



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Dialogic® Brooktrout® SR140 Fax Software with Avaya Aura® Communication Manager and Avaya Aura® Session Manager via SIP Trunk Interface using Transport Layer Security (TLS) - Issue 1.1

Abstract

These Application Notes describe the procedures for configuring the Dialogic® Brooktrout® SR140 Fax Software version 6.9.2 with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Session Manager 8.0 via a SIP trunk interface using Transport Layer Security (TLS). Dialogic Brooktrout SR140 is fax software that sends and receives fax calls over an IP network. In the tested configuration, Dialogic Brooktrout SR140 interoperated with Avaya Aura® Session Manager to send/receive faxes using SIP trunk facilities.

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 procedures for configuring Dialogic® Brooktrout® SR140 (SR140) with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager) using SIP trunks.

Dialogic Brooktrout SR140 is host-based Fax over IP that uses Dialogic Brooktrout Fax/Voice Diagnostic Test Tool (FDTool) to send and receive fax calls over an IP network. In the tested configuration, Dialogic SR140 interoperated with Avaya Aura® Session Manager to send/receive faxes using a SIP trunk interface.

2. General Test Approach and Test Results

This section describes the compliance test approach used to verify interoperability of Dialogic SR140 with Session Manager. By using a SIP trunk that was established between the Communication Manager and SR140 via Session Manager, faxes were sent and received between these two systems.

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 the Dialogic Brooktrout SR140 utilizes TLS and secure media encryption features as requested by Dialogic. Operation using TCP and UDP over the SIP trunk is also supported

2.1. Interoperability Compliance Testing

The compliance test tested interoperability between SR140 and Session Manager by making intra-site fax calls between SR140 fax software client and an analog fax machine that was connected to a Communication Manager via Session Manager using SIP trunks. For inter-site fax, calls were made between SR140 and an analog fax machine that was connected on a remote site. The remote site connection used ISDN and SIP trunks. Specifically, the following fax operations were tested in the setup for the compliance test:

- Fax from/to SR140 fax software client to/from fax machine at a local site
- Fax from/to SR140 fax software client to/from fax machine at a remote site

Both T.38 standard and G.711 pass-through were tested. Faxes were sent with various page lengths and resolutions.

Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources, and restarts of FDTTool.

Fax calls were also tested with the integrated VoIP engine of the Avaya G450 Media Gateway and the Avaya MM760 Media Module installed in the Avaya G450 Media Gateway.

2.2. Test Results

Dialogic SR140 successfully passed all compliance testing with the following observations:

- During sending or receiving of a fax, if the SR140 fax software client is interrupted with network outage or a reboot, the faxes will not be complete after the SR140 service is restored. A fax that is being sent will show the status as being sent and will have to be manually sent again. A fax that is being received will not be completed and has to be resent.
- The Fax transmission rate depends on the Media Gateway or the card being used. In a G450 Media gateway, the negotiation is seen at V.29 (9600 bits).
- An incoming fax call from Communication Manager to SR140 will be dropped if encrypted video functionality is enabled in the signaling group that is configured to use for the fax call. To resolve this issue, the video call feature should be set to “n” in the signaling group in **Section 5.5**.
- When the secure media SRTP is enabled in the configuration (**Section 7.5**), Dialogic SR140 does not accept regular media (RTP) in SDP of incoming INVITE message for SIP TLS, only enforced secure media SRTP is accepted.
- For interoperability with Avaya gateways, it is recommended that the V.34 fields be disabled on the SR140, as shown in Section 7.3.

Note1: Fax calls consume DSP (Digital Signal Processing) resources for processing fax data on the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G450 Media Gateway. To increase the capacity to support simultaneous fax calls, additional Avaya MM760 Media Module or Modules need to be installed in the Avaya G450 Media Gateway. Customers should work with their Avaya sales representatives to ensure that their fax solutions have adequate licenses and DSP resources to match the intended Fax capacity/usage.

Note2: The SIP trunk group on Communication Manager for connecting to Session Manager at each site, as well as the SIP or ISDN-PRI trunk group for connecting the two sites, must be configured with adequate number of trunk group members to support the number of simultaneous fax calls intended.

2.3. Support

North American Technical support for Brooktrout SR140 Fax Software can be obtained by contacting Dialogic at.

- North America: 973-993-1443
- Singapore: +65 6407 7376
- Japan: +81 3-3234-2176
- EMEA: +44 1628 641 792
- Email: support@dialogic.com
- Website: <https://support.dialogic.com>

3. Reference Configuration

The test configuration was designed to emulate a local site and a remote site. **Figure 1** illustrates the configuration used in these Application Notes. In the sample configuration, Communication Manager, G450 Media Gateway, Avaya Aura® Session Manager, System Manager, Dialogic Brooktrout SR140 and an analog fax machine are considered to be a local site. The Brooktrout SR140 fax software client communicates to the Communication Manager via the Session Manager using SIP TLS. In turn, Communication Manager used a SIP Trunk to communicate with Session Manager. An analog fax port is configured on the Communication Manager to which a fax machine is connected. The equipment involved in the remote site is beyond the scope of this document and is shown here for reference only. The local and remote sites communicate via ISDN-PRI and SIP trunks that are configured between the Communication Manager, Session Manager and the PBXs available at the remote site. This same scenario was also repeated using SIP over TCP, and SIP over UDP. The following are typical scenarios verified during the compliance test:

- Bi-directional faxed between SR140 Fax software client and the local fax endpoint 1 that connected to an analog port in the G450 Media Gateway.
- Bi-directional faxes between SR140 Fax software client and PSTN fax endpoint 2 via PRI trunk.
- Bi-directional faxes between SR140 Fax software client and PSTN fax endpoint 3 via SIP trunk.

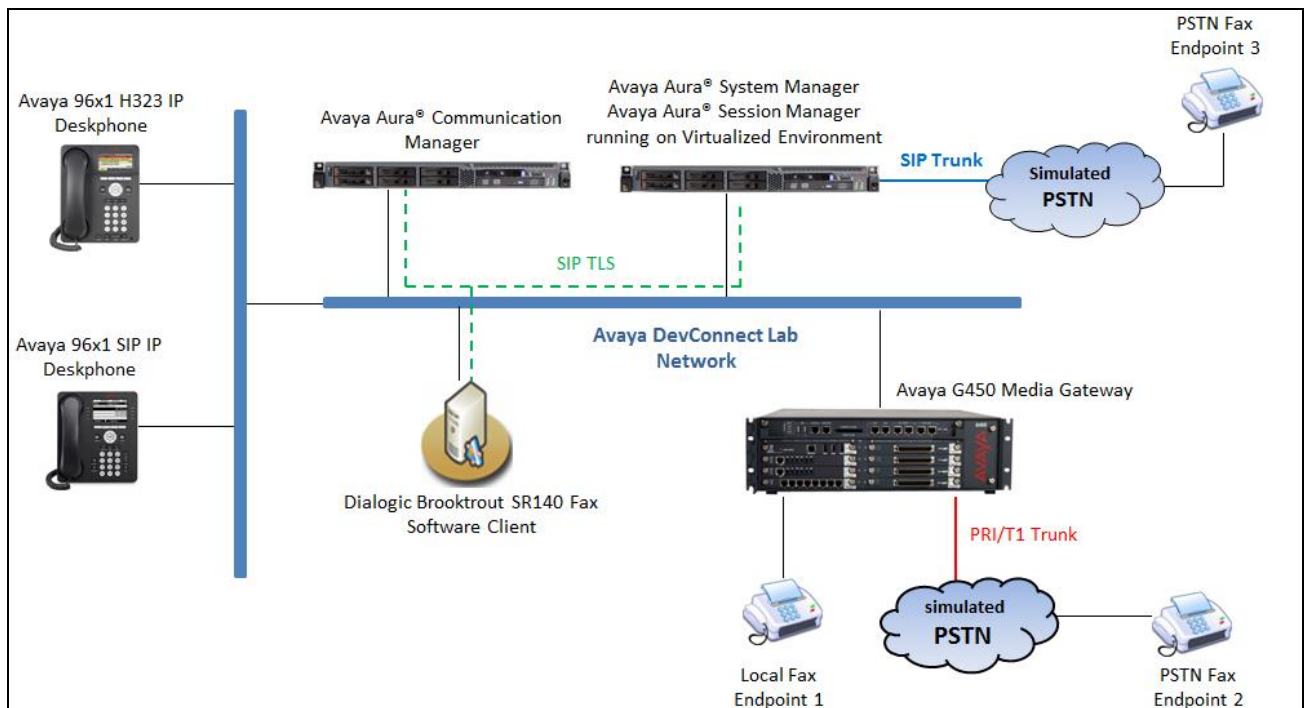


Figure 1: Brooktrout SR140 interoperating with Session Manager via SIP Trunk

4. Equipment and Software Validated

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

Equipment	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	8.0 R018x.00.0.822.0 Patch 24826
Avaya G450 Media Gateway	8.0.0.150
Avaya Aura® System Manager running on Virtualized Environment	8.0 Build 8.0.0.0.931077
Avaya Aura® Session Manager running on Virtualized Environment	8.0 Build 8.0.0.0.800035
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.150
Avaya 96x1 IP Deskphones	6.6604 (H.323) 7.1.3 (SIP)
Dialogic Brooktrout SR140 Fax Software running on Microsoft Windows 10	v6.9.2 Build 2

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with Session Manager and Brooktrout SR140. It focuses on the configuration of the SIP trunks connecting Communication Manager to the Avaya SIP infrastructure with the following assumptions:

- The examples shown in this section refer to the local site.
- The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, the **save translation** command was used to make the changes permanent.

The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager License
- Administer IP Node Names
- Administer Codecs
- Administer IP Network Region
- Administer Signaling Group
- Administer Trunk Group
- Administer Private Numbering
- Administer Outbound Routing

5.1. Verify Communication Manager License

Use the **display system-parameters customer-options** command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:		12000 20
Maximum Concurrently Registered IP Stations:		18000 4
Maximum Administered Remote Office Trunks:		12000 0
Maximum Concurrently Registered Remote Office Stations:		18000 0
Maximum Concurrently Registered IP eCons:		128 0
Max Concur Registered Unauthenticated H.323 Stations:		100 0
Maximum Video Capable Stations:		36000 2
Maximum Video Capable IP Softphones:		18000 6
Maximum Administered SIP Trunks:		12000 58
Maximum Administered Ad-hoc Video Conferencing Ports:		12000 0
Maximum Number of DS1 Boards with Echo Cancellation:		522 0

5.2. Administer IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager (**procr**) and for Session Manager (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section 5.5**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AMS1	10.33.1.30	
default	0.0.0.0	
interopASM	10.33.1.12	
procr	10.33.1.6	

5.3. Administer Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the local and remote sites. For the compliance test, codec G.711MU and G.729A was configured using ip-codec-set 1. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Note that the **Media Encryption** has only “1-srtp-aescm128-hmac80” configured which enforce secure media used for fax call and matched with the media encryption in Dialogic SR140. Default values can be used for all other fields.

change ip-codec-set 1

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: 1-srtp-aescm128-hmac80

2:

3:

On **Page 2**, set the **FAX** mode to “t.38-standard”. Retain default values for all other fields.

change ip-codec-set 1

Page2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? y

Maximum Call Rate for Direct-IP Multimedia: 1024:Kbits

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

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

Media Connection IP Address Type Preferences

1: IPv4

2:

5.4. Administer IP Network Region

For the compliance test, IP network region 1 was chosen. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the local site. In this configuration, the domain name is **bvwdev.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field. This is optional.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.3**.
- Retain default values for all other fields.

change ip-network-region 1		Page	1 of 20
IP NETWORK REGION			
Region: 1	NR Group: 1		
Location: 1	Authoritative Domain: bvwdev.com		
Name: Loc-1	Stub Network Region: n		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 1		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3329			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			

On **Page 4**, define the IP codec set to be used for traffic between various regions. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. In the case of the compliance test, only one IP network region was used, so no inter-region settings were required and therefore only codec set 1 is used.

change ip-network-region 1				Page	4 of 20
Source Region: 1				Inter Network Region Connection Management	
				I	M
				G	t
dst	codec	direct	WAN-BW-limits	Video	Intervening
rgn	set	WAN	Units	Total Norm	Prio Shr Regions
1	1				
2	2	y	NoLimit	n	t

5.5. Administer Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by SIP trunks. This signaling group is used for inbound and outbound calls between the Communication Manager and Session Manager. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- The compliance test was conducted with the **Transport Method** set to “tls”. The transport method specified here is used between Communication Manager and Session Manager. Whatever protocol is used here, it must also be used on the Session Manager entity link defined in **Section 6.5**. Compliance testing was also conducted with **Transport Method** set to “tcp” and “udp.” (Note: for TCP and UDP operation, refer to an earlier Application Note: <https://www.devconnectprogram.com/fileMedia/download/b2a7ac70-0eab-4a9f-aff0-b706ec465be3>)
- Set the **IP Video** to “n” – Note that the IP Video should be set to “n” to disable the video call capability for incoming fax call from Communication Manager to SR140 to work.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to “procr”. This node name maps to the IP address of the Communication Manager as defined in **Section 5.2**.
- Set the **Far-end Node Name** to “InteropASM”. This node name maps to the IP address of Session Manager as defined in **Section 5.2**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a default well-known port value. (For TCP the well-known port value is 5060).
- Set the **Far-end Network Region** to the IP network region defined for the local site in **Section 5.4**.
- Set the **Far-end Domain** to the domain of the local site.
- Set **Direct IP-IP Audio Connections** to “y”. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to “rtp-payload”. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Retain default values for all other fields.

SIGNALING GROUP

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

Far-end Domain: bvwdev.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? n
Alternate Route Timer(sec): 6

5.6. Administer Trunk Group

Use the “add trunk-group” command to create a trunk group for the signaling group created in **Section 5.5**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to “sip”.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to “tie”.
- Set **Member Assignment Method** to “auto”.
- Set the **Signaling Group** to the signaling group shown in **Section 5.5**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Retain default values for all other fields.

```
add trunk-group 1                                     Page 1 of 22
TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
Group Name: Private Trunk                          COR: 1                 TN: 1                TAC: #01
Direction: two-way                                Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                  Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 1
                                                Number of Members: 14
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. The **Numbering Format** was set to “private” and the **Numbering Format** in the route pattern was set to “lev0-pvt” (see **Section 5.8**).

```
add trunk-group 1                                     Page 3 of 22
TRUNK FEATURES
ACA Assignment? n                                Measured: none
                                                Maintenance Tests? y

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

                                                Hold/Unhold Notifications? y
                                                Modify Tandem Calling Number: no
Send UCID? y
```

5.7. Administer Private Numbering

Private numbering defines the calling party number to be sent to the far-end. Use the **change private-numbering** command to create an entry that will be used by the trunk groups defined in **Section 5.6**. In the example shown below, all calls originating from a 4-digit extension beginning with “3” and routed across trunk group 1 are sent with a 4-digit calling number.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3	1		4	Total Administered: 5
4					Maximum Entries: 540

5.8. Administer Outbound Routing

In these Application Notes, the Automatic Alternate Routing (AAR) feature is used to route outbound calls via the SIP trunk to the FDTTool fax server. In the sample configuration, the dial prefix “52” is used as the Dialed String. Local site users will dial “52xx” to reach the FDTTool fax server. This common configuration is illustrated below with little elaboration. Use the “change dialplan analysis” command to define a dialed string beginning with 52 of length 4 as uniform dialing plan (UDP).

change dialplan analysis										Page 1 of 12
DIAL PLAN ANALYSIS TABLE										
Location: all							Percent Full: 5			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type		
52	4	udp								

Use the “change uniform-dialplan” command to create a matching pattern that matches with the dial pattern used to reach the FDTTool fax server. The example below shows entries created for local site. Extension 51xx was used and configured as shown below where “52” is the Matching Pattern with a Length of 4, no digits to be deleted and using the aar feature.

change uniform-dialplan 0								Page 1 of 2
UNIFORM DIAL PLAN TABLE								
								Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num		
52	4	0		aar	n			

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the “change route-pattern” command to configure the parameters for the local site route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP trunk. For the compliance test, trunk group **1** was used.
- **FRL:** 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.
- **Numbering Format:** “lev0-pvt”. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in **Section 5.6** for full details.
- Retain default values for all other fields.

change route-pattern 1										Page	1	of	3
Pattern Number: 1					Pattern Name: SIP-TLS-To-SM								
SCCAN? n		Secure SIP? n			Used for SIP stations? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC					
No			Mrk	Lmt	List	Del	Digits	QSIG					
							Dgts	Intw					
1:	1	0						n	user				
2:								n	user				
3:								n	user				
4:								n	user				
5:								n	user				
6:								n	user				
BCC		VALUE		TSC	CA-TSC		ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR
0	1	2	M	4	W	Request					Dgts	Format	
1:	y	y	y	y	y	n	n	rest				lev0-pvt	next
2:	y	y	y	y	y	n	n	rest					none
3:	y	y	y	y	y	n	n	rest					none

Use the “change aar analysis” command to create an entry in the AAR Digit Analysis Table for this purpose. The example below shows entries created for the local site “aar analysis 52”. The highlighted entry specifies that 4 digit dial string 52 was to use route pattern 1 to route calls to the FDTool fax server at the local site via Session Manager.

change aar analysis 51										Page 1 of 2		
AAR DIGIT ANALYSIS TABLE												
Location: all										Percent Full: 2		
Dialed		Total		Route		Call	Node	ANI				
String		Min	Max	Pattern		Type	Num	Reqd				
52		4	4	1		aar		n				

6. Configure Avaya Aura® Session Manager

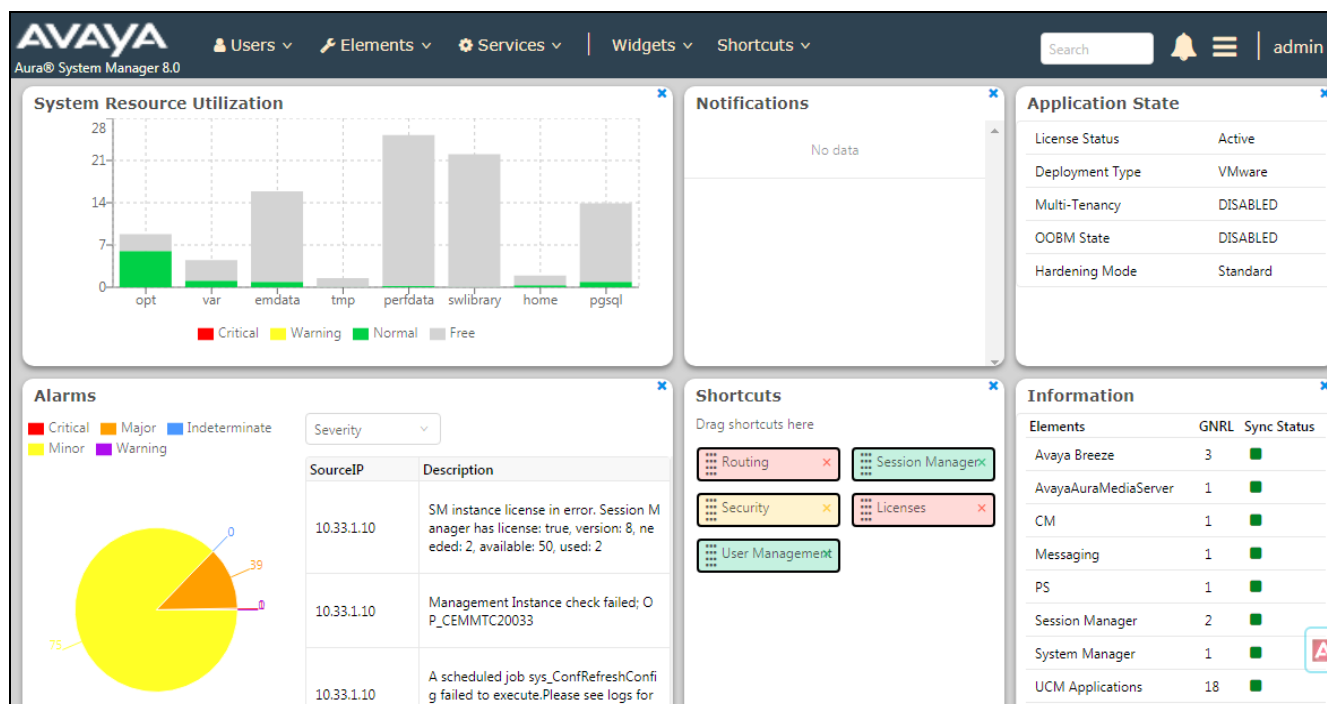
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns

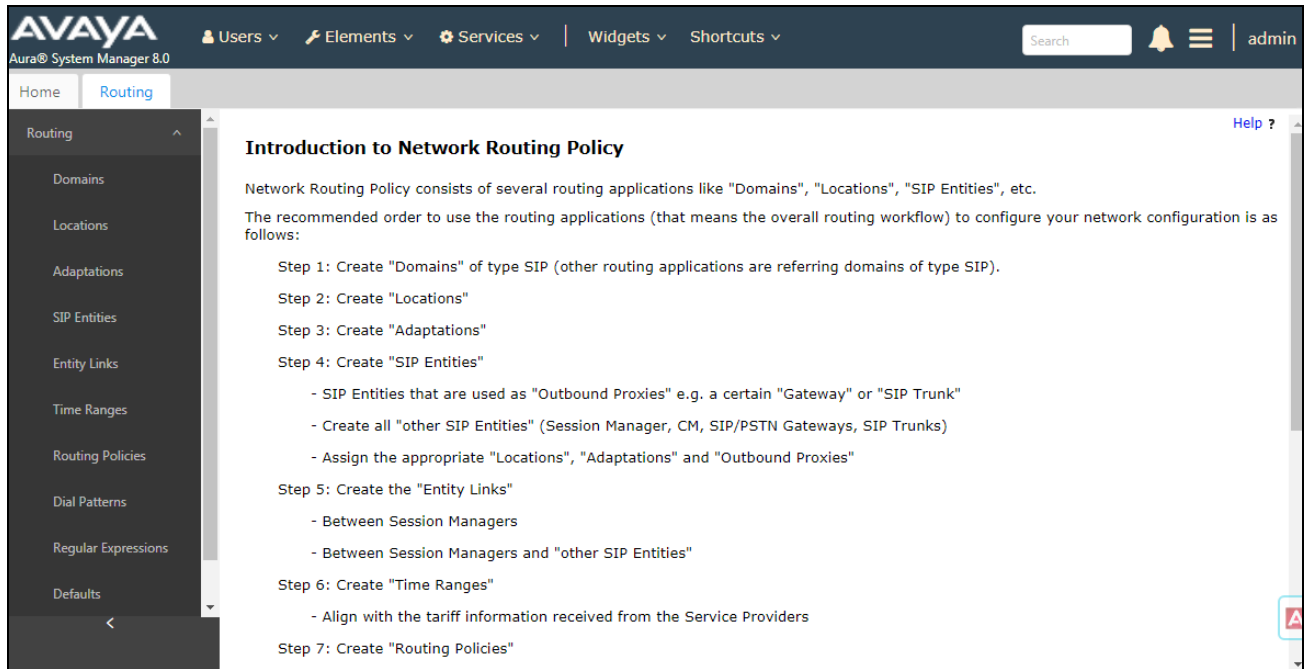
For detail configuration details of the Session Manager refer to **Section 10**.

6.1. Logging into the Avaya Aura® System Manager

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log on** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements** → **Routing** link highlighted below.



Clicking the **Elements** → **Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.



6.2. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the domain (**bvwdev.com**) as defined in **Section 5.4**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select “sip” from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the added domain.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left-hand navigation pane is expanded, showing 'Routing' as the active section, with 'Domains' selected. The main content area is titled 'Domain Management' and features a table with one item. The table has columns for Name, Type, and Notes. The Name column contains 'bvwdev.com', the Type column contains 'sip', and the Notes column contains 'SIP Domain'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table.

Name	Type	Notes
bvwdev.com	sip	SIP Domain

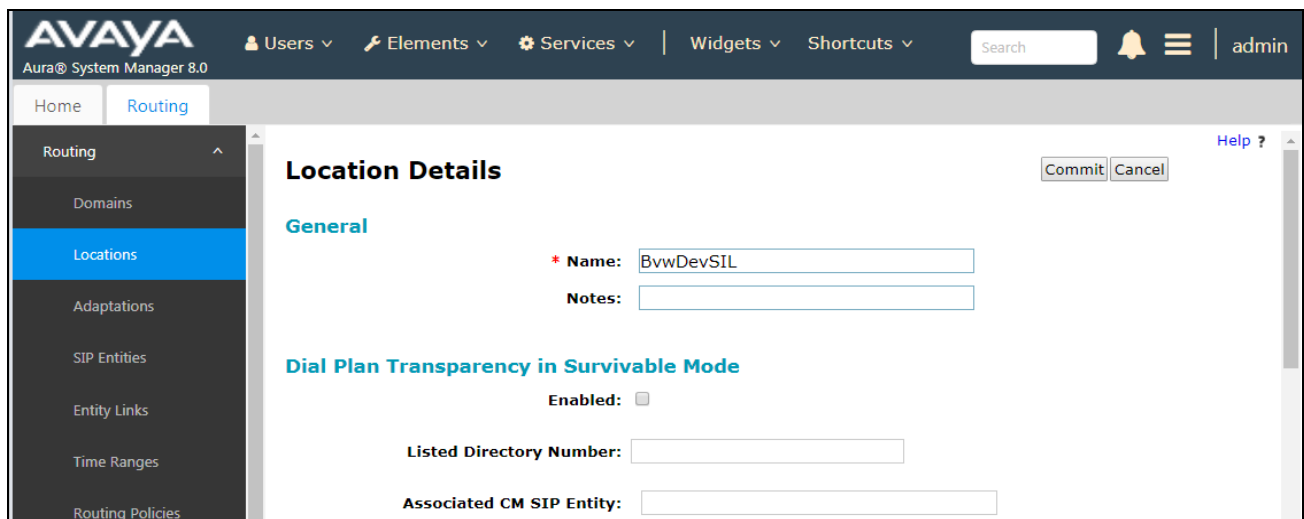
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **BvwDevSIL**, which includes all equipment at the enterprise including Communication Manager, Session Manager and the Dialogic SR140 PC.

To add a Location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

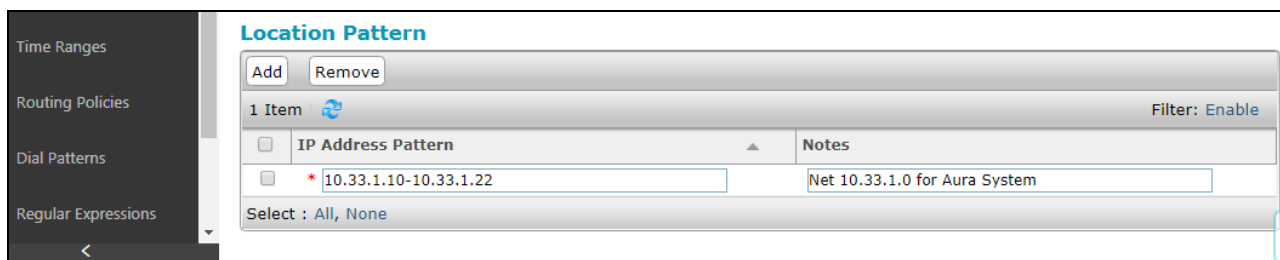
- **Name:** Enter a descriptive name for the Location.
- **Notes:** Add a brief description (optional).



Scroll down to the **Location Pattern** section. Click **Add** and enter the following values.

- **IP Address Pattern:** Add all IP address patterns used to identify the location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



6.4. Add SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the SR140 PC. Navigate to **Routing** → **SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the SR140 PC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name**. During compliance testing no adaptation rule was used.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **BvwDevSIL** created in **Section 6.3**.
- **Time Zone:** Select the time zone where the server is located.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The top navigation bar includes the Avaya logo, user information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' section. The form fields are as follows:

- Name:** ASM70A
- IP Address:** 10.33.1.12
- SIP FQDN:** (empty field)
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** BvwDevSIL (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/Toronto (dropdown menu)
- Minimum TLS Version:** Use Global Setting (dropdown menu)
- Credential name:** (empty text field)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area. A 'Help ?' link is also present.

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:


- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the SIP domain.

Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, three entries were used. They are the standard ports used for SIP traffic: port 5061 for TLS, port 5060 for UDP and TCP. These ports were provisioned as part of the Session Manager installation and not covered by this document.

Listen Ports

AddRemove

6 Items 

Filter: [Enable](#)

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5062	TLS ▼	bvwdev.com ▼	<input type="checkbox"/>	
<input type="checkbox"/>	5067	TLS ▼	bvwdev.com ▼	<input type="checkbox"/>	
<input type="checkbox"/>	5080	TCP ▼	bvwdev.com ▼	<input type="checkbox"/>	

Select : [All](#), [None](#)

The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager; this requires the creation of a SIP Entity for Communication Manager for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. The **Location** field is set to **BvwDevSIL** which is the Location defined for the subnet where Communication Manager resides. See **Section 6.3**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The top navigation bar includes the Avaya logo, a search bar, and links for Users, Elements, Services, Widgets, and Shortcuts. The user is logged in as 'admin'. The left sidebar shows a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields and values:

- Name:** ACM-Trunk1-Private
- FQDN or IP Address:** 10.33.1.6
- Type:** CM
- Notes:** Private SIP trunk for SIP phone
- Adaptation:** (empty dropdown)
- Location:** BvwDevSIL
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** both

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area. A 'Help ?' link is also present.

The following screen shows the addition of the SR140 fax software that is installed on a Windows based client. The **FQDN or IP Address** field is set to the IP address of the client. The **Location** field is set to **BevDevSIL** which is the Location defined for the subnet where the SR140 fax software client resides.

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 several menu items: '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 contains a 'General' tab. The form fields are as follows:

- Name:** Dialogic
- FQDN or IP Address:** 10.10.97.58
- Type:** Other
- Notes:** (empty text area)
- Adaptation:** (empty dropdown)
- Location:** BvwDevSIL
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** egress

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area. A 'Help ?' link is also visible.

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager and one to the SR140 fax software client. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.5**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **Connection Policy:** Select **trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group configuration in **Section 5.5**.

Entity LinksCommitCancel

1 Item

Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
<input type="checkbox"/>	* ASM70_ACM_Trunk1_5	* ASM70A	TLS ▾	* 5061	* ACM-Trunk1-Private

Select : All, None

The following screen illustrates the Entity Link to the SR140 fax software client.

Entity Links

CommitCancel

1 Item

Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
<input type="checkbox"/>	* ASM70A_Dialogic_5061	* <input type="text" value="ASM70A"/>	TLS	* <input type="text" value="5061"/>	* <input type="text" value="Dialogic"/>

Select : All, None

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added: one for Communication Manager and one for the SR140 PC. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

The following screen shows the Routing Policy for Communication Manager.

26 of 45
SR140_CMSM80

The following screen shows the Routing Policy for the SR140 fax software client.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left-hand navigation pane is expanded to 'Routing', and 'Routing Policies' is selected. The main pane displays the 'Routing Policy Details' for a policy named 'To-Dialogic'. The 'General' section includes fields for Name (To-Dialogic), Disabled (unchecked), Retries (0), and Notes. The 'SIP Entity as Destination' section shows a table with one entry: Dialogic, 135.10.97.58, Other. The 'Time of Day' section shows a table with one entry: 0, 24/7, with checkboxes for all days of the week and a time range of 00:00 to 23:59.

Name	FQDN or IP Address	Type	Notes
Dialogic	135.10.97.58	Other	

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

6.7. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to the SR140 fax software client and vice versa. Dial Patterns define which Route Policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the Dial Patterns used for the compliance test are shown below. The first example shows the pattern (4 digits) that begins with “33” and has a destination domain of “bvwddev.com” from “All” location use route policy “ACM-Trunk1-Private”.

AVAYA Users v Elements v Services v Widgets v Shortcuts v Search admin

Aura® System Manager 8.0

Home Routing

Routing

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns**
- Regular Expressions
- Defaults

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: bvwddev.com

Notes: Dial pattern to CM71 from all locations

Originating Locations and Routing Policies

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM-Trunk1	0	<input type="checkbox"/>	ACM-Trunk1-Private	
<input type="checkbox"/>	-ALL-		To-LSP-Trunk1	1	<input type="checkbox"/>	LSP-Trunk1-Private	

The second example shows the pattern (4 digits) that starts with a “52” using domain “bvwddev.com” and originating from “All” locations use route policy “To-Dialogic”.

AVAYA
Aura® System Manager 8.0

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

Home Routing

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 52

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: bvwddev.com ▾

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

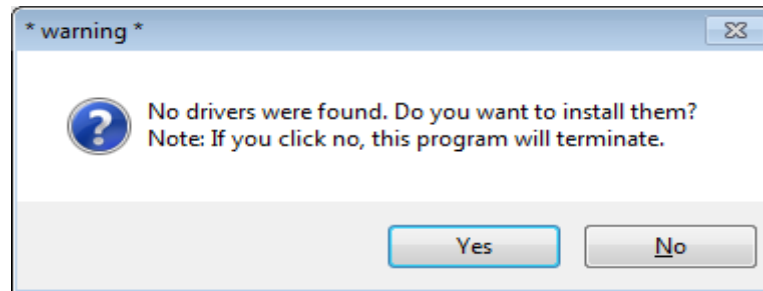
<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-Dialogic	0	<input type="checkbox"/>	Dialogic	

7. Configure Dialogic FDTTool and SR140 Driver

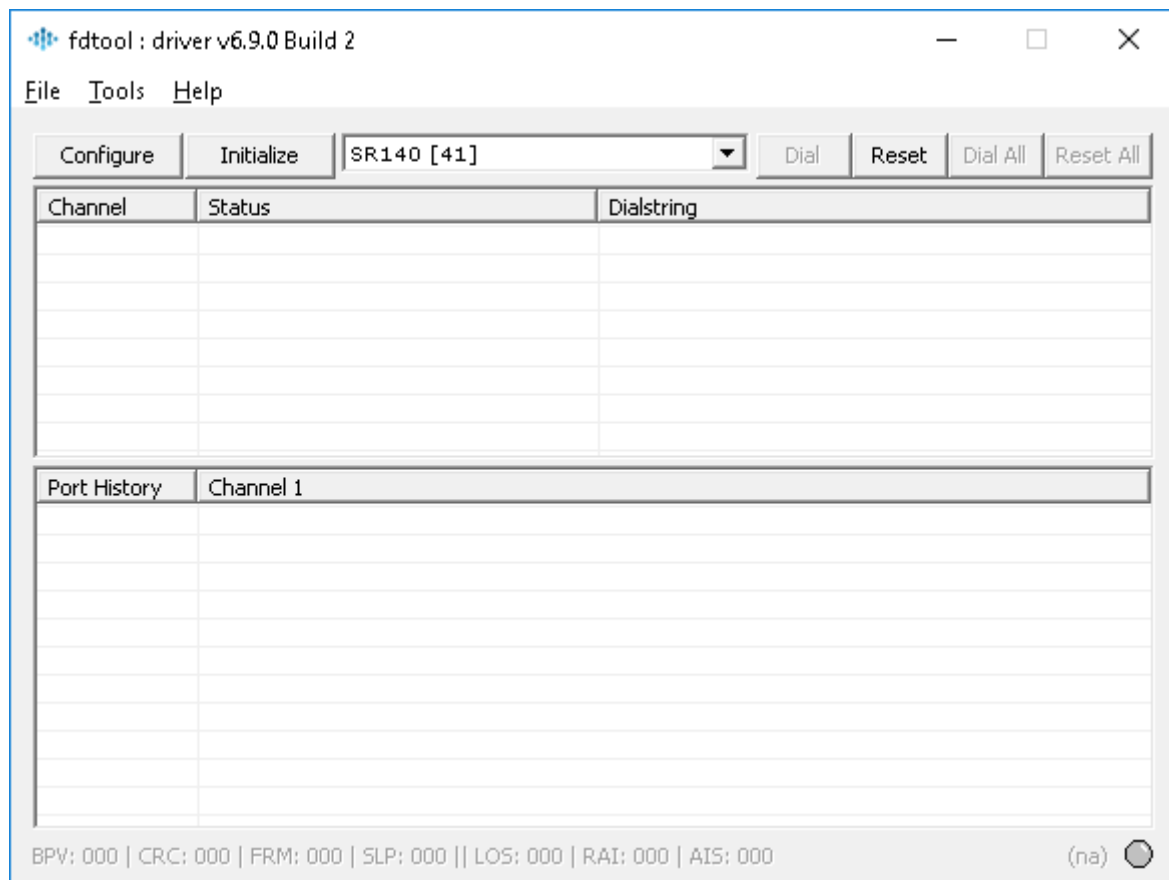
This section describes the configuration of Dialogic FDTTool and the embedded Brooktrout SR140 virtual fax board software. For instructions on installing FDTTool, refer to **Section 10**.

7.1. Install Dialogic FDTTool Application

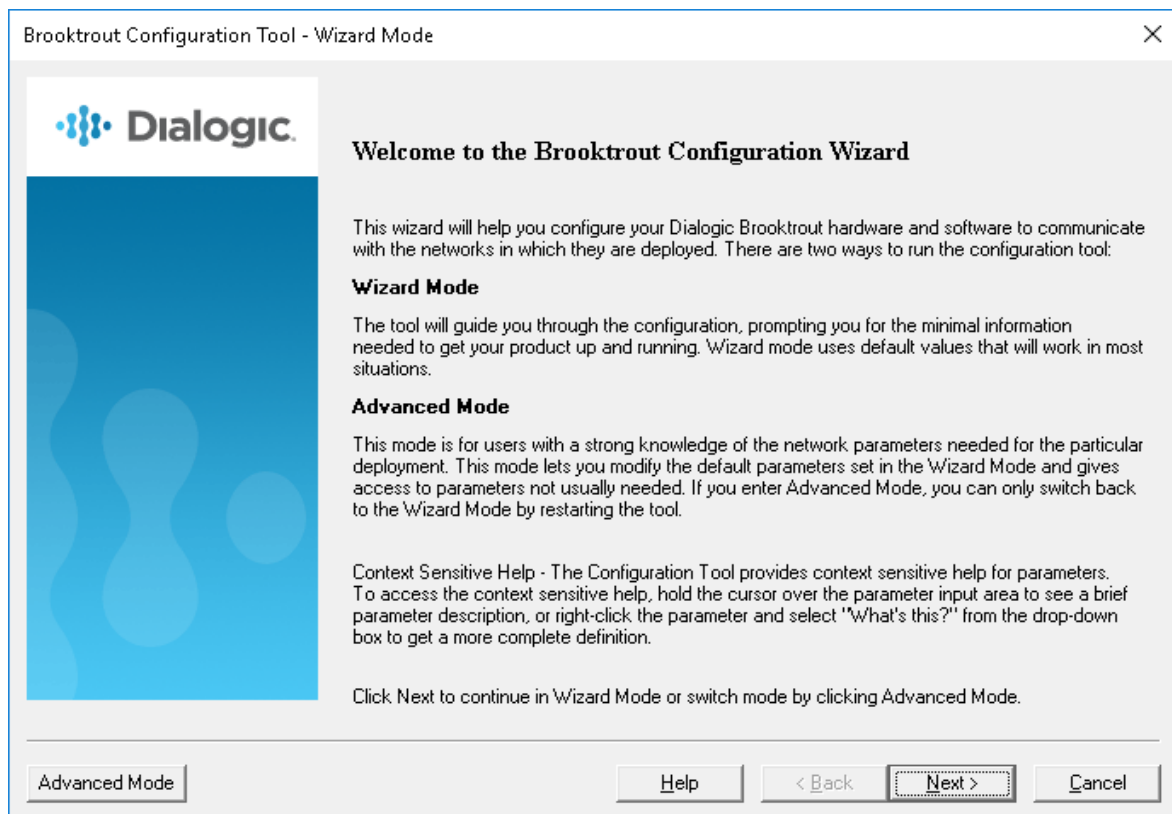
The FDTTool can be downloaded from Dialogic's website. From the folder where the application is saved, do a right-click on the "fdtool.exe" application and select "Run as administrator". Select **Yes** when prompted to install drivers in the popup window as shown below.



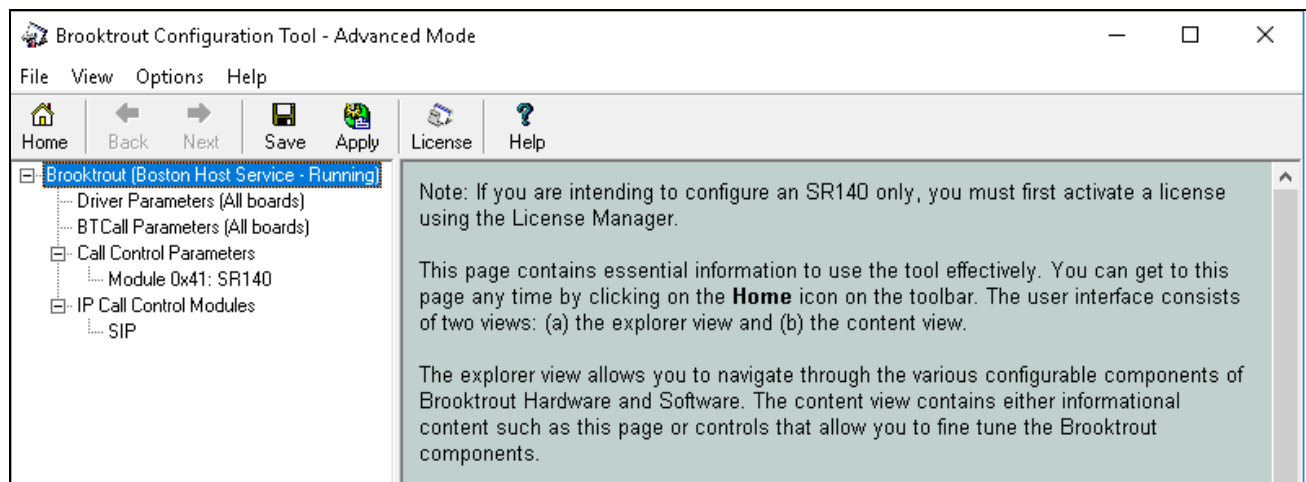
After the driver is installed, the FDTTool window is displayed as shown picture below with the SR140 component.



Select **Configure** button on the FDTool, the “Brooktrout Configuration Tool – Wizard Mode” window is displayed. Select **Advance Mode** button in the bottom.

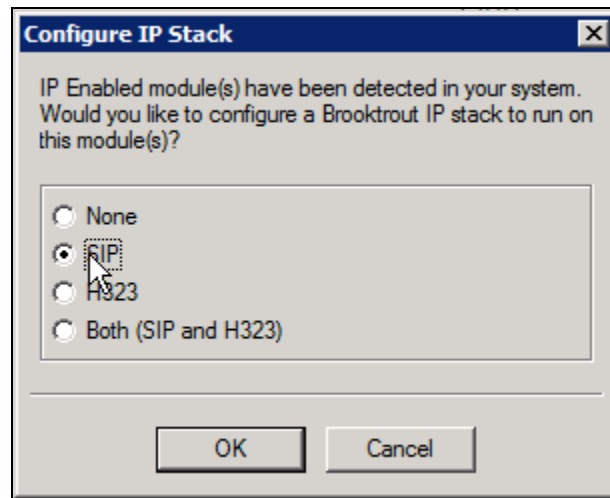


The “Brooktrout Configuration Tool – Advanced Mode” window is displayed as shown in the picture below.

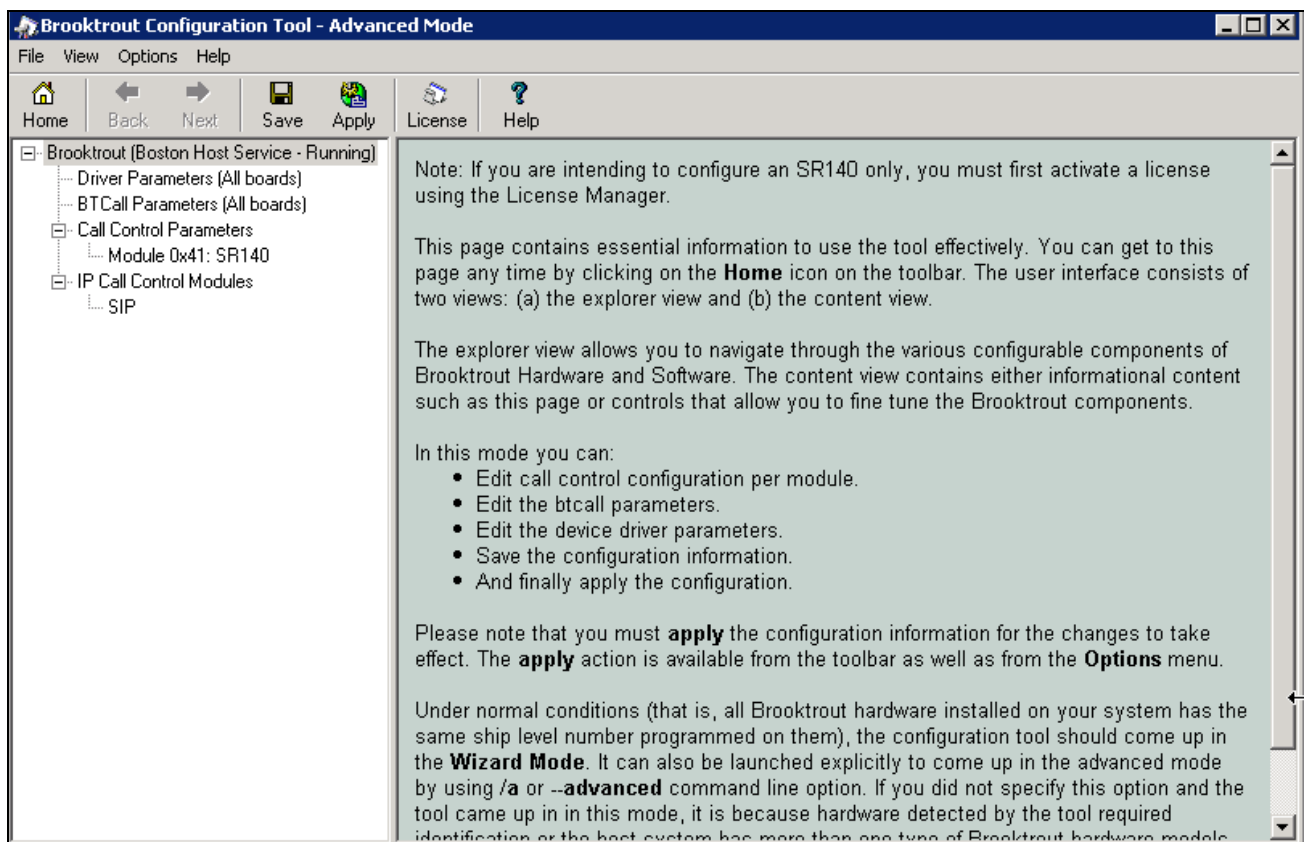


7.2. Configure IP Stack

A Configure IP Stack window is displayed on first invocation of the Brooktrout configuration tool:



Choose **SIP** and click **OK**. The following Brooktrout Configuration Tool window is displayed.

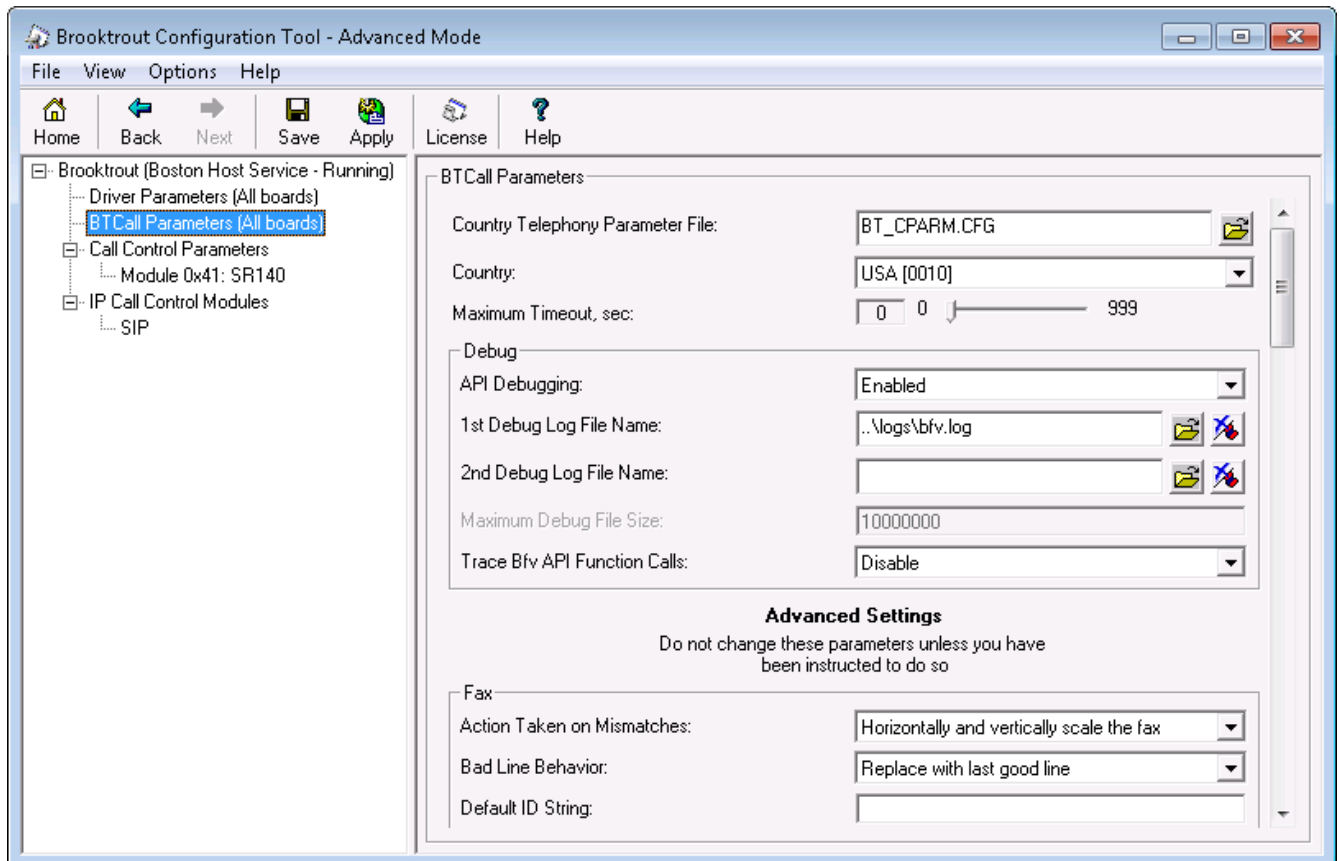


Note that IP Stack can be viewed/reconfigured from the Brooktrout Configuration Tool menu **Options → Configure IP Stack** (not shown).

7.3. Configure BtCall Parameters

Note: During the compliance testing, the following settings were retained at the default settings. In practice, these settings may not be required for full functionality.

Navigate to **Brooktrout → BtCall Parameters (All boards)** in the left navigation menu. Click the **Show Advanced** button.



Under Advanced Settings, use default values for the fields as shown below. Note that the V.34 fields should be set to “disable”, since the Avaya gateways do not support it.

The screenshot shows the Brooktrout Configuration Tool - Advanced Mode. The left sidebar shows a tree view with the following items: Brooktrout (Boston Host Service - Running), Driver Parameters (All boards), BTCall Parameters (All boards), Call Control Parameters, Module 0x41: SR140, IP Call Control Modules, and SIP. The main window is divided into two sections: BTCall Parameters and Advanced Settings.

BTCall Parameters

- Country Telephony Parameter File: BT_CPARM.CFG
- Country: USA [0010]
- Maximum Timeout, sec: 0 0 999
- Debug**
 - API Debugging: Enabled
 - 1st Debug Log File Name: ..Vogs\bfv.log
 - 2nd Debug Log File Name:
 - Maximum Debug File Size: 10000000
 - Trace Bfv API Function Calls: Disable

Advanced Settings

Do not change these parameters unless you have been instructed to do so

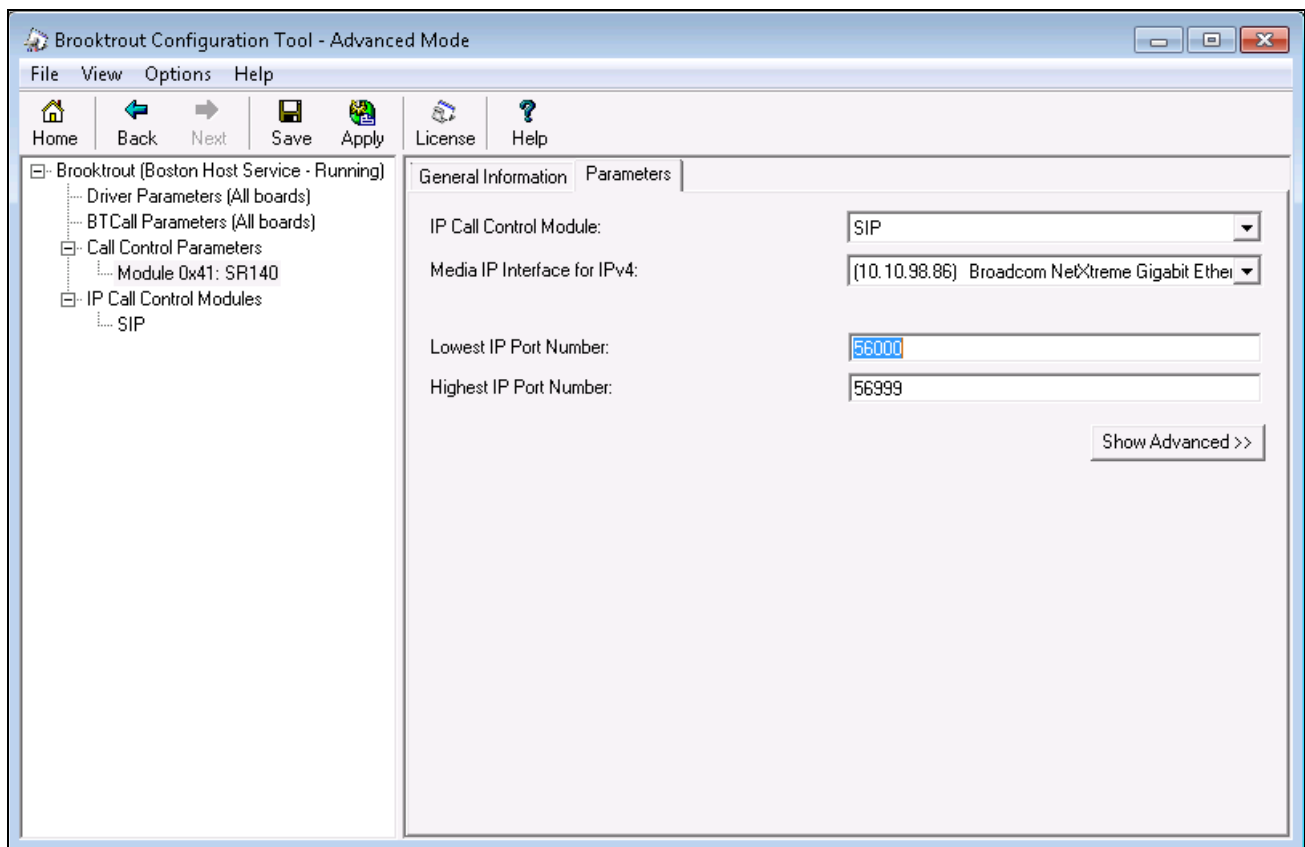
Fax

- Action Taken on Mismatches: Horizontally and vertically scale the fax
- Bad Line Behavior: Replace with last good line
- Default ID String:
- Error Correction Mode: ECM enabled 256-byte frames
- Error Threshold Value: 3
- Font Files: ..bfv.api/fonts/lbmpps.fz8 0, ..bfv.api/fonts/lbmpps.fz8 255
- Maximum Error Multiplication Value: 200
- Maximum Number of Pages: 30
- Maximum Page Width: 215mm A4 1728 Normal resolution pixels
- Minimum Error Multiplication Value: 40
- Minimum Number of Lines, x10 units: 0 0 255
- Permitted Compression Types: MMR or MR or MH
- Send RTP FSK: Enabled
- Time to Wait for CED Tone, x10msec: 4000
- V.34 Enable Send Call Indicator: Disable**
- V.34 High Speed Control Signaling: Disable**
- V.34 Modulation Capability: Disable**
- IAF Capability: Disable
- IAF Maximum Bit Rate, bps: 0

7.4. Configure Call Control Parameters

Navigate to **Brooktrout** → **Call Control Parameters** → **Module 0x41: SR140** in the left navigation menu. Ensure the following configuration parameters in the **Parameters** tab are properly set:

- **IP Call Control Module: SIP**
- **Media IP Interface for IPv4:** If the SR140 fax software client contains multiple network interface cards (NICs), ensure a correct interface that is able to communicate with the Session Manager.
- **Lowest/Highest IP Port Numbers:** Ensure your RTP range matches the port range configured on the Avaya SIP infrastructure. By default, the port range for SR140 is 56000 to 56999. A maximum range of 1000 ports may be specified. When you change the Lowest IP Port Number value, the Highest IP Port Number value will adjust automatically.



7.5. Configure SIP IP Parameters

Navigate to **Brooktrout** → **IP Call Control Modules** → **SIP** in the left navigation menu. Select the **IP Parameters** tab in the right pane. Configure the fields as follows:

- **Primary Gateway** – Enter the signaling IP address of Session Manager.
- **From Value** – If required by the Avaya environment, set this to an appropriate “UserInfo@sipdomain”. During compliance testing this value was configured as “SR140<5200@bvwddev>”
- **Contact Address** – Enter the IP address assigned to the FDTool.
- **Username** – Required. Default value is a dash (‘-’) character.

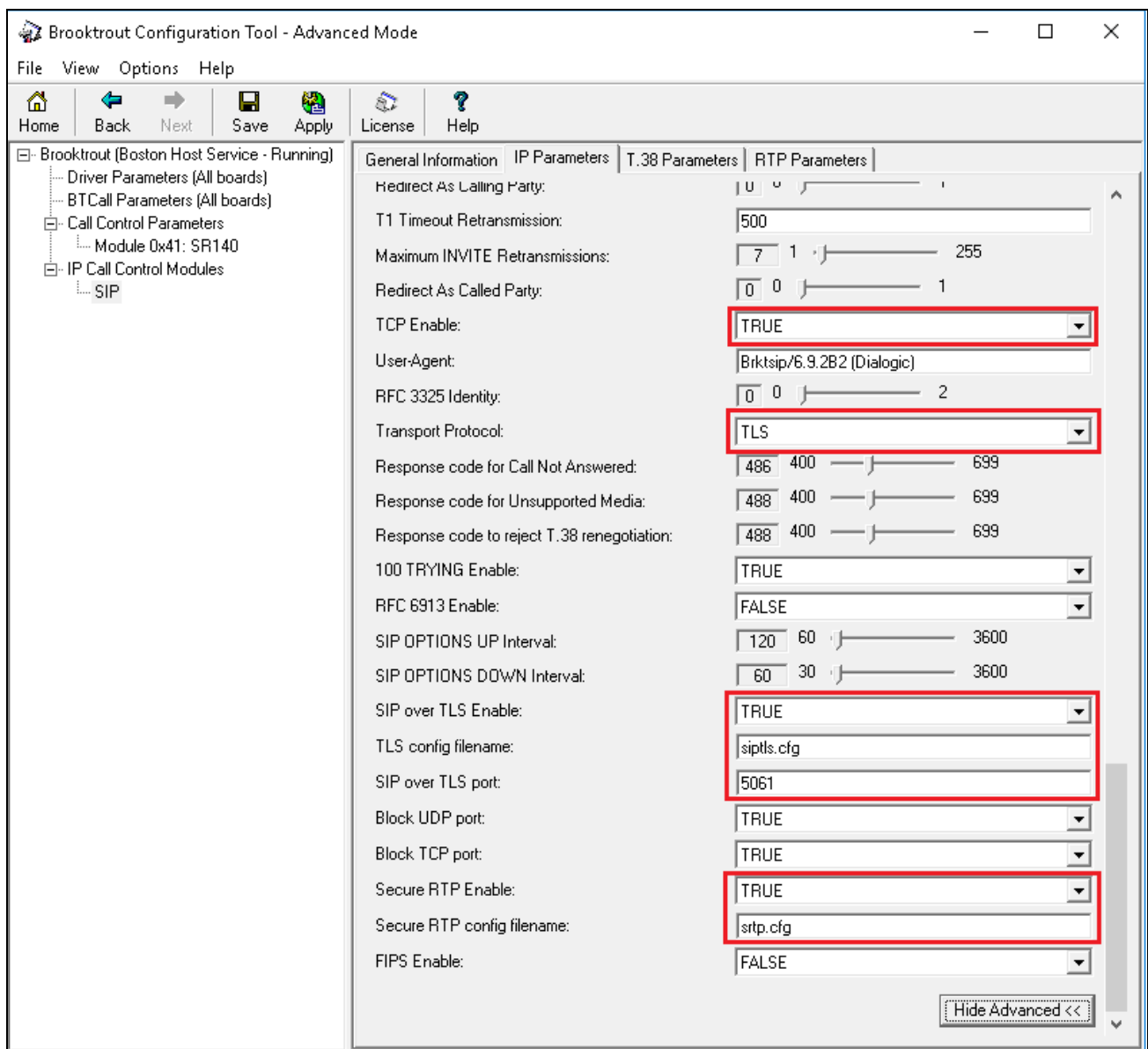
Use default values for all other fields.

The screenshot shows the Brooktrout Configuration Tool in Advanced Mode. The left sidebar shows the navigation tree with 'SIP' selected under 'IP Call Control Modules'. The main pane has tabs for 'General Information', 'IP Parameters', 'T.38 Parameters', and 'RTP Parameters'. The 'IP Parameters' tab is active, displaying various configuration fields. The 'From Value' field is pre-filled with 'SR140<sip:5200@bvwddev.com>'. The 'Contact IPv4 Address' field is pre-filled with '10.10.97.58'. The 'Username' field contains a dash character. The 'Session Name' field contains 'no_session_name'. A 'Show Advanced >>' button is located at the bottom right of the configuration area.

Field	Value
Maximum SIP Sessions:	256
Primary Gateway:	10.33.1.12 :5061
Additional SIP Gateway #2:	:0
Additional SIP Gateway #3:	:0
Additional SIP Gateway #4:	:0
Primary Proxy Server:	:0
Additional Proxy Server #2:	:0
Additional Proxy Server #3:	:0
Additional Proxy Server #4:	:0
Primary Registrar Server URL:	:0
Additional Registrar Server #2:	:0
Additional Registrar Server #3:	:0
Additional Registrar Server #4:	:0
From Value:	SR140<sip:5200@bvwddev.com>
Contact IPv4 Address:	10.10.97.58
Username:	-
Session Name:	no_session_name
Session Description:	
Description URL:	
Email Address:	
Phone Number:	

Click on **Show Advanced** tab to display the advanced parameters. To enable TLS connection, select highlighted values as shown in the picture.

- **TCP Enable** – Select TRUE.
- **Transport Protocol** – Select TLS.
- **SIP over TLS Enable** – Select TRUE.
- **TLS config filename** – the file “siptls.cfg” that needs to be configured for TLS, the detail of this file is shown in the next step.
- **SIP over TLS port** – Enter the port 5061.
- **Secure RTP Enable** – Select TRUE.
- **Secure RTP config filename** – the “srtp.cfg” file that needs to be configured for secure media SRTP. The detail of this file is shown in the next step.



Below is the “siptls.cfg” file stored under the config directory of fdtool. During the compliance test, System Manager was used to sign the certificate for Dialogic SR140.

```
##### parameters for SIP over TLS
sip_tls_method=tlsv1.2
local_rsa_private_key_filename = C:\1917_fdtool-692\config\sr140.key
local_rsa_private_key_password = avaya123
local_rsa_cert_filename      = C:\1917_fdtool-692\config\sr140.pem
local_dss_private_key_filename =
local_dss_private_key_password =
local_dss_cert_filename      =
ca_cert_number  = 1
ca_cert_filename = C:\1917_fdtool-692\config\sr140.pem
chain_cert_number = 0
chain_cert_filename =
crl_number  = 0
crl_filename =
local_cipher_suite =
dh_param_512_filename =
dh_param_1024_filename =
dh_param_2048_filename =
session_id =
client_cert_required=false
allow_self_signed_certs=true
```

Below is the “srtp.cfg” file that is set in the **Secure RTP config filename** field. Note that the values without the hash sign in the front are enabled .

```
##### parameters for SRTP
srtp_accept = true
#srtp_enforce = true
srtp_crypto_suite = AES_CM_128_HMAC_SHA1_80
srtp_master_key_len = 128
#srtp_salting_key_len = 112
#srtp_num_keys = 1
#srtp_mki_len = 1
#srtp_lifetime = 48
#srtpcp_lifetime = 31
#srtp_kdr = 0
#srtp_window_size = 64
#srtp_unencrypted_flag = false
srtpcp_unencrypted_flag = true
#srtp_unauthenticated_flag = false
```

7.6. Configure T.38 Parameters

Select the **T.38 Parameters** tab. Configure the fields as shown below in the screenshot.

***Note:** During the compliance testing, the following settings were configured as the default settings. In practice, these settings may not be required for full functionality.*

- **Fax Transporting Protocol** – select “T.38 only” from the list.
- **Maximum Bit Rate, bps** – set to 14400, which is the default setting.

The screenshot displays the 'Brooktrout Configuration Tool - Advanced Mode' window. The left sidebar shows a tree view with 'Brooktrout (Boston Host Service - Running)' expanded, containing 'Driver Parameters (All boards)', 'BTCall Parameters (All boards)', 'Call Control Parameters' (with 'Module 0x41: SR140' selected), and 'IP Call Control Modules' (with 'SIP' selected). The main panel has four tabs: 'General Information', 'IP Parameters', 'T.38 Parameters' (active), and 'RTP Parameters'. The 'T.38 Parameters' tab contains the following settings:

Parameter	Value
Fax Transporting Protocol:	T.38 only
Generate CED tone over RTP:	Yes
Maximum Bit Rate, bps:	14400
Media Passthrough Timeout Inbound, msec:	1000
Media Passthrough Timeout Outbound, msec:	4000
Media Renegotiate Delay Inbound, msec:	1000
Media Renegotiate Delay Outbound, msec:	-1
T30 Fast Notify:	No
UDPTL Redundancy Depth Control:	5 0 ————— J 5
UDPTL Redundancy Depth Image:	2 0 ————— J 2

A 'Show Advanced >>' button is located at the bottom right of the configuration area.

7.7. Configure RTP Parameters

Select the **RTP Parameters** tab and set the **RTP codec list** value to use only a single codec, either “pcmu” or “pcma” to match the codec used in your region.

The screenshot shows the 'Brooktrout Configuration Tool - Advanced Mode' window. The left sidebar contains a tree view with the following structure:

- Brooktrout (Boston Host Service - Running)
 - Driver Parameters (All boards)
 - BT Call Parameters (All boards)
 - Call Control Parameters
 - Module 0x41: SR140
 - IP Call Control Modules
 - SIP

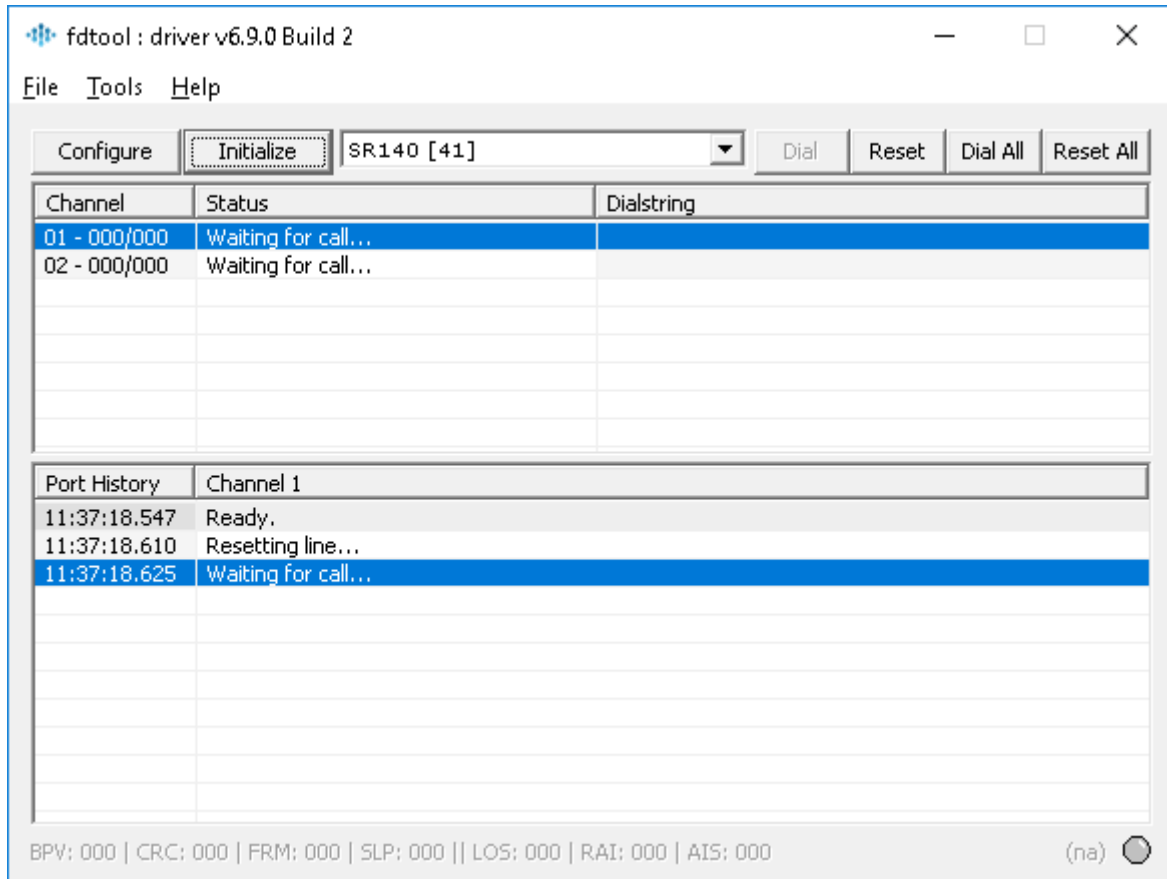
The main panel has tabs for 'General Information', 'IP Parameters', 'T.38 Parameters', and 'RTP Parameters'. The 'RTP Parameters' tab is selected. It contains the following settings:

- RTP codec list:
- Silence Control:
- Advanced Settings**
 - Do not change these parameters unless you have been instructed to do so
 - Frame Duration:
 - Jitter Buffer Depth: 0 —
 - T.38 offer as CED tone:
 - Voice Frame Replacement:

A 'Hide Advanced <<' button is located at the bottom right of the 'Advanced Settings' section.

After verifying all the above parameters are properly set, click **Save** and then Apply in the button menu. Exit the Brooktrout Configuration Tool.

From the FDTool window, click on “**Initialize**” button to start the Brooktrout SR140 service, the Status shows “Waiting for call...”.



8. Verification Steps

The following steps may be used to verify the configuration:

- From Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling groups configured in **Section 5.5** are in-service.

```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

- From Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Section 5.6** is in-service.

```
status trunk 1
                TRUNK GROUP STATUS


Member  Port   Service State  Mtce Connected Ports
                Busy

0001/001 T00001  in-service/idle  no
0001/002 T00002  in-service/idle  no
0001/003 T00003  in-service/idle  no
```

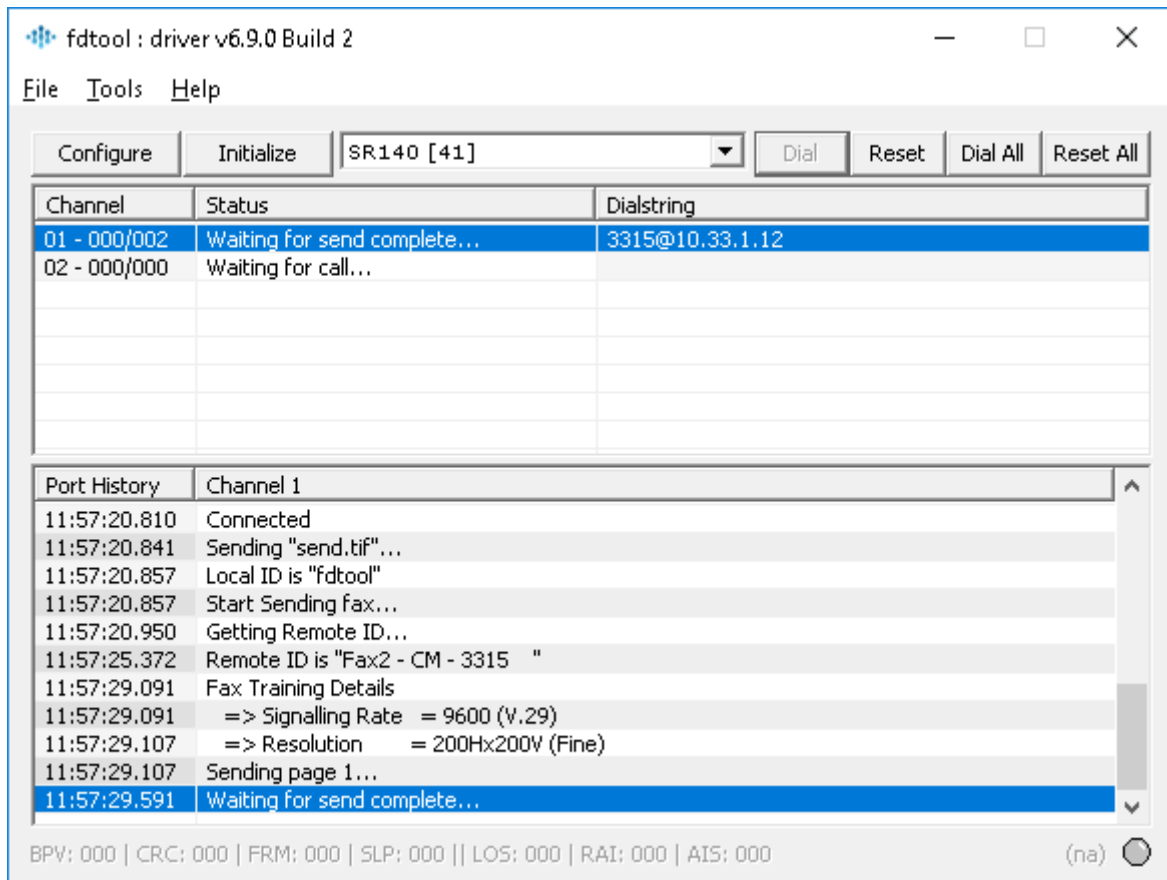
- Verify that fax calls can be placed to/from Dialogic FDTTool PC from both local and remote sites.
- From Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed to the expected trunks.
- From System Manager, confirm that the Entity Link between Session Manager and the Dialogic SIP Entity is UP.

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: Dialogic									
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"/>	ASM70A	IPv4	10.10.97.58	5061	TLS	FALSE	UP	200 OK	UP
Select : None									

- Verify that fax calls can be placed to/from the FDTTool from both local and remote sites. The picture below shows the FDTTool was sending fax to the local fax endpoint that is connected to the G450 Media Gateway.



9. Conclusion

These Application Notes describe the procedures required to configure Dialogic Brooktrout SR140 Fax Software to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Please refer to **Section 2.2** for any exceptions or observations.

10. Additional References

This section references the documentation relevant to these Application Notes. The following and additional Avaya product documentation is available at <http://support.avaya.com>.

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 8.0.
4. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.
7. *Administering Avaya Aura® Communication Manager*, Release 8.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, 555-245-205.

Dialogic Brooktrout SR140 Fax Software products information may be found at <https://www.dialogic.com/sr140>

Brooktrout manuals can be found at <https://www.dialogic.com/manuals/brooktrout/brooktrout>

©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.