



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Open Text RightFax with Avaya Aura[®] Communication Manager and Avaya Aura[®] Session Manager via SIP Trunk Interface - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Open Text RightFax with Avaya Aura[®] Communication Manager and Avaya Aura[®] Session Manager using a SIP trunk interface.

Open Text RightFax is a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, Open Text RightFax 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 Open Text RightFax (RightFax) with Avaya Aura[®] Communication Manager (Communication Manager) and Avaya Aura[®] Session Manager (Session Manager) using SIP trunks.

Open Text RightFax is a software based fax server that sends and receives fax calls over an IP network. Open Text RightFax utilizes the Brooktrout SR140 T.38 Fax over Internet Protocol (FoIP) virtual fax board software from Dialogic. In the tested configuration, Open Text RightFax 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 OpenText RightFax with Session Manager. By using a SIP trunk that was established between the Communication Manager and RightFax 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.

2.1. Interoperability Compliance Testing

The compliance test tested interoperability between RightFax and Session Manager by making intra-site fax calls between a RightFax server 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 a RightFax server and an analog fax machine that was connected on a remote site. The remote site connection used ISDN trunks. Specifically, the following fax operations were tested in the setup for the compliance test:

- Fax from/to RightFax to/from fax machine at a local site
- Fax from/to RightFax to/from fax machine at a remote site

Faxes were sent with various page lengths and resolutions. Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources and restarts of RightFax server.

Fax calls were also tested with different Avaya Media Gateway media resources used to process the fax data between sites. This included the TN2302 MedPro circuit pack, the TN2602 MedPro circuit pack in the Avaya G650 Media Gateway; 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

OpenText RightFax successfully passed all compliance testing with the following observation,

- During sending or receiving of a fax, if the fax server is interrupted with network outage or a reboot, the faxes will not be complete after the server services are 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 again.
- The Fax transmission rate depends on the Media Gateway or the card being used. When TN2302 card (in G650 Media gateway) is used, the negotiation is seen at V.17 (14400 bits). When TN2602 card (in G650 Media gateway) is used, the negotiation is seen at V.29 (9600 bits). In a G450 Media gateway, the negotiation is seen at V.29 (9600 bits).

Note: Fax calls consume DSP (Digital Signal Processing) resources for processing fax data on the TN2302AP IP Media Processor (MedPro) circuit pack, the TN2602AP IP Media Processor circuit pack in the Avaya G650 Media Gateway and the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G450 Media Gateway. To increase the capacity to support simultaneous fax calls, additional TN2302AP and/or TN2602AP MedPro circuit packs need to be installed in the Avaya G650 Gateway, and additional Avaya MM760 Media Module or Modules need to be installed in the Avaya G450 Media Gateway. The information contained in the table below indicates DSP capacities/usage in the Avaya media processors. 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.

Platform Device	DSP Resources per Platform Device	DSP Resources per FoIP Call
TN2302, G450, MM760	64	4
TN2602	64	1

Note: 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 2 sites, must be configured with adequate number of trunk group members to support the number of simultaneous fax calls intended. On RightFax, adequate number of fax channels must also be appropriately configured for the intended capacity.

2.3. Support

North American Technical support for RightFax can be obtained by contacting Open Text at

- Phone: (800) 540-7292
- Email: support@opentext.com

For other locations go to <http://www.opentext.com/2/global/company/company-contact.html>

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 (G650 and G450 Media Gateway), Avaya Aura® Session Manager, Avaya Aura® System Manager, RightFax server and an analog fax machine are considered to be a local site. The RightFax server communicates to the Communication Manager via the Avaya Aura® Session Manager using SIP trunks. In turn, Communication Manager used a SIP Trunk which terminated on a CLAN circuit pack in port network 1 to communicate with Session Manager. IP media resources were provided by Media Processor (MedPro) circuit packs. Two versions of the MedPro circuit pack were tested in this configuration: TN2302AP and TN2602AP. 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 site communicates via ISDN-PRI trunks that are configured between the Communication Manager and the PBX available at the remote site. Since remote site is an emulated PSTN setup, the configuration details of setting the ISDN-PRI trunks between the local and remote sites are beyond the scope of this document. However, note that clock slips on the ISDN-PRI link will lead to failure of fax transmission. Therefore ensure that the ISDN-PRI link is configured correctly on both the Communication Manager and the PBX available at the remote site so that their respective clocks are in synchronized state.

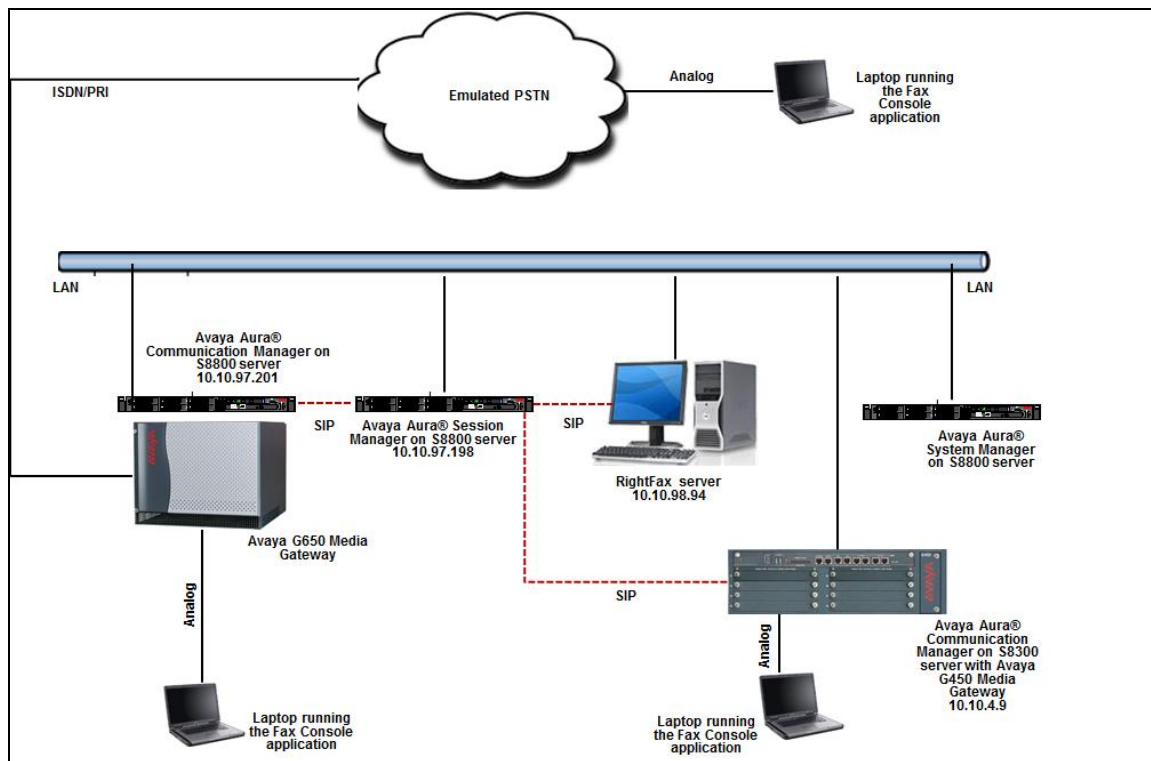


Figure 1: RightFax interoperating with Session Manager via SIP Trunk

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 an Avaya S8800 Server	6.3 (R016x.03.0.124.0)
Avaya G650 Media Gateway <ul style="list-style-type: none">- CLAN- 2 MedPros – TN2302- 2 MedPros – TN2602	TN799DP - HW01 FW026 TN2302AP - HW20 FW117 TN2602AP - HW02 FW055
Avaya Aura® Communication Manager running on an Avaya S8300 Server	6.3 (R016x.03.0.124.0)
Avaya G450 Media Gateway	33.13.0 /1
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Aura® System Manager	6.3.10.7.2656
OpenText RightFax on Windows 2008R2 Enterprise SP1	10.6.0.3093
Dialogic Brooktrout SR140 SDK	6.6.0.Build 2

5. Configure Avaya Aura[®] Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with Session Manager and Open Text RightFax. 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
- Identify IP Interfaces
- 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 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	11
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	2
Maximum Video Capable IP Softphones:	18000	3
Maximum Administered SIP Trunks:	24000	100
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	1
Maximum Media Gateway VAL Sources:	250	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	1
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. Identify IP Interfaces

Use the **list ip-interface clan** and **list ip-interface medpro** commands to identify IP interfaces in each network region. Interfaces in cabinet 01 (port network 1) as indicated in the **Slot** field are in IP network region 1 as indicated in the **Net Rgn** field.

Testing with the TN2302 and TN2602 circuit packs were done separately. When testing with the TN2302, the TN2602 was disabled (turned off) and vice versa as indicated in the **ON** field.

```
list ip-interface clan
```

IP INTERFACES										
ON	Slot	Code/Sfx	Node Name/ IP-Address	Mask	Gateway Node	Skts Warn	Net Rgn	VLAN	Eth Link	
--	----	-----	-----	----	-----	----	---	----	----	----
y	01A02	TN799	D CLAN1 10.10.97.217	/26	GW	400	1	n	1	

```
list ip-interface medpro
```

IP INTERFACES										
ON	Slot	Code/Sfx	Node Name/ IP-Address	Mask	Gateway Node	Net Rgn	VLAN	Virtual Node		
--	----	-----	-----	----	-----	---	----	-----		
y	01A07	TN2302	MedPro1 10.10.97.218	/26	GW	1	n			
n	01A08	TN2602	MedPro2 10.10.97.233	/26	GW	1	n			

5.3. 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 (**SM61**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
CLAN1	10.10.97.217	
CLAN2	10.10.97.238	
MedPro1	10.10.97.218	
MedPro2	10.10.97.233	
SM61	10.10.97.198	
default	0.0.0.0	
procr	10.10.97.201	
(16 of 17 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

5.4. Administer 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. Default values can be used for all other fields.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2: G.729	n	2	20
3: G.722-64K		2	20
4: G.711A	n	2	20
5:			
6:			
7:			

On **Page 2**, set the **FAX Mode** to **t.38-standard**. Default values can be used for all other fields.

change ip-codec-set 1		Page 2 of 2	
IP Codec Set			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia: 4096:Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia: 4096:Kbits			
	Mode	Redundancy	
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

5.5. 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 **bvwddev.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 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: bvwddev.com
Name:                               Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Codec Set: 1    Inter-region IP-IP Direct Audio: yes
                      UDP Port Min: 2048      IP Audio Hairpinning? n
                      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
                      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

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 at the local and remote sites, 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	A		t
dst	codec	direct	WAN-BW-limits	Video	Intervening					Dyn	A	G	c
rgn	set	WAN	Units	Total Norm	Prio	Shr	Regions			CAC	R	L	e
1	1											all	
2	2	y	NoLimit								n		t

5.6. 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 **tcp**. 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**.
- 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 5.3**.
- Set the **Far-end Node Name** to **SM61**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- 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 5.5**.
- 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.
- Default values may be used for all other fields.

add signaling-group 1

Page 1 of 2

SIGNALING GROUP

Group Number: 1

Group Type: sip

IMS Enabled? n

Transport Method: tcp

Q-SIP? n

IP Video? y

Priority Video? n

Enforce SIPS URI for SRTP? y

Peer Detection Enabled? y Peer Server: SM

Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y

Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr

Far-end Node Name: SM61

Near-end Listen Port: 5060

Far-end Listen Port: 5060

Far-end Network Region: 1

Far-end Domain: bvwdev.com

Bypass If IP Threshold Exceeded? n

Incoming Dialog Loopbacks: eliminate

RFC 3389 Comfort Noise? n

DTMF over IP: rtp-payload

Direct IP-IP Audio Connections? y

Session Establishment Timer(min): 3

IP Audio Hairpinning? n

Enable Layer 3 Test? y

Initial IP-IP Direct Media? y

H.323 Station Outgoing Direct Media? n

Alternate Route Timer(sec): 30

5.7. Administer Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. 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 5.6**.
- 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.
- Default values were used 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: #001
  Direction: two-way                               Outgoing Display? y
  Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                    Member Assignment Method: auto
                                                    Signaling Group: 1
                                                    Number of Members: 15
```

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 5.9**).

change trunk-group 1
Page 3 of 22

TRUNK FEATURES

ACA Assignment? n
Measured: none
Maintenance Tests? y

Numbering Format: private

UI Treatment: shared

Maximum Size of UI Contents: 128

Replace Restricted Numbers? n

Replace Unavailable Numbers? n

Send UCID? y
Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

5.8. 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 5.7**. In the example shown below, all calls originating from a 5-digit extension beginning with 5 or 7 and routed across trunk group 1 are sent with a 5-digit calling number.

change private-numbering 1
Page 1 of 2

NUMBERING - PRIVATE FORMAT				
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len
5	5	1		5
5	7	1		5

Total Administered: 2

Maximum Entries: 540

5.9. 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 RightFax server. In the sample configuration, 760 is used as the Dialed String. Local site users will dial 760xx to reach the RightFax server. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 760 of length 5 as a uniform dial plan (**udp**).

change dialplan analysis										Page 1 of 12
DIAL PLAN ANALYSIS TABLE										
Location: all										Percent Full: 6
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call		
String	Length	Type	String	Length	Type	String	Length	Type		
760	5	udp								

Use the **change uniform-dialplan** command to create a matching pattern that matches with the dial pattern used to reach the RightFax server. The example below shows entries created for local site **uniform-dialplan 7**. Extension 760xx was used and configured as shown below where 760 is the Matching Pattern with a Length of 5, no digits to be deleted and using the aar feature.

change uniform-dialplan 7										Page 1 of 2
UNIFORM DIAL PLAN TABLE										
										Percent Full: 0
Matching			Insert			Node				
Pattern	Len	Del	Digits	Net	Conv	Num				
760	5	0		aar		n				

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 7**. The highlighted entry specifies that 5 digit dial string 760 was to use route pattern 1 to route calls to the RightFax fax server at the local site via Session Manager.

change aar analysis 7										Page 1 of 2
AAR DIGIT ANALYSIS TABLE										
Location: all										Percent Full: 1
Dialed	Total		Route	Call	Node	ANI				
String	Min	Max	Pattern	Type	Num	Reqd				
760	5	5	1	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 5.7** for full details.
- Default values were used for all other fields.

change route-pattern 1													Page 1 of 3		
Pattern Number: 1													Pattern Name: To-SM61		
SCCAN? n													Secure SIP? n		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits						QSIG		
Dgts													Intw		
1:	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	No.	Numbering	LAR
0		1 2 M 4 W			Request								Dgts	Format	
													Subaddress		
1:	y	y	y	y	y	n	n	rest						lev0-pvt	none
2:	y	y	y	y	y	n	n	rest							none
3:	y	y	y	y	y	n	n	rest							none
4:	y	y	y	y	y	n	n	rest							none
5:	y	y	y	y	y	n	n	rest							none
6:	y	y	y	y	y	n	n	rest							none

6. Configure Avaya Aura® Session Manager

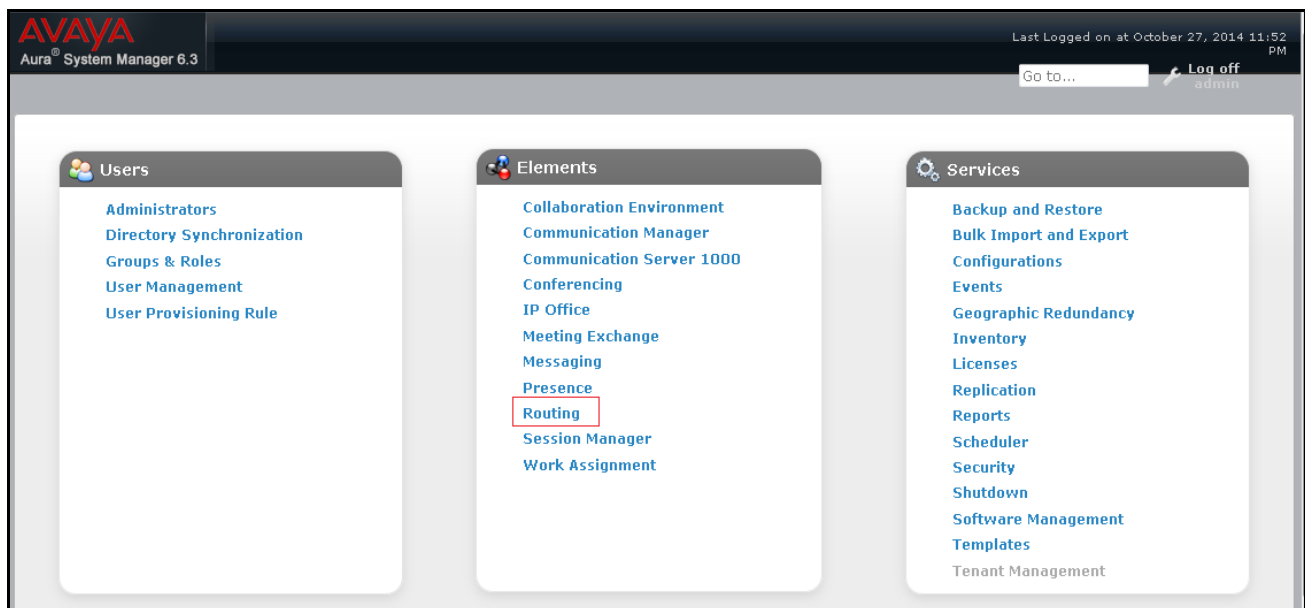
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

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

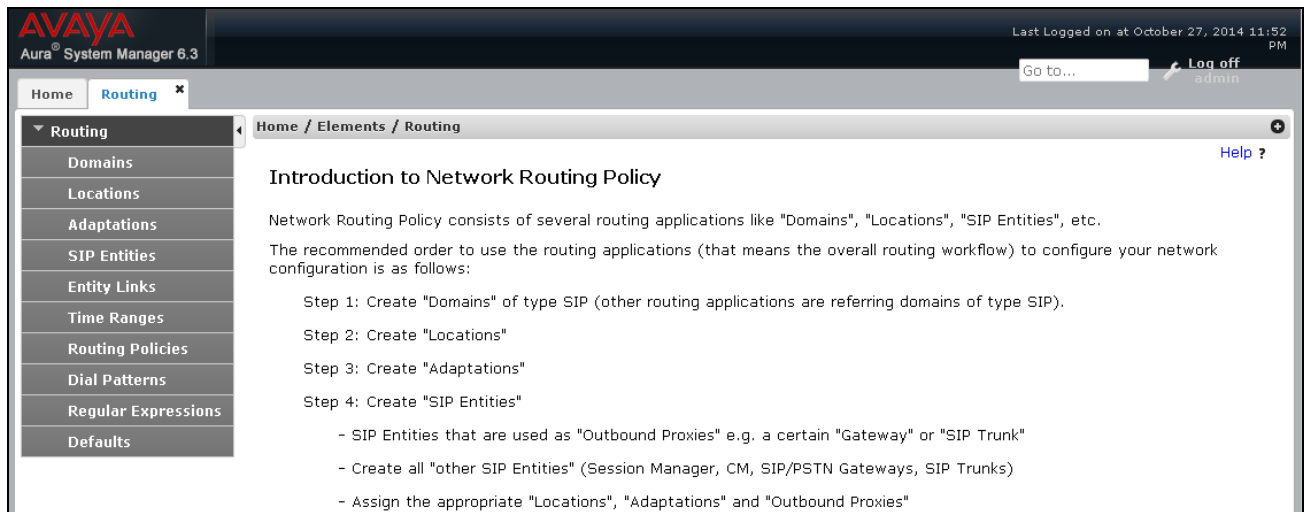
For detail configuration details of the Session Manager refer to **Section 10**

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 5.5**. 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 a web application window titled "Home / Elements / Routing / Domains". The main heading is "Domain Management". There are "Commit" and "Cancel" buttons at the top right. Below the heading is a table with the following structure:

Name	Type	Notes
* bvwdev.com	sip	

At the bottom right, there are "Commit" and "Cancel" buttons. The table has a "Filter: Enable" link at the top right.

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 **Belleville**, which includes all equipment at the enterprise including Communication Manager, Session Manager and the RightFax server.

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).

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: Belleville

Notes:

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.

Location Pattern

Add Remove

5 Items Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.5.0	
<input type="checkbox"/>	* 10.10.97.00	
<input type="checkbox"/>	* 10.10.98.00	
<input type="checkbox"/>	* 10.20.0.00	
<input type="checkbox"/>	* 10.178.169.**	

Select : All, None

Commit Cancel

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 RightFax server. 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 RightFax server.
- **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 **Belleville** 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 shows the 'SIP Entity Details' form in the Avaya Session Manager configuration interface. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The form is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. The 'General' section is active, showing the following fields: 'Name' (DevSM), 'FQDN or IP Address' (10.10.97.198), 'Type' (Session Manager), 'Notes' (SIP Entity for Session Manager), 'Location' (Belleville), 'Outbound Proxy' (empty), 'Time Zone' (America/Toronto), and 'Credential name' (empty). The 'SIP Link Monitoring' section is also visible, with 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

Field	Value
Name	DevSM
FQDN or IP Address	10.10.97.198
Type	Session Manager
Notes	SIP Entity for Session Manager
Location	Belleville
Outbound Proxy	
Time Zone	America/Toronto
Credential name	
SIP Link Monitoring	Use Session Manager Configuration

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, two port entries were used. They are the standard ports used for SIP traffic: port 5060 for UDP/TCP. These ports were provisioned as part of the Session Manager installation not covered by this document.

Port
TCP Failover port:
TLS Failover port:

3 Items 

Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	bvwdev.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	bvwdev.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	bvwdev.com	<input type="text"/>

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 **Belleville** which is the Location defined for the subnet where Communication Manager resides. See **Section 6.3**.

The screenshot shows a web interface for configuring SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". There are "Commit" and "Cancel" buttons in the top right. A "Help ?" link is also present. The "General" section is active and contains the following fields: "Name" (DevCM), "FQDN or IP Address" (10.10.97.201), "Type" (CM), "Notes" (CM SIP Entity in the main lab), "Adaptation" (empty), "Location" (Belleville), "Time Zone" (America/Toronto), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), and "Call Detail Recording" (both). The "Loop Detection" section has a "Loop Detection Mode" (Off). The "SIP Link Monitoring" section has a "SIP Link Monitoring" (Use Session Manager Configuration).

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help ?

General

* Name: DevCM

* FQDN or IP Address: 10.10.97.201

Type: CM

Notes: CM SIP Entity in the main lab

Adaptation:

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: both

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the RightFax server. The **FQDN or IP Address** field is set to the IP address of the server. The **Location** field is set to **Belleville** which is the Location defined for the subnet where the sever resides.

Home / Elements / Routing / SIP Entities

Help ?

SIP Entity Details

CommitCancel

General

* Name: RightFax

* FQDN or IP Address: 10.10.98.94

Type: Other

Notes: SIP Entity For RightFax

Adaptation:

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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 RightFax server. 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 5.6**.
- **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 5.6**.
- **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 5.6**.
- **Connection Policy:** Select **trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager (**DevSM_DevCM_5060**). The protocol and ports defined here must match the values used on the Communication Manager signaling group configuration in **Section 5.6**.

Entity Links

Commit Cancel

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service
* DevSM_DevCM_5060	* DevSM	TCP	* 5060	* DevCM	<input type="checkbox"/>	* 5060	trusted	<input type="checkbox"/>


Select : All, None

Commit Cancel

The following screen illustrates the Entity Link to the RightFax server (**DevSM_RightFax_5060**).

Home / Elements / Routing / Entity Links [Help ?](#)

Entity Links

1 Item  Filter: [Enable](#)

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
<input type="checkbox"/>	* DevSM_RightFax_5060	* DevSM ▼	UDP ▼	* 5060	* RightFax ▼	<input type="checkbox"/>	* 5060	trusted ▼

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

6.6. Add Routing Policies

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 RightFax server. 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:

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

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy for Communication Manager.

The screenshot shows the 'Routing Policy Details' page in a web application. The breadcrumb trail at the top is 'Home / Elements / Routing / Routing Policies'. There are 'Commit' and 'Cancel' buttons in the top right, and a 'Help ?' link. The page is divided into two main sections: 'General' and 'SIP Entity as Destination'. In the 'General' section, the 'Name' field is 'To-DevCM', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is 'Route to DevCM with G650'. In the 'SIP Entity as Destination' section, there is a 'Select' button and a table listing SIP entities. The table has columns for Name, FQDN or IP Address, Type, and Notes. One entity, 'DevCM', is listed with FQDN '10.10.97.201', Type 'CM', and Notes 'CM SIP Entity in the main lab'.

Name	FQDN or IP Address	Type	Notes
DevCM	10.10.97.201	CM	CM SIP Entity in the main lab

The following screen shows the Routing Policy for the RightFax server.



Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel Help ?

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
RightFax	10.10.98.94	Other	SIP Entity For RightFax

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 RightFax server 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 outbound number (5 digits) that begin with **53** and have a destination domain of **bvwdev.com** from **ALL** locations use route policy **To-DevCM**.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

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-DevCM	0	<input type="checkbox"/>	DevCM	Route to DevCM with G650

Select : All, None

The second example shows that outbound 5 numbers that start with a **76** to domain **bvwdev.com** and originating from **Belleville** locations use route policy **To-RightFax**.

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 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"/>	Belleville	Belleville DevConnect Location	To-RightFax	0	<input type="checkbox"/>	RightFax	Route to RightFax

Select : All, None

7. Configure OpenText RightFax

This section describes the configuration of OpenText RightFax and the embedded RightFax Original Equipment Manufacturer (OEM) or Brooktrout SR140 virtual fax board software from Dialogic (hereafter referred to as “SR140”). It assumes that the application and all required software components, including Brooktrout SR140 and the database software (Microsoft SQL Server 2012), have been installed and properly licensed. For instructions on installing RightFax, refer to **Section 10**.

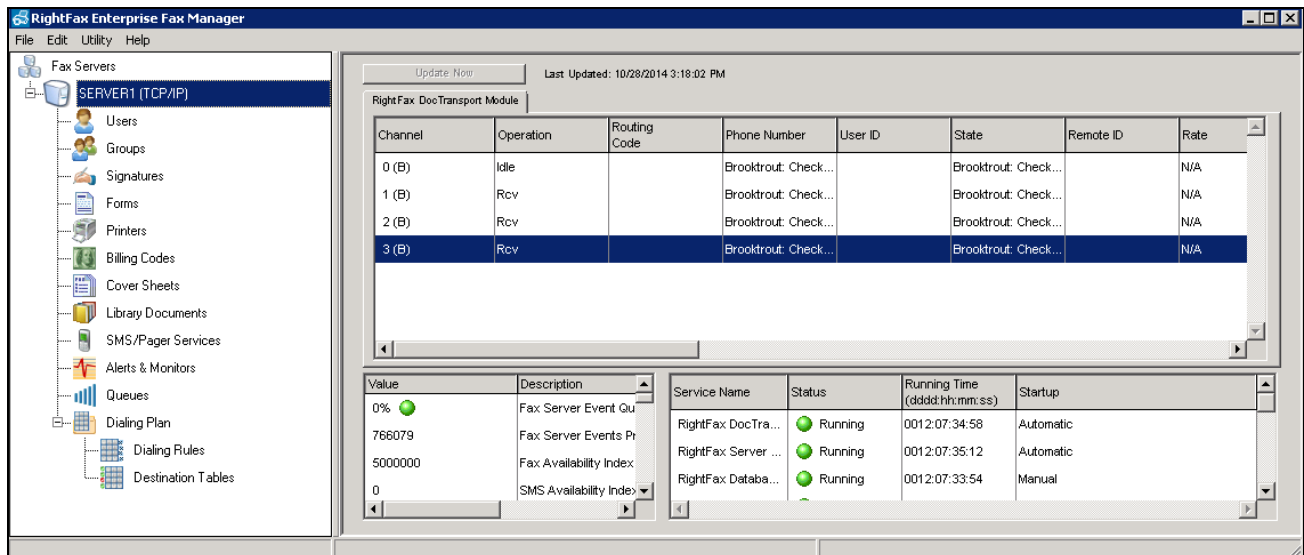
Note that the configurations documented in this section pertain to interoperability between RightFax and the Avaya SIP infrastructure. The standard configurations pertaining to RightFax itself (e.g., administering fax channels) are not covered. For instructions on administering and operating RightFax, refer to **Section 10**.

The configuration procedures covered in this section include the following:

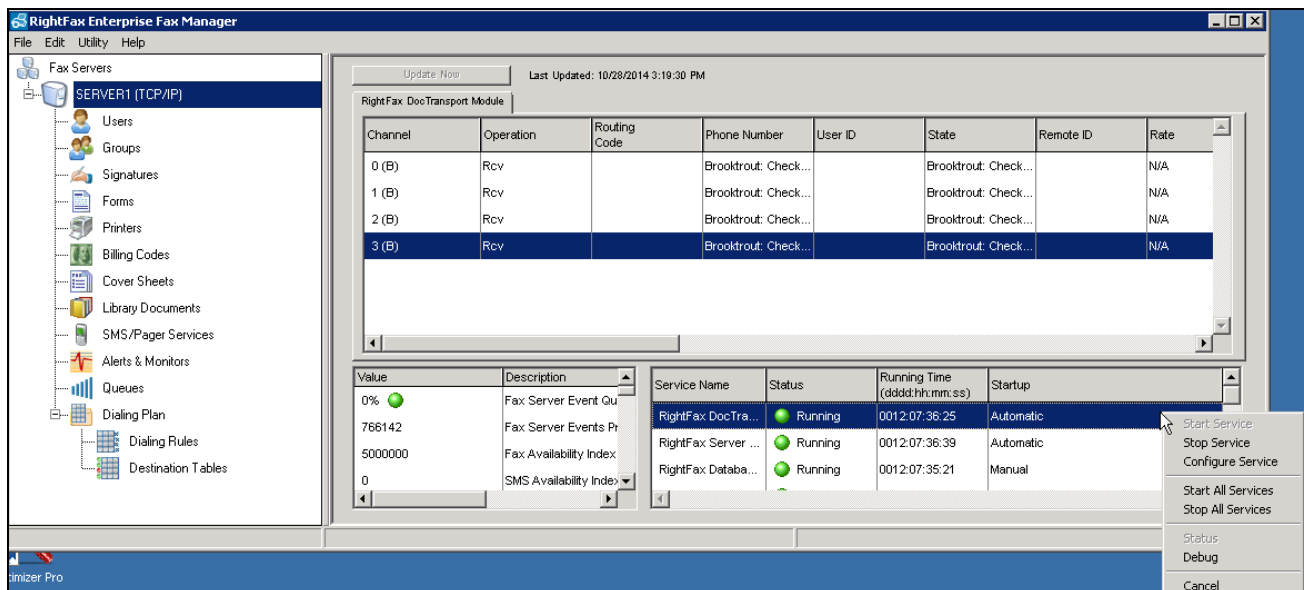
- Launch RightFax Enterprise Fax Manager and Brooktrout Configuration Tool
- Configure IP stack
- Configure BTCall parameters
- Configure Call Control parameters
- Configure SIP IP parameters
- Configure T.38 parameters
- Configure RTP parameters
- Administer RightFax dialing rules
- Administer RightFax users

7.1. RightFax Enterprise Fax Manager and Brooktrout Configuration Tool

The RightFax configuration is performed using the RightFax Enterprise Fax Manager. Launch the RightFax Enterprise Fax Manager from the Windows Start menu. At the main window, highlight the host name of the fax server (created during the installation process) from the navigation menu in the left pane:



The Brooktrout SR140 was configured during installation. To view or modify the settings, the RightFax DocTransport Module must be stopped. Right-click this module in the lower right pane and select **Stop All Services**. After all the service modules indicate the stopped status, right-click the **RightFax DocTransport Module** name again to select **Configure Service**.



In the **DocTransport Configuration-LOCAL** window that appears, click **RightFax OEM** (left side of screen), then click on the **Configure Brooktrout** button.

DocTransport Configuration - LOCAL

Auto Billing Code Settings
Global DocTransport Settings
[-] **Brooktrout**
 Global Transport Settings
 + **Advanced Settings**
 [-] **RightFax OEM**
 Channel #0
 Channel #1
 Channel #2
 Channel #3

Board module number: []
Number from the rotary switch on the board.

DID Settings
Number of digits for routing: 4 []

☒ Set Fax ID for all channels: Fax Server
☐ Set Capability for all channels: Both []

Configure Brooktrout Board
Configure Brooktrout

Number of SR140 channels: 4 []

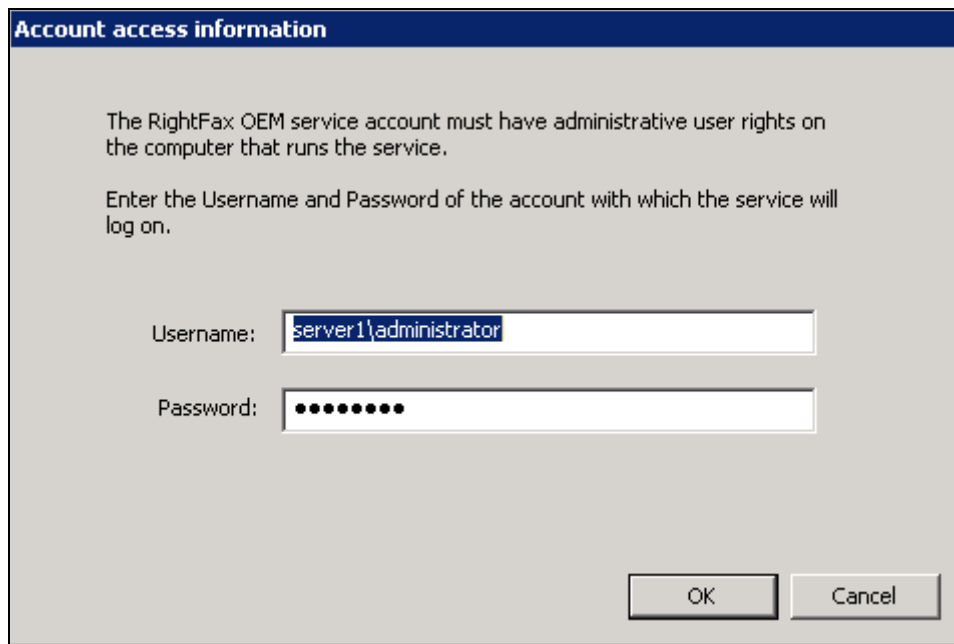
Exchange 2010 UM Fax Routing
☐ Route to SMTP Email Only
☐ Route to RightFax User Only
☒ Route to Both

SMTP Authentication to Exchange 2010 Unified Messaging Server
Exchange Server Name or IP: UnifiedMessageExchangeServer
Domain: ExchangeServerDomain
User Account: []
Password: []

SQL Connections
Driver={SQL Server};Server=SERVER1;Database=RightFax;Trusted_Connection []

Delete Device Add Transport Select Service Account... OK Cancel

Enter the credentials for the RightFax Service account used for the RightFax DocTransport Module. This account must have administrative user rights on the computer that runs the service.



The dialog box is titled "Account access information" in a blue header bar. Below the header, there is a light gray background area. The text inside reads: "The RightFax OEM service account must have administrative user rights on the computer that runs the service." followed by "Enter the Username and Password of the account with which the service will log on." There are two input fields: "Username:" with the text "server1\administrator" and "Password:" with ten black dots. At the bottom right, there are two buttons: "OK" and "Cancel".

Account access information

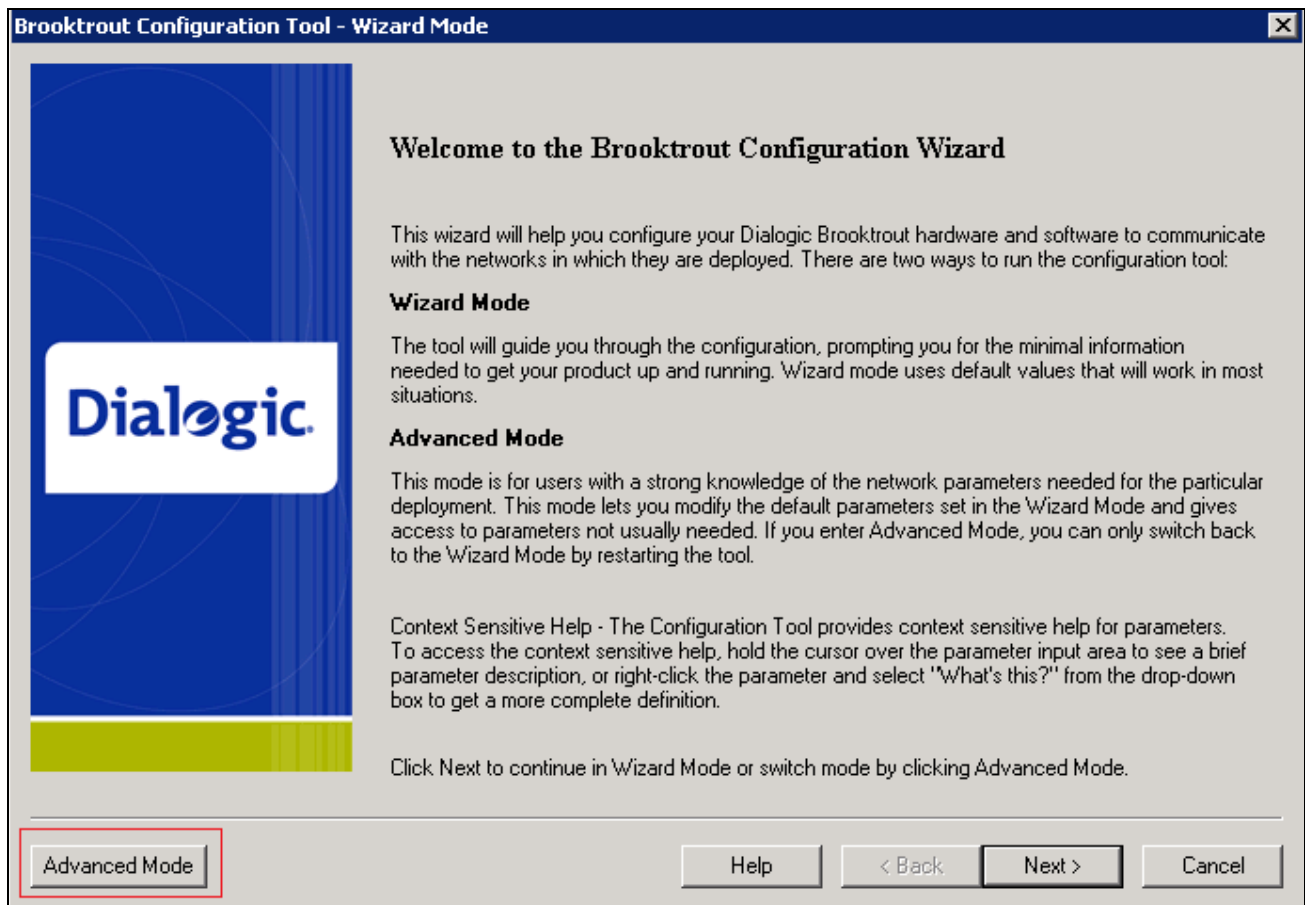
The RightFax OEM service account must have administrative user rights on the computer that runs the service.

Enter the Username and Password of the account with which the service will log on.

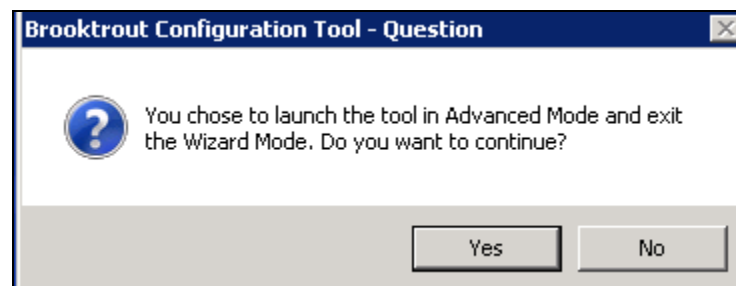
Username:

Password:

The **Brooktrout Configuration Tool – Wizard Mode** window gets displayed. Click the **Advanced Mode** button in this window.

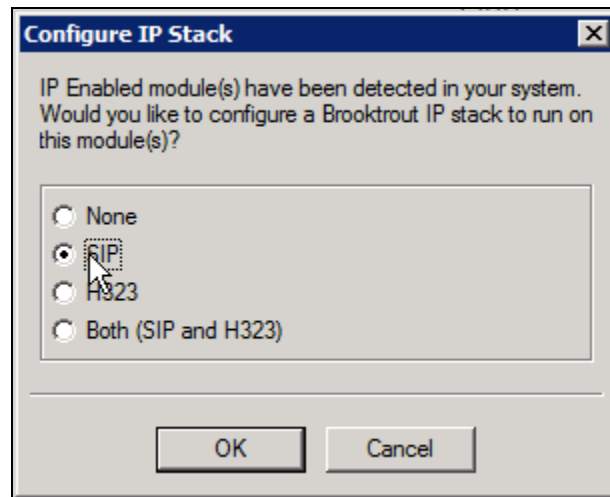


Click **Yes** when prompted to launch the Configuration Tool in Advanced mode.

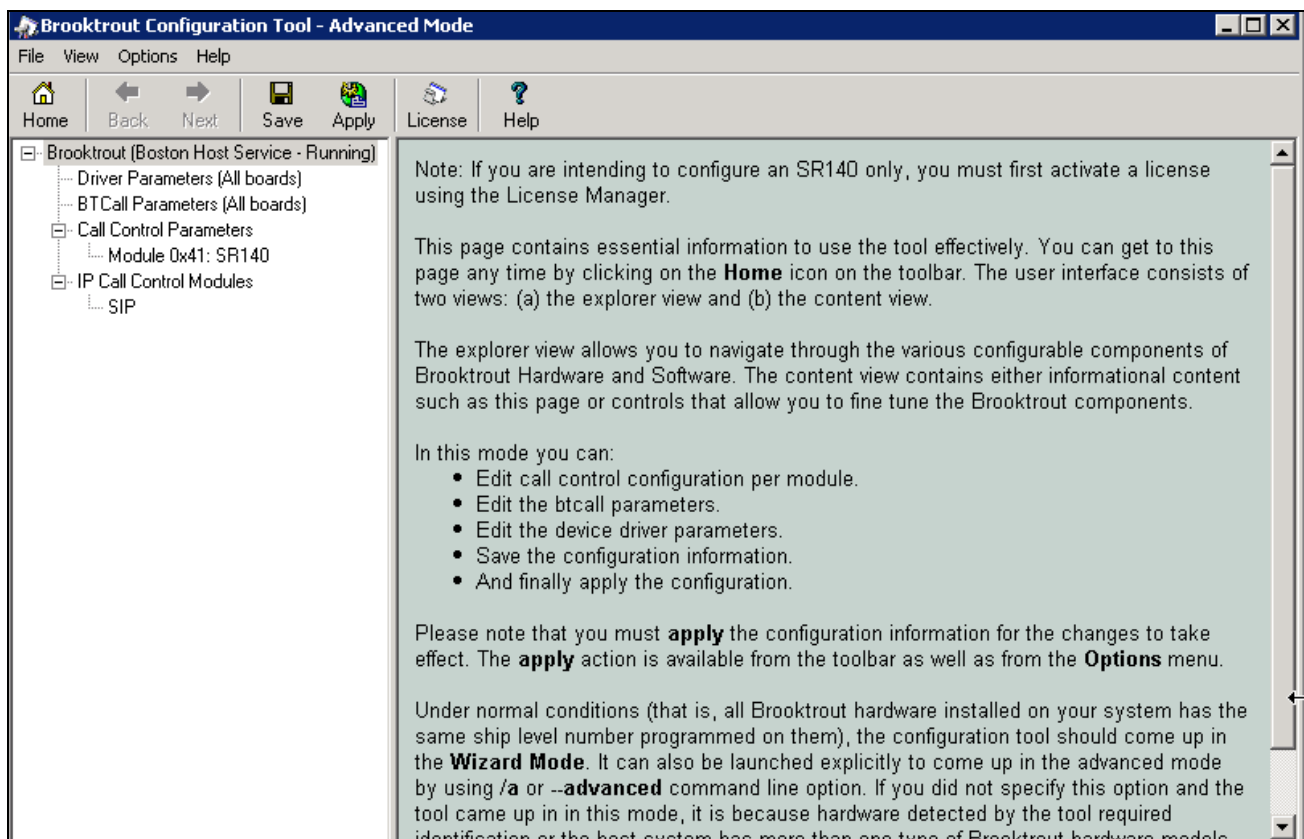


7.2. Configure IP Stack

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.

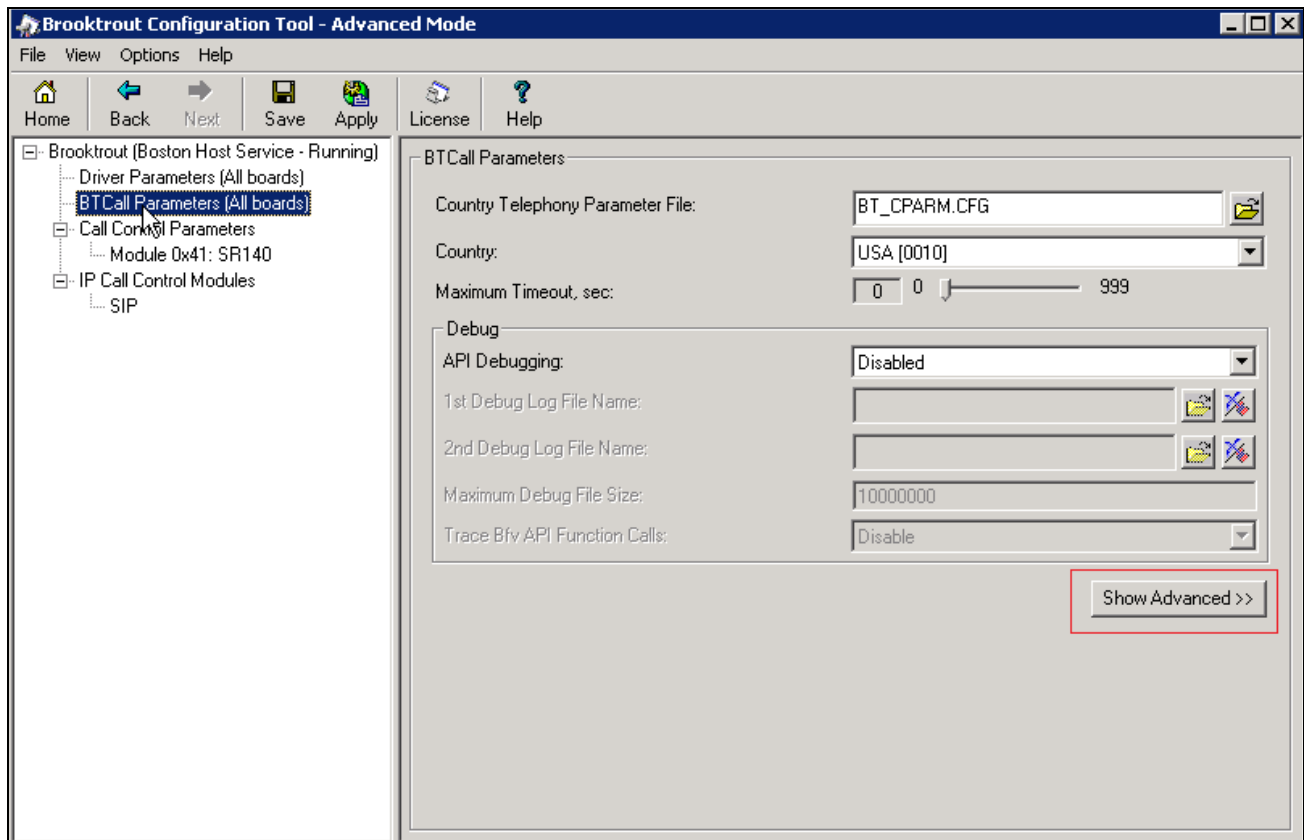


Note that IP Stack can be viewed/reconfigured from the Brooktrout Configuration Tool menu **Options → Configure IP Stack** (not shown).

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.

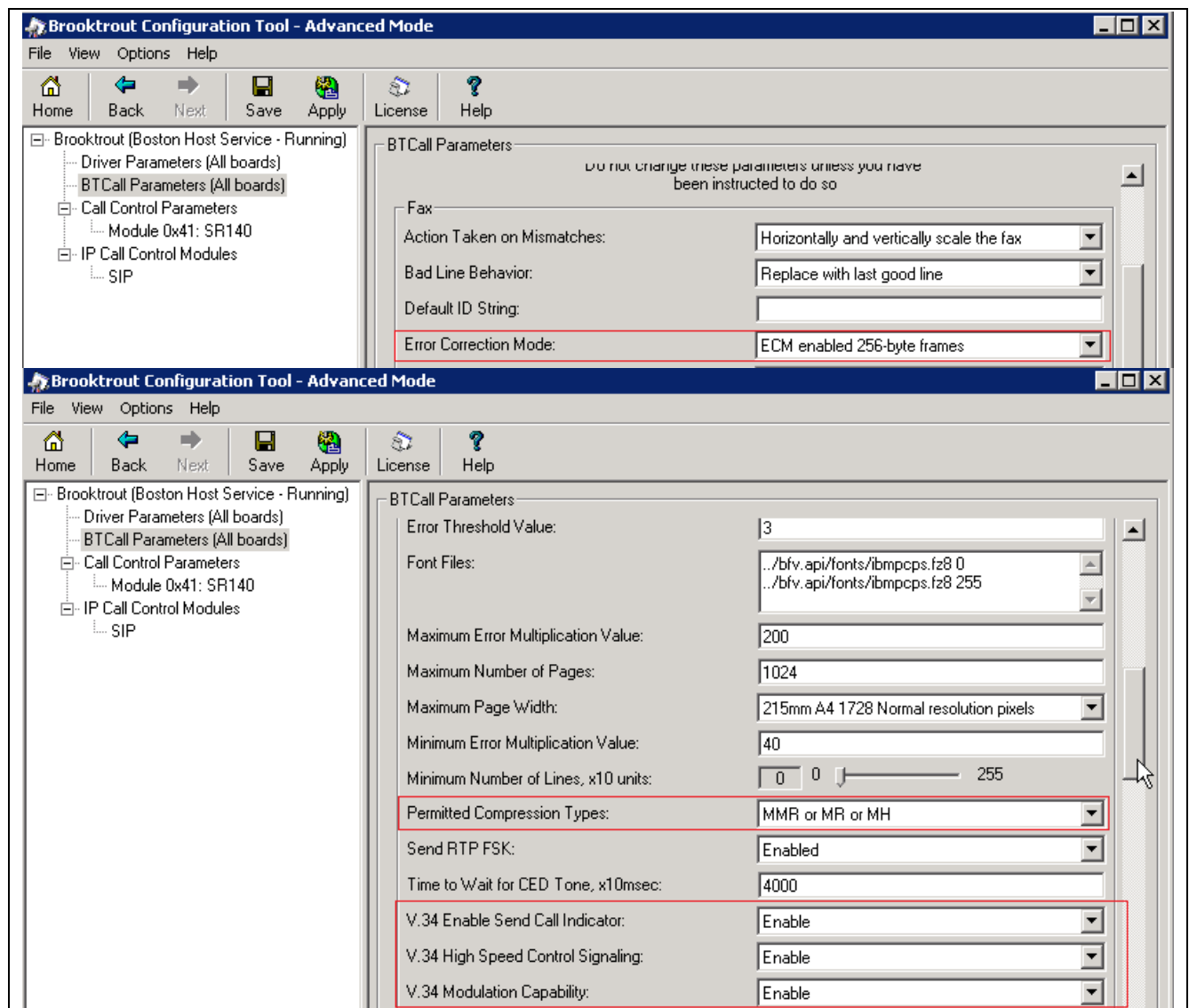
Navigate to **Brooktrout → BTCall Parameters (All boards)** in the left navigation menu. Click the **Show Advanced** button.



Under Advanced Settings, configure the fields as follows:

- **Error Correction Mode:** *ECM enabled 256-byte frames*
- **Permitted Compression Types:** *MMR or MR or MH*
- **V.34 Enable Send Call Indicator:** *Enable*
- **V.34 High Speed Control Signaling:** *Enable*
- **V.34 Modulation Capability:** *Enable*

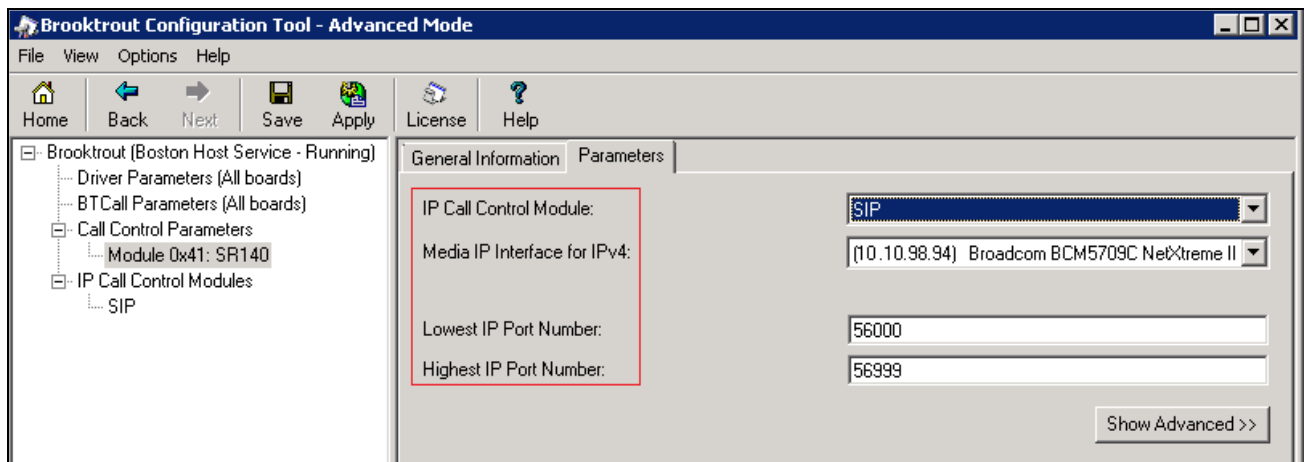
Use default values for other fields.



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 correct for your environment:

- **IP Call Control Module: SIP**
- **Media IP Interface for IPv4:** If the server contains multiple network interface cards (NICs), ensure you have selected an 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** – The IP address of Session Manager and the Port number to communicate with.
- **From Value** – If required by the Avaya environment, set this to an appropriate *UserInfo@ServerIP*. During compliance testing this value was configured as *2125551212@10.10.98.94*.
- **Contact Address** – Enter the IP address assigned to RightFax and the port number *5060*. During compliance testing this value was left at default.
- **Username** – Required. Default value is a dash ('-') character.

Use default values for all other fields.

The screenshot shows the 'Brooktrout Configuration Tool - Advanced Mode' window. The left sidebar shows a tree view with 'Brooktrout (Boston Host Service - Running)' expanded, and '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. The configuration fields are as follows:

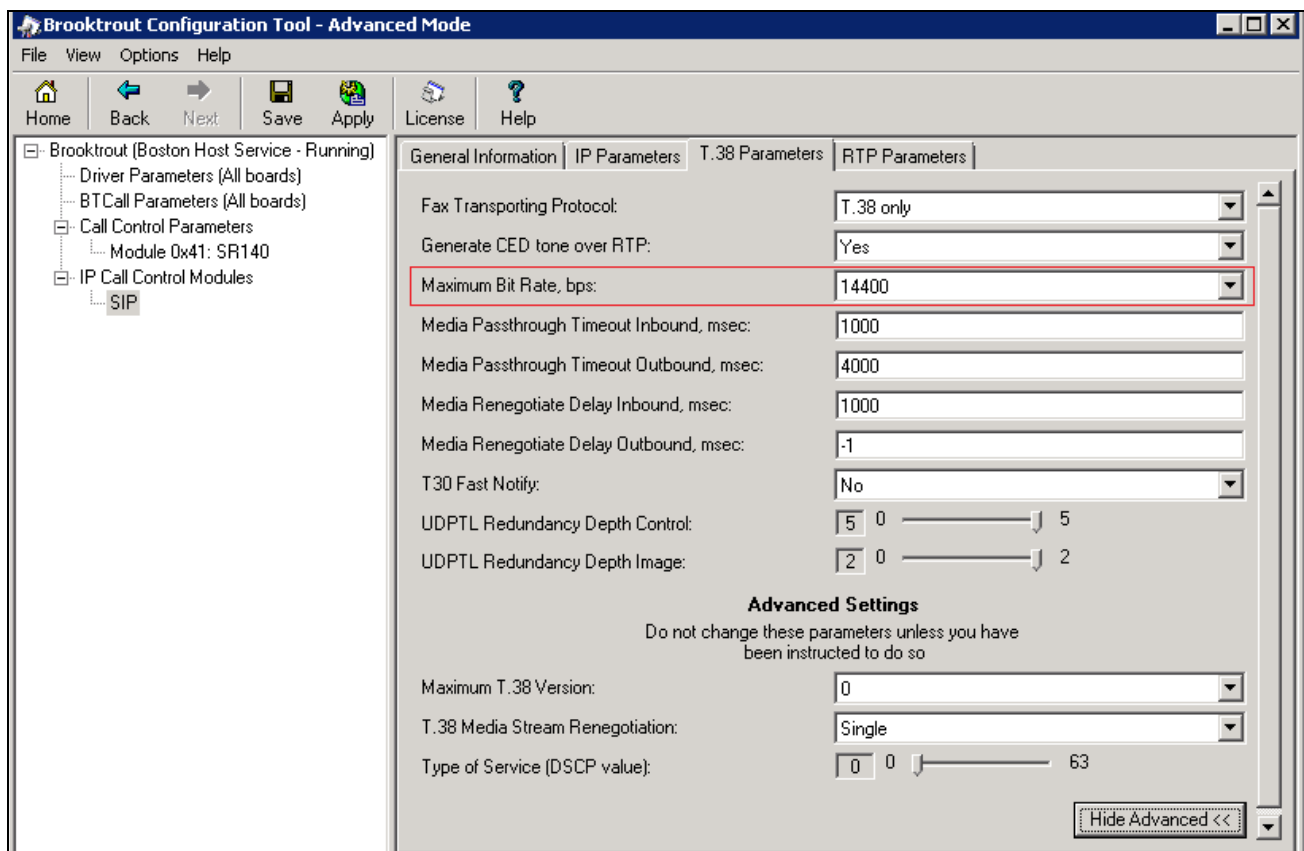
Field	Value
Maximum SIP Sessions:	256
Primary Gateway:	10.10.97.198 : 5060
Primary Proxy Server:	: 0
Additional Proxy Server #2:	: 0
Additional Proxy Server #3:	: 0
Additional Proxy Server #4:	: 0
Primary Registrar Server URL:	: 0
Additional Registrar Server #2:	: 0
Additional Registrar Server #3:	: 0
Additional Registrar Server #4:	: 0
From Value:	RightFax <sip:2125551212@10.10.98.94>
Contact IPv4 Address:	10 . 10 . 98 . 94 : 5060
Username:	-
Session Name:	no_session_name
Session Description:	
Description URI:	

7.6. Configure T.38 Parameters

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

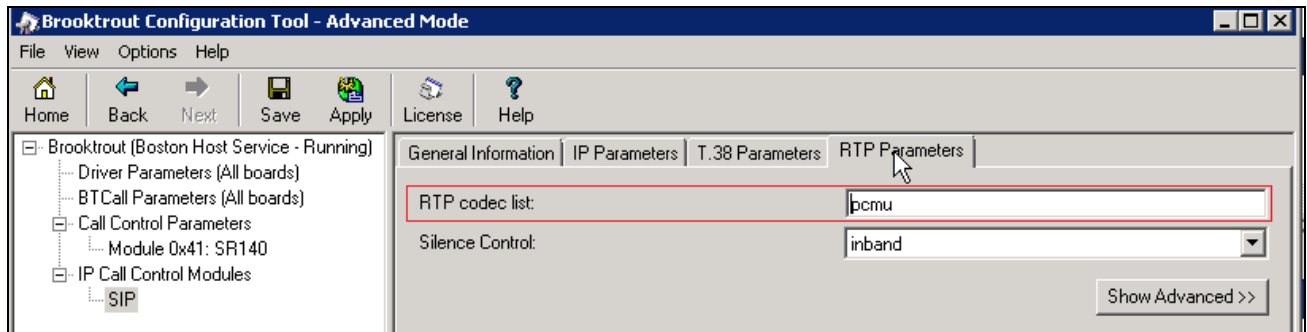
***Note:** During the compliance testing, the following settings were configured at the default settings. In practice, these settings may not be required for full functionality.*

- “Maximum Bit Rate, bps” is set to maximum, 14400, which is the default setting.



7.7. Configure RTP Parameters

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



After verifying all the above parameters are properly set, click **Save** in the button menu.

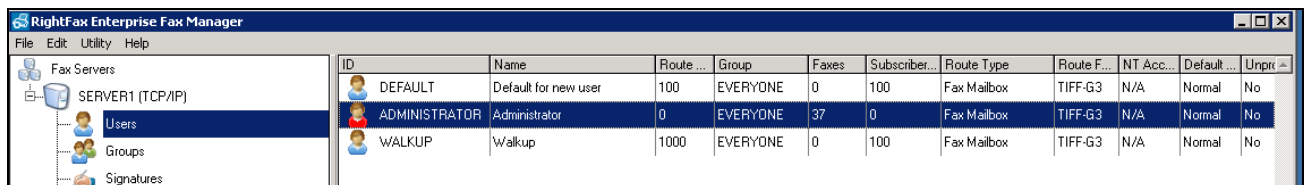
Exit the Brooktrout Configuration Tool.

In the **DocTransport Configuration** screen, click the **OK** button (See screen shot in **Section 7.1**).

Restart all RightFax service modules by right clicking the **RightFax DocTransport Module** name in the lower right pane of the RightFax Enterprise Fax Manager window and select **Start All Services** (See screen shot in **Section 7.1**).

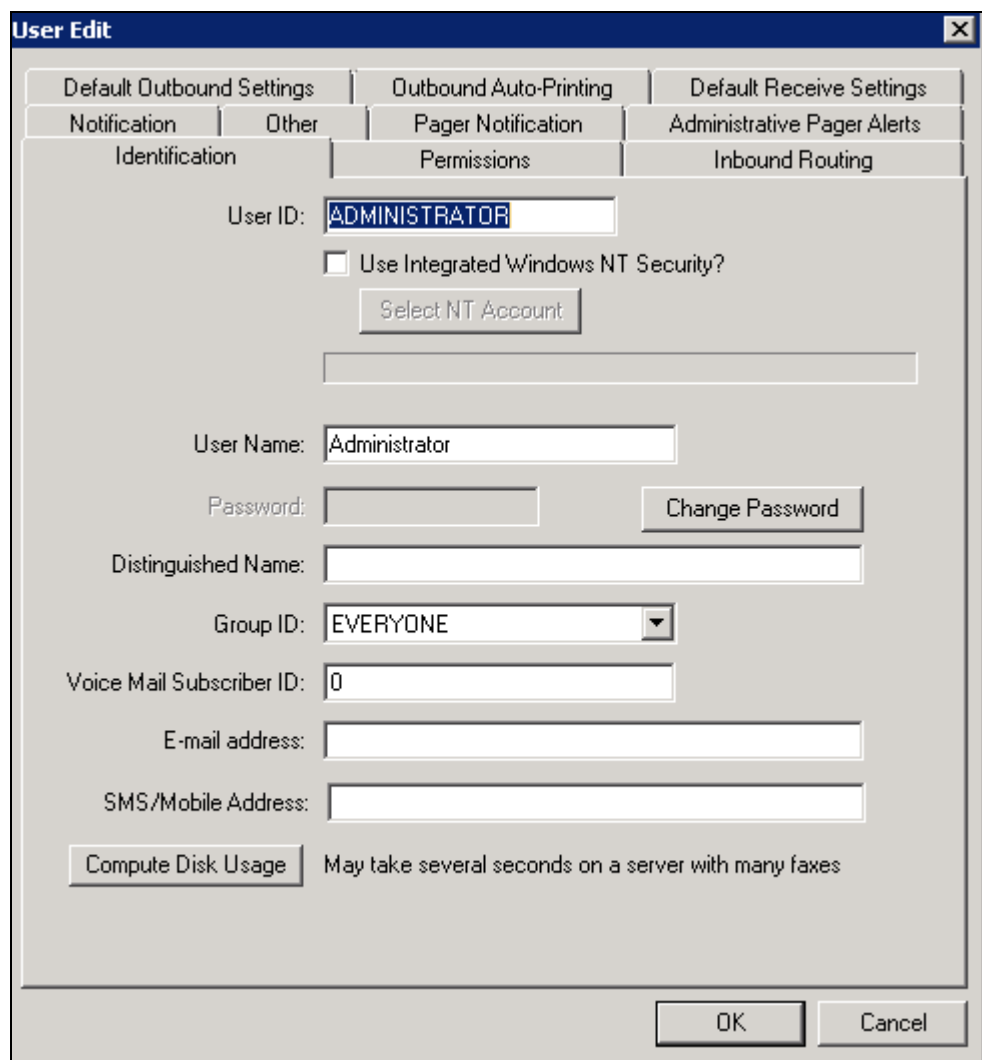
7.8. Administer RightFax Users

A user is created on the RightFax server for each incoming fax number. The user represents the fax recipient. To view the list of users, navigate to **Users** in the left navigation menu under the host name of the fax server. The example below shows a list of three users. To view the details of a user, double-click on the user entry in the right pane. During compliance testing the **ADMINISTRATOR** user was used. This section is mentioned here for reference only and therefore no details of configuring a user will be discussed in these application notes.



The screenshot shows the 'RightFax Enterprise Fax Manager' application window. On the left, a tree view shows 'Fax Servers' expanded to 'SERVER1 (TCP/IP)', with 'Users' selected. The main pane displays a table of users.

ID	Name	Route ...	Group	Faxes	Subscriber...	Route Type	Route F...	NT Acc...	Default ...	Unpr...
DEFAULT	Default for new user	100	EVERYONE	0	100	Fax Mailbox	TIFF-G3	N/A	Normal	No
ADMINISTRATOR	Administrator	0	EVERYONE	37	0	Fax Mailbox	TIFF-G3	N/A	Normal	No
WALKUP	Walkup	1000	EVERYONE	0	100	Fax Mailbox	TIFF-G3	N/A	Normal	No



The 'User Edit' dialog box is shown with the 'Identification' tab selected. The 'User ID' field is set to 'ADMINISTRATOR'. The 'Use Integrated Windows NT Security?' checkbox is unchecked. The 'User Name' field is set to 'Administrator'. The 'Group ID' dropdown is set to 'EVERYONE'. The 'Voice Mail Subscriber ID' field is set to '0'. The 'E-mail address' and 'SMS/Mobile Address' fields are empty. The 'Compute Disk Usage' button is visible at the bottom left, with a note: 'May take several seconds on a server with many faxes'. The 'OK' and 'Cancel' buttons are at the bottom right.

Default Outbound Settings | Outbound Auto-Printing | Default Receive Settings
Notification | Other | Pager Notification | Administrative Pager Alerts
Identification | Permissions | Inbound Routing

User ID: ADMINISTRATOR
☐ Use Integrated Windows NT Security?
Select NT Account
User Name: Administrator
Password: Change Password
Distinguished Name:
Group ID: EVERYONE
Voice Mail Subscriber ID: 0
E-mail address:
SMS/Mobile Address:
Compute Disk Usage May take several seconds on a server with many faxes
OK Cancel

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 5.6** are in-service.
- From Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Section 5.7** is in-service.
- Verify that fax calls can be placed to/from Open Text RightFax server 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 Open Text RightFax server is in service.

9. Conclusion

These Application Notes describe the procedures required to configure OpenText RightFax to interoperate with Avaya 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] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.4, July 2014.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3.4, July 2014.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.3, July 2014, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, July 2014, Document Number 555-245-205.
- [5] *Administering Avaya Aura® System Manager for Release 6.3.8*, Release 6.3.8, August 2014.
- [6] *Administering Avaya Aura® Session Manager*, Release 6.3, August 2014.

RightFax products may be found at <https://knowledge.opentext.com>. (Valid login required).

- *OpenText RightFax 10.6 Administrator Guide*
- *OpenText RightFax 10.6 Installation Guide*

©2014 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.