



Avaya Solution & Interoperability Test Lab

Application Notes for Sangoma IMG 2020 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Sangoma IMG 2020 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Sangoma IMG 2020 is an integrated media gateway that enables interworking between IP and PSTN networks. In the compliance test, Sangoma IMG 2020 delivered SIP signaling and media from an Avaya SIP-based enterprise network to the PSTN via ISDN-PRI. Sangoma IMG 2020 connected to Avaya Aura® Session Manager via a SIP trunk and to the PSTN via an ISDN-PRI trunk.

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.

1 Introduction

These Application Notes describe the configuration steps required to integrate the Sangoma IMG 2020 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Sangoma IMG 2020 is an integrated media gateway that enables interworking between IP and PSTN networks. In the compliance test, Sangoma IMG 2020 delivered SIP signaling and media from an Avaya SIP-based enterprise network to the PSTN via ISDN-PRI. Sangoma IMG 2020 connected to Avaya Aura® Session Manager via a SIP trunk and to the PSTN via an ISDN-PRI trunk.

Note: These Application Notes will focus on the configuration of the SIP trunk between Sangoma IMG 2020 and Avaya Aura® Session Manager and call routing. The configuration of the ISDN-PRI trunk to the PSTN is outside the scope of these Application Notes and will not be covered.

2 General Test Approach and Test Results

Interoperability compliance testing covered feature and serviceability testing. The feature testing focused on establishing calls between an Avaya SIP-based enterprise network and the PSTN, where all calls traversed Sangoma IMG 2020. Various telephony features, such as hold/resume, call transfers, conference calls, call forwarding, and calling number display/block were exercised.

The serviceability testing focused on verifying that IMG 2020 came back into service after re-establishing IP network connectivity and after a reboot.

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 this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and Sangoma IMG 2020 did not include use of any specific encryption features as requested by Sangoma.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing SIP trunk between IMG 2020 and Session Manager and verifying the exchange of SIP Options messages.
- Establishing voice calls between an Avaya SIP-based enterprise network and the PSTN with all calls traversing IMG 2020. SIP and H.323 endpoints on the Avaya enterprise network were used.
- Support of direct IP-to-IP media (also known as “Shuffling” which allows IP endpoints to send audio RTP packets directly to each other without using media resources on the Avaya Media Gateway or Avaya Aura® Media Server).
- Telephony features such as hold/resume, call transfers, conference calls, call forwarding, calling number display/block, and voicemail coverage.
- Establishing T.38 fax calls between an Avaya SIP-based enterprise network and the PSTN with fax calls traversing IMG 2020.
- Support of G.711 mu-law and G.729 codecs.
- DTMF support using RFC2833.
- Proper system recovery after reconnecting IMG2020 to the IP network and after a reboot.

2.2 Test Results

All test cases passed with the following observations:

- When Sangoma IMG 2020 receives a fax call, it’s supposed to detect the fax tone in order to switch the call from G.711 to T.38 fax. During the compliance test, IMG 2020 was not properly detecting the fax tone from the computer fax software being used; and therefore, didn’t classify the call as a fax call preventing it from sending the re-Invite with T.38 fax. The call was being detected as a data call and not a fax call. The workaround is to disable **Modem Behavior** as shown in **Section 7.5.2** so that IMG 2020 would assume the incoming call is a fax call and switch from G.711 to T.38 fax. If the customer is using modems in their network, then this field should be enabled and fax calls would have to use G.711 since the re-Invite with T.38 fax would not be sent to Communication Manager.
- For incoming PSTN calls, with the calling party number included, an Adaptation was required to replace the domain in the P-Asserted-Identity header on the egress side only; otherwise, the call would not complete. The domain had to match the configured domain in the SIP signaling group on Communication Manager. Leaving the domain in the SIP signaling group blank would allow all domains to match so this would be another solution. Refer to **Section 6.2**.

2.3 Support

For technical support on Sangoma IMG2020, contact Sangoma Customer Support via the web at <https://www.sangoma.com/support/customer-support>.

3 Reference Configuration

The network diagram below illustrates the test configuration. In this configuration, Sangoma IMG 2020 delivered SIP signaling and media from an Avaya SIP-based enterprise network to the PSTN via ISDN-PRI. Sangoma IMG 2020 connected to Avaya Aura® Session Manager via a SIP trunk and to the PSTN via an ISDN-PRI trunk. Voice calls were established with Avaya H.323 / SIP Deskphones and T.38 fax calls were established using computer fax software.

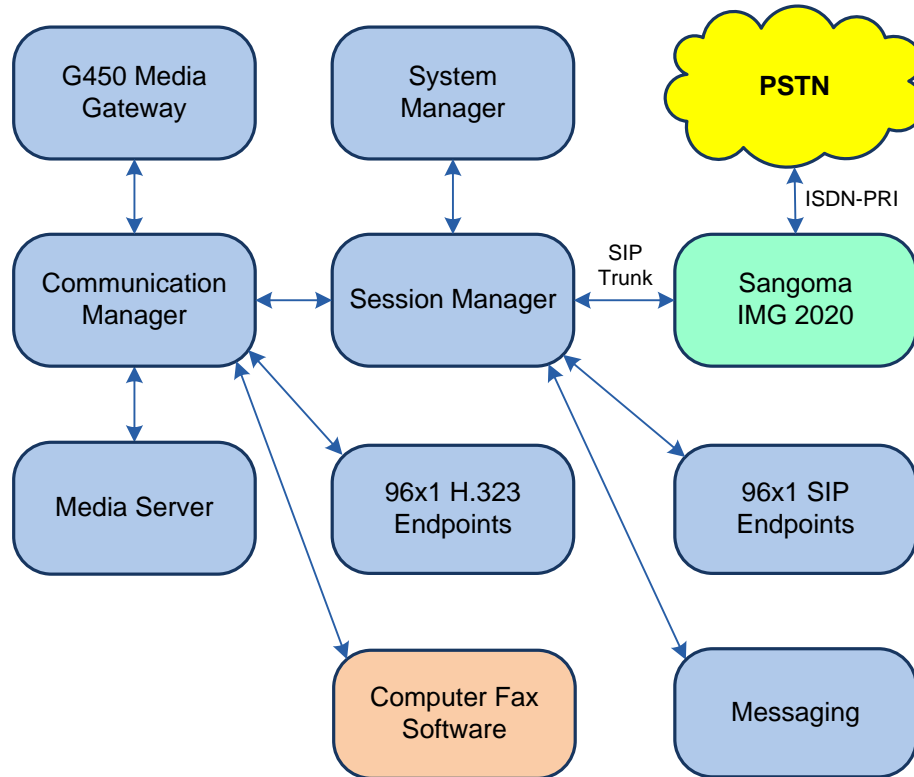


Figure 1: Avaya SIP-based Enterprise Network with Sangoma IMG 2020

4 Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	8.0.1.1.0-FP1SP1 (R018x.00.0.822.0 with Patch 25183)
Avaya G450 Media Gateway	FW 40.25.0
Avaya Aura® Media Server	v.8.0.0.173
Avaya Aura® System Manager	8.0.1.1 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.1.039340 Service Pack 1
Avaya Aura® Session Manager	8.0.1.1.801103
Avaya Aura® Messaging	7.1.3.1.0-FP3SP1
Avaya 96x1 Series IP Deskphones	6.8003 (H.323) 7.1.5.0.11 (SIP)
Sangoma IMG 2020	2.3.1

5 Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer Private Numbering Format
- Administer Incoming Call Handling Treatment
- Administer ARS Call Routing for PSTN Calls

Note: AAR call routing to Avaya SIP endpoints registered to Session Manager is not covered in these Application Notes.

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

5.1 Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
default	0.0.0.0	
devcon-aes	10.64.102.119	
devcon-ams	10.64.102.118	
devcon-sm	10.64.102.117	
procr	10.64.102.115	
procr6	::	
(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		

5.2 Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec types supported for calls routed over the SIP trunk to IMG 2020. The form is accessed via the **change ip-codec-set 1** command. The default settings of the **IP Codec Set** form are shown below. IMG 2020 supports the G.711 and G.729 codecs.

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.729	n	2	20
3:			

5.3 Administer IP Network Region

In 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 *avaya.com*. 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 Avaya G450 Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

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: 50999		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

5.4 Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify the Communication Manager (*procr*) and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- Enable **Initial IP-IP Direct Media**.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 10		Page 1 of 2
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: devcon-sm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Avaya SIP endpoints and for PSTN calls over the IMG 2020. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

add trunk-group 10		Page 1 of 22	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: To devcon-sm	COR: 1	TN: 1	TAC: 1010
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: 10		
	Number of Members: 10		

On **Page 2**, the **Preferred Minimum Session Refresh Interval (sec)** field was set to a value equal to or greater than the **Session Timer** set on IMG 2020 in **Section 7.5.2**. The **Session Timer** was set to 600 seconds.

add trunk-group 10		Page 2 of 5	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 600			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n			
Caller ID for Service Link Call to H.323 1xC: station-extension			

On **Page 3**, set the **Numbering Format**. For this test, the **private** numbering table was used to set the calling party number format for outgoing calls. In this case, 5-digit extensions beginning with '7' were converted to 732-777-xxxx as shown in **Section 5.5**.

add trunk-group 10		Page 3 of 5
TRUNK FEATURES		
ACA Assignment? n	Measured: none	
		Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private	
	UUI Treatment: shared	
	Maximum Size of UUI Contents: 128	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Hold/Unhold Notifications? y	
	Modify Tandem Calling Number: tandem-cpn-form	
Send UCID? y		
Show ANSWERED BY on Display? y		

5.5 Administer Private Numbering Format

In the **Numbering – Private Format** form, add entry to prepend 73277 to calls from extensions beginning with ‘7’ and routed over SIP trunk group 10. This will convert the calling number from a 5-digit extension to a 10-digit number in the format 732-777-xxxx. The calling number could then be displayed by the called party, if supported.

change private-numbering 0				Page 1 of 2
NUMBERING - PRIVATE FORMAT				
Ext	Ext	Trk	Private	Total
Len	Code	Grp(s)	Prefix	Len
5	7	10	73277	10
				Total Administered: 1
				Maximum Entries: 540

5.6 Administer Incoming Call Handling Treatment

The DID numbers for PSTN calls to the Avaya enterprise network were in the format of 732-777-xxxx, where the last 5 digits mapped to the extension. The calls were received by Communication Manager on SIP trunk group 10. The **Incoming Call Handling Treatment** table for trunk group 10 was modified to delete the first 5 digits, as shown below, so that the calls would terminate on the proper extension.

change inc-call-handling-trmt trunk-group 10				Page 1 of 30
INCOMING CALL HANDLING TREATMENT				
Service/	Number	Number	Del Insert	
Feature	Len	Digits		
tie	10	73277	5	

5.7 Administer ARS Call Routing for PSTN Calls

PSTN calls are routed to Session Manager over a SIP trunk via ARS call routing. Add an entry to the ARS analysis form to route calls in the 908 or 732 area codes to route pattern 10 as shown below. The ARS feature access code of '9' steers calls to ARS routing.

change ars analysis 7							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
732	10	10	10	hnpa		n	
908	10	10	10	hnpa		n	

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 10 to Session Manager as shown below.

change route-pattern 10													Page 1 of 3
Pattern Number: 10 Pattern Name: To devcon-sm													
SCCAN? n Secure SIP? n Used for SIP stations? n													
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						
			Mrk	Lmt	List	Del	Digits						
Dgts								DCS/	IXC				
								QSIG	Intw				
1:	10	0						n	user				
2:								n	user				
3:								n	user				
4:								n	user				
5:								n	user				
6:								n	user				
								Service/Feature	PARM	Sub	Numbering	LAR	
BCC VALUE													
0 1 2 M 4 W													
								Request					
1:	y	y	y	y	y	n	n	rest			unk-unk	none	
2:	y	y	y	y	y	n	n	rest				none	
3:	y	y	y	y	y	n	n	rest				none	
4:	y	y	y	y	y	n	n	rest				none	
5:	y	y	y	y	y	n	n	rest				none	

6 Configure Avaya Aura® Session Manager

This section provides the procedure for configuring Session Manager. The procedure includes adding the following items:

- Launch System Manager
- Adaptations to modify SIP messages for egress only
- SIP Entities corresponding to Session Manager, Communication Manager, and IMG 2020
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies
- Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

Note: It is assumed that basic configuration of Session Manager has already been completed. This section will focus on the configuration of the SIP trunk to IMG 2020 and routing calls to it.

6.1 Launch System Manager

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

6.2 Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decision have been made; for example, changing the domain in the P-Asserted-Identity in a SIP INVITE message. To create an **Adaptation** that will be applied to the Communication Manager SIP entity in **Section 6.3.2**, navigate to **Elements → Routing → Adaptations** and click on the **New** button (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., *CM-Adaptation-For-Sangoma*).
- **Module Name:** Select **DigitConversionAdapter**.
- **Module Parameter Type:** Select **Name-Value Parameter**. The section will expand with an area to enter **Name** and **Value** pairs. Click **Add**. To replace the domain in the P-Asserted-Identity header on the egress side of Session Manager (i.e., towards Communication Manager) enter the keyword **osrcd** in the **Name** field and *avaya.com* in the **Value** field. This will replace the IP address used in the domain with *avaya.com*, the domain configured in the SIP signaling group in **Section 5.4**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'Routing' selected, with sub-items like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'Regular Expressions', 'SIP Entities', and 'Entity Links'. The main content area is titled 'Adaptation Details' and has a 'Commit' button. The 'General' section is active, showing the following fields:

- * Adaptation Name:** CM-Adaptation-For-Sangoma
- * Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for Name-Value pairs. The 'Add' button is clicked, and a new row is added with 'osrcd' in the Name field and 'avaya.com' in the Value field. The 'Egress URI Parameters' and 'Notes' fields are also visible.

6.3 Add SIP Entities

This section covers the configuration of SIP entities for Session Manager, Communication Manager, and IMG 2020.

6.3.1 Avaya Aura® Session Manager

From the System Manager **Home** screen, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined.
- **Time Zone:** Time zone for this location.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area displays the 'SIP Entity Details' form under the 'General' tab. The form includes the following fields and values:

- Name:** devcon-sm
- IP Address:** 10.64.102.117
- SIP FQDN:** (empty)
- Type:** Session Manager
- Notes:** (empty)
- Location:** Thornton
- Outbound Proxy:** (empty)
- Time Zone:** America/New_York
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

Scroll down to the **Listen Ports** section and verify that the UDP transport network protocol used by IMG 2020 is specified as shown below.

Listen Ports

Add Remove					
3 Items		Filter: Enable			
	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input type="checkbox"/>	
Select : All, None					

6.3.2 Avaya Aura® Communication Manager

A SIP Entity must be added for the Communication Manager. From the System Manager **Home** screen, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Communication Manager (*procr*).
- **Type:** Select *CM*.
- **Adaptation:** Adaptation configured in **Section 6.2**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 8.0 web 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 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form contains the following fields: 'Name' (devcon-cm), 'FQDN or IP Address' (10.64.102.115), 'Type' (CM), 'Notes' (empty), 'Adaptation' (CM-Adaptation-For-Sangoma), 'Location' (Thornton), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (unchecked), and 'Call Detail Recording' (none). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

6.3.3 Sangoma IMG 2020

A SIP Entity must be added for IMG 2020. To add a SIP Entity, navigate to **Elements** → **Routing** → **SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IMG 2020 IP address.
- **Type:** Select *SIP Trunk*.
- **Location:** Select one of the locations previously defined.
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 8.0 web 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 icon labeled 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' with a 'General' tab. The form contains the following fields: 'Name' (SangomaIMG2020), 'FQDN or IP Address' (192.168.100.190), 'Type' (SIP Trunk), 'Notes' (empty), 'Adaptation' (empty), 'Location' (Thornton), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (checkbox), and 'Call Detail Recording' (egress). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

6.4 Add Entity Links

This section covers the configuration of Entity Links for Communication Manager and IMG 2020.

6.4.1 Communication Manager Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *devcon-cm Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *trusted*. *Note: If trusted is not selected, calls from the associated SIP Entity specified in Section 6.3.2 will be denied.*

Click **Commit** to save the Entity Link definition.

The following Entity Link is between Session Manager and Communication Manager.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (which is currently selected). The main content area is titled 'Entity Links' and includes a table with 5 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The 'devcon-cm Link' is highlighted with a red box. Below the table, there is a 'Select' dropdown menu set to 'All, None'.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-cm Link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-ipose Link	devcon-sm	UDP	5060	devcon-ipose	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Sangoma IMG 2020 Link	devcon-sm	UDP	5060	SangomaIMG2020	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.4.2 Sangoma IMG 2020 Entity Link

The SIP trunk between Session Manager and IMG 2020 is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *Sangoma IMG 2020 Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select UDP transport protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the *SangomaIMG2020* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Selected *trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in Section 6.3.3 will be denied.*

Click **Commit** to save the Entity Link definition.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (which is currently selected). The main content area is titled 'Entity Links' and features a table with 5 items. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row for 'Sangoma IMG 2020 Link' is highlighted with a red border. Below the table, there is a 'Select' dropdown menu set to 'All, None'.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-cm Link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	devcon-ipose Link	devcon-sm	UDP	5060	devcon-ipose	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Sangoma IMG 2020 Link	devcon-sm	UDP	5060	SangomaIMG2020	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.5 Add Routing Policies

Routing policies describe the conditions under which calls are routed to Communication Manager and IMG 2020 SIP entities. To add a routing policy, navigate to **Elements** → **Routing** → **Routing Policies** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

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

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition.

The following screen shows the Routing Policy for Communication Manager.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, version information, and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and user profile (admin) are also present. The left sidebar shows a tree view with categories like Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, and Regular Expressions. 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 fields for Name (devcon-cm Policy), 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, a table with columns for days of the week, Start Time, End Time, and Notes, and a 'Filter: Enable' option.

Routing Policy Details Commit Cancel

General

* **Name:** devcon-cm Policy

Disabled: ☐

* **Retries:** 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
devcon-cm	10.64.102.115	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

The following screen shows the Routing Policy for IMG 2020.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, version information, and user roles (Users, Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon are also present. The left sidebar shows a navigation menu with options like Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, and Regular Expressions. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section contains fields for Name (Sangoma Policy), Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section shows a table with one entry: SangomaIMG2020, 192.168.100.190, SIP Trunk. The 'Time of Day' section includes an 'Add' button, a 'Remove' button, and a 'View Gaps/Overlaps' button. It also shows a table with one item: 0, 24/7, with checkboxes for days of the week (Mon-Sun) all checked, and a time range of 00:00 to 23:59. A 'Filter: Enable' button is also visible.

Routing Policy Details Commit Cancel Help ?

General

* **Name:** Sangoma Policy

Disabled: ☐

* **Retries:** 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SangomaIMG2020	192.168.100.190	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps Filter: Enable

1 Item

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.6 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, 10-digit numbers starting with 73277 are routed to Communication Manager and calls to 732 or 908 area codes are routed to IMG 2020.

To add a dial pattern, navigate to **Elements → Routing → Dial Patterns** and click on the **New** button (not shown). Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

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 **Dial Pattern** shows the dial pattern definition for 73277 being routed to Communication Manager.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

Dial Pattern Details Commit Cancel

General

* **Pattern:** 73277

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes: CM Stations

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"/>	Thornton		devcon-cm Policy	0	<input type="checkbox"/>	devcon-cm	

Select : All, None

The following **Dial Pattern** shows the dial pattern definition for calls in the 908 area code being routed to IMG 2020.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar lists navigation options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The 'Routing' tab is active, and the 'Dial Patterns' sub-tab is selected. The main content area displays the 'Dial Pattern Details' for a pattern of 908. The 'General' section includes fields for Pattern (908), Min (10), Max (10), Emergency Call (unchecked), SIP Domain (-ALL-), and Notes (Sangoma IMG 2020). Below this is the 'Originating Locations and Routing Policies' section, which contains a table with one item: Thornton, Sangoma Policy, Rank 0, and Routing Policy Destination SangomaIMG2020.

Dial Pattern Details

General

* Pattern: 908

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Sangoma IMG 2020

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"/>	Thornton		Sangoma Policy	0	<input type="checkbox"/>	SangomaIMG2020	

Select : All, None

The following **Dial Pattern** shows the dial pattern definition for calls in the 732 area code being routed to IMG 2020.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar lists navigation options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The 'Routing' tab is active, and the 'Dial Patterns' sub-tab is selected. The main content area displays the 'Dial Pattern Details' for a pattern of 732. The 'General' section includes fields for Pattern (732), Min (10), Max (10), Emergency Call (unchecked), SIP Domain (-ALL-), and Notes (Sangoma IMG 2020). Below this is the 'Originating Locations and Routing Policies' section, which contains a table with one item: Thornton, Sangoma Policy, Rank 0, and Routing Policy Destination SangomaIMG2020.

Dial Pattern Details

General

* Pattern: 732

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Sangoma IMG 2020

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"/>	Thornton		Sangoma Policy	0	<input type="checkbox"/>	SangomaIMG2020	

Select : All, None

6.7 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, user information (Users, Elements, Services, Widgets, Shortcuts), a search bar, and a user profile (admin). The left sidebar shows the navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Global Settings, Communication Profile, Network Configuration, Device and Location, Application Configuration, System Status, System Tools, and Performance. The main content area is titled 'Edit Session Manager' and features tabs for General, Security Module, Monitoring, CDR, Personal Profile Manager (PPM), Connection Settings, and Event Server. The 'General' tab is selected, showing fields for SIP Entity Name (devcon-sm), Description, *Management Access Point Host Name/IP (10.64.102.116), *Direct Routing to Endpoints (Enable), Data Center (None), Avaya Aura Device Services Server Pairing (None), and Maintenance Mode (checkbox). The 'Security Module' tab is also visible, showing fields for SIP Entity IP Address (10.64.102.117), *Network Mask (255.255.255.0), *Default Gateway (10.64.102.1), *Call Control PHB (46), and *SIP Firewall Configuration (SM 6.3.8.0). The top right of the main content area has 'Commit' and 'Cancel' buttons.

The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to IMG 2020. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 900 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.

Monitoring ▼

Enable SIP Monitoring ☒

*Proactive cycle time (secs)

900

*Reactive cycle time (secs)

120

*Number of Tries

1

*Number of Successes

1

Enable CRLF Keep Alive Monitoring ☐

*CRLF Ping Interval (secs)

0

7 Configure Sangoma IMG 2020

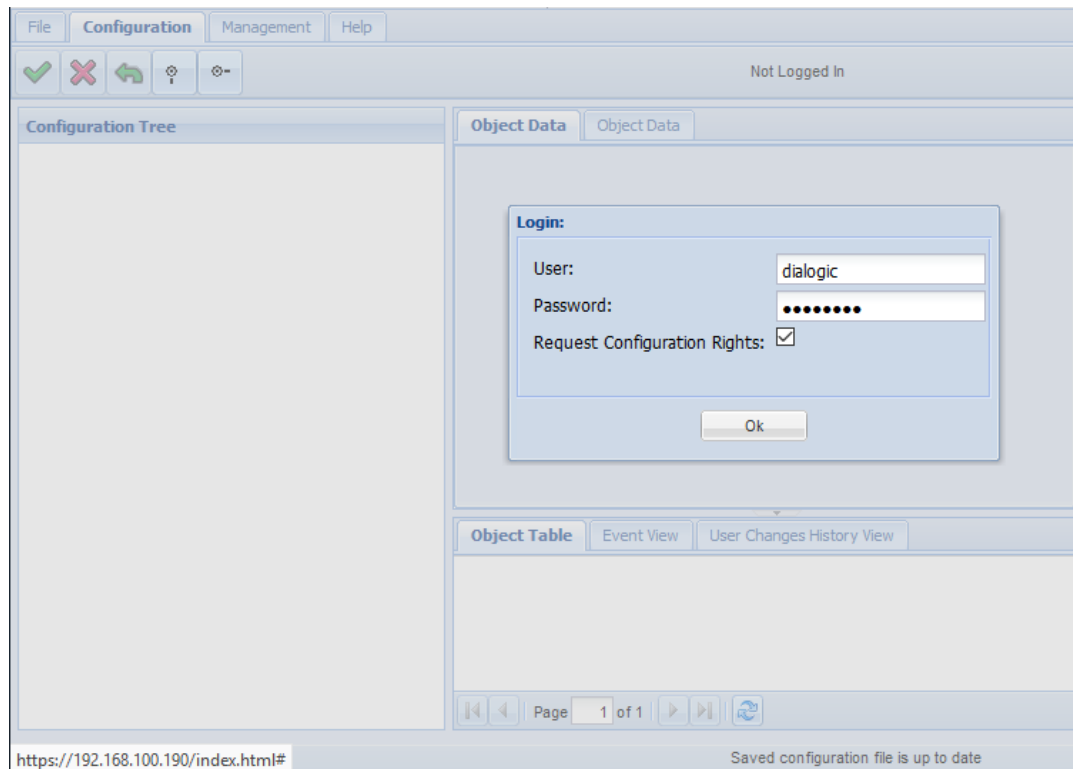
The IMG 2020 was configured with two trunk interfaces, a SIP trunk used to connect to Session Manager and an ISDN-PRI trunk used to connect to the PSTN. This section will cover the configuration of the SIP trunk, media interfaces, and call routing. It is assumed that the ISDN-PRI trunk has already been completed. Refer to [4] for additional configuration details.

This section covers the following configuration areas:

- Launch Web GUI
- Create IMG 2020 Physical Node
- Create IP Interface for Media
- Create IP Interface for Signaling
- Configure Profiles
- Configure External Network Element
- Configure Routing
- Save Configuration

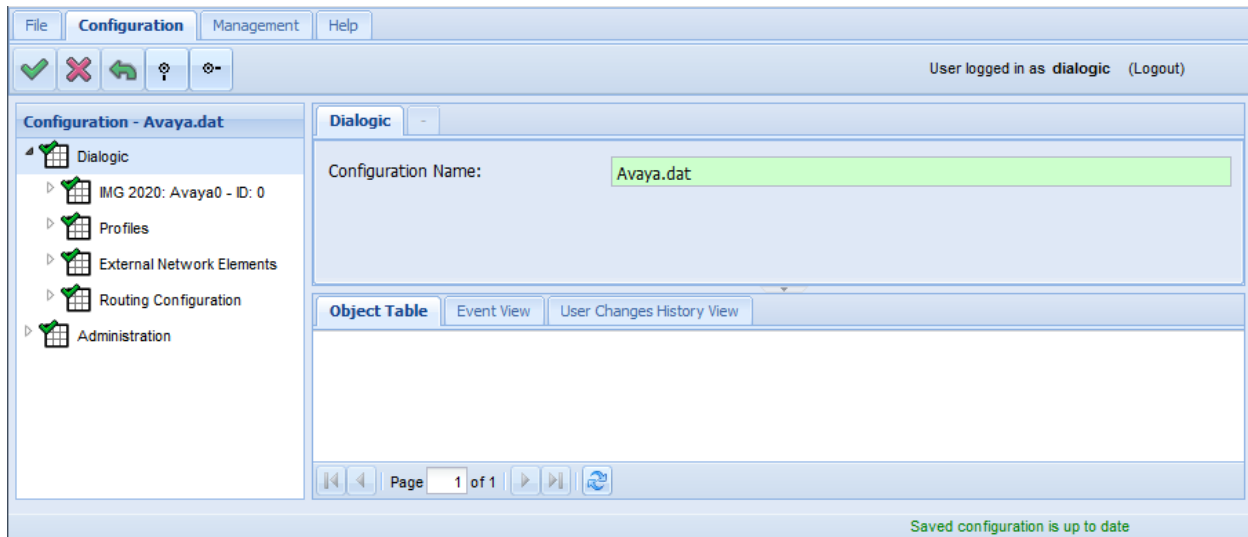
7.1 Launch Web GUI

The Web GUI is a real-time web based Graphical User Interface used to configure, monitor, and provision the IMG 2020. Access the Web GUI by using the URL “https://ip-address” in a supported web browser, where “ip-address” is the IMG 2020 IP address. Log in using the appropriate credentials when prompted as shown below.



The following window is displayed from which basic functionality on the IMG 2020 is configured.

Note: After configuring an object, click on the commit check mark .



7.2 Create IMG 2020 Physical Node

Create the physical IMG 2020 node. Right-click on the **Dialogic** object in the configuration tree and select **New IMG 2020**. Specify a **Name** (e.g., *Avaya0*) to identify the node and enter the IMG 2020 IP address (e.g., *192.168.100.190*). Select the **Media Mode** from the drop-down menu (i.e., *Audio LBR*). Keep the default values for the remaining fields.

The screenshot displays the Avaya Configuration Manager interface. The top menu bar includes 'File', 'Configuration', 'Management', and 'Help'. Below the menu bar, there are icons for saving, undo, redo, and other actions. The user is logged in as 'dialogic'. The main window is titled 'Configuration - Avaya.dat'. On the left, a tree view shows the configuration hierarchy: Dialogic, IMG 2020: Avaya0 - ID: 0, IP Network, Facility, Signaling, Profiles, External Network Elements, Routing Configuration, and Administration. The right pane shows the configuration details for the selected node. The fields are as follows:

Field	Value
ID:	0
Name:	Avaya0
Media Mode:	Audio LBR
Audio SRTP Support:	Disabled
ACL:	Unrestricted
IP Address (nn.nn.nn.nn):	192.168.100.190
Type:	2020
Trunk Type:	T1
Interface Type:	DS-3/OC3
Software Version:	2.3.1:1
Total IP Channels:	2520
Total Licensed IP Channels:	768
Packet Audio Channels:	2520
Packet Multimedia Channels:	0
Serial Number:	00000009
Security ID:	0000001be1a0

Below the configuration fields, there are buttons for 'Reset IMG 2020', 'Graceful Out Of Service', 'Out Of Service', 'In Service', and 'Download New License'. At the bottom, there is an 'Object Table' tab, 'Event View', and 'User Changes History View'. The status bar at the bottom indicates 'Saved configuration is up to date'.

7.3 Create IP Interface for Media

To stream media (i.e., RTP data), an interface on the IMG 2020 must be configured and be given a Media 0 Endpoint IP address. Follow the steps below.

1. Right-click on the IMG 2020 Physical Node (i.e., **IMG 2020** in the configuration tree) and select **New Network**.
2. Right-click on the **IP Network** object and select **New Logical Interfaces**.
3. Right-click on the **Logical Interfaces** → **Control** object and select **New IP Interface**.

In the **IP Interface** screen, set the **Source Endpoint** to *Media 0*. In the **IP Address** field, enter an IP address that will be used for RTP data and enter the **Network Prefix Len** and **Default Gateway**.

The screenshot displays the Avaya configuration interface. The left sidebar shows a tree view with the following structure: Dialogic > IMG 2020: Avaya0 - ID: 0 > IP Network > Logical Interfaces > Control > Media 0 - 192.168.100.191 / 24. The main panel is titled 'Media 0 - 192.168.100.191 / 24' and contains the following configuration fields:

Source Endpoint:	Media 0
Address Type:	IPv4
IP Address:	192.168.100.191
/ Network Prefix Len:	24
Default Gateway:	192.168.100.1
ARP/ND:	Enable
ICMP:	Enable
VLAN:	Disable
VLAN ID (2-4094):	2
VLAN Priority (0-7):	0
FQDN (SIP Only):	
ACL:	Unrestricted

Below the configuration fields, there are three tabs: 'Object Table', 'Event View', and 'User Changes History View'. The 'Object Table' tab is currently selected and is empty. At the bottom of the interface, there is a status bar that reads 'Saved configuration is up to date'.

7.4 Create IP Interface for Signaling

A Signaling object needs to be configured to allow SIP signaling to be utilized on the IMG 2020. To configure the SIP signaling interface, right-click on the **IMG 2020** Physical Node and select **New Signaling**. Next, right-click on the **Signaling** object that was created and select **New SIP**. Select the **SIP** object in the configuration tree and configure the fields as shown below. Set the **IP Operation Mode** to *Multiple IP*.

Note: For the compliance test, there was only one IP address defined for SIP, but it is recommended to set the **IP Operation Mode** field to *Multiple IP* to allow another SIP address to be added in the future without having to perform a major re-configuration.

The screenshot displays the Avaya configuration interface for the 'Configuration - Avaya.dat' file. The left-hand 'Configuration Tree' shows a hierarchy starting with 'Dialogic', followed by 'IMG 2020: Avaya0 - ID: 0', 'IP Network', 'Logical Interfaces', 'Control', 'Media 0 - 192.168.100.191 / 24', 'Facility', 'Signaling', 'ISDN', and finally 'SIP'. The 'SIP' object is selected, showing its IP address as '192.168.100.190'. Below the tree are links for 'Profiles', 'External Network Elements', 'Routing Configuration', and 'Administration'. The main configuration area on the right is titled 'SIP' and contains the following settings:

- Compact Header: Disable
- Message Restriction Setting: Default
- UserName (AOR): DIALOGIC-BDN0
- Authentication User Name: (empty field)
- Authentication Password: (empty field)
- SIP-T Enabled: No
- SIP-T Behavior: Not Used
- IP Operation Mode: Multiple IP
- Incoming UAC Routing: IP address and port
- Retry-After (# of Seconds): 5

Below the configuration fields are tabs for 'Object Table', 'Event View', and 'User Changes History View'. The 'Object Table' tab is active, showing an empty table. At the bottom of the interface, a status bar indicates 'Saved configuration is up to date'.

Right-click on the **SIP** object and select **New IP Address**. The **SIP IP Address** screen is displayed. Select the appropriate **IP Address** from the drop-down menu (e.g., *192.168.100.190*). Set the **Transport Type** to *UDP* and the **Port** to *5060*. Keep the default values for the remaining fields.

The screenshot shows a network management interface with a 'Configuration' tab. On the left, a tree view shows the configuration hierarchy: Dialogic > IMG 2020: Avaya0 - ID: 0 > IP Network > Logical Interfaces > Control > Media 0 - 192.168.100.191 / 24 > SIP > SIP IP Address: 192.168.100.190. The main panel displays the configuration for this specific SIP IP Address. The fields are as follows:

Field	Value
IP Type:	IPv4
IP Address:	192.168.100.190
Transport Type:	UDP
Port:	5060
TLS Port:	5061
DNS Client:	Not Used
DNS Query Mode:	MIX
Secure Profile:	Not Used
Default Secure Profile:	Not Used
Fully Qualified Domain Name:	
TOS Precedence:	Routine
TOS Delay:	Normal Delay
TOS Throughput:	Normal Throughput
TOS Reliability:	Normal Reliability
TOS Cost:	Normal Cost

Below the configuration fields, there are tabs for 'Object Table', 'Event View', and 'User Changes History View'. The 'Object Table' tab is currently selected and is empty. At the bottom of the interface, a status bar indicates 'Saved configuration is up to date'.

7.5 Configure Profiles

Some objects need to be associated with a specific profile for them to function in a network. The profiles are first created and then associated with an object. This section covers the configuration of the **IP Profiles** and **SIP Profiles**. The **IP Profile** will be associated with the **Routing** object created in **Section 7.7** and the **SIP Profile** will be associated with the **External Network Element** object created in **Section 7.6**.

7.5.1 Configure IP Profile

The **IP Profile** will be configured for T.38 fax, DTMF using RFC2833, and allow G.711 and G.729 codecs along with the preference order. Follow the procedure below to create the **IP Profile**.

1. Right-click on the **Dialogic** object and select **New Profiles**.
2. Right-click on the **Profiles** object and select **New IP Profiles**.
3. Right-click on the **IP Profiles** object and select **New IP Profile**.

In the **IP Profile** screen, enter a descriptive in the **Name** field (e.g., *T38_fallback*). For **Digit Relay**, select *DTMF Packetized* to use RFC 2833. For **Fax Mode**, select *Relay Fallback to Bypass*. For **Fax Bypass Codec**, select *G711 ulaw*. Keep the default values for the remaining fields.

Note: For the compliance test, **Modem Behavior** was set to *Disabled* so that IMG 2020 would assume the incoming call is a fax call, as opposed to a data call, and switch from G.711 to T.38; otherwise, IMG 2020 would not properly detect the fax tone from the computer fax software used during the compliance test. If the customer is using modems in their configuration, then this field should be enabled and fax calls would use G.711 since the T.38 re-Invite from IMG 2020 would not be sent to Communication Manager.

File Configuration Management Help

User logged in as dialogic (Logout)

Configuration - Avaya.dat

Dialogic

IMG 2020: Avaya0 - ID: 0

IP Network

Logical Interfaces

Control

Media 0 - 192.168.100.191 / 24

Facility

Signaling

ISDN

SIP

SIP IP Address: 192.168.100.190

Profiles

IP Profiles

IP Profile: T38_fallback

SIP Profiles

TDM Profiles

External Network Elements

Routing Configuration

Administration

IP Profile: T38_fallback

Name: T38_fallback

Silence Suppression: Disable

Echo Cancellation: Enabled (NLP Enabled)

RTP Redundancy: No Redundancy

RTP Payload Type for Redundancy: Not Used

Digit Relay: DTMF Packetized

Fax Mode: Relay Fallback to Bypass

Fax Bypass Codec: G711 ulaw

Fax Packet Redundancy: No Redundancy

Initial Media Inactivity Timer: Disable

Initial Media Inactivity Timer Value: Seconds: 181

Media Inactivity Timer: Disable

Media Inactivity Timer Value: Seconds: 30

Digit Relay Packet Type: 101

Digit Relay Packet Type (16000): 102

Modem Behavior: Disabled

Source Port Validate: Enable

High Jitter: Disable

SIP Maximum Call Duration: Disable

SIP Maximum Call Duration value: Minutes: 60

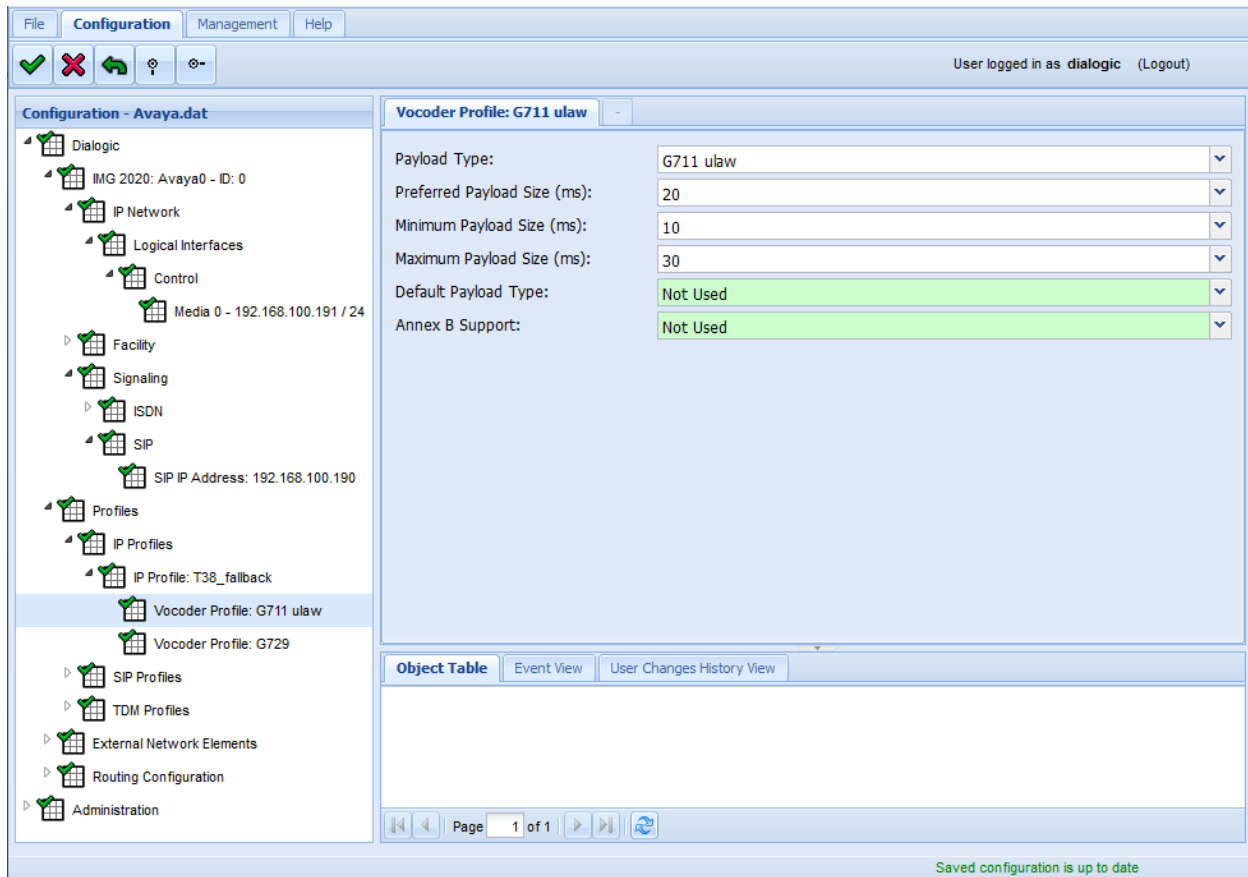
Object Table Event View User Changes History View

Page 1 of 1

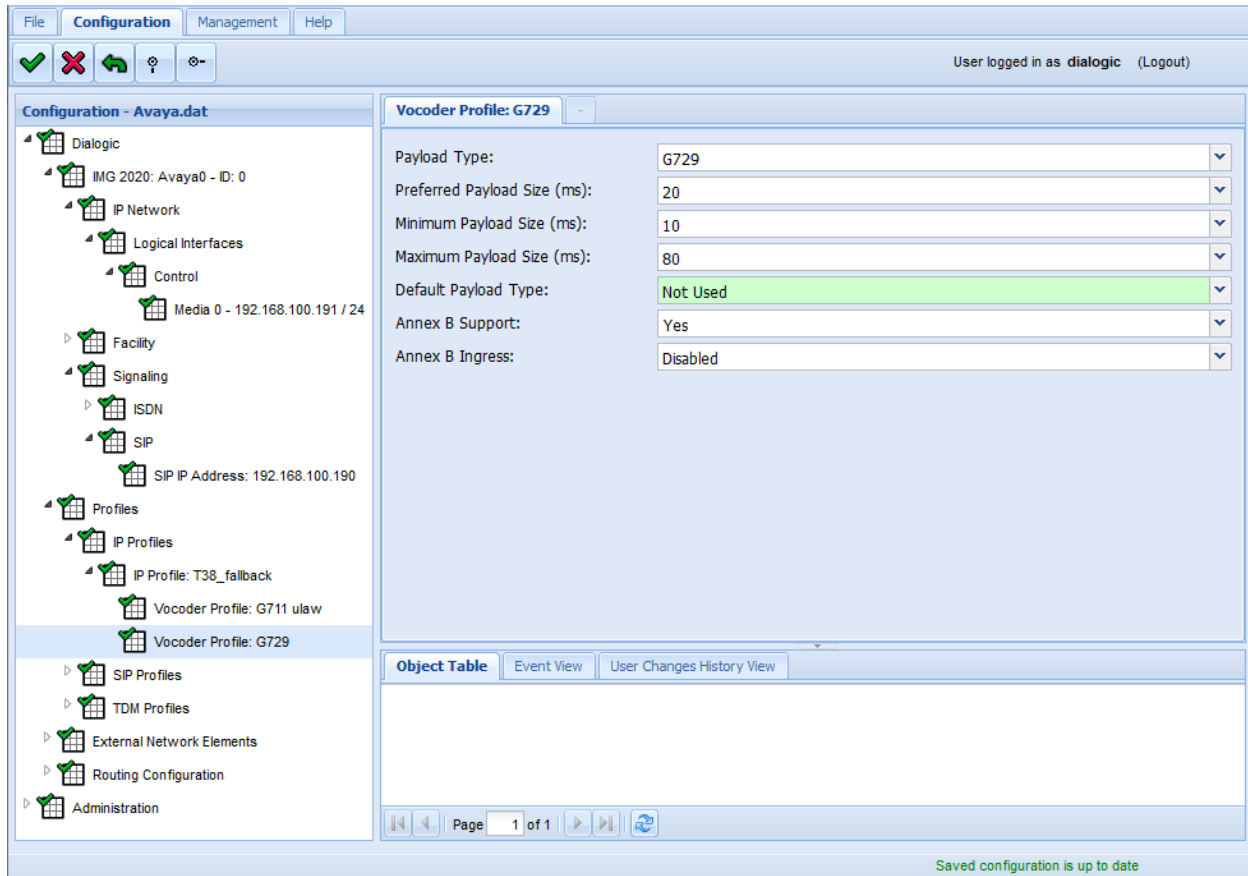
Saved configuration is up to date

In the next step, the G.711 and G.729 codecs will be associated with the profile. Note that the order in which the codecs are listed indicate their preference order.

Right-click on the **IP Profile: T38_fallback** object (name may vary) and select **New Vocoder Profile** to associate the G.711 codec with the profile. In the **Vocoder Profile**, set the **Payload Type** to *G711 ulaw*.



Repeat the step above to associate the G.729 codec with the profile. Right-click on the **IP Profile: T38_fallback** object and select **New Vocoder Profile** to associate the G.729 codec with the profile. In the **Vocoder Profile**, set the **Payload Type** to *G729* and **Annex B Support** to *Yes*.



7.5.2 Configure SIP Profile

The **SIP Profile** configures the attributes and features needed to communicate with a specific external gateway (i.e., Session Manager and Communication Manager). To configure the **SIP Profile**, follow these steps.

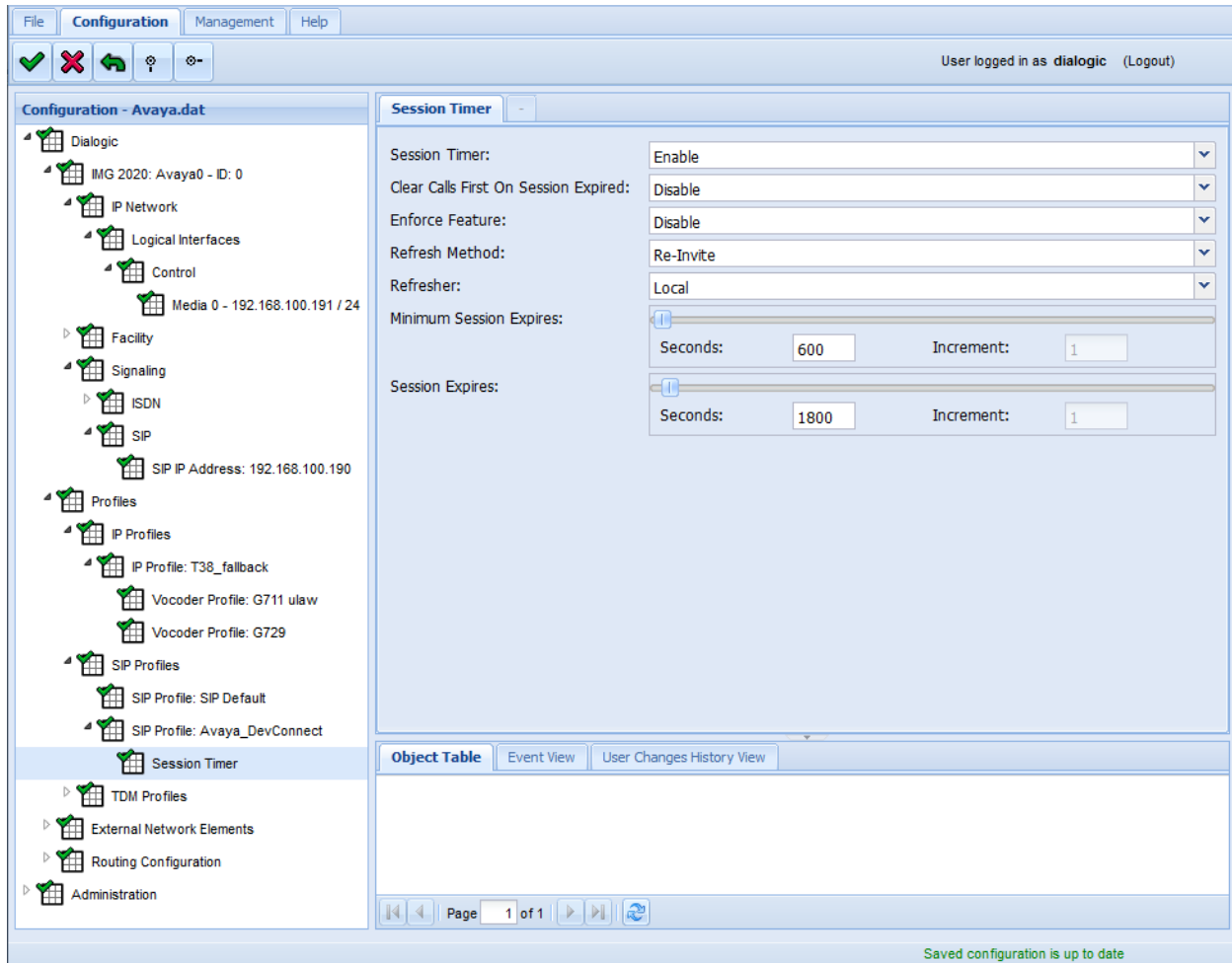
1. Right-click on the **Profiles** object and select **New SIP Profiles**.
2. Right-click on the **SIP Profiles** object and select **New SIP Profile**.

In the **SIP Profile** screen, enter a descriptive name in the **Name** field (e.g., *Avaya_DevConnect*). For **Codec Priority**, select **Remote**. This gives the codec preference order of the remote side priority during codec negotiation. Keep the default values for the remaining fields.

The screenshot displays the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy: Dialogic > MG 2020: Avaya0 - ID: 0 > IP Network > Logical interfaces > Control > Media 0 - 192.168.100.191 / 24 > Facility > Signaling > ISDN > SIP > SIP IP Address: 192.168.100.190 > Profiles > IP Profiles > IP Profile: T38_fallback > Vocoder Profile: G711 ulaw > Vocoder Profile: G729 > SP Profiles > SIP Profile: SIP Default > SIP Profile: Avaya_DevConnect. The main panel shows the configuration for 'SIP Profile: Avaya_DevConnect'. The 'Name' field is set to 'Avaya_DevConnect'. The 'Codec Priority' is set to 'Remote'. Other settings include: PRACK Support: Disabled, PRACK Timer (s): 150, Precondition Support: Disabled, Precondition Loose Validation: Disabled, Early 183: Disabled, 3XX Redirect Support: Enabled, Redirection To Same IP/Port: Disallow, Loop Detection: Enabled, Loop Detection Method: To Header, INVITE Retransmission Attempts: Retransmit All, Trusted: Enabled, Privacy: P-Asserted only, PAID RPID Display Name: When none received send user part of URI, INFO Keep-Alive Support: Disabled, Outbound Delayed Media: Disabled, SRTP Mode: Disabled, 180 Ringing Behavior: Send 183 Progress w/SDP, Ptime Source For SDP Answer: Match Remote, Force Digit Relay Setting For Answer: Disabled, Allow SDP empty S line: Disabled, and Re-attempt Outgoing Call On MID: Disabled. The bottom of the interface shows a status bar with 'Saved configuration is up to date'.

Field	Value
Name	Avaya_DevConnect
PRACK Support	Disabled
PRACK Timer (s)	150
Precondition Support	Disabled
Precondition Loose Validation	Disabled
Early 183	Disabled
Codec Priority	Remote
3XX Redirect Support	Enabled
Redirection To Same IP/Port	Disallow
Loop Detection	Enabled
Loop Detection Method	To Header
INVITE Retransmission Attempts	Retransmit All
Trusted	Enabled
Privacy	P-Asserted only
PAID RPID Display Name	When none received send user part of URI
INFO Keep-Alive Support	Disabled
Outbound Delayed Media	Disabled
SRTP Mode	Disabled
180 Ringing Behavior	Send 183 Progress w/SDP
Ptime Source For SDP Answer	Match Remote
Force Digit Relay Setting For Answer	Disabled
Allow SDP empty S line	Disabled
Re-attempt Outgoing Call On MID	Disabled

Right-click on the **SIP Profile: Avaya_DevConnect** object (name may vary) and select **New SIP Session Timer**. In the **Session Timer** screen, set the **Minimum Session Expires** field to the appropriate value. For the compliance test, this timer was set to 600 seconds to match the default value in the SIP trunk group on Communication Manager.



7.6 Configure External Network Element

Configure the **External Network Element**, which in this case the external SIP gateway is Session Manager. The **External Network Element** will be associated with the **Channel Group** configured in **Section 7.7.1**. To create the **External Network Element**, follow these steps.

1. Right-click on the **Dialogic** object and select **New Network Elements**.
2. Right-click on the **External Network Elements** object and select **New External Gateways**.
3. Right-click on the **External Gateways** object and select **New External Gateway**.

In the **External Gateway** screen, provide a descriptive name in the **Name** field (e.g., *Avaya_SM*). Set the **Protocol** to *SIP* and the **IP Address** to the IP address of the Session Manager signaling interface (e.g., *10.64.102.117*). Set the **Transport Type** and **Transport Port** to *UDP* and *5060*, respectively. Set the **Profile** to *Avaya_DevConnect* to associate the external network element with the **SIP Profile** created in **Section 7.5.2**. Lastly, enable **OPTIONS Keep Alive** to allow IMG 2020 to send SIP Options messages to Session Manager.

The screenshot displays the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy: Dialogic > IMG 2020: Avaya0 - ID: 0 > IP Network > Logical Interfaces > Control > Media 0 - 192.168.100.191 /... > Facility > Signaling > ISDN > SIP > SIP IP Address: 192.168.100.191 /... > Profiles > IP Profiles > IP Profile: T38_fallback > Vocoder Profile: G711 ulaw > Vocoder Profile: G729 > SIP Profiles > SIP Profile: SIP Default > SIP Profile: Avaya_DevConnect > Session Timer > TDM Profiles > External Network Elements > External Gateways > Avaya_SM. The main panel shows the configuration for Avaya_SM. The fields are: Name: Avaya_SM, Protocol: SIP, Address Type: IP Address, IP Type: IPv4, IP Address: 10.64.102.117, Allowed Gateway Subnet Prefix: 32, HostName: (empty), Keep HostName in outgoing SIP request: Disabled, Transport Type: UDP, Transport Port: 5060, Registration Required: No, Registration Interval: 3600, Profile: ID: 1 - Avaya_DevConnect, Secure Profile: Not Used, and OPTIONS Keep Alive: Enable. The bottom status bar shows 'Saved configuration is up to date'.

Field	Value
Name	Avaya_SM
Protocol	SIP
Address Type	IP Address
IP Type	IPv4
IP Address	10.64.102.117
Allowed Gateway Subnet Prefix	32
HostName	
Keep HostName in outgoing SIP request	Disabled
Transport Type	UDP
Transport Port	5060
Registration Required	No
Registration Interval	3600
Profile	ID: 1 - Avaya_DevConnect
Secure Profile	Not Used
OPTIONS Keep Alive	Enable

7.7 Configure Routing

This section covers the configuration for routing calls between the Avaya enterprise network and the PSTN. For the compliance test, basic routing was set up where calls received from the SIP trunk was automatically routed out the ISDN-PRI trunk and vice versa. To configure routing, **Channel Groups** and **Routing Tables** need to be created as specified in this section.

7.7.1 Configure Channel Group

To configure the Channel Group for the SIP trunk, follow these steps.

1. Right-click on the **Dialogic** object and select **New Routing Configuration**.
2. Right-click on the **Routing Configuration** object and select **New Channel Groups**.
3. Right-click on the **Channel Groups** object and select **New Channel Group**.

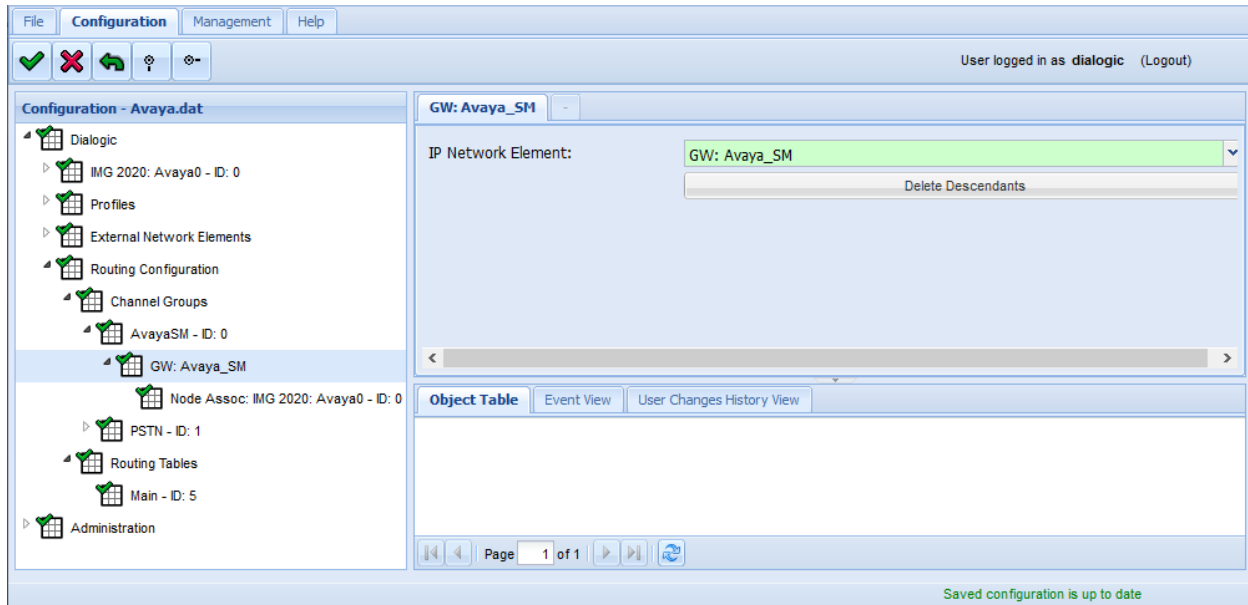
In the **Channel Group** screen, provide a descriptive name in the **Name** field (e.g., *AvayaSM*). Set the **Signaling Type** to *SIP* and set the **Incoming IP Profile** and **Outgoing IP Profile** to the *T38_fallback* IP Profile created in **Section 7.5.1**. Set the **Route Table** to the one configured in **Section 7.7.2**. Keep the default values for the remaining fields.

The screenshot displays the AvayaSM configuration window. The left sidebar shows a tree view with 'Dialogic' expanded, containing 'IMG 2020: Avaya0 - ID: 0', 'Profiles', 'External Network Elements', 'Routing Configuration', 'Channel Groups', 'AvayaSM - ID: 0' (selected), 'GW: Avaya_SM', 'Node Assoc: IMG 2020: Avaya0', 'PSTN - ID: 1', 'Routing Tables', 'Main - ID: 5', and 'Administration'. The main area shows the configuration for 'AvayaSM - ID: 0'. The fields are as follows:

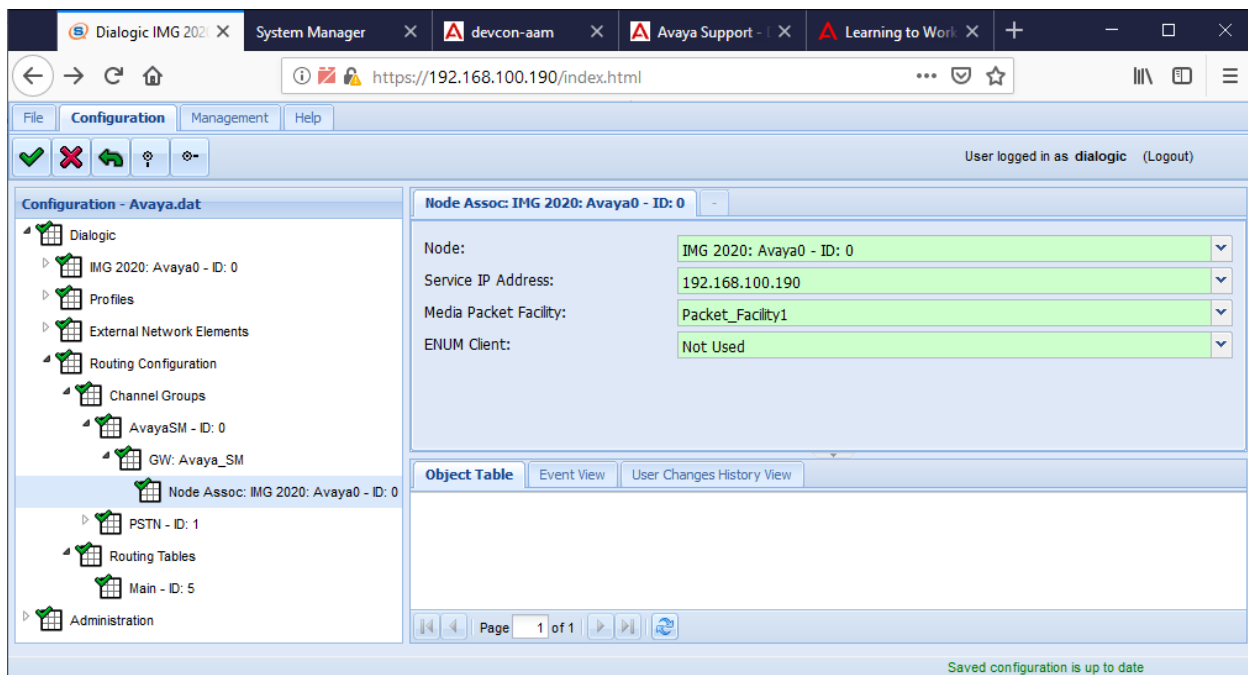
Field	Value
ID	0
Name	AvayaSM
Trunk Direction	Incoming/Outgoing
Signaling Type	SIP
Route Table	Main - ID: 5
Cause Code Table	None
Incoming IP Profile	T38_fallback
Outgoing IP Profile	T38_fallback
Incoming Treatment	Release w/Cause
Outgoing Treatment	Release w/Cause
Incoming Translation Table	None
Outgoing Translation Table	None
Hunting Options	Round Robin Clockwise
Ingress Side will Play Call Progress Tones	False
Re-Attempt Cause Code	Not Used
Support Digit A to F	False

Below the fields is an 'Object Table' section with tabs for 'Object Table', 'Event View', and 'User Changes History View'. The 'Object Table' tab is active, showing an empty table. At the bottom, a status bar indicates 'Saved configuration is up to date'.

Right-click on the **AvayaSM** channel group object (name may vary) and select **New IP Network Element**. In the **Network Element** screen, set **IP Network Element** to the **Avaya_SM External Gateway** configured in **Section 7.6**.



Right-click on the **GW: Avaya_SM** object (name may vary) and select **New Node Association**. Set **Node** to the IMG 2020 Physical Node created in **Section 7.2**, set the **Service IP Address** to the IMG 2020 Signaling IP address (e.g., *192.168.100.190*), and set the **Media Packet Facility** to *Packet_Facility1*.



7.7.2 Configure Routing Table

For the compliance test, basic routing was set up where calls received from the SIP trunk was automatically routed out the ISDN-PRI trunk and vice versa. To create the Routing table, follow these steps.

1. Right-click on the **Routing Configuration** object and select **New Routing Table**.
2. Right-click on the **Routing Tables** object and select **New Route Table**.

In the **Route Table** screen, enter a descriptive name in the **Name** field (e.g., *Main*).

The screenshot displays the Avaya CMS interface for configuring a routing table. The left sidebar shows a tree view with 'Routing Tables' expanded, highlighting 'Main - ID: 5'. The main panel shows the configuration for 'Main - ID: 5' with the following details:

- ID:** 5
- Name:** Main
- Routing Criteria Order:** A list box containing: Prefix, Dialed Number, Originating Number, Channel Group, and Called NOA.
- Buttons:** Download Routing Table, Delete All Route Elements

Below the configuration fields is an 'Object Table' with the following data:

ID	Enable	Route Criteria Type	Router String	In Channel Group	Crite
2	True	Channel Group		AvayaSM	Not
1	True	Channel Group		PSTN	Not

At the bottom, a status bar indicates 'Saved configuration is up to date'.

Right-click on the **Main – ID 5** object (name may vary) and select **New Route Element**. In the **Element** tab, set **Route Criteria Type** and **Route Action Type** to *Channel Group*. Set the **In Channel Group** to the channel group for the ISDN-PRI interface (not shown in these Application Notes). Set the **Outgoing Channel Group** to the *AvayaSM* channel group configured in **Section 7.7.1**. This routing configuration specifies that incoming calls on the ISDN-PRI trunk from the PSTN will be routed out the SIP trunk to the Avaya enterprise site.

Configuration - Avaya.dat

Main - ID: 5 Element: 1

ID: 1

Enable: True

Route Criteria Type: Channel Group

Router String:

In Channel Group: PSTN

Criteria Values: Not Used

FCI - M Bit: Not Used

Route Action Type: Channel Group

Outgoing Channel Group: AvayaSM

Object Table

ID	Enable	Route Criteria Type	Router String	In Channel Group	Criteria
2	True	Channel Group		AvayaSM	Not
1	True	Channel Group		PSTN	Not

Page 1 of 1

Saved configuration is up to date

Repeat the step above. Right-click on the **Main – ID 5** object (name may vary) and select **New Route Element**. In the **Element** tab, set **Route Criteria Type** and **Route Action Type** to *Channel Group*. Set the **In Channel Group** to the *AvayaSM* channel group configured in **Section 7.7.1**. Set the **Outgoing Channel Group** to the channel group for the ISDN-PRI interface (not shown in these Application Notes). This routing configuration specifies that incoming calls on the SIP trunk from the Avaya enterprise site will be routed out the ISDN-PRI trunk to the PSTN.

Configuration - Avaya.dat

Main - ID: 5 **Element: 2**

ID: 2

Enable: True

Route Criteria Type: Channel Group

Router String:

In Channel Group: AvayaSM

Criteria Values: Not Used

FCI - M Bit: Not Used

Route Action Type: Channel Group

Outgoing Channel Group: PSTN

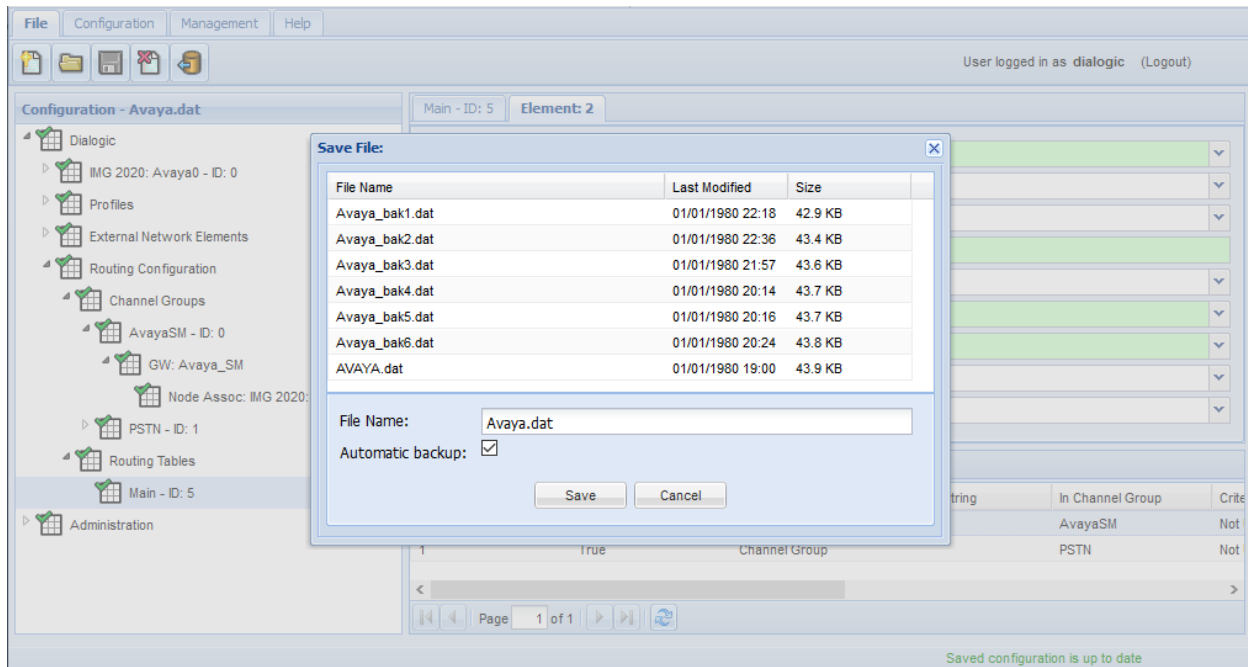
ID	Enable	Route Criteria Type	Router String	In Channel Group	Crite
2	True	Channel Group		AvayaSM	Not
1	True	Channel Group		PSTN	Not

Page 1 of 1

Saved configuration is up to date

7.8 Save Configuration

Once the configuration is complete, save the configuration by navigating to **File → Save** and specify the appropriate **File Name** in the dialog box as shown below. Click **Save**.



8 Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Sangoma IMG 2020.

1. The **status trunk** command may be used on Communication Manager to view the **Service State** of the SIP trunk to Session Manager. The trunk members should be in the *in-service/idle* state when no calls are active as shown below.

```
status trunk 10
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0010/0001	T00001	in-service/idle	no
0010/0002	T00002	in-service/idle	no
0010/0003	T00003	in-service/idle	no
0010/0004	T00004	in-service/idle	no
0010/0005	T00005	in-service/idle	no
0010/0006	T00006	in-service/idle	no
0010/0007	T00007	in-service/idle	no
0010/0008	T00008	in-service/idle	no
0010/0009	T00009	in-service/idle	no
0010/0010	T00010	in-service/idle	no

2. Alternatively, the connection status of the SIP trunk between Communication Manager and Session Manager may be viewed on System Manager by navigating to **Elements → Session Manager → System Status → SIP Entity Monitoring** and clicking on the appropriate SIP entities. Below is the status of the SIP trunk to Communication Manager. The **Conn. Status** should be *UP*.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, user information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled "SIP Entity, Entity Link Connection Status" and provides a summary view of the connection status for the selected Session Manager instance, devcon-sm. The table below shows the connection status for the selected SIP entity.

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	10.64.102.115	5061	TLS	FALSE	UP	200 OK	UP

- Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Session Manager

Session Manager

Dashboard

Session Manager Ad...

Global Settings

Communication Pro...

Network Configur...

Device and Locati...

Application Confi...

System Status

SIP Entity Monit...

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: SangomaIMG2020

Summary View

1 Item

Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	devcon-sm	IPv4	192.168.100.190	5060	UDP	FALSE	UP	200 OK	UP

Select : None

9 Conclusion

These Application Notes describe the configuration steps required to integrate the Sangoma IMG 2020 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Voice and fax calls were successfully established between the Avaya enterprise site and the PSTN. In addition, telephony features such as hold/resume, call transfers, conference calls, call forwarding, calling number display/block, and voicemail coverage were also exercised. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10 References

This section references the Avaya and Sangoma documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.0.1, Issue 3, December 2018, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager for Release 8.0.1*, Release 8.0.x, Issue 7, January 2019, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018, available at <http://support.avaya.com>.
- [4] *Sangoma IMG 2020 User Manual*, available at <https://wiki.sangoma.com/display/DIMG/IMG+2020+Documentation>

©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.