk group 2 will be sent as a 5 digit calling number. This calling party number will be sent to the far-end in the SIP "From" header. **change private-numbering 6** **Page 1 of 2** NUMBERING - PRIVATE FORMAT Ext Ext Trk Private Total Len Code Grp(s) Prefix Len **5 3** **2** **5** Total Administered: 2 **5 6** **2** **5** Maximum Entries: 540

©2015 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Create a route pattern that will use the SIP trunk to Session Manager** To create a route pattern, use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values may be retained for all other fields. **change route-pattern 3** **Page 1 of 3** Pattern Number: 3 **Pattern Name: To sm5031** SCCAN? n Secure SIP? n **Grp FRL** NPA Pfx Hop Toll No. Inserted DCS/ IXC **No** Mrk Lmt List Del Digits QSIG Dgts Intw **1: 2 0 0 n user** 2: n user 3: n user 4: n user 5: n user 6: n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: y y y y y n n rest 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
7.	**Configure the Phone Settings File** The settings file is not actually configured in Communication Manager, but is included in this section for brevity. The goal was to use a single settings file that could be used for all endpoints, in the branch. The complete settings file is not provided as it will differ in each deployment, but the following settings were required for survivable server functionality to apply to the phones. Full details of these settings can be found in the phone documentation [6]. Note, a SIP_CONTROLLER_LIST setting can be included, but is overridden by any configuration done in Session Manager for Survivability Servers (see section 6, Step 3). SET REGISTERWAIT "60" SET CONTROLLER_SEARCH_INTERVAL 4 SET FAST_RESPONSE_TIMEOUT 2 SET RECOVERYREGISTERWAIT 10

©2015 Avaya Inc. All Rights Reserved.

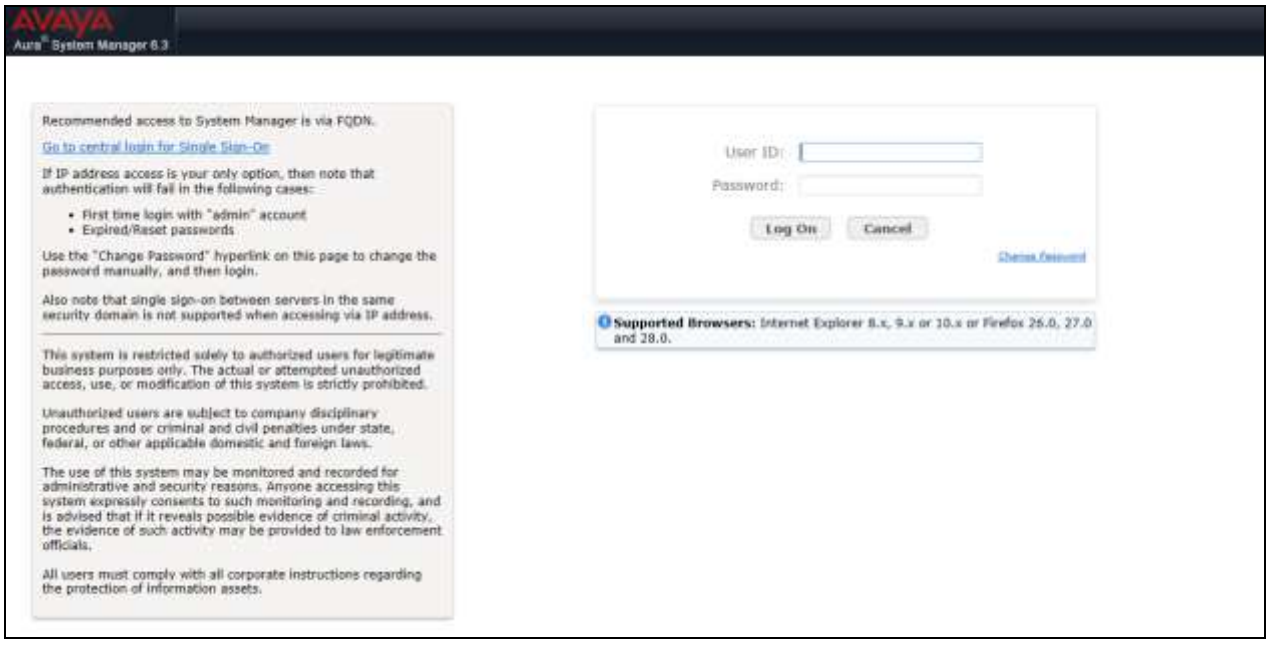
6. Configure Avaya Aura® Session Manager

This section covers the configuration of Session Manager. Session Manager is configured via System Manager using an Internet browser.

As this test used an in-place, standard configuration for the core SIP elements, only those steps relevant to the configuration of the AudioCodes MSBR will be described. Additional details pertaining to call routing are also provided in order to understand the functional elements of this tested solution.

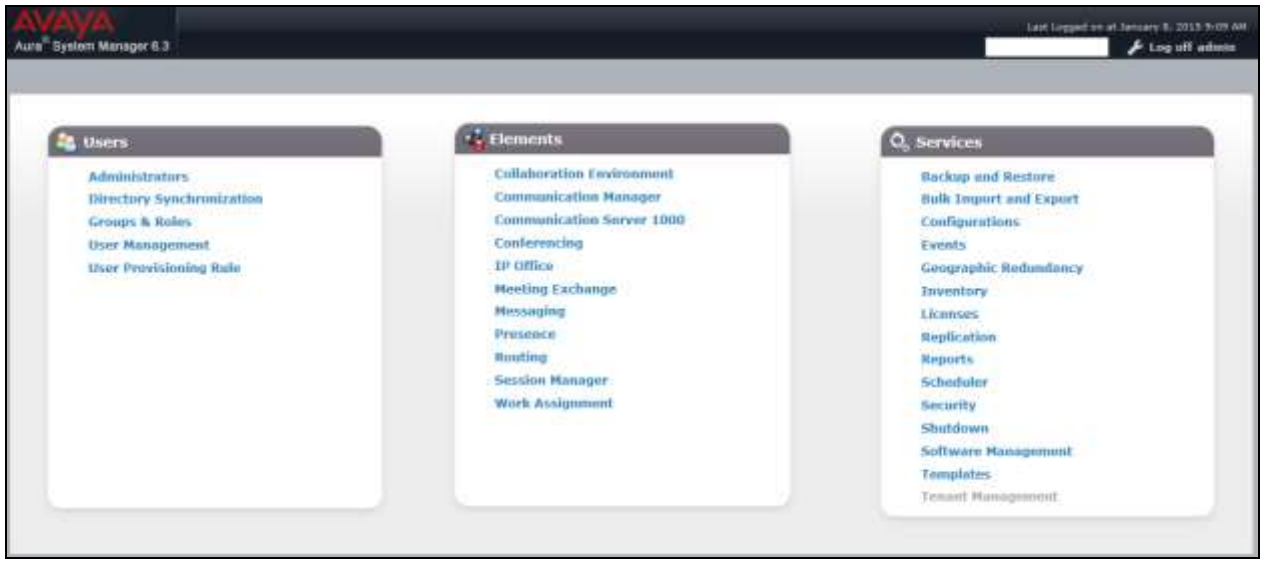
For additional information on these and other configuration tasks, refer to [2].

Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as **https://<*hostname*>/SMGR** where **<*hostname*>** is the ip address or the Fully Qualified Domain Name of the System Manager. Login using appropriate credentials.

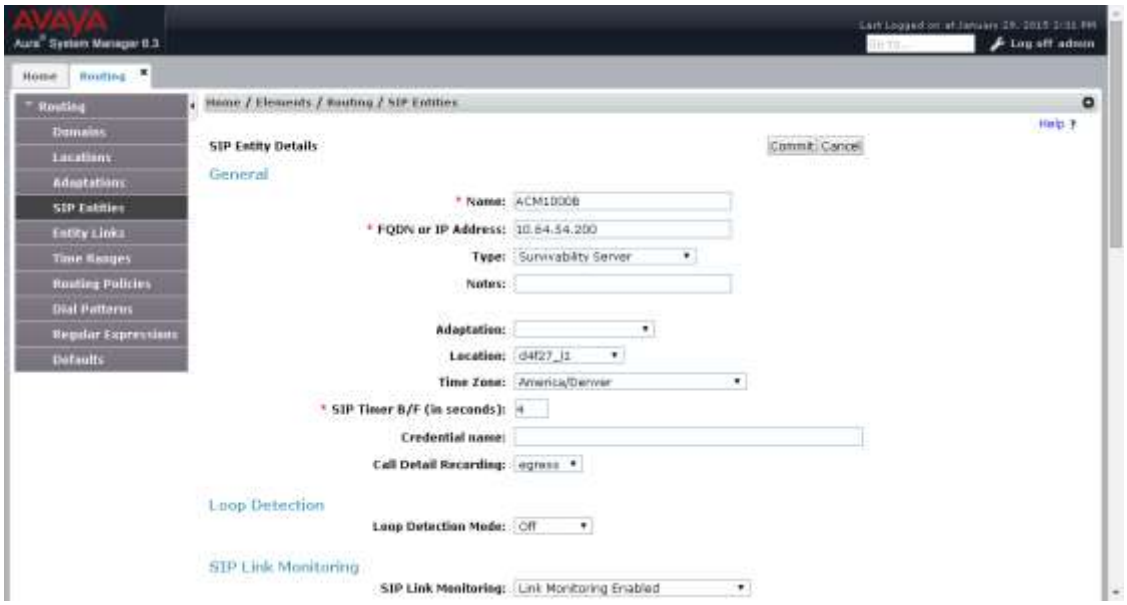


The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment.

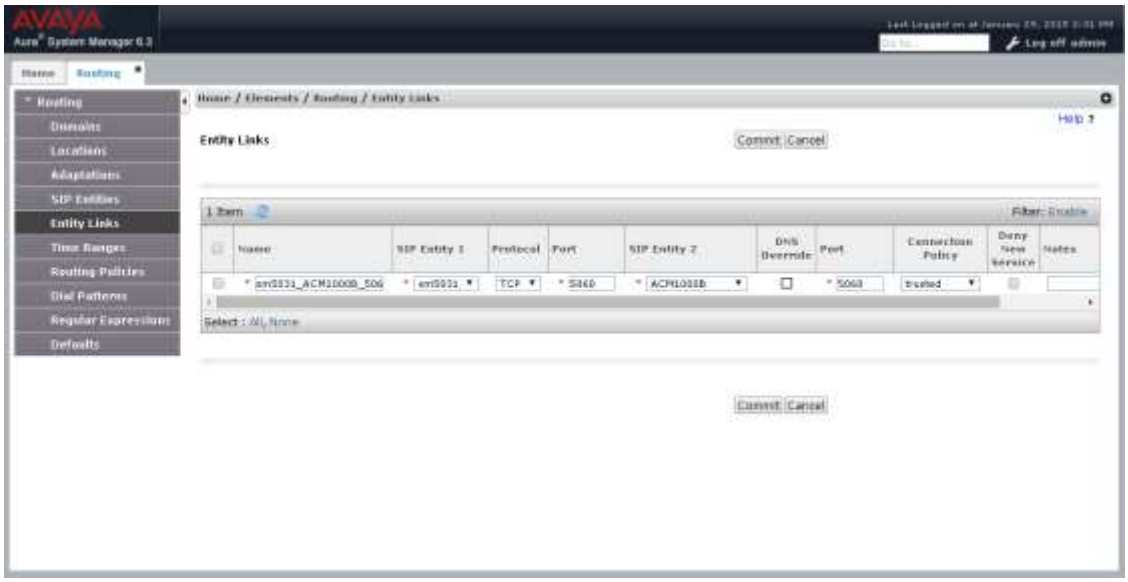
©2015 Avaya Inc. All Rights Reserved.



©2015 Avaya Inc. All Rights Reserved.

Step	Description
1	**Add SIP Entity and Entity Links for the MSBR Branch Router** The AudioCodes MSBR establishes a TCP SIP connection to Session Manager. The purpose is to establish a socket for heartbeats so the gateway knows when the WAN link is in service. Additionally, when the MSBR is used by the Enterprise for call routing, an established SIP Entity Link with the SIP Peer is required in order for calls to be routed to the MSBR. The Mediant 1000 was administered as a "***Survivability Server***" Entity **Type.** The **Location** (***d4f27_l1***) correlated to the location of **Branch** endpoints and the Mediant 1000 gateway. This location was previously defined and can be used in routing rules as described in **Step 3** below. Note: During compliance testing the 46xxsettings.txt file was modified to assign the SIP phone with registration information for the MSBR when in survivability mode. The Audio Codes MSBR listens for registration from phones on port 5080 using TCP. See **Step 4** below. 

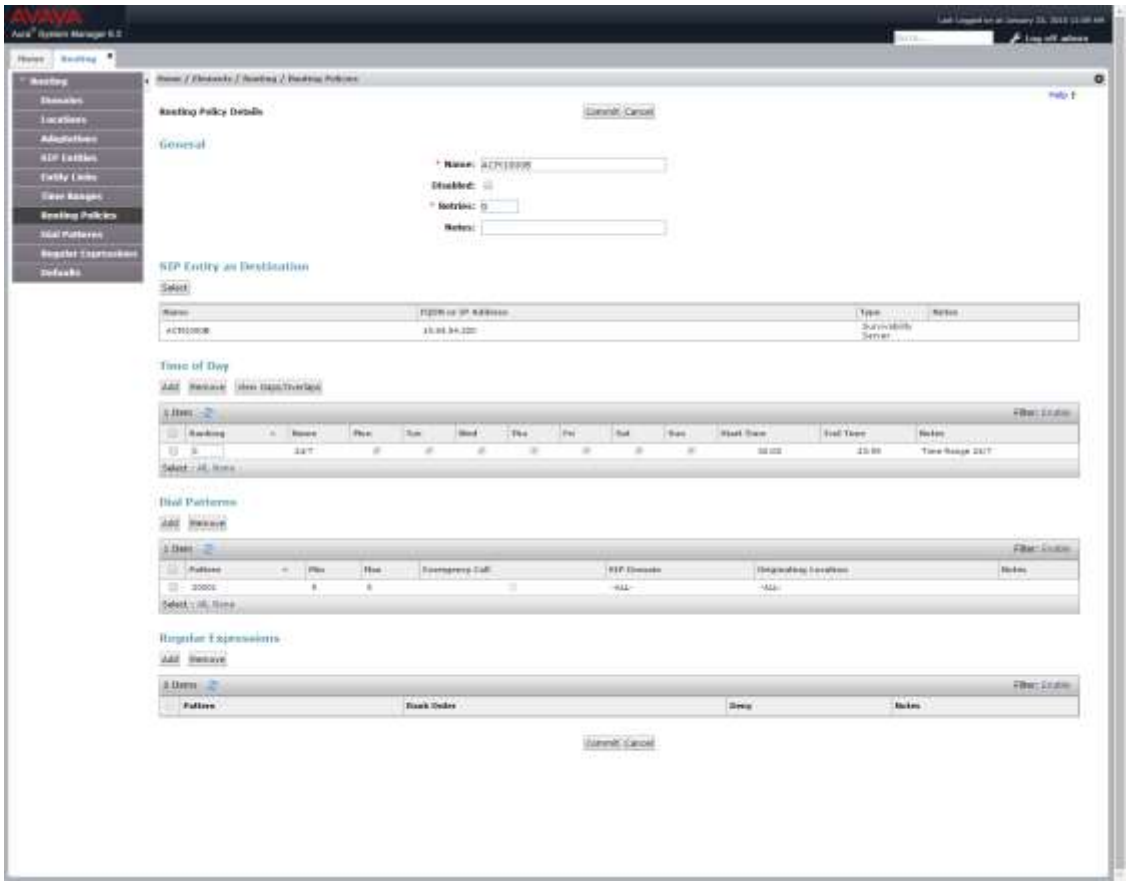
©2015 Avaya Inc. All Rights Reserved.

Step	Description
	Add SIP Entity and Entity Links for MSBR (Continued) **Entity Links** were administered after completing the **SIP Entity** above by clicking the **Entity Links** navigation link (not shown) and separately administering these settings as shown below. 

©2015 Avaya Inc. All Rights Reserved.

2 **Configure Routing Policies**

In order for calls to be routed to the PSTN through the MSBR's Analog FXO lines to the PSTN, a Routing Policy was created for the Branch. Below is a summary snapshot of the **Routing Policies**:

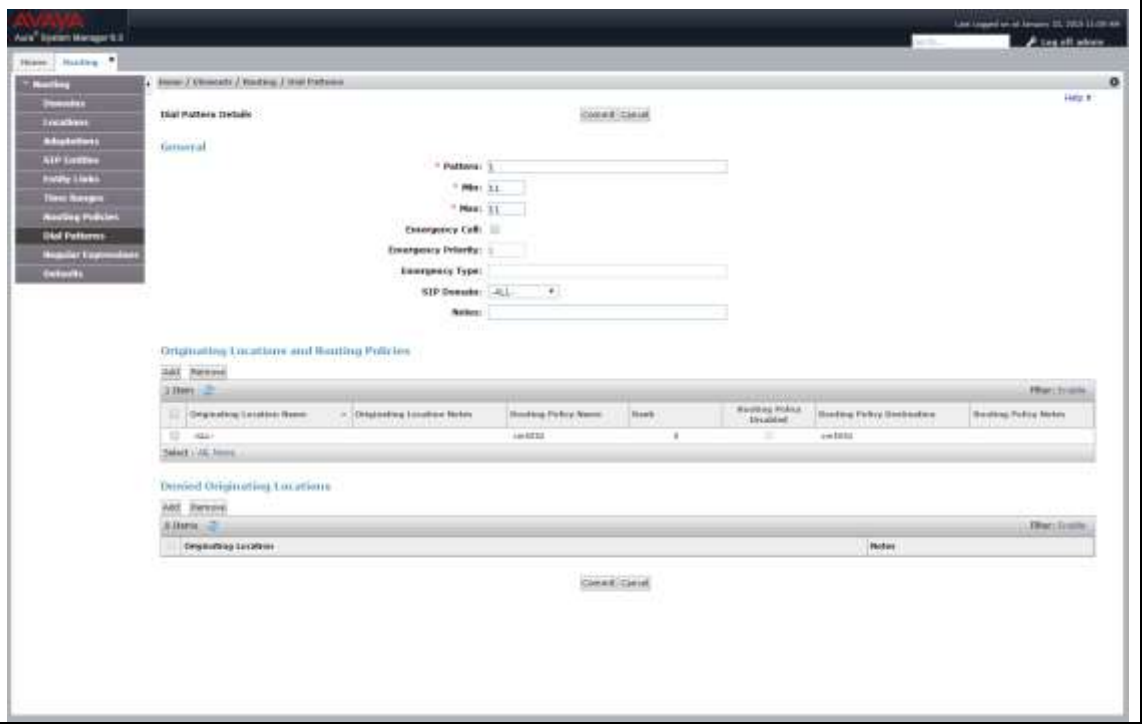


Each routing policy was created by selecting **Routing Policies** in the left pane, then clicking the **New** button (not shown). For SIP Entity as Destination, the ***AudioCodes M1000*** SIP Entity created in **Step 1** was selected from a list of all entities (not shown), and ***20001*** was from previously administered **Dial Patterns**. When this policy was enabled, calls to 20001 from any Enterprise user were routed to the SIP Entity **ACM1000B** at the **Branch**.

©2015 Avaya Inc. All Rights Reserved.

Configure Routing Policies (Continued)

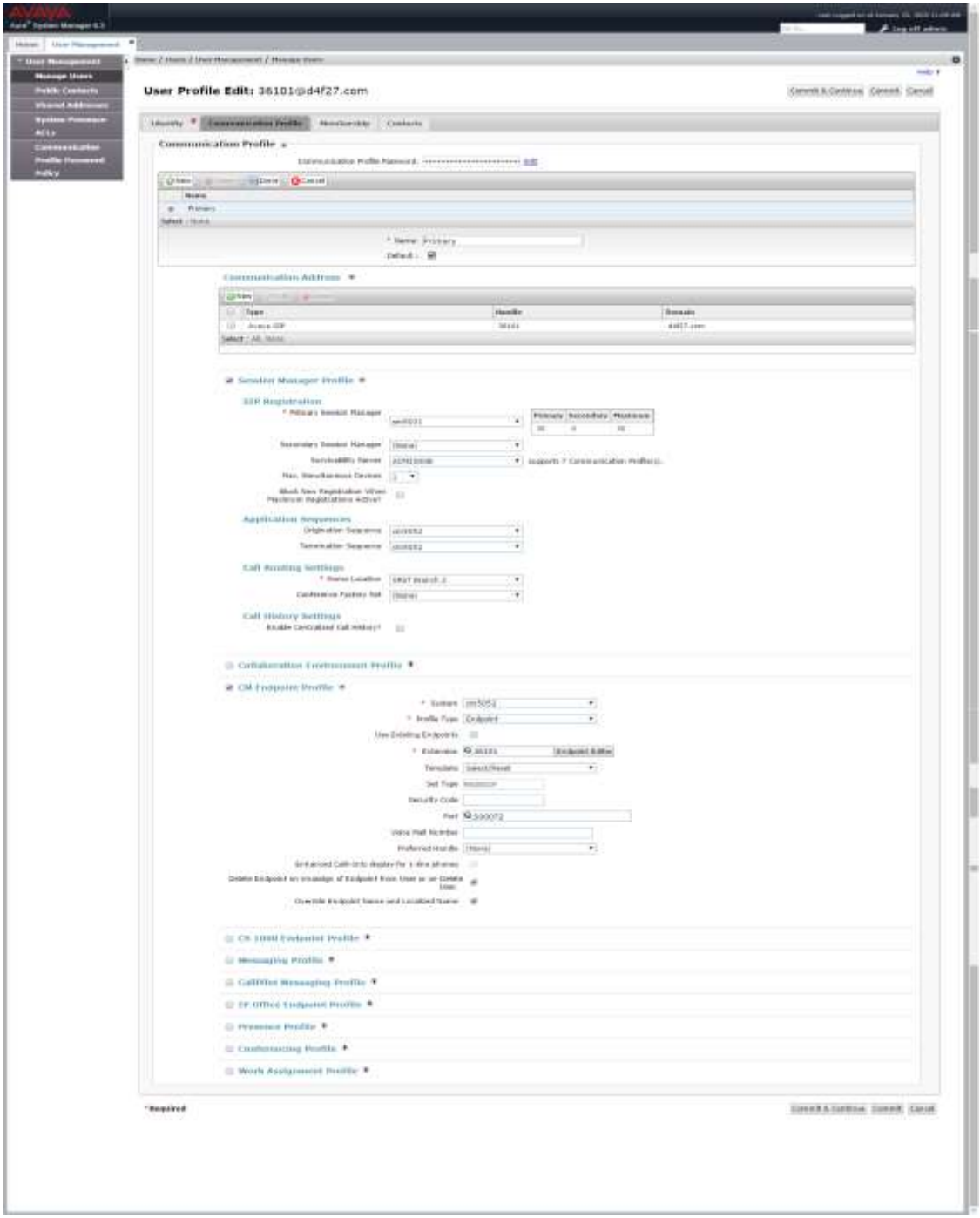
The ***1*** **Dial Pattern** was previously configured as follows. Note that this Dial Pattern was configured to apply to calls originating from ***ALL*** locations. However, dial patterns can also be administered to only apply to calls originating or destined to/from endpoints in the **d4f27_l1** location as mentioned in **Step 1** above (not shown).



©2015 Avaya Inc. All Rights Reserved.

3 **Modify Existing Users to add a Survivable Server**

All endpoints were previously created, existing SIP accounts were used for the analog FXS ports at each branch which were previously administered as 9608 SIP set types. Configuration of these endpoints is not covered in these Application Notes as they followed standard practice. However, the one setting that is enabled on each endpoint is to assign the **Survivability Server** defined in Step 1 above. This is done by editing each User and navigating to the **Communication Profile** tab.



©2015 Avaya Inc. All Rights Reserved.

4 46xxsettings File

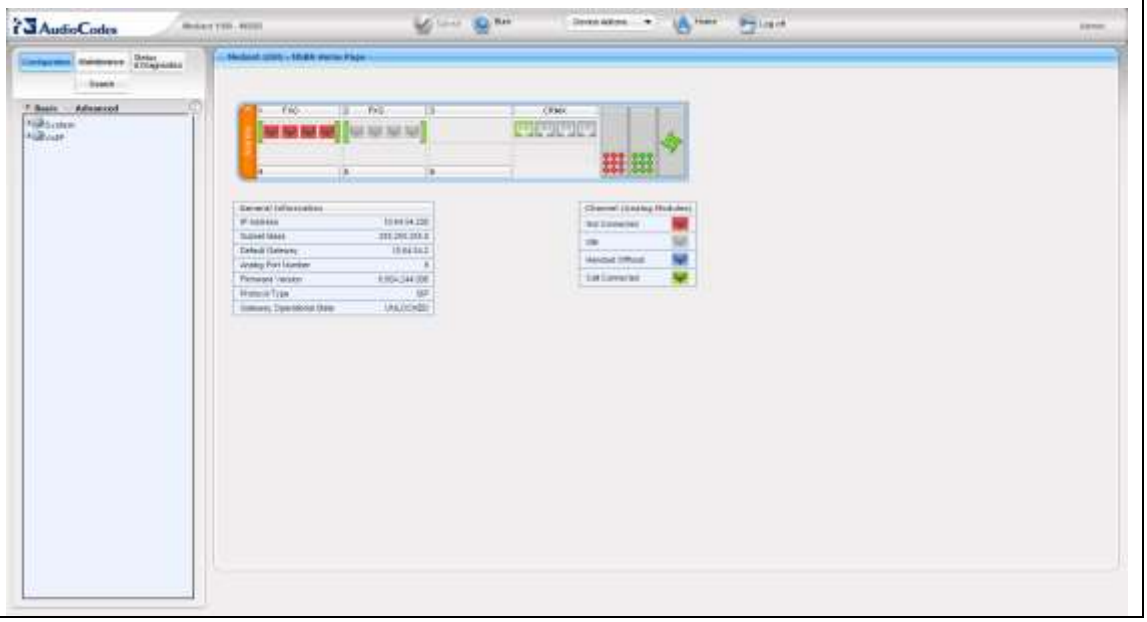
The configuration parameters of the Avaya 9600 series telephones specific to SIP Survivability and the sample configuration are described in this section.

46xxsettings.txt Parameter Name	Values Used in Sample Configuration	Description
SIPDOMAIN	d4f27.com	Sets the SIP domain name to be used during registration.
SIP_CONTROLLER_LIST	10.64.50.31:5060; transport=tcp, 10.64.54.200:5080;transport=tcp	A priority list of SIP Servers for the phone to use for SIP services. The port and transport use the default values of 5061 and TLS when not specified. The current settings have the Session Manager as the primary SIP registration server and the local branch MSBR as the secondary SIP registration server. Note: Port 5080 matches port used by the MSBR when in SAS mode.
FAST_RESPONSE_TIMEOUT	2	The timer terminates SIP INVITE transactions if no SIP response is received within the specified number of seconds after sending the request. Useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss. The default value is 4 seconds. After the SIP INVITE is terminated, the phone immediately transitions to Survivability Mode.
SIMULTANEOUS_REGISTRATIONS	1	The number of Session Managers in the configuration that the phone will simultaneously register with. Range: (1-3) Default Value: 3 (release 2.6 and above)
ENABLE_PPM_SOURCED_SIPPROXYSRVR	0	Enables PPM as a source of SIP Proxy server information. When this is set to 1 then proxy server information discovered via PPM will be used. The default value of this parameter is 1. This value is set to 0 in this configuration to allow the SIP_CONTROLLER_LIST setting to take effect from the 46xxsettings.txt file.

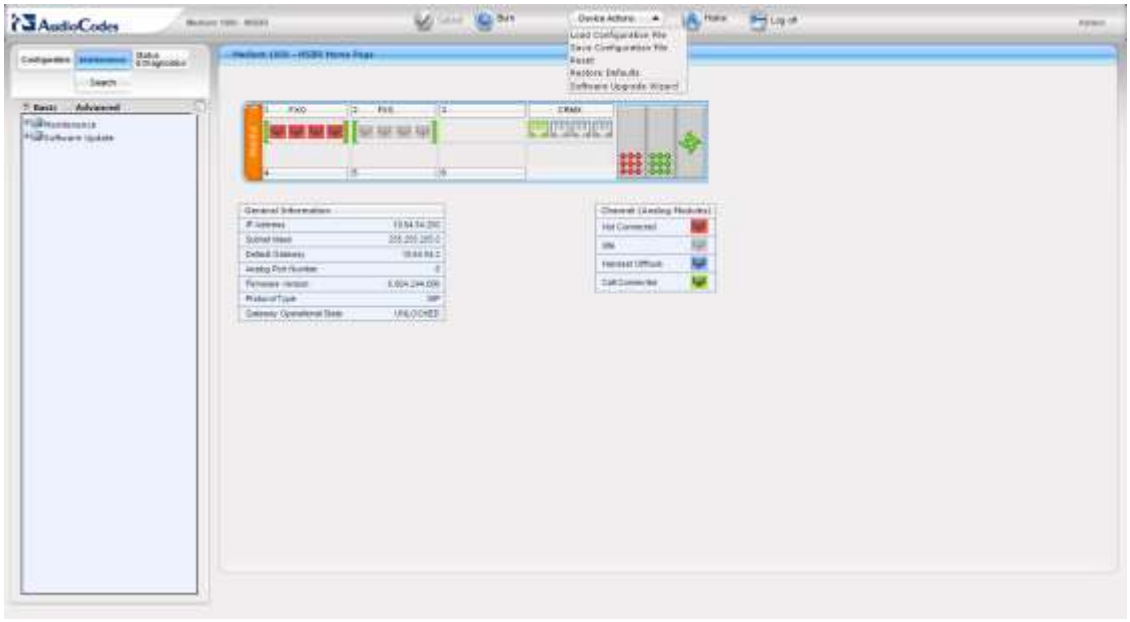
©2015 Avaya Inc. All Rights Reserved.

7. AudioCodes MSBR Configuration

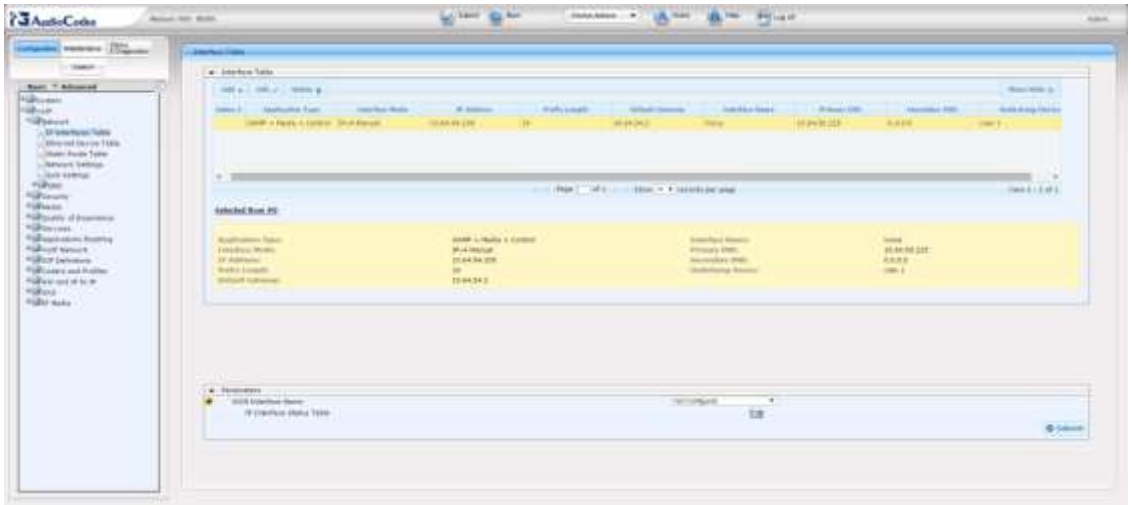
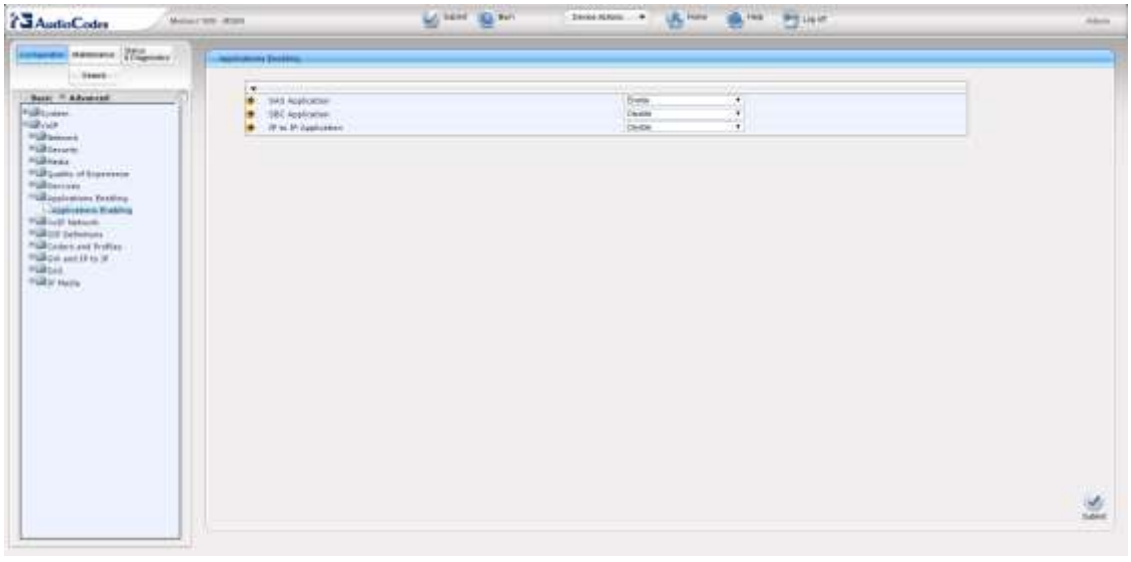
This section describes the procedures for configuring the Mediant 1000 MSBR. These procedures assume the MSBR has been installed using the procedures documented in the AudioCodes Installation Manual and has been assigned an IP address for network connectivity.

Step	Description
1.	**Login to the MSBR** The configuration of the Mediant 1000 MSBR is done via a Web browser. To access the device, enter the **IP address** of the MSBR in the **Address** field of the web browser. The IP address was entered during **Installation.**
2.	**Login credentials** The following pop-up window will appear. **Login** with the proper credentials. 
3.	**MSBR Main Page at Login** The MSBR main page will appear as shown below. 

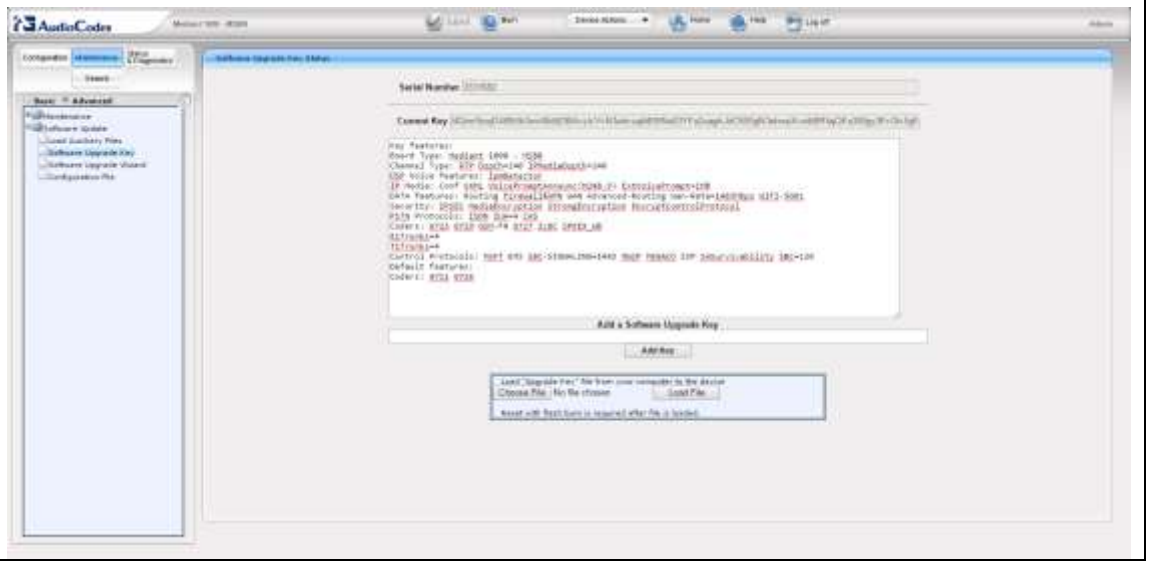
©2015 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Saving the MSBR Configuration** It is recommended to periodically save the configuration as the following steps of this configuration guide are completed. Return to the home web page and select **Maintenance** in the left pane. Under **Maintenance Actions c**lick the **BURN** button (also in the menu buttons bar on top of the window). The **Device Actions** button on the top can be used as well for access to the same page. 

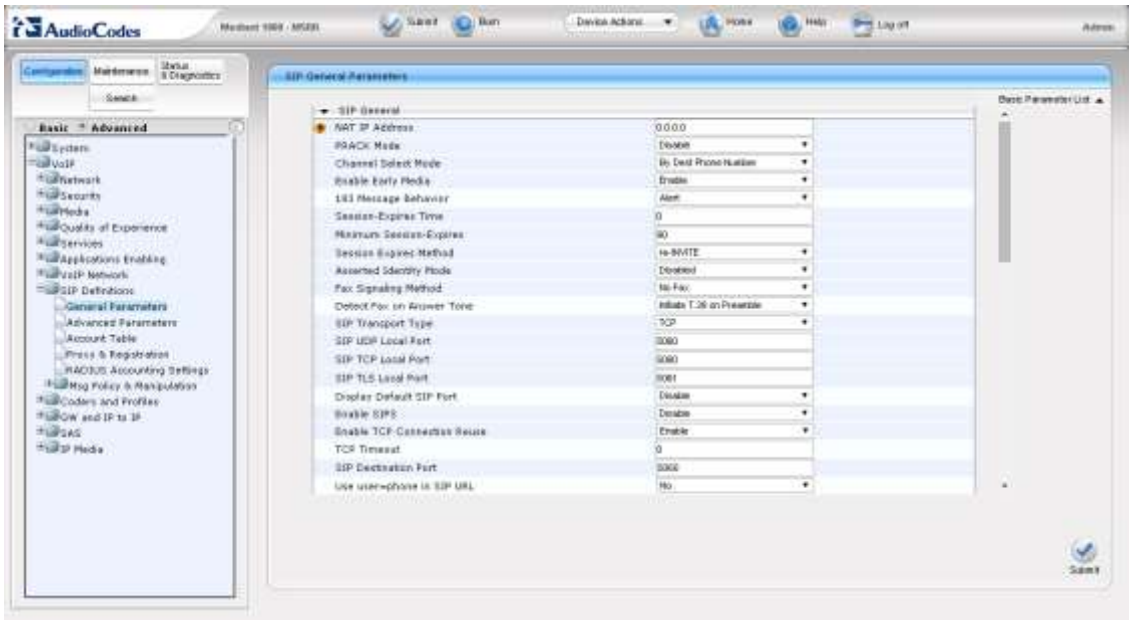
©2015 Avaya Inc. All Rights Reserved.

Step	Description
5.	**View Network Settings** The network settings that were configured during installation can be viewed by selecting **Configuration** in the left pane then navigating to **VoIP → Network → IP Interface Table** for displaying the **Interface Table** in the right pane. If necessary, changes can be made to the settings on this page followed by clicking **Submit**. For the compliance test, the **IP Address**, **Subnet Mask** and **Default Gateway Address** were set to values consistent with the test configuration shown in **Figure 1**. 
6.	**Set Application Enabling for SAS** To access these parameters, select **VoIP → Applications Enabling → Applications Enabling** in the left pane. The pull-down choices for Applications Enabling are shown below. Note the *yellow-bolt icon* indicator requires that a "***device reset***" be performed. This alters the content of the configuration screens from this point forward. 

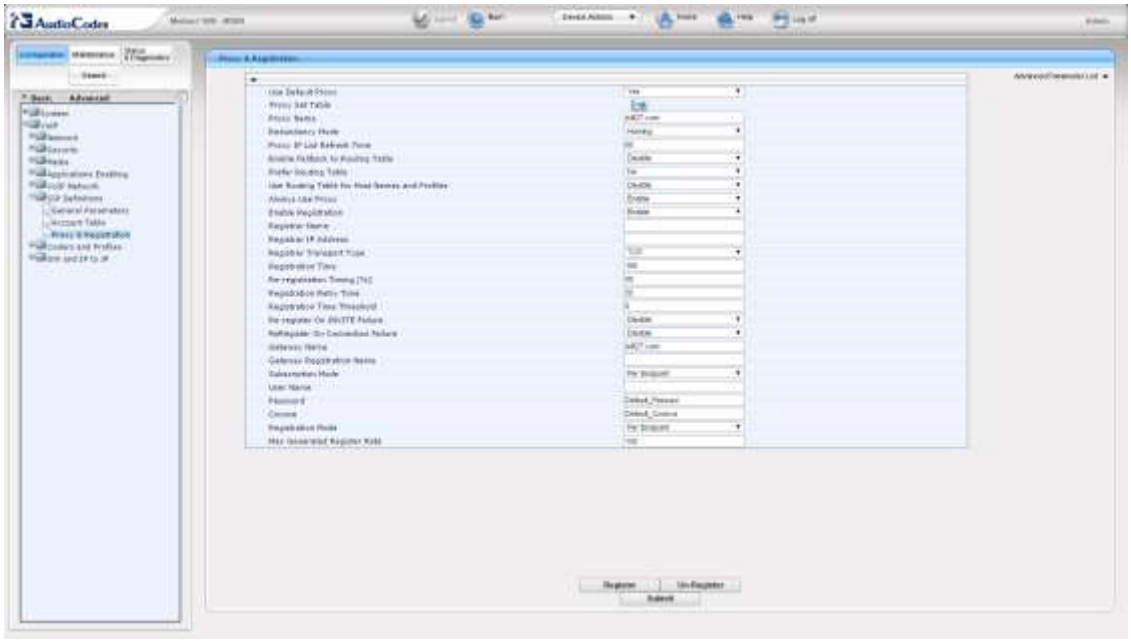
©2015 Avaya Inc. All Rights Reserved.

Step	Description
7.	**Feature and License Key** To access the Feature Key information, go to the main **HOME** page of the MSBR GUI. Select **MAINTENANCE** tab on the left, then **Software Options** in the left pane and drop-down to **Software Update Key**. The features licensed and supported on the MSBR for compliance testing are displayed below: 

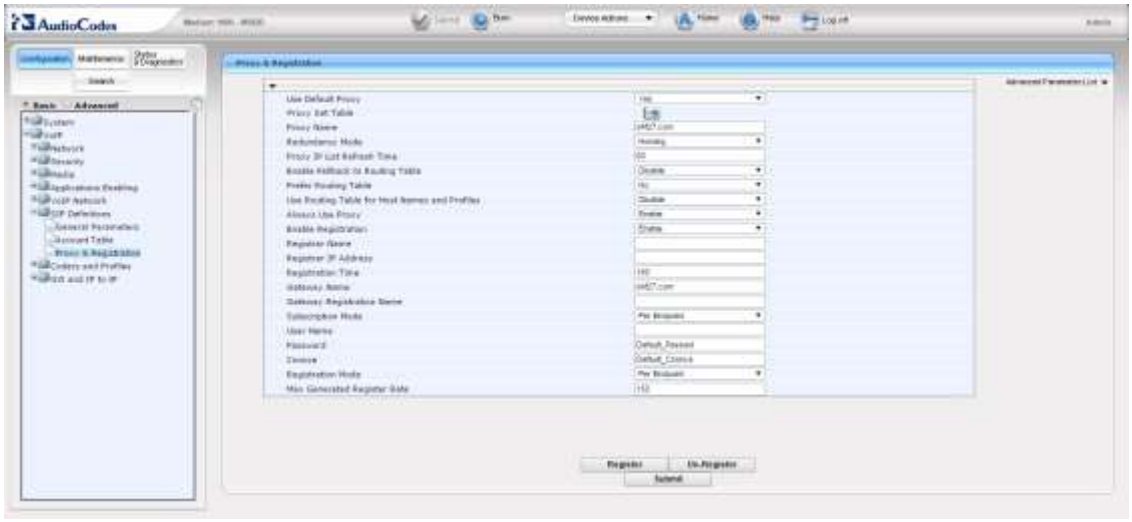
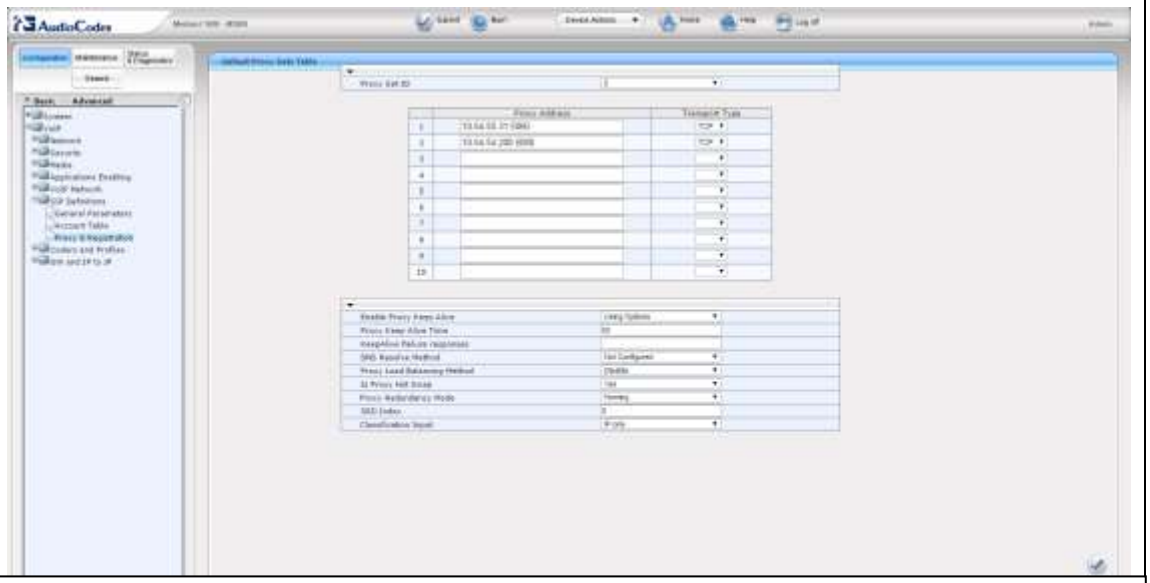
©2015 Avaya Inc. All Rights Reserved.

Step	Description
8.	**SIP General Parameters** To access these parameters, select **VoIP → SIP Definitions → General Parameters** in the left pane. Configure the parameters as described below. ▪ For the **Channel Select Mode** field, select ***By Dest Phone Number***. ▪ For the **Enable Early Media** field, select ***Enabled***. If enabled, the MSBR sends Session Description Protocol (SDP) information in the 18x responses allowing the media stream to be set up prior to answering the call. ▪ Select ***TCP*** for the **SIP Transport Type** field; Enter port ***5060*** for **SIP UDP Local Port**. ▪ Select ***No*** for the **Use user=phone in SIP URL** field. Default values may be retained for all other fields. Scroll down to the bottom of the page and click **Submit**. 

©2015 Avaya Inc. All Rights Reserved.

Step	Description
9.	**Proxy and Registration** From the menu shown in Step 3, navigate to **VoIP → SIP Definition → Proxy & Registration**. Configure the parameters as described below. ▪ For the **Use Default Proxy** field, select ***Yes*** from the pull-down menu. ▪ Enter "***d4f27.com***" for the **Proxy Name** ▪ Set **Redundancy Mode** to ***Homing*** ▪ For the **Always Use Proxy** field, select ***Enable***. ▪ For the **Enable Registration** field, select ***Enable***. This will allow the MSBR to register the FXS endpoints with the Avaya Session Manager. ▪ In the **Gateway Name** field, enter the SIP domain configured on Session Manager ▪ **Registration Mode** is set to ***Per Endpoint*** Click **Submit**. *Note: Homing provides the ability to revert registrations back to Session Manager when connection is re-established.* Default values may be retained for all other fields. Scroll down to continue configuring parameters on the lower half of the screen. 

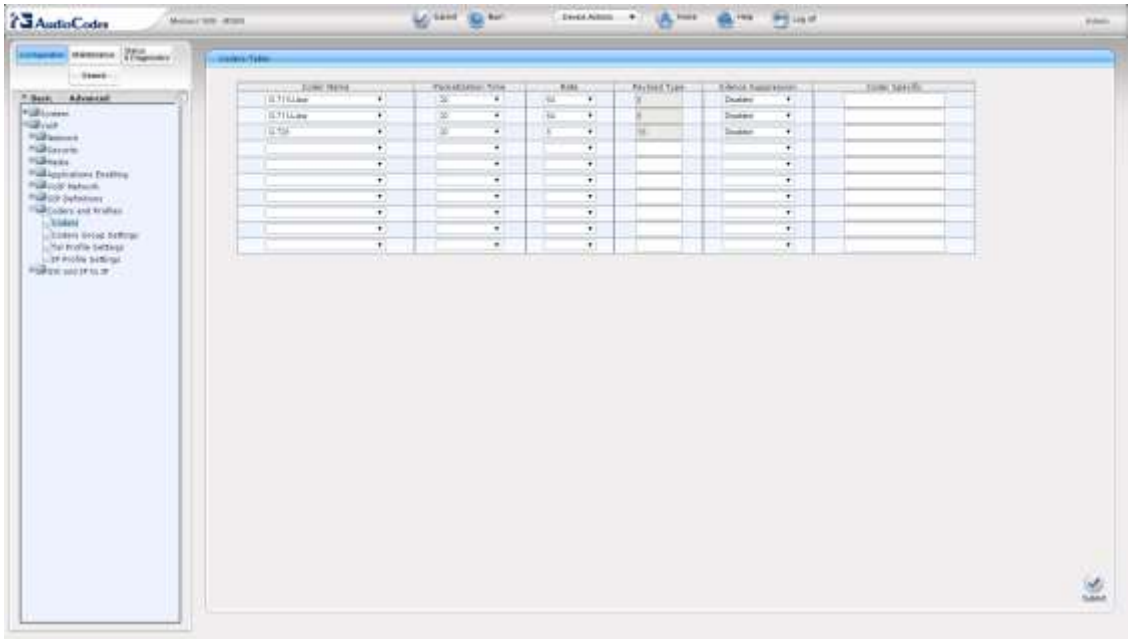
©2015 Avaya Inc. All Rights Reserved.

Step	Description
10.	**Proxy Set Table** From the menu shown in Step 3, navigate to **VoIP → SIP Definitions → Proxy & Registration.** Click on the right-arrow icon button for **Proxy Set Table.** See the drop down menu below.  Enter the **Proxy Address** for the Session Manager in Line 1 specifying port ***5060***. Set address transport to ***TCP***. Enter the **Proxy Address** for the MSBR SAS specifying port ***5080*.** Set address transport to **TCP**. For **Enable Proxy Keep Alive** select ***Using Options*** from the pull-down menu. See Notes below: 

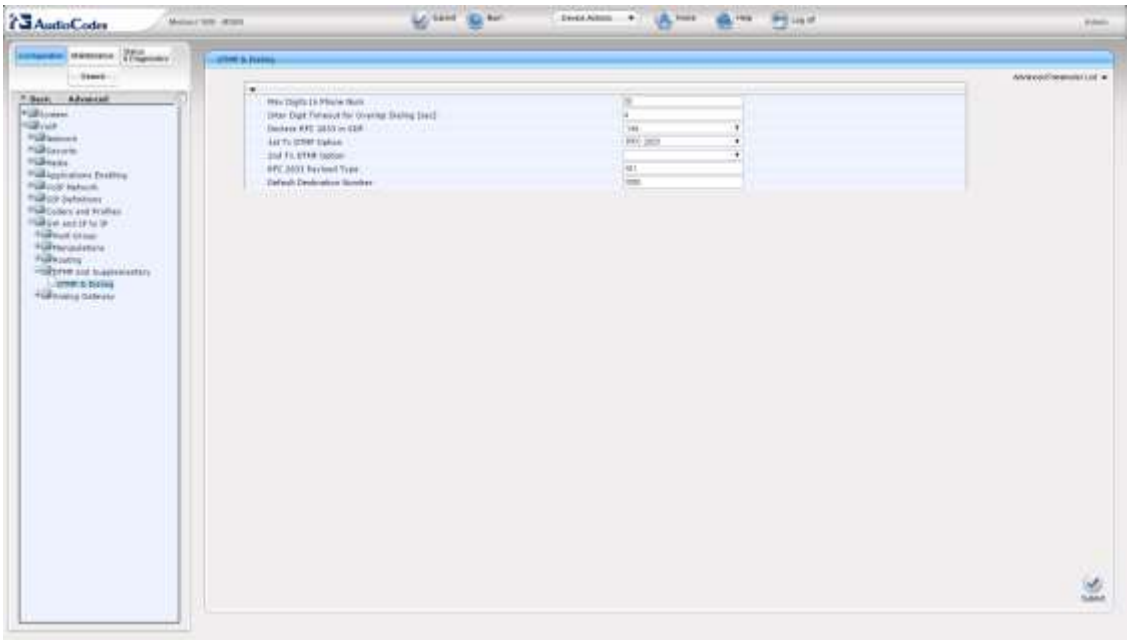
Note: The Proxy Set table prioritizes calls based upon availability. The first line is the Proxy that calls normally use. The second line is the Proxy that is used if the first is not available. With SAS, the first PROXY is not available so the second proxy is the primary address. This is the SAS gateway IP Address and 5080 is the port that is typically assigned. The SAS Gateway provides routing (Hunt Group) to a FXO port for outbound calls.

Note: The MSBR will use the SIP OPTIONS message as a handshake mechanism with Session Manager to determine if the SIP connection is up. If the connection is down, the MSBR will failover to the SAS application which will in turn utilize the FXO ports.

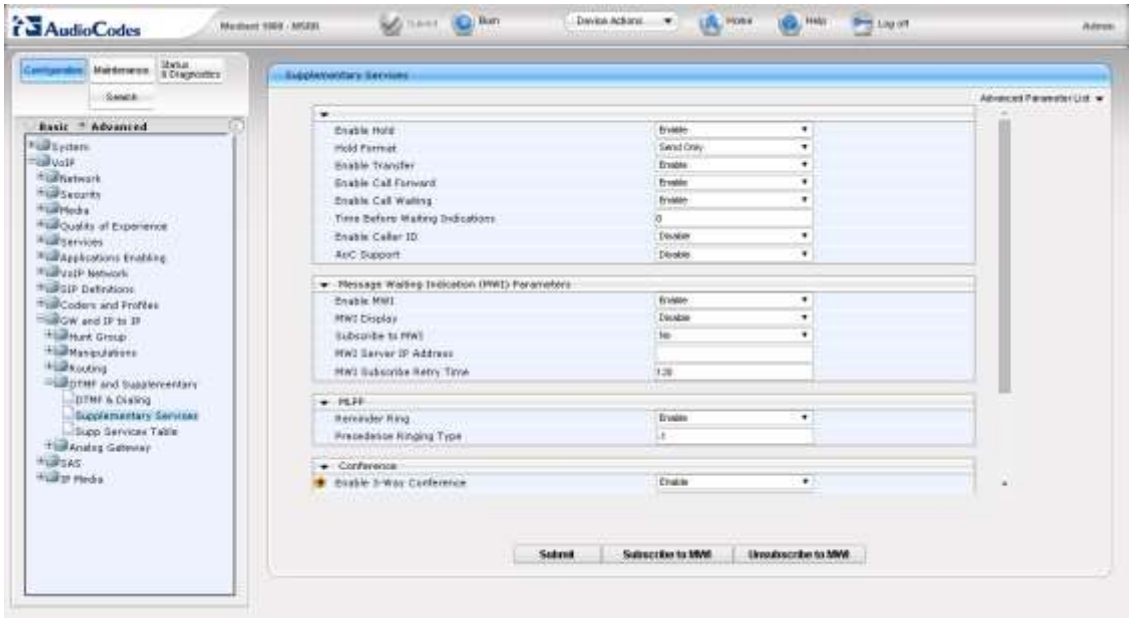
©2015 Avaya Inc. All Rights Reserved.

Step	Description
11.	**CODECS** From the menu shown in Step 3, navigate to **VoIP → Coders And Profiles → Coders**. In the screen below, select the list of preferred codecs to be used by the MSBR with the most preferred codec at the top and working downward to the least preferred. This list must have an overlap with the list provided on Communication Manager. The codec is selected from the pull-down menu under the **Coder Name** field. The codec list used for the compliance test is shown in the example below. ***G.711U-law*** was selected as the most preferred followed by ***G.711A-law*** and followed by ***G.729*** as the next-preferable codec. Click **Submit**. 

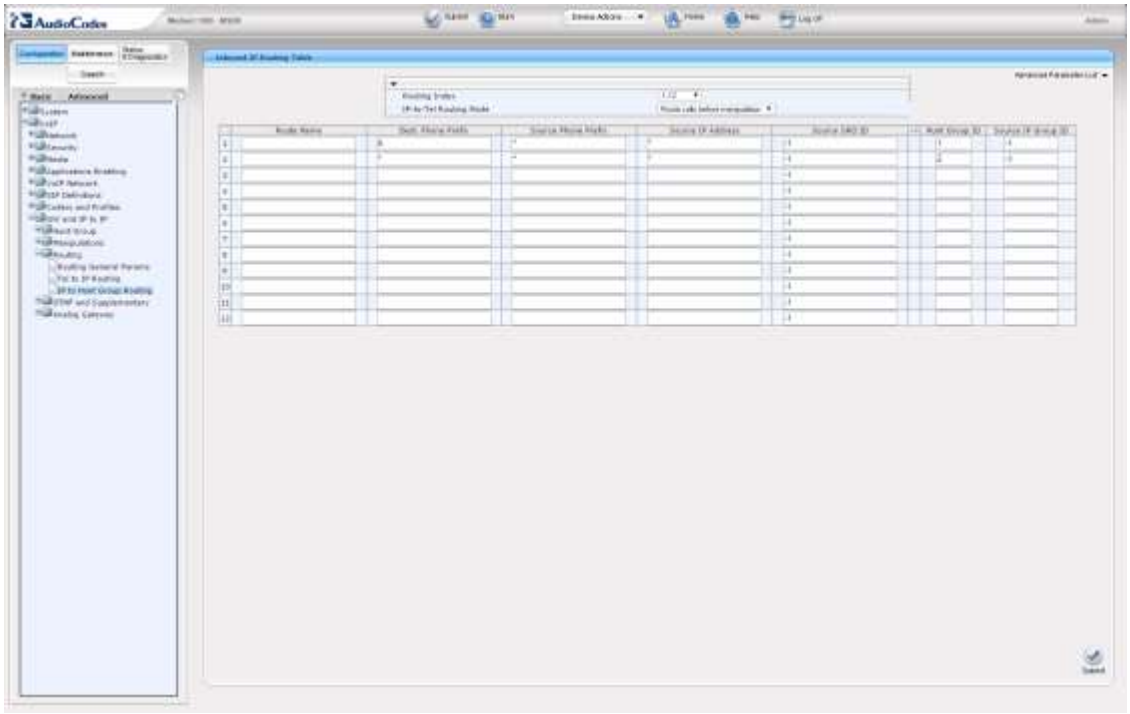
©2015 Avaya Inc. All Rights Reserved.

Step	Description
12.	**DTMF and Dialing** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → DTMF & Dialing**. Configure the parameters as described below. ▪ In the **Max Digits in Phone Num** field, enter the maximum number of digits that can be dialed. ▪ For the **Declare RFC 2833 in SDP** field, select ***Yes***. ▪ For the **1st Tx DTMF Option** field, select ***RFC 2833***. This selects RFC 2833 as the preferred DTMF transmission method. ▪ Enter ***101*** as the **RFC 2833 Payload Type** to match the value used by the Avaya SIP Telephones. Media may not be redirected (shuffled) in all scenarios from Communication Manager to the endpoints if this value is not the same as the SIP Telephones. Default values may be retained for all other fields. Click **Submit**. 

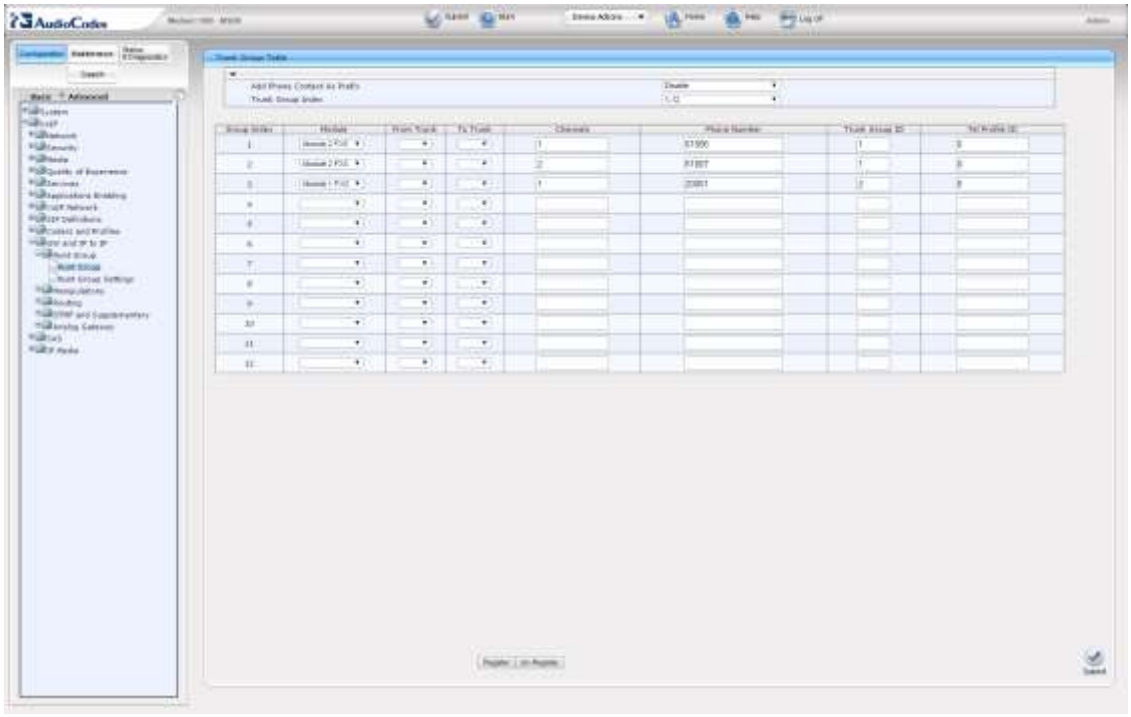
©2015 Avaya Inc. All Rights Reserved.

Step	Description
13.	**Supplementary Services** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → DTMF & Supplementary → Supplimentary Services**. Configure the parameters as described below. ▪ If the analog phones connected to the MSBR support Caller ID then set the **Enable Caller ID** field to ***Enable***. For the compliance test, this field was set to ***Disable*** since none of the analog phones used had a display. ▪ The **Hold Format** field is set to ***Send Only*.** ▪ Select ***Enable*** for the **Enable MWI** field if the analog phones support a visual MWI indicator. For the compliance test, even though these fields were enabled, MWI was only tested for stutter dial tone. ▪ Hold, Transfer, Call Forward and Call Waiting are enabled by default. Default values may be retained for all other fields. Scroll down to the bottom of the page and click **Submit** (not shown). 
14.	**Manipulation Tables**. Digit Manipulation was not included during testing but can be added and configured per the applicable AudioCodes User's Manual available on the AudioCodes website.

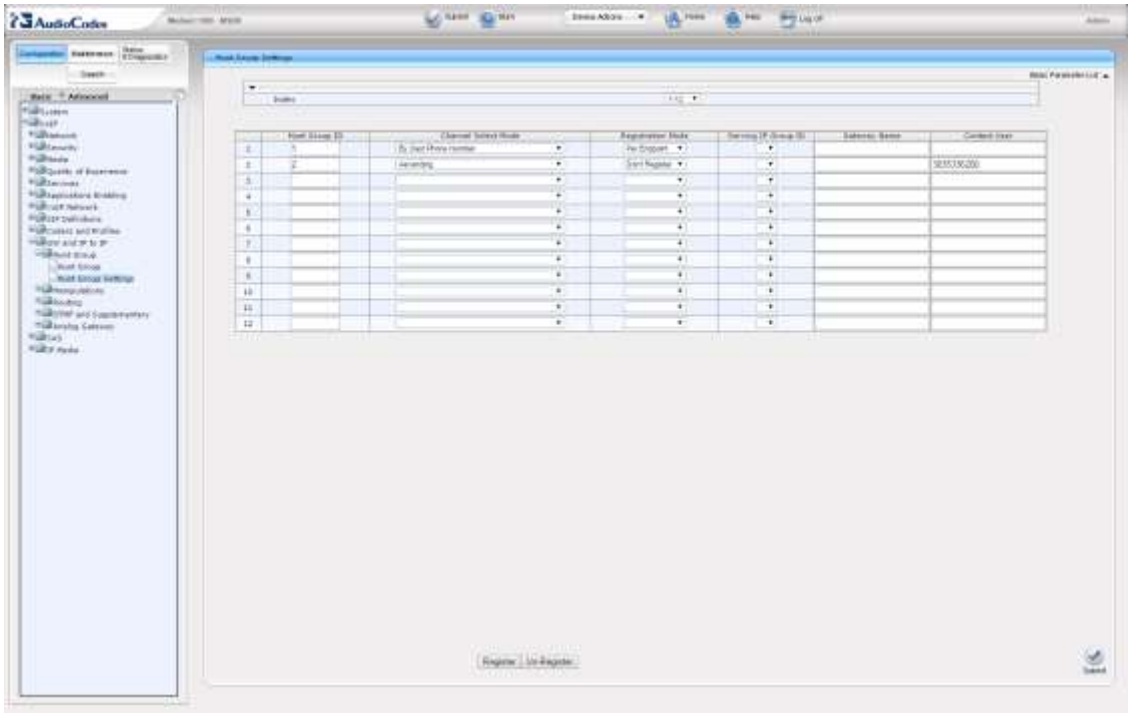
©2015 Avaya Inc. All Rights Reserved.

Step	Description
15.	**Routing Tables** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → Routing → IP to Hunt Group Routing** in the left pane. The pull-down choices for the **Routing Tables** are shown below. This table defines the mapping of IP calls to a group of channels or "hunt group". In Step 19, the **FXS ports** are assigned to **hunt group 1** and the **FXO ports** are assigned to **hunt group 2**. **NOTE: Trunk Group** and **Hunt Group** are interchangeable terminology**.** A **Hunt Group** refers to analog functionality. A **Trunk Group** is a more generic terminology and is also applicable to *digital trunks*. The **Dest. Phone Prefix**, **Source Phone Prefix** and **Source IP Address** columns define which calls are mapped to the hunt group in the **Hunt Group ID** column. In the first entry in the example below, all calls to any **extension 6xxxx** from any source extension and source IP will be routed to **hunt group 1**. Thus, the dialed number must be an exact match. The second entry routes any other call to **hunt group 2**. This entry is needed for the failover case. If a user dials an outbound number and it cannot reach the main site, this table will direct the call to **hunt group 2** which contains the FXO ports for access to the PSTN. Click **Submit**. 

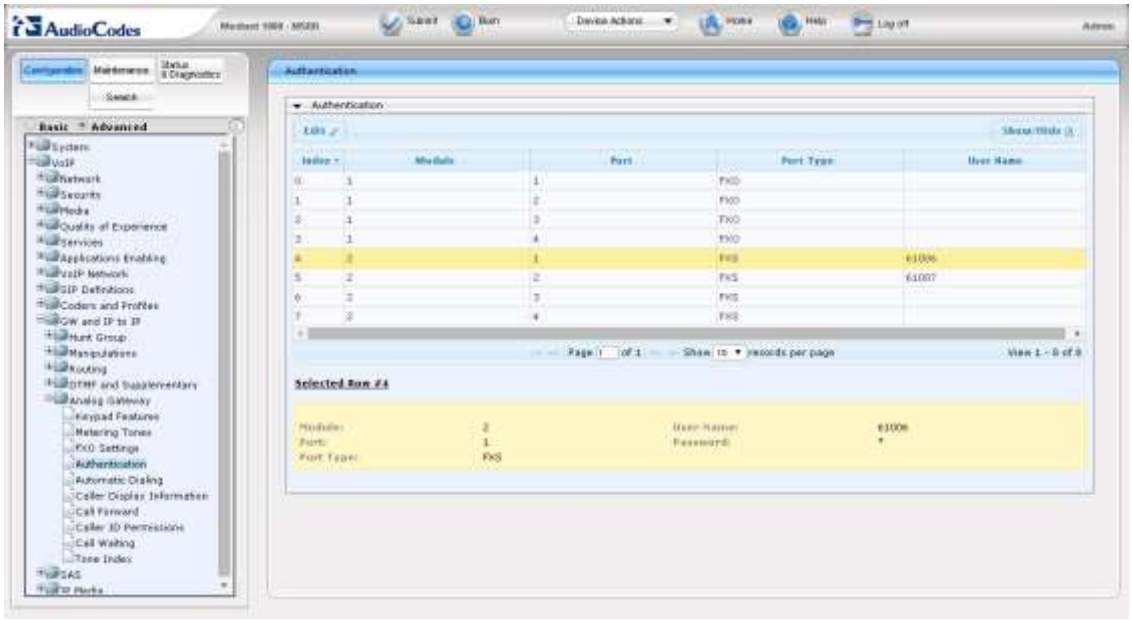
©2015 Avaya Inc. All Rights Reserved.

Step	Description
16.	**Endpoint Phone Numbers** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → Hunt Group → Hunt Group** in the left pane. The Hunt Group maps a particular channel/port to a phone number and hunt group. In the **Channel(s)** column, enter a range of channels to be assigned. In the **Phone Number** column, enter the starting extension for the range of extensions. In the **Trunk Group ID** column, enter the hunt group that contains these extensions. In the example below, the third entry assigns **FXO** channel ***1*** (the first FXO port) with extension ***20001*** to Trunk Group ID ***2***. The first and second entries assign **FXS** channels ***1*** and ***2*** with extensions **61006** and **61007** respectively to Trunk Group ID ***1***. Since only the first FXO port was connected to the PSTN, only channel 1 was enter in this table. Click **Submit**. 

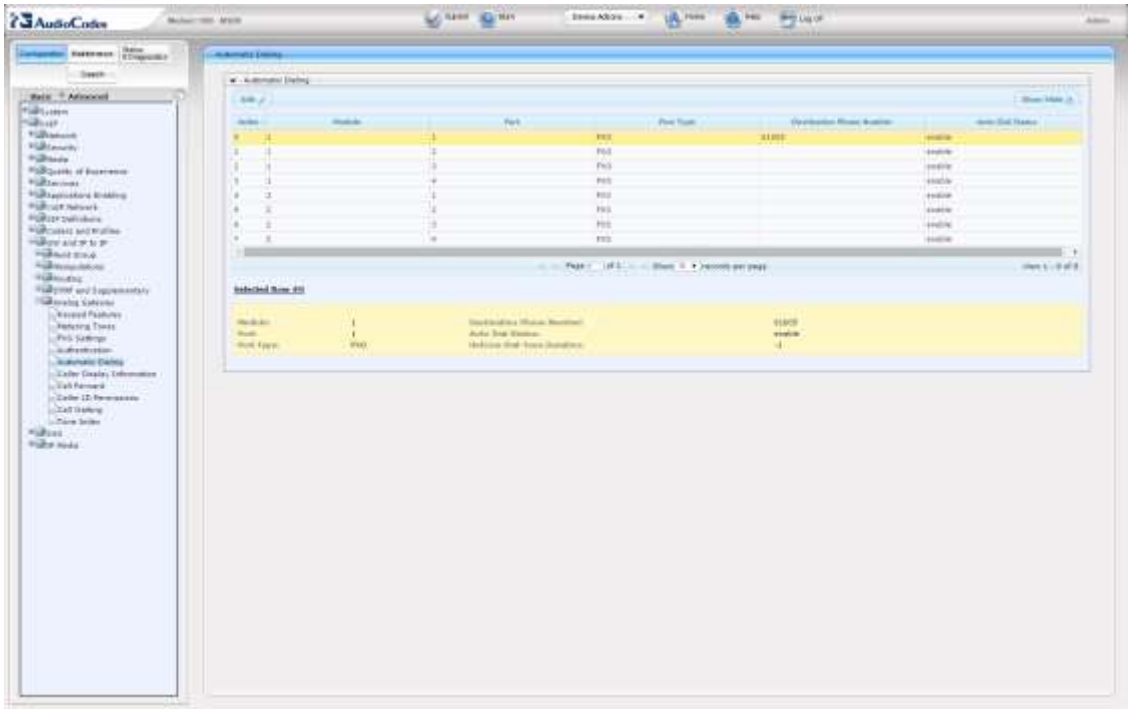
©2015 Avaya Inc. All Rights Reserved.

Step	Description
17.	**Hunt Group Settings** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → Hunt Group → Hunt Group Settings** in the left pane. Configure the parameters are described below. ▪ For **Hunt Group ID 1** which contain the FXS (endpoint) ports, select the **Channel Select Mode** as ***By Dest Phone Number***. Thus, each port in this hunt group will only be selected if its destination phone number is dialed. Select the **Registration Mode** to be ***Per Endpoint***. ▪ For **Hunt Group ID 2** which contain the FXO (POTS) ports, select the **Channel Select Mode** as ***Ascending***. The ports in this hunt group are treated as a pool, and each will be selected in ascending order. Select the **Registration Mode** to be ***Don't Register***. Set the **CONTACT** as **3035336200** for **Caller ID.** ▪ This allows the MSBR to register **per endpoint** for all the FXS port using the gateway extension entered in Step 17. The MSBR requires that only the FXS port be registered since registration was enabled in Step 9. Click **Submit**. 

©2015 Avaya Inc. All Rights Reserved.

Step	Description
18.	**Analog Gateway Settings Authentication** From the menu shown in Step 3, navigate to **VoIP → GW and IP to IP → Analog Gateway → Authentication**. The Authentication page defines a username and password combination for authentication of each MSBR port with Session Manager. Highlight an FXS row and click **Edit** (Not Shown) to enter a **User Name** and **Password** that matches the values configured on Session Manager for the user extension. 

©2015 Avaya Inc. All Rights Reserved.

Step	Description
19.	**Automatic Dialing** From the menu shown in Step 3, navigate to navigate to **VoIP → GW and IP to IP → Analog Gateway →Automatic Dialing**. The Automatic Dialing page provides the mapping of incoming calls on the FXO ports to a branch extension when the data WAN is unavailable. In the example below, an FXO port is mapped to an extension at the branch location. The destination extension is placed in the **Destination Phone Number** column. Click **Submit**. 
20.	**Fax/Modem/CID Settings** Fax was not included in testing but can be added and configured per the applicable AudioCodes User's Manual available on the AudioCodes website.

©2015 Avaya Inc. All Rights Reserved.

Step	Description
21.	For setting the disconnect detection time for Current Disconnect of talk-battery to signal a media disconnect event, an additional parameter must be changed in the ini file. From a web browser, enter <*ip_address*>/*AdminPage* in the **Address** field where <*ip_address*> is the IP address of the MSBR. The main page will appear as shown below. In this instance, the detection is reported as a disconnect at 600ms of no talk-battery. Enter parameter name: CURRENTDISCONNECTDURATION and Enter Value: 600 

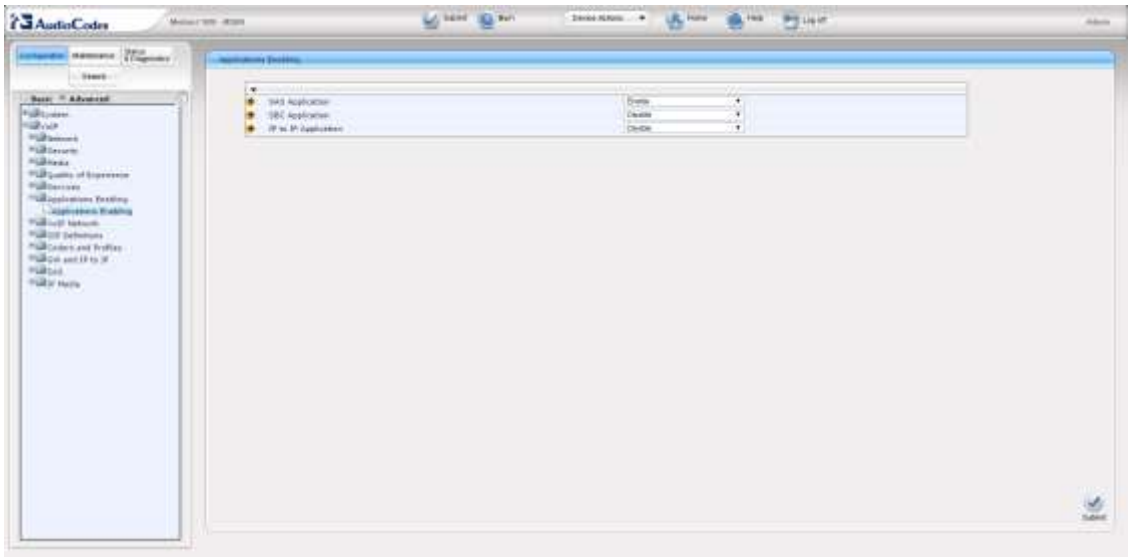
Additional SAS Configuration for MSBR

SAS supports various configuration possibilities, depending on how the device is deployed in the network and the network architecture requirements. This section provides step-by-step procedures on configuring the SAS application, using the device's Web interface.

The SAS configuration includes the following:

- General SAS settings - common to all deployment types
- SAS redundant mode
- MSBR running the Gateway application together with the SAS application
- Optional, advanced SAS features

©2015 Avaya Inc. All Rights Reserved.

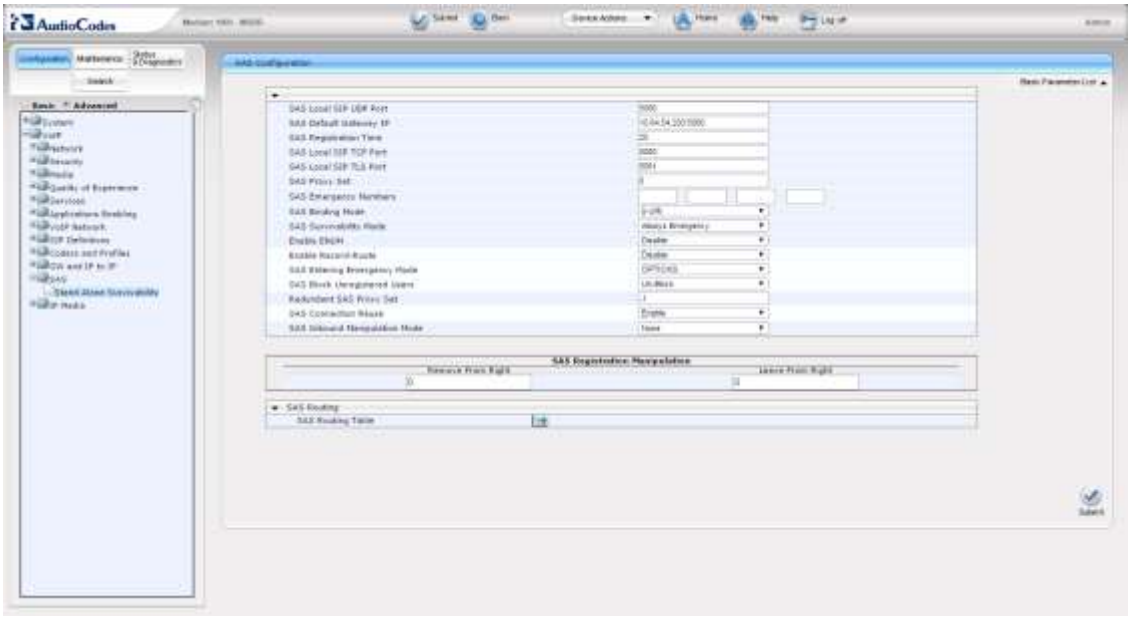
Step	Description
1.	**Enabling the SAS Application on the MSBR** Before beginning to configuring SAS, SAS application must be enabled on the device. Once enabled, the device's Web interface provides the SAS pages for configuring SAS. **Note: The SAS application is available only if the device is installed with the SAS Software Upgrade Key. If the device is not installed with the SAS feature, please contact an AudioCodes representative** **To enable the SAS application:** (*configured in Section 7, Step 6*) Open the 'Applications Enabling' page (**VoIP → Applications Enabling → Applications Enabling**). From the **Enable SAS** drop-down list, select ***'Enable'***.  Click **Submit**. Save the changes to the flash memory with a device reset; after the device resets, the **SAS** menu appears and the SAS application configuration can be started.

©2015 Avaya Inc. All Rights Reserved.

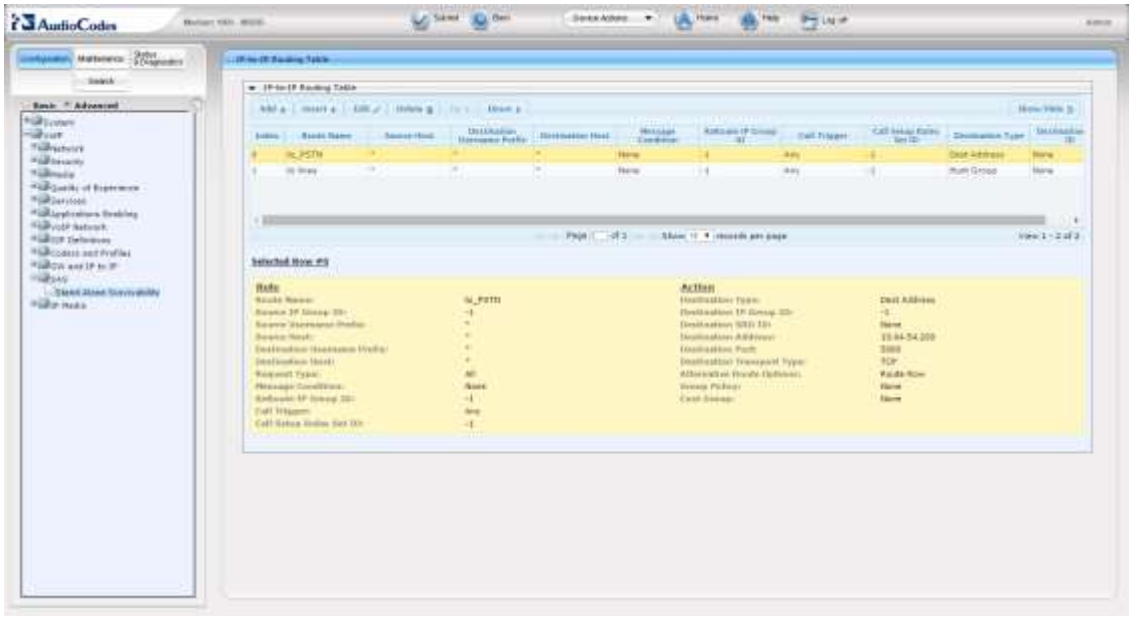
Step	Description

2.	**Defining MSBR SAS Settings**
	The common SAS settings include configuring the various SAS parameters and defining the Proxy Set ID for the SAS proxy. This configuration must be completed to replicate the test scenarios. The procedure below describes how to configure SAS settings that are common to all SAS modes.
	
	To configure common SAS settings:
	• Open the 'SAS Configuration' page (**VoIP → SAS → Stand Alone Survivability**).
	• Define the port used for sending and receiving SAS messages. This can be any of the following port types:
	  o UDP port - defined in the 'SAS Local SIP UDP Port' field
	  o TCP port - defined in the 'SAS Local SIP TCP Port' field
	  o TLS port - defined in the 'SAS Local SIP TLS Port' field
	
	 **Note:** This SAS port must be different to the device's local gateway port (i.e., that defined for the 'SIP UDP/TCP/TLS Local Port' parameter in the 'SIP General Parameters' page.
	
	In the **SAS Default Gateway IP** field, define the IP address and port (in the format x.x.x.x:port) of the device (i.e., Gateway application). Note that the port of the device is defined by the parameter **SIP TCP Local Port** (refer to the note above).
	
	In the **SAS Registration Time** field, define the value for the SIP Expires header that is sent in the 200 OK response to an incoming REGISTER message when SAS is in emergency state.
	
	From the **SAS Binding Mode** drop-down list, select the database binding mode:
	• ***0-URI***: If the incoming AOR in the REGISTER request uses a 'tel:' URI or 'user=phone', the binding is done according to the Request-URI user part only. Otherwise, the binding is done according to the entire Request-URI (i.e., user and host parts - user@host).
	• ***1-User Part Only***: Binding is done according to the user part only.
	
	Select '1-User Part Only' in cases where the UA sends REGISTER messages as SIP URI, but the INVITE messages sent to this UA include a Tel URI. For example, when the AOR of an incoming REGISTER is sip:3200@domain.com, SAS adds the entire SIP URI (e.g., sip:3200@domain.com) to its database (when the parameter is set to '0-URI'). However, if a subsequent Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS searches its database for "3200", which it does not find. Alternatively, when this parameter is set to '1-User Part Only', then upon receiving a REGISTER message with sip:3200@domain.com, SAS adds only the user part (i.e., "3200") to its database. Therefore, if a Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS can successfully locate the UA in its database.

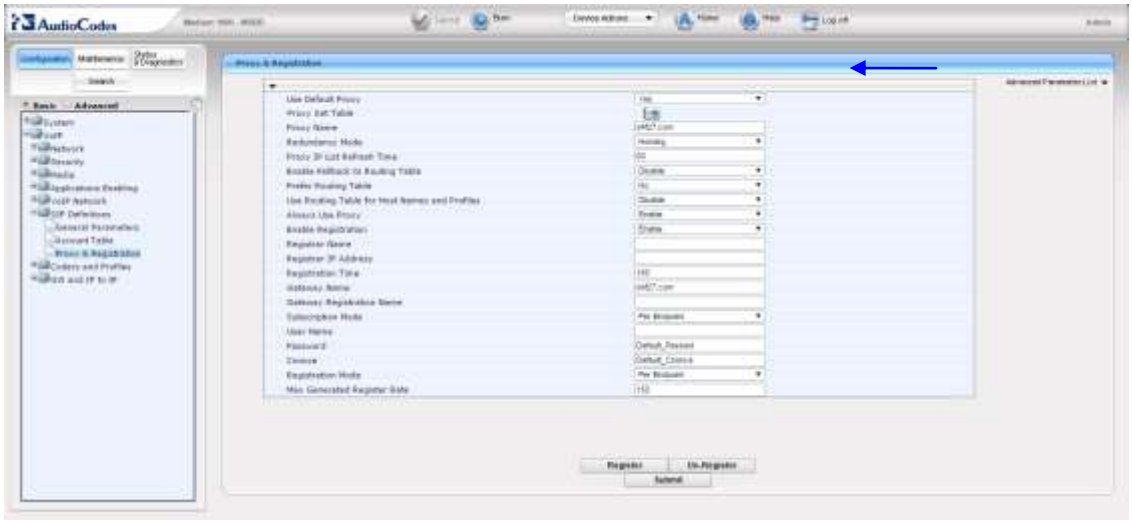
©2015 Avaya Inc. All Rights Reserved.

Step	Description
	Defining MSBR SAS Settings (Continued) This section describes how to configure the SAS redundant mode. This configuration must be completed to replicate the test scenarios. These settings are in addition to the ones described previously. **Note:** The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their primary proxy is the external proxy and the **redundant** proxy destination addresses and port is the same as that configured for the device's SAS IP address and SAS SIP port. **To configure SAS redundant mode:** • Open the 'SAS Configuration' page (**VoIP → SAS → Stand Alone Survivability**). • From the **SAS Survivability Mode** drop-down list, select one of the following depending on whether the UAs support homing (i.e., they always attempt to operate with the primary proxy, and if using the redundant proxy, they switch back to the primary proxy whenever it's available): **UAs support homing:** Select ***Always Emergency***. This is because SAS does not need to communicate with the primary proxy of the UAs; SAS serves only as the redundant proxy of the UAs. When the UAs detect that their primary proxy is available, they automatically resume communication with it instead of with SAS.  Click **Submit** to apply settings.

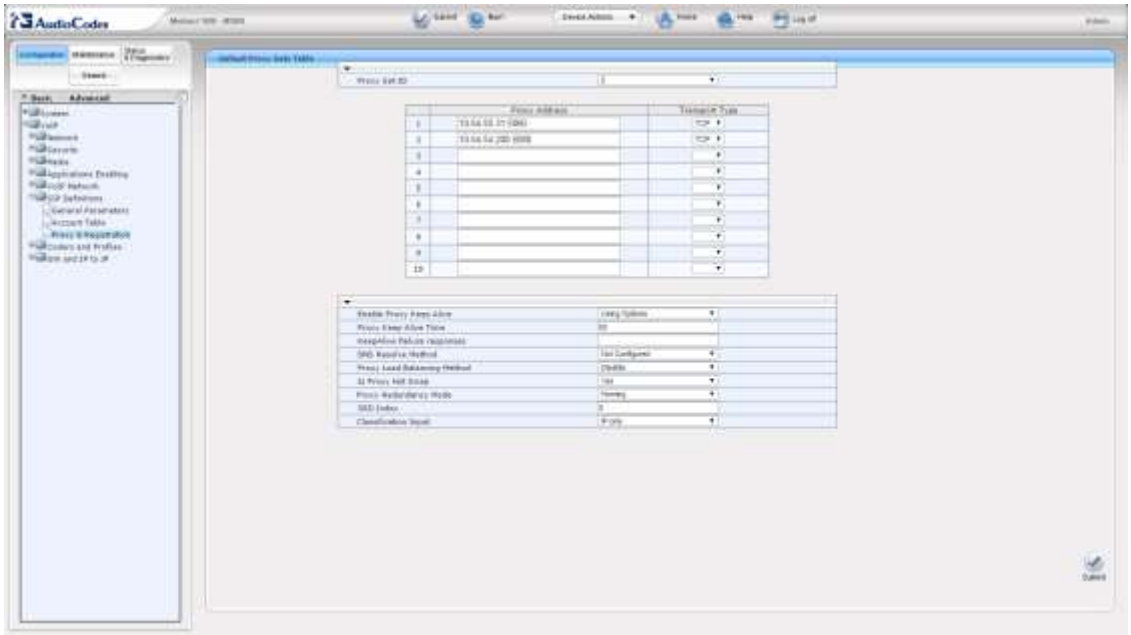
©2015 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Configuring MSBR SAS Routing Table** In this example, the device first attempts to find a user's address within its AOR table. If a user is not found, then the device goes to the routing table. In the instance for index '0', the device will route the call attempt which was not found in the AOR table to the gateway portion of the device. Under **Action**, the destination type is 'Dest Address' and the 'Destination Address' is the same IP address of the overall device. The 'Destination Port' is 5060. This is the Gateway side of the device. The call will then be attempted on the gateway side in which the destination will be attempted to match as in Section 7 Steps 16, 17, and 18. The device in this instance will look to match the destination number to the members of Hunt Group 1 (FXS ports beginning with the digit 6) and if there is no specific match, the call will route to Hunt Group 2 which is the FXO port to the PSTN.  Click **Submit**.

©2015 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Configuring MSBR Gateway Application with SAS** If the device is to run the Gateway and SAS applications, the configuration described in this section is required. The configuration steps apply only to SAS in redundant mode. These configurations were included in Section 7 to configure MSBR testing. **Note:** The Gateway application must use the same SAS operation mode as the SIP UAs. For example, if the UAs use the SAS application as a redundant proxy (i.e., SAS redundancy mode), then the Gateway application must do the same. **To configure Gateway application with SAS redundant mode:** Define the proxy servers for the Gateway application: • Open the 'Proxy & Registration' page (**VoIP → SIP Definitions → Proxy & Registration**). • From the **'Use Default Proxy'** drop-down list, select ***'Yes'***.  Click **Submit**.

©2015 Avaya Inc. All Rights Reserved.

Step	Description
	Configuring MSBR Gateway Application with SAS (Continued) Open the 'Proxy Sets Table' page (**VoIP → SIP Definitions → Proxy & Registration**). From the **Proxy Set ID** drop-down list, select ***0***. In the first **Proxy Address** field, enter the IP address of the external proxy server. In the second **Proxy Address** field, enter the IP address and port of the device (in the format *x.x.x.x:port*). 

©2015 Avaya Inc. All Rights Reserved.

8. Verification Steps

The following steps may be used to verify the configuration from the Avaya side:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the System Manager web administration interface, verify that all branch endpoints are registered with the Session Manager.
- Verify that calls can be placed to/from the analog endpoints behind the branch gateways from Enterprise and Branch SIP users.
- Verify that calls can be placed to/from the analog endpoints and the PSTN.
- Verify that calls can be placed from the analog and SIP endpoints behind the branch gateways when a simulated data WAN failure is introduced.

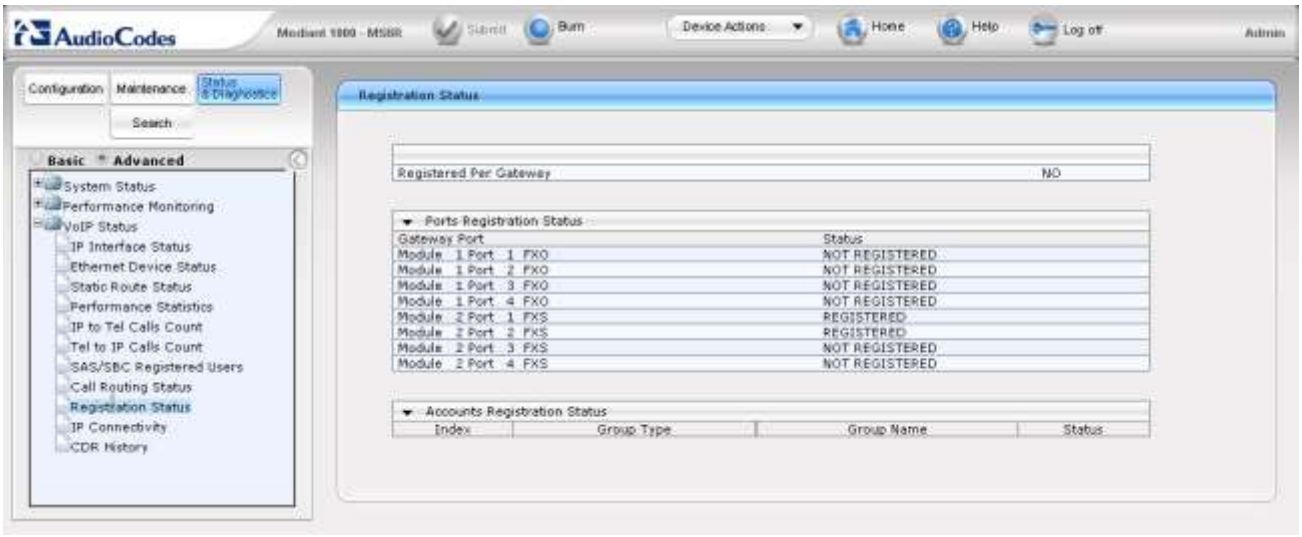
The following steps may be used to verify the configuration from the Audio Codes side:

- To view SAS registered users, open the **SAS/SBC Registered Users** page (**Status & Diagnostics → VoIP Status → SAS/SBC Registered Users**).

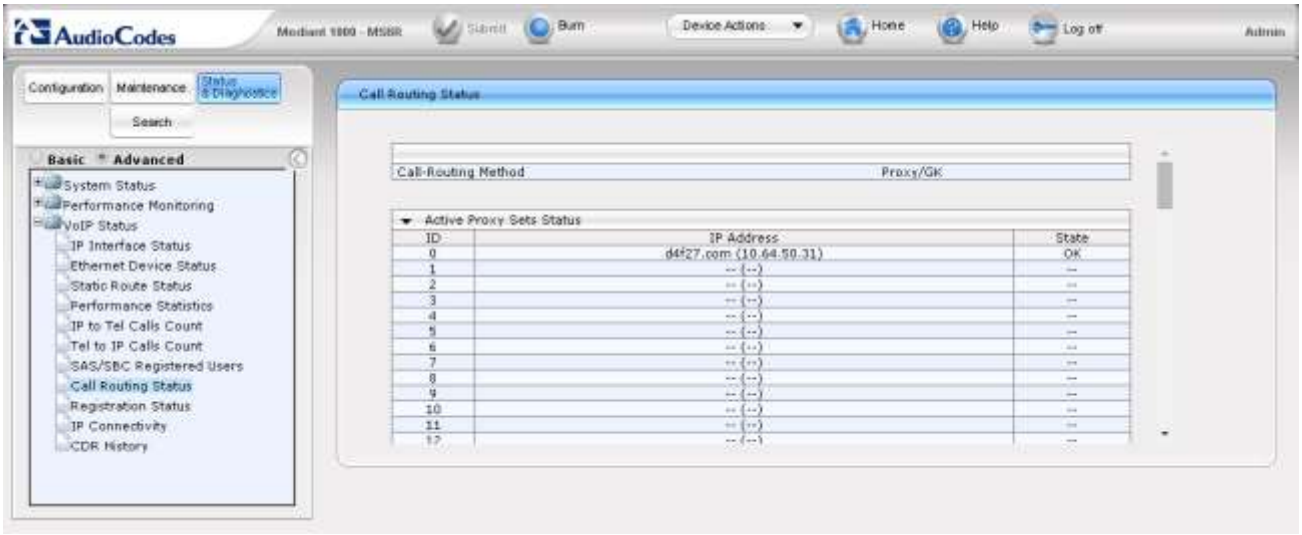


©2015 Avaya Inc. All Rights Reserved.

- To view FXS Port Registration Status, open the **Registration Status** page (**Status & Diagnostics → VoIP Status →Registration Status**).



- To view call routing status, open the **Call Routing Status** page (**Status & Diagnostics → VoIP Status → Call Routing Status**).



©2015 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the procedures required to configure the AudioCodes Mediant 1000 Multi Service Business Router to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The AudioCodes Multi Service Business Router 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] *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*, Document 16-601944

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

[5] *Mediant™ 1000B Gateway & E-SBC User's Manual* Document # LTRT-27034 Version 6.8 November 2014

[6] *Multi-Service Business Routers Configuration Guide Stand-Alone Survivability (SAS) Application* Document # LTRT-29807 Version 6.8 September 2014

[7] *SIP Release Notes, Version 6.8*, Document #: LTRT-26930

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.

©2015 Avaya Inc. All Rights Reserved.

A. Appendix

AudioCodes M1000 .ini file generated after following the configuration instructions contained in the Application Notes is as follows: Please use it only for reference purposes.

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

;Board: Mediant 1000 - MSBR
;HW Board Type: 47  FK Board Type: 67
;Serial Number: 3331682
;Slot Number: 1
;Software Version: 6.80A.244.006
;DSP Software Version: 204IM3=> 660.11
;Second DSP Software Version: 204IM3=> 660.11
;Board IP Address: 10.64.54.200
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.54.2
;Ram size: 497M   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 - MSBR ;Channel Type: RTP
DspCh=240 IPMediaDspCh=240 ;DSP Voice features: IpmDetector ;IP Media:
Conf VXML VoicePromptAnnounc(H248.9) ExtVoicePrompt=1MB ;DATA features:
Routing FireWall&VPN WAN Advanced-Routing Wan-Rate=1483Mbps WIFI-5GHz
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;PSTN Protocols: ISDN IUA=4 CAS ;Coders: G723 G729 GSM-FR G727 ILBC
SPEEX_WB ;E1Trunks=4 ;T1Trunks=4 ;Control Protocols: MSFT EMS SBC-
SIGNALING=1483 MGCP MEGACO SIP SASurvivability SBC=120 ;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 = 10.64.54.199
EnableSyslog = 1
```


©2015 Avaya Inc. All Rights Reserved.

```
;VpFileLastUpdateTime is hidden but has non-default value
TLSVersion = 1
NTPServerIP = '0.0.0.0'
OAMPDEFAULTNETWORKSOURCE = 1
;PM_gwINVITEDialogs is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
EnableLANWatchdog = 0
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

FarEndDisconnectType = 7
CurrentDisconnectDuration = 600
;Offline: initial val of CurrentDisconnectDuration param is '500' (new
val is '600')

[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]


[SS7 Params]


[Voice Engine Params]

BrokenConnectionEventTimeout = 100
RFC2833TxPayloadType = 101
EnableDSPIPMDetectors = 1
FarEndDisconnectSilenceMethod = 2
FarEndDisconnectSilencePeriod = 120
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]
```


©2015 Avaya Inc. All Rights Reserved.

```
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;WEBAccessUserUserLevel is hidden but has non-default value

[SIP Params]

;ISUSEFREECHANNEL is hidden but has non-default value
MEDIACHANNELS = 2
ISPROXYUSED = 1
ISREGISTERNEEDED = 1
AUTHENTICATIONMODE = 0
PLAYRBTONE2TEL = 3
ISWAITFORDIALTONE = 1
ISTWOSTAGEDIAL = 0
ENABLECURRENTDISCONNECT = 1
CHANNELSELECTMODE = 0
GWDEBUGLEVEL = 5
ENABLEEARLYMEDIA = 1
ISUSERPHONE = 0
PROXYNAME = 'd4f27.com'
SIPGATEWAYNAME = 'd4f27.com'
PROGRESSINDICATOR2IP = -1
ALWAYSSENDTOPROXY = 1
PROXYREDUNDANCYMODE = 1
PRACKMODE = 0
DISCONNECTONBROKENCONNECTION = 0
CDRSYSLOGSERVERIP = 0.0.0.0
ENABLEMWI = 1
PSTNALERTTIMEOUT = 180
LineTransferMode = 1
HOLDFORMAT = 1
SIPTRANSPORTTYPE = 1
SIP183BEHAVIOUR = 1
SIPSREQUIRECLIENTCERTIFICATE = 1
ENABLE3WAYCONFERENCE = 1
SASDEFAULTGATEWAYIP = '10.64.54.200:5080'
ENABLESAS = 1
REDUNDANTROUTINGMODE = 2
EmergencyNumbers = '', '', '', ''
REGISTRARTRANSPORTTYPE = 1
SBCREGISTRATIONTIME = 0
TLSREMOTESUBJECTNAME = '10.64.50.31'
SIPREROUTINGMODE = 1
SASSURVIVABILITYMODE = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 2157969408

[SCTP Params]
```


©2015 Avaya Inc. All Rights Reserved.

```
[VXML Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 0 = 1, "", "vlan 1";

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.64.54.200, 24, 10.64.54.2, 1, "Voice",
10.64.50.225, 0.0.0.0, "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 ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
```


©2015 Avaya Inc. All Rights Reserved.

```
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "DefaultRealm", "Voice", "", 6000, 330, 9290, 1, "", "";

[ \CpMediaRealm ]


[ TrunkGroup ]

FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel,
TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber,
TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module;
TrunkGroup 0 = 1, 255, 1, 1, "61006", 0, 255, 2;
TrunkGroup 1 = 1, 255, 2, 2, "61007", 0, 255, 2;
TrunkGroup 2 = 2, 255, 1, 1, "20001", 0, 255, 1;

[ \TrunkGroup ]


[ PstnPrefix ]

FORMAT PstnPrefix_Index = PstnPrefix_RouteName, PstnPrefix_DestPrefix,
PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix,
PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID,
PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix, PstnPrefix_SrcSRDID,
PstnPrefix_TrunkId, PstnPrefix_CallSetupRulesSetId;
PstnPrefix 0 = "", "6", 1, "*", "*", 0, -1, "", "", "", -1, -1;
PstnPrefix 1 = "", "*", 2, "*", "*", 0, -1, "", "", "", -1, -1;

[ \PstnPrefix ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "10.64.50.31:5060", 1, 0;
ProxyIp 1 = "10.64.54.200:5080", 1, 0;

[ \ProxyIp ]


[ TxDtmfOption ]

FORMAT TxDtmfOption_Index = TxDtmfOption_Type;
TxDtmfOption 0 = 4;

[ \TxDtmfOption ]


[ TrunkGroupSettings ]
```


©2015 Avaya Inc. All Rights Reserved.

```
FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,
TrunkGroupSettings_ChannelSelectMode,
TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName,
TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroup,
TrunkGroupSettings_MWIInterrogationType,
TrunkGroupSettings_TrunkGroupName;
TrunkGroupSettings 0 = 1, 0, 0, "", "", -1, 255, "";
TrunkGroupSettings 1 = 2, 2, 4, "", "3035336200", -1, 255, "";

[ \TrunkGroupSettings ]


[ TargetOfChannel ]

FORMAT TargetOfChannel_Index = TargetOfChannel_Destination,
TargetOfChannel_Type, TargetOfChannel_HotLineToneDuration,
TargetOfChannel_Module, TargetOfChannel_Port, TargetOfChannel_PortType;
TargetOfChannel 0 = "61005", 1, -1, 1, 1, "FXO";

[ \TargetOfChannel ]


[ Authentication ]

FORMAT Authentication_Index = Authentication_UserId,
Authentication_UserPassword, Authentication_Module, Authentication_Port,
Authentication_PortType;
Authentication 4 = "61006", "$1$tIWHhYONjw==", 2, 1, "FXS";
Authentication 5 = "61007", "$1$tIWHhYONjw==", 2, 2, "FXS";

[ \Authentication ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 1, 60, 0, 1, 0, 0, "-1", 1, -1, "";

[ \ProxySet ]


[ SASRegistrationManipulation ]

FORMAT SASRegistrationManipulation_Index =
SASRegistrationManipulation_RemoveFromRight,
SASRegistrationManipulation_LeaveFromRight;
```


©2015 Avaya Inc. All Rights Reserved.

```
SASRegistrationManipulation 0 = 0, 0;

[ \SASRegistrationManipulation ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "to_PSTN", -1, "*", "*", "*", "*", 0, "", -1, 0, -1, 1,
-1, "", "10.64.54.200", 5060, 1, 0, 0, "";

[ \IP2IPRouting ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]


[ CodersGroup0 ]

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

[ \CodersGroup0 ]


[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
```


©2015 Avaya Inc. All Rights Reserved.

```
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```


©2015 Avaya Inc. All Rights Reserved.

©2015 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.

©2015 Avaya Inc. All Rights Reserved.