



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring OpenText RightFax with Avaya Communication Server 1000 and Avaya Aura® Session Manager via SIP Trunk Interface - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the OpenText RightFax with Avaya Communication Server 1000 and Avaya Aura® Session Manager using a SIP trunk interface.

OpenText RightFax is a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, OpenText RightFax interoperated with Avaya Aura® Session Manager to send/receive faxes using SIP trunk facilities.

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.

Introduction

These Application Notes describe the procedures for configuring OpenText RightFax with Avaya Communication Server 1000 (Communication Server 1000) and Avaya Aura® Session Manager (Session Manager) using SIP trunks.

OpenText RightFax is a software based fax server that sends and receives fax calls over an IP network. OpenText RightFax utilizes the Brooktrout SR140 T.38 Fax over Internet Protocol (FoIP) virtual fax board software from Dialogic. In the tested configuration, OpenText RightFax interoperated with Avaya Aura® Session Manager to send/receive faxes using a SIP trunk interface.

General Test Approach and Test Results

This section describes the compliance test approach used to verify interoperability of OpenText RightFax with Session Manager.

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.

1.1. 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 Server 1000 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.

1.2. Test Results

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

- ◆ Not all services of RightFax start automatically after a reboot of the fax server. Some services need to be manually restarted. Also if the fax server reboots in the midst of a fax transmission, the status of the fax does not change after the reboot. Open Text indicates this is abnormal behavior, not attributable to telephony components of the product. Customers experiencing similar problems should contact OpenText Technical Support for further assistance.

Note: The SIP trunks on Communication Server 1000 for connecting to Session Manager at Site 1, as well as the ISDN-PRI trunks for connecting the two sites must be configured with adequate number of trunk members to support the number of simultaneous fax calls intended. On RightFax, an adequate number of fax channels must also be appropriately configured for the intended capacity.

1.3. Support

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

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

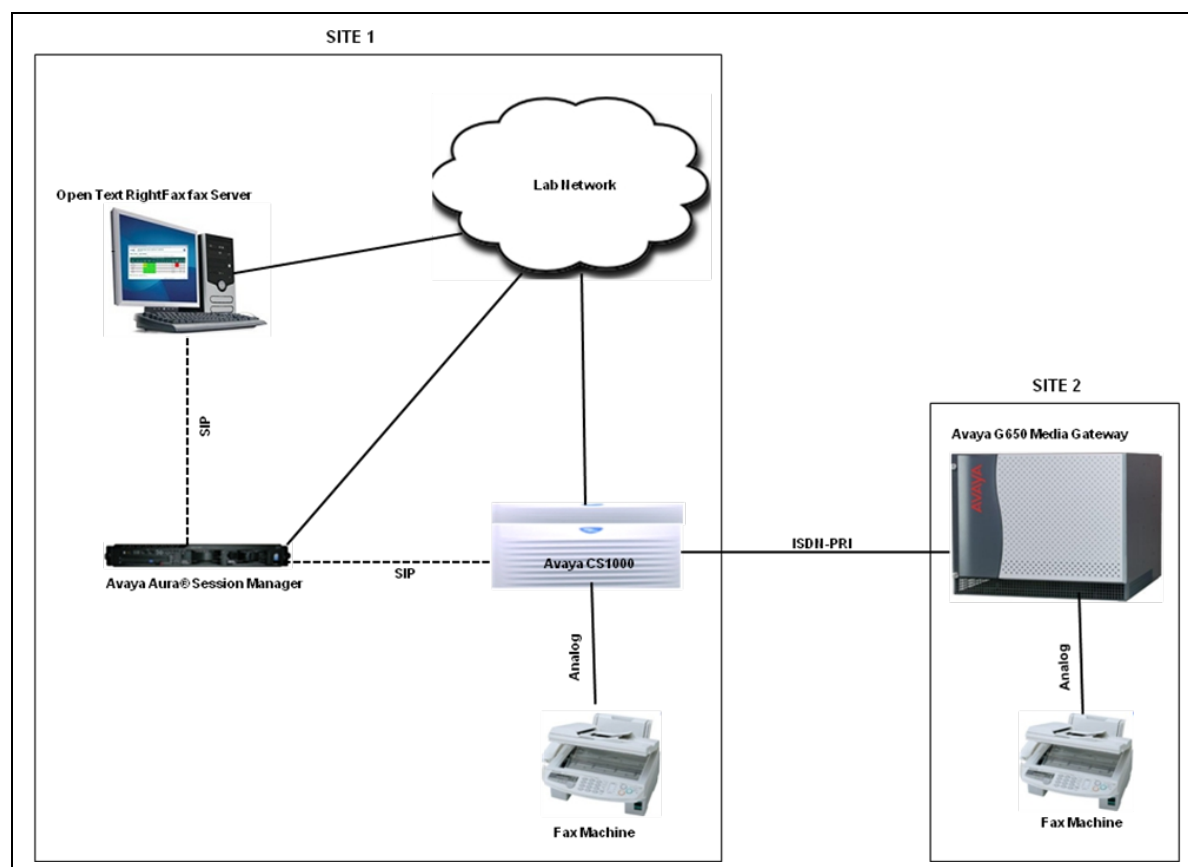
For other locations go to <http://www.opentext.com/2/global/company/company-contact.html>

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 Server 1000, Avaya Aura® Session Manager, RightFax server and an analog fax machine belong to Site 1 (local site). The RightFax server communicates to the Communication Server 1000 via the Avaya Aura® Session Manager using SIP trunks. An analog fax port is configured on the Communication Server 1000 to which a fax machine is connected. The equipment involved in Site 2 is beyond the scope of this document and is shown here for reference only. Site 2 (remote) can consist of any PBX with an analog fax machine configured. During compliance testing in the lab, Site 2 consisted of an Avaya G650 Media Gateway and an analog fax machine. Site 1 and Site 2 communicate via ISDN-PRI trunks that are configured between the Communication Server 1000 and Avaya G650 Media Gateway.

Since Site 2 is an emulated PSTN setup, the configuration details of setting the ISDN-PRI trunks between Site 1 and Site 2 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 Server 1000 and Avaya G650 Media Gateway so that their respective clocks are in synchronized state.



**Figure 1: RightFax interoperating with Avaya Aura® Session Manager
via SIP Trunk for Local Site and ISDN-PRI for Remote Site**

Equipment and Software Validated

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

Equipment	Release/Version
Avaya Communication Server 1000	7.50
Avaya Aura® Session Manager	6.2
Avaya Aura® System Manager	6.2
OpenText RightFax on Windows 2008R2 Enterprise SP1	10.5.0.895 (RightFax 10.5 Release version) with Dialogic Brooktrout SR140 SDK 6.5.2
Analog Fax Machine	N/A

Configure Avaya Communication Server 1000


This section describes the Communication Server 1000 configuration necessary to interoperate with Session Manager and OpenText RightFax. It provides the procedures for configuring Avaya Communication Server 1000 system. The procedures include the following areas:

- ◆ Logging into the Element Manager via Unified Communications Manager.
- ◆ Configuring the SIP Signaling Gateway.
- ◆ Configuring a D-Channel.
- ◆ Configuring Route and Trunks.
- ◆ Configuring Digit Manipulation Block.
- ◆ Configuring Route List Block.
- ◆ Configuring Distant Steering Code.

For detail configuration details of the Communication Server 1000 refer to **Section 10**.

1.4. Logging into Element Manager via Unified Communication Manager

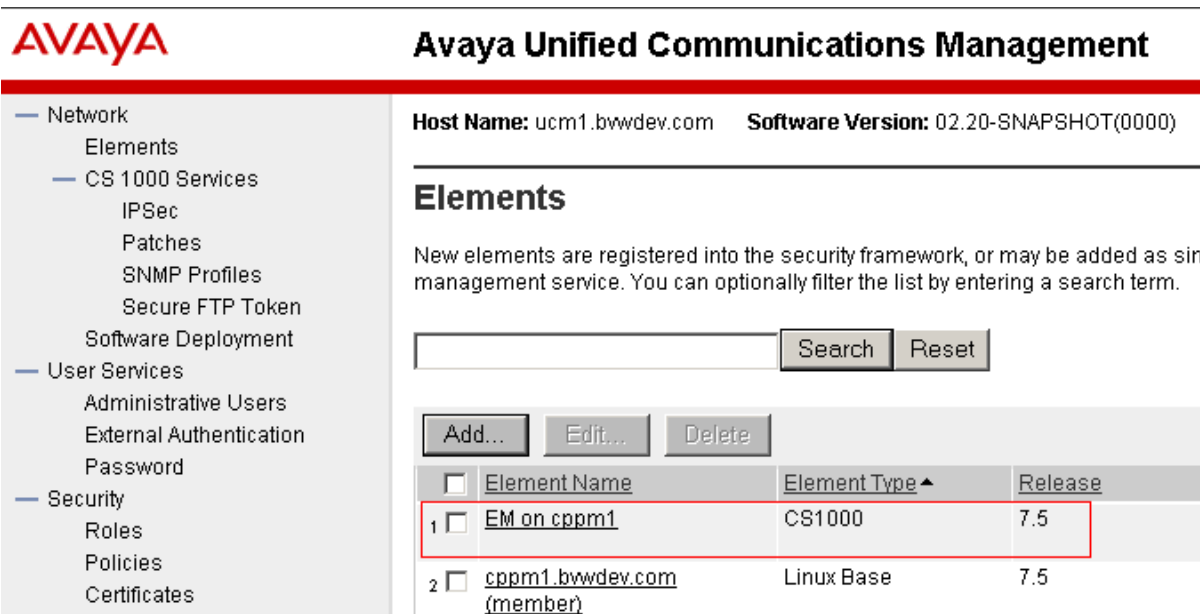
To login to the Unified Communications Manager (UCM) open an IE browser and type in the IP address of the UCM in the URL (not shown). Screen below shows the login screen of the UCM. Enter the **User ID** and **Password** credentials and click on **Log In** to continue.



The login screen features a large red header with the AVAYA logo in the bottom right corner. Below the header, on the left, is a disclaimer: "This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network." To the right of the disclaimer is a login form with fields for "User ID:" and "Password:", and a "Log In" button.

Copyright © 2002-2010 Avaya Inc. All rights reserved.

From the UCM main screen as shown in screen below, click on the Element **EM on cppm1**. This is the element which is configured to access the Element Manager (EM) for the Communication Server 1000 Call Server.



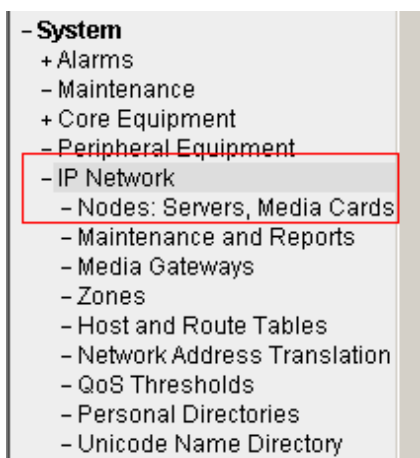
The main screen displays the AVAYA logo and the title "Avaya Unified Communications Management". It includes a left-hand navigation menu with categories like Network, Elements, CS 1000 Services, User Services, and Security. The main content area shows system information (Host Name: ucm1.bwwdev.com, Software Version: 02.20-SNAPSHOT(0000)) and an "Elements" section. This section contains a search bar, buttons for "Add...", "Edit...", and "Delete", and a table of registered elements.

	Element Name	Element Type ^	Release
1	EM on cppm1	CS1000	7.5
2	cppm1.bwwdev.com (member)	Linux Base	7.5

1.5. Configuring the SIP Signaling Gateway

This section describes the configuration required on the SIP Signaling Gateway present on the Communication Server 1000 so that Communication Server 1000 can communicate with the Avaya Aura® Session Manager via SIP Trunks. Assumption is made here that the IP Telephony node is already added.

To access the Node in the EM left navigator screen, navigate to **IP Network → Nodes: Servers, Media Cards** as shown below.



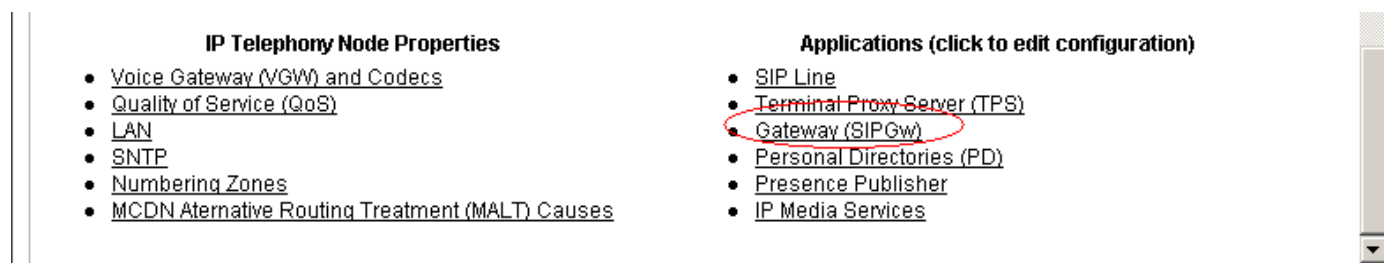
During compliance testing Node **551** was already created. Click on this Node as shown in screen below.

IP Telephony Nodes

Click the Node ID to view or edit its properties.

Add...	Import...	Export...	Delete	Print Refresh		
<input type="checkbox"/> Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 550	1	SIP Line	-	110.10.10.133		Synchronized
<input type="checkbox"/> 551	1	LTPS, PD, Gateway (SIPGw) -		110.10.10.130		Synchronized
Show: <input checked="" type="checkbox"/> Nodes <input type="checkbox"/> Component servers and cards <input checked="" type="checkbox"/> IPv6 address						

Open the SIP Signaling Gateway configuration by clicking on **Gateway (SIPGw)** as shown below.



In the **General** tab, select the values as shown in screen below. A **SIP domain name** of **bvwdev.com** was chosen since this is the domain name that will be configured on the Session Manager. Similarly **cppm1** was configured as **Gateway endpoint name**.

Node ID: 551 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: bvwdev.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: cppm1 *

Gateway password: *

Application node ID: 551 * (0-9999)

Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP: Add

Monitor addresses: Remove

Under the **Proxy or Redirect Server** section enter the IP address of the Session Manager and select **UDP** as the Transport protocol as shown below. Leave the remaining values at default. During compliance testing **110.10.10.198** was the IP address of the Session Manager.

Node ID: 551 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 110.10.10.198
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

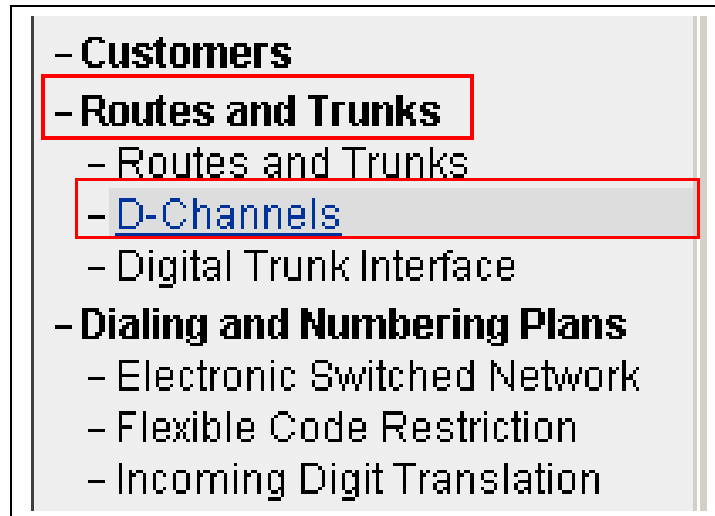
Transport protocol: UDP ▼

Options: ☐ Support registration
☐ Primary CDS proxy

Save and transmit (not shown) these Node properties to complete the SIPGw configuration.

1.6. Configuring D-Channel

This section explains the configuration of a D-Channel for SIP Trunking. From the EM navigation screen, navigate to **Routes and Trunks** → **D-Channels** as shown below.



Choose a D-Channel number to add as shown below. During compliance testing D-Channel number **10** was selected. Click on **to Add** to continue.

D-Channels

Maintenance

[D-Channel Diagnostics \(LD 96\)](#)
[Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)
[MSDL Diagnostics \(LD 96\)](#)
[TMDI Diagnostics \(LD 96\)](#)
[D-Channel Expansion Diagnostics \(LD 48\)](#)

Configuration

Choose a D-Channel Number: **10** and type: **DCH** **to Add**

Configure the **Basic Configuration** values for the D-Channel as shown below.

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	SIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> more PRI
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

To edit the **Remote Capabilities** of the D-Channel, click on **Edit** button as shown below.

Signalling server resource capacity: 3700 Range: 0 - 3700

- Basic options (BSCOPT)

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number: []

- Progress signal: []

- Calling Line Identification: []

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive. (1)

- Remote Capabilities: **Edit**

Select the boxes values for the Remote Capabilities as shown in screen below. Click on **Return - Remote Capabilities** button to return back to the main screen to complete the D-Channel configuration.

Remote D-channel is on a MSDL card (MSL) ☐

Message waiting interworking with DMS-100 (MMI) ☒

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☐

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☐

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

NI-2 name display option. (NDS) ☐

Message waiting indication using integer values (QMVI) ☐

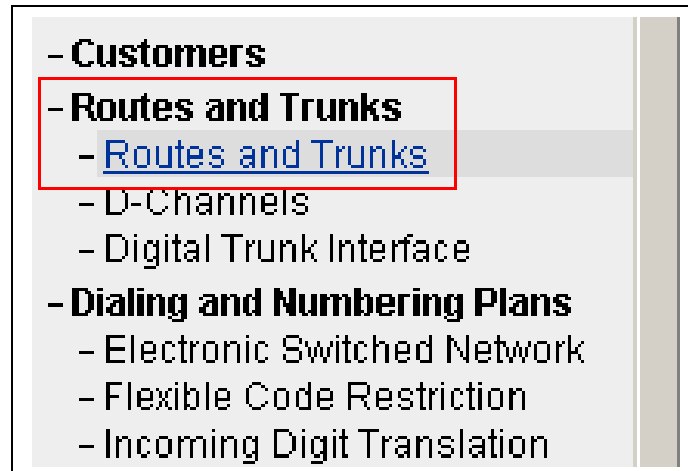
Message waiting indication using object identifier (QMVO) ☐

User to user signalling (UUI) ☐

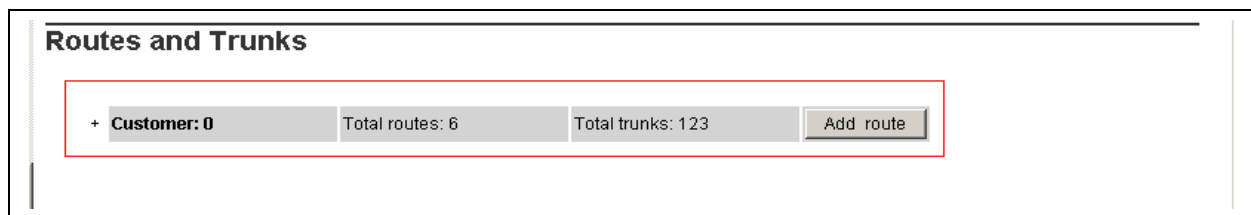
Return - Remote Capabilities Cancel

1.7. Configuring Route and Trunks

This section explains the configuration of the SIP route and trunks which will be used by Communication Server 1000 to communicate with the RightFax server. To add a new route, navigate to **Routes and Trunks** → **Routes and Trunks** from the EM left hand navigator window as shown in screen below.



From the Routes and Trunks screen click on **Add route** button to start configuring a new route as shown in below.



During compliance testing **Route number 10** was added. Select the values from the drop down menu and configure the values as shown in the next three screens below.

- Basic Configuration

Route data block (RDB) (TYPE) :	<input type="text" value="RDB"/>
Customer number (CUST) :	<input type="text" value="00"/>
Route number (ROUT) :	<input type="text" value="10"/>
Designator field for trunk (DES) :	<input type="text" value="SIP"/>
Trunk type (TKTP) :	<input type="text" value="TIE"/>
Incoming and outgoing trunk (ICOG) :	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access code for the trunk route (ACOD) :	<input type="text" value="1111"/>
Trunk type M911P (M911P) :	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK) :	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE) :	<input type="text" value="00254"/> (0 - 8000)
- Node ID of signaling server of this route (NODE) :	<input type="text" value="551"/> (0 - 9999)
- Protocol ID for the route (PCID) :	<input type="text" value="SIP (SIP)"/>
- Print correlation ID in CDR for the route (CRID) :	<input checked="" type="checkbox"/>
Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	<input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>
- D channel number (DCH) :	<input type="text" value="10"/> (0 - 254)
- Interface type for route (IFC) :	<input type="text" value="Meridian M1 (SL1)"/>
- Private network identifier (PNI) :	<input type="text" value="00001"/> (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>

Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	<input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>
- D channel number (DCH) :	<input type="text" value="10"/> (0 - 254)
- Interface type for route (IFC) :	<input type="text" value="Meridian M1 (SL1)"/>
- Private network identifier (PNI) :	<input type="text" value="00001"/> (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO) :	<input type="checkbox"/>
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :	<input type="checkbox"/>
- Channel type (CHTY) :	<input type="text" value="B-channel (BCH)"/>
- Call type for outgoing direct dialed TIE route (CTYP) :	<input type="text" value="Unknown Call type (UKWN)"/>
- Insert ESN access code (INAC) :	<input checked="" type="checkbox"/>
- Integrated service access route (ISAR) :	<input type="checkbox"/>
- Display of access prefix on CLID (DAPC) :	<input type="checkbox"/>
- Mobile extension route (MBXR) :	<input type="checkbox"/>
- Mobile extension outgoing type (MBXOT) :	<input type="text" value="National number (NPA)"/>
- Mobile extension timer (MBXT) :	<input type="text" value="0"/> (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) :	<input type="text" value="Unknown (UKWN)"/>

+ Basic Route Options

Process notification networked calls (PNNC) : ☐

- Network Options

Electronic switched network pad control (ESN) : ☐

Signaling arrangement (SIGO) : Standard (STD)

Route class (RCLS) : Route Class marked as external (EXT)

Off-hook queuing (OHQ) : ☐

Off-hook queue threshold (OHQT) : 0

Call back queuing (CBQ) : ☐

Number of digits (NDIG) : 2

Authcode (AUTH) : ☐

Configure the trunk values as shown in screen below. During compliance testing **Terminal number** used was **100 1 00 00** since it is a virtual trunk. Click on **Edit** button to configure the required **Class of Service** for the trunks.

Customer 0, Route 10, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block: IPTI

Terminal number: 100 1 00 00

Designator field for trunk: SIP

Extended trunk: VTRK

Member number: 1 *

Level 3 Signaling:

Card density: 8D

Start arrangement Incoming : Immediate (IMM)

Start arrangement Outgoing: Immediate (IMM)

Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: Edit

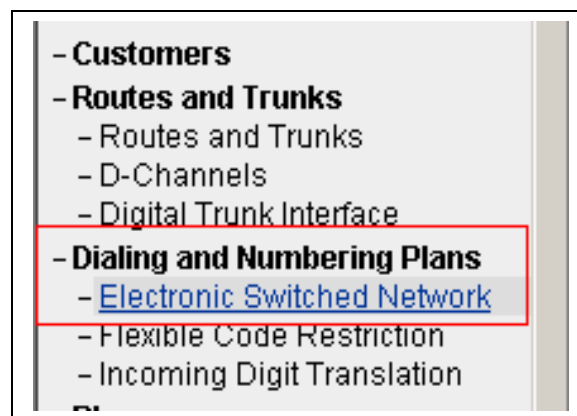
+ Advanced Trunk Configurations

Screen below shows the **Class of Service** values selected for the compliance testing from the drop down menu. Ensure that the **Restriction level** drop down table is set to **Unrestricted (UNR)**. Rest of the values are left at default. Click on **Return Class of Service** button (not shown) to complete the trunks configuration.

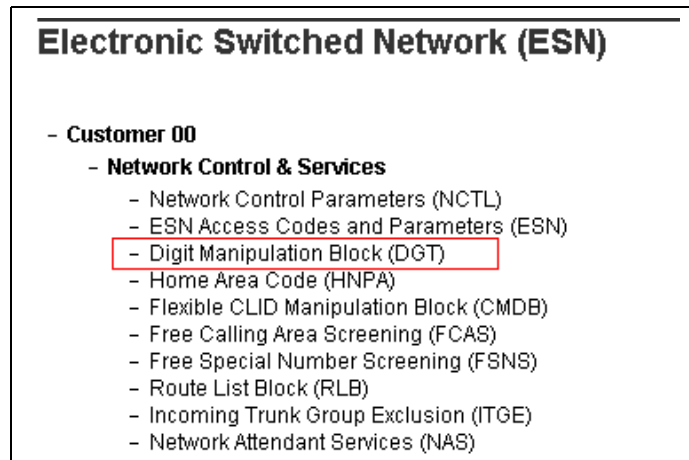
- Calling party:	Calling party Denied (CND)
- Central Office Ringback:	
- Centrex Switchhook Flash:	Centrex Switchhook Flash Denied (THFD)
- Dial Pulse:	Dial Pulse (DIP)
- DTR PAD value:	
- Echo Canceling:	Echo Canceling Denied (ECD)
- Hong Kong DTI:	
- Loop Break Supervised COT:	
- Make-break ratio for dial pulse:	10 pulses per second (P10)
- Manual Incoming:	Manual Incoming Denied (MID)
-Media Security:	Media Security Never (MSNV)
-Network Hook Flash Over M911P:	
- Polarity:	
- Priority:	Low Priority (LPR)
- Restriction level:	Unrestricted (UNR)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)

1.8. Configuring Digit Manipulation Block

This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the RightFax server. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown below.



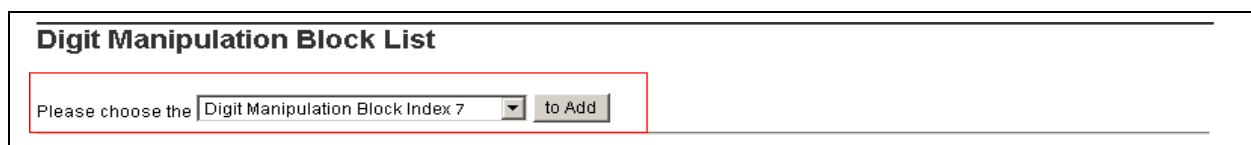
Click on **Digit Manipulation Block (DGT)** option as shown below.



Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - **Digit Manipulation Block (DGT)**
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)

Screen below shows the Digit Manipulation Block Index users can add. However during compliance testing **Digit Manipulation Block Index of 0** was used which is already added in the Communication Server 1000 system by default.

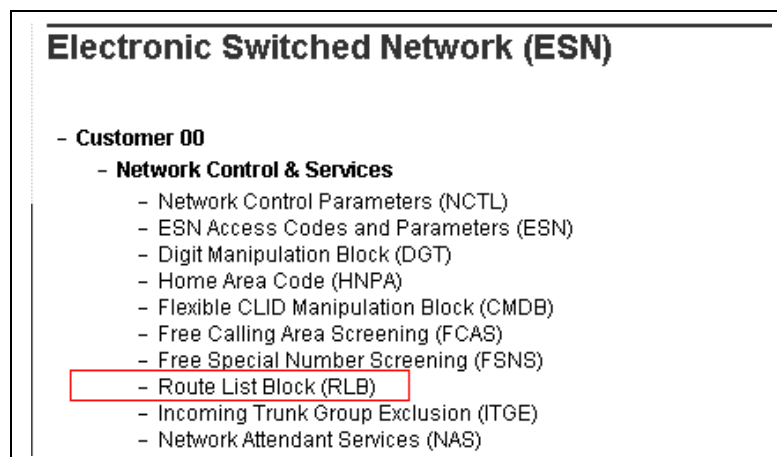


Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 7

1.9. Configuring Route List Block

This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the RightFax server. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in the screen in the beginning of this section. Click on **Route List Block (RLB)** option as shown below.



Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - **Route List Block (RLB)**
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)

Start adding a **route list index** as shown below. During compliance testing list index **10** was added. Click on **to Add** to continue.

Route List Blocks

Please enter a route list index (0 - 1999)

Click on **Edit** for **Data Entry Index 0** as shown below. This Data Entry Index value of 0 is already added in the Communication Server 1000 system by default.

Please choose the

+

Screen below show the values configured for the index block used during compliance testing. **Route Number** of **10** and **Digit Manipulation Index** of **0** were selected as per the configuration explained in **Sections 5.4** and **5.5** respectively. Click **Submit** (not shown) to complete the configuration.

Route List Block Index: 10

General Properties

Entry Number for the Route List:

Indexes

Time of Day Schedule:

Facility Restriction Level: (0 - 7)

Digit Manipulation Index:

ISL D-Channel Down Digit Manipulation Index: (0 - 1999)

Free Calling Area Screening Index:

Free Special Number Screening Index:

Business Network Extension Route: ☐

Incoming CLID Table: (0 - 100)

Options

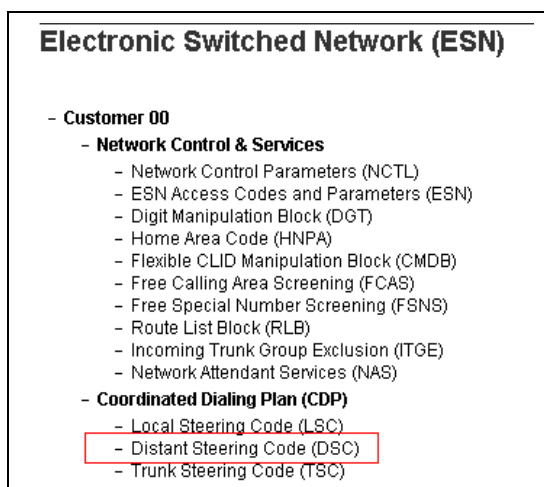
Local Termination entry: ☐

Route Number:

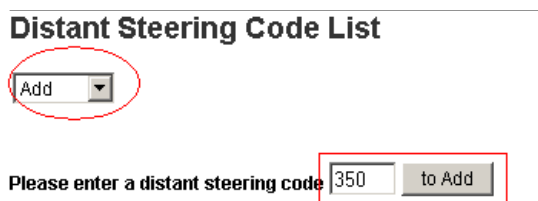
Skip Conventional Signaling: ☐

1.10. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the RightFax server. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in the screen in the beginning of this section. Click on **Distant Steering Code (DSC)** option as shown below.



From the drop down menu select **Add** and enter a distant steering code to add as shown in below. During compliance testing a code of **350** was added since the fax number assigned to the RightFax server was 35000. Click on **to Add** to continue.



Enter the values as shown in screen below. Note that **Route List to be accessed for trunk steering code** value selected is **10** based on the configuration explained in **Section 5.6** above. Click on **Submit** to complete the configuration.

Distant Steering Code

Distant Steering Code:

Flexible Length number of digits: (0 - 10)

Display:

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code:

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

Configure Avaya Aura® Session Manager

This section provides the procedures for configuring routing using Avaya Aura ® System Manager. The procedures include the following areas:

- ◆ Logging into the System Manager.
- ◆ Adding Domain.
- ◆ Adding Location.
- ◆ Adding SIP entities.
- ◆ Adding Entity Links.
- ◆ Adding Routing Policies.
- ◆ Adding Dial Patterns.

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

1.11. Logging into the Avaya Aura® System Manager

This section explains the steps to launch the login screen of the System Manager and accessing the Network Routing Policy.

To launch the System Manager Login screen, start an IE browser and type the IP address of the System Manager in the URL (not shown). Screen below shows the Log On Screen. Type the required **User ID** and **Password** credentials and click on **Log On** to continue.

AVAYA Avaya Aura ® System Manager 6.2

Home / Log On

Log On

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

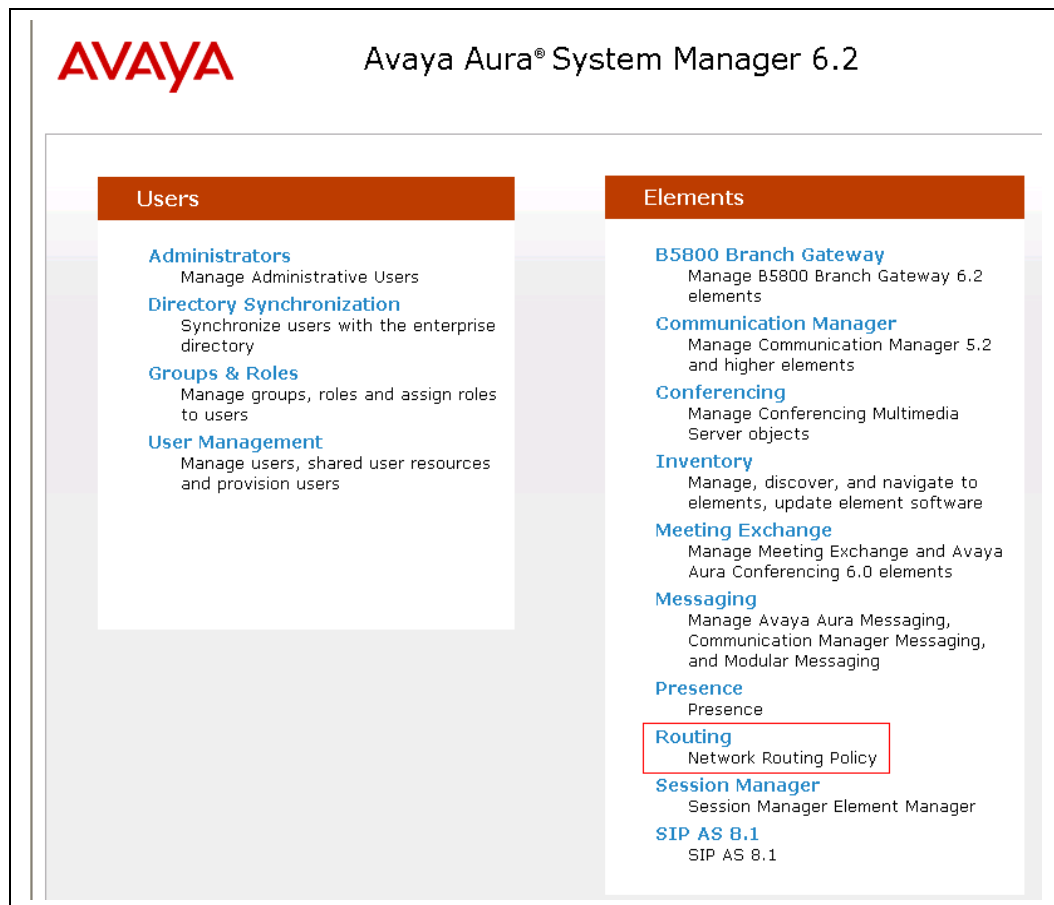
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

From the main screen of System Manager access the Network Routing Policy by selecting **Routing** as shown below.



1.12. Adding Domain

To add a domain, select **Domains** from the left hand window of the Routing screen and click on **New** (not shown). Configure the **Name** as shown in screen below and click on **Commit** to complete adding a domain. During compliance testing a domain name of **bwvdev.com** was used. Additional domains can be added in a similar fashion.

Name	Type	Default	Notes
* bwvdev.com	sip	<input type="checkbox"/>	

1.13. Adding Location

To add a location, select **Locations** from the left hand window of the Routing screen and click on **New** (not shown). Configure the **Name** as shown in screen below and click on **Commit** to add a Domain. During compliance testing a location name of **Belleville,Ont,Ca** was used. Click on **Commit** to complete adding a location. Additional locations can be added in a similar fashion.

Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns

Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: Belleville,Ont,Ca

Notes:

Commit Cancel Help ?

1.14. Adding SIP Entities

This section explains the adding of SIP entities for the Session Manager, RightFax server and the Communication Server 1000 system routing. To add SIP Entities, select **SIP Entities** from the left hand window of the Routing screen and click on **New** (not shown).

Next two screens show the SIP Entity Details for the Session Manager routing.

Enter a descriptive name for the **Name** field.

Populate the **FQDN or IP Address** field with **110.10.10.198**, which is the IP address of the Session Manager.

Select **Type** as **Session Manager**.

Select the location configured in **Section 6.3** in the **Location** field.

Select **Use Session Manager Configuration** option under the **SIP Link Monitoring** field.

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

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: DevASM

* FQDN or IP Address: 110.10.10.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville,Ont,Ca

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel Help ?

Under the Port section, add both TCP and UDP protocol along with the Port value and the Default Domain value.

Click on **Commit** to complete adding the SIP Entity.

Port

TCP Failover port:

TLS Failover port:

10 Items | [Refresh](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	15060	TLS	avaya.com	
<input type="checkbox"/>	5060	TCP	bvwddev.com	
<input type="checkbox"/>	5060	UDP	bvwddev.com	

Next two screens show the SIP Entity Details for the RightFax server routing.

Enter a descriptive name for the **Name** field.

Populate the **FQDN or IP Address** field with **110.10.5.64**, which is the IP address of the RightFax server.

Select the location configured in **Section 6.3** in the **Location** field.

Select **Use Session Manager Configuration** option under the **SIP Link Monitoring** field.

AVAYA Avaya Aura® System Manager 6.2 [Help](#)

Routing / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: RightFax

* FQDN or IP Address: 110.10.5.64

Type: Other

Notes: For RightFax Testing

Adaptation:

Location: Belleville

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Under the **Entity Links** section, add **DevASM** as **SIP Entity 1** and **RightFax** as **SIP Entity 2** with **UDP Protocol** and **5060** as **Port**.

Click on **Commit** (not shown) to complete adding the SIP Entity.

Entity Links

Add Remove

1 Item Refresh Filter: Ena

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	DevASM	UDP	* 5060	RightFax	* 5060	Trusted

Select : All, None

Next two screens show the SIP Entity Details for the Communication Server 1000 System routing.

Enter a descriptive name for the **Name** field.

Populate the **FQDN or IP Address** field with **110.10.10.130**, which is the IP address of the SIP Signaling Gateway of the Communication Server 1000 System.

Select the location configured in **Section 6.3** in the **Location** field.

Select **Link Monitoring Disabled** option under the **SIP Link Monitoring** field. This was the value used during compliance testing however **Use Session Manager Configuration** option can also be used here.

SIP Entity Details

General

* Name: cppm1

* FQDN or IP Address: 110.10.10.130

Type: Other

Notes: Connectivity to CS1K 7.5 Enterpri

Adaptation:

Location: Belleville, Ont, Ca

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

* Proactive Monitoring Interval (in seconds): 900

Under the **Entity Links** section, add **DevASM** as **SIP Entity 1** and **cppm1** as **SIP Entity 2** with **UDP** and **TCPPProtocol** and **5060** as **Port**.

Click on **Commit** to complete adding the SIP Entity.

Entity Links

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	TCP	* 5060	c ppm1	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	c ppm1	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required

Commit Cancel

1.15. Adding Entity Links

This section explains the adding of Entity Links RightFax server and the Communication Server 1000 system routing. To add Entity Links, select **Entity Links** from the left hand window of the Routing screen and click on **New** (not shown).

Next three screens show the Entity Links for Communication Server 1000 and the RightFax server. For the Communication Server 1000 both TCP and UDP protocols were used.

Enter a descriptive name under the **Name** field. Select **DevASM** under **SIP Entity 1**. Select **cppm1** for Communication Server 1000 and **RightFax** for RightFax server under **SIP Entity 2**. Select the required **Protocol** and enter the **Port** value of **5060**. Click on **Commit** to complete adding an Entity Link.

Home /Elements / Routing / Entity Links

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* DevASM_cppm1_5060	* DevASM	TCP	* 5060	* cppm1	* 5060	Trusted

Home /Elements / Routing / Entity Links

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* DevASM_cppm1_5060	* DevASM	UDP	* 5060	* cppm1	* 5060	Trusted

Home /Elements / Routing / Entity Links

Entity Links

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* RightFax_To_DevS	* DevASM	UDP	* 5060	* RightFax	* 5060	Trusted	For Right Fax

* Input Required

Commit

1.16. Adding Routing Policies

This section explains the Routing Policy configuration for RightFax server and Communication Server 1000 Systems. To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown).

Screen below shows the Routing Policy Details for the RightFax server. Enter a descriptive name in the **Name** field and include some notes in the **Notes** field if required. Leave the rest of the values at default.

Click on the **Select** button and various SIP Entities configured are displayed (not shown). Select the **RightFax** server as the SIP Entity Destination. To add a dial pattern, click on **Add** and various dial patterns that are configured is displayed (not shown). Select the dial pattern that needs to be associated with RightFax server. A dial pattern can be added once it has been configured as explained in **Section 6.7** below. Click on **Commit** to complete adding a routing policy.

Routing Policy Details

General

* Name: RightFax_routing

Disabled: ☐

* Retries: 0

Notes: Routing for RightFax Server

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
RightFax	110.10.5.64	Other	For RightFax Testing

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enat

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

Select : All, None

Dial Patterns

Add Remove

1 Item Refresh Filter: Enat

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
350	5	5	<input type="checkbox"/>	bwvdev.com	-ALL-	Routing for Right Fax server

Screen below shows the Routing Policy Details for the Communication Server 1000 System. Enter a descriptive name in the **Name** field and include some notes in the **Notes** field if required. Leave the rest of the values at default.

Click on the **Select** button and various SIP Entities configured are displayed (not shown). Select the **cppm1** as the SIP Entity Destination. To add a dial pattern, click on **Add** and various dial patterns that are configured is displayed (not shown). Select the dial pattern that needs to be associated with Communication Server 1000.. A dial pattern can be added once it has been configured as explained in **Section 6.7** below. Click on **Commit** to complete adding a routing policy.

Additional routing policies can be configured as required in a similar fashion.

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit

Cancel

General

Name

TO-CS1K75-TOP-System

Disabled

☐

Retries

0

Notes

TO-CS1K75-TOP-System (CPPM1)

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cppm1	110.10.97.130	SIP Trunk	Connectivity to CS1K 7.5 Ent. 1 -top

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Refresh

Filter: Enabled

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

Select : All, None

Dial Patterns

Add

Remove

8 Items

Refresh

Filter: Enabled

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	1613985	11	11	<input type="checkbox"/>	bwvdev.com	-ALL-	Route to CS1K75_TOP as PSTN number
<input type="checkbox"/>	27	3	36	<input type="checkbox"/>	bwvdev.com	Belleville	
<input type="checkbox"/>	58	5	12	<input type="checkbox"/>	bwvdev.com	-ALL-	Dial Pattern for CS1000 Routing

1.17. Adding Dial Patterns

This section explains the steps to add a dial pattern for the RightFax and Communication Server 1000 systems. To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown).

Screen below shows the Dial Pattern Details for the RightFax server. During compliance testing extensions range on RightFax server started with 350xx and therefore **350** are used in the **Pattern** field. The minimum and maximum size of the extension is defined as **5**. Add the **RightFax_routing** policy as configured in **Section 6.6** above. Click on **Commit** to complete adding the dial pattern. Additional dial patterns can be configured as required in a similar fashion.

Routing / Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 350

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bwvdev.com

Notes: Routing for Right Fax server

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh 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-	Any Locations	RightFax_routing	0	<input type="checkbox"/>	RightFax	Routing for RightFax Server

Select : All, None

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:

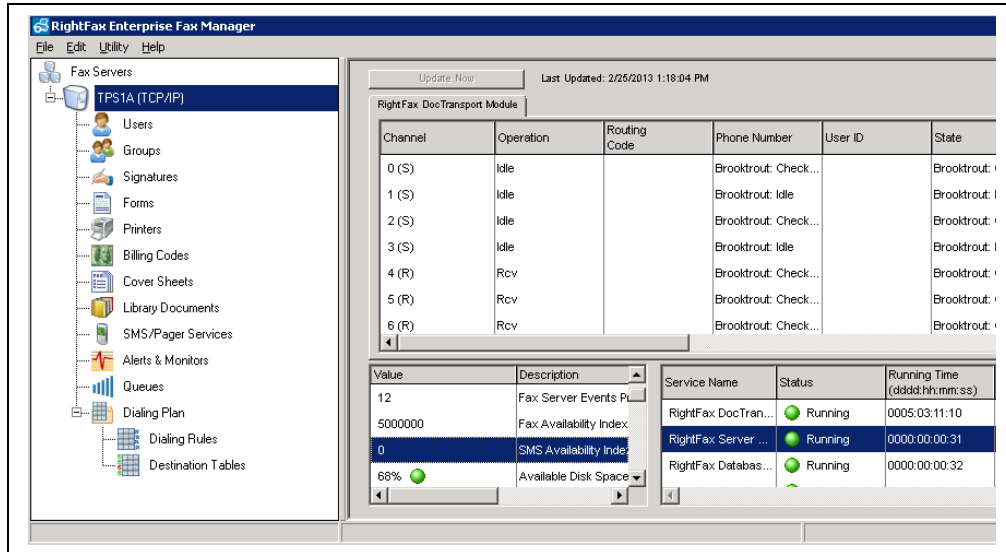
- ◆ Launch RightFax Enterprise Fax Manager and Brooktrout Configuration Tool (Steps 1 – 6)
- ◆ Configure IP stack (Step 7)
- ◆ Configure BTCall parameters (Steps 8 – 9)
- ◆ Configure Call Control parameters (Step 10)
- ◆ Configure SIP IP parameters (Step 11)
- ◆ Configure T.38 parameters (Step 12)
- ◆ Configure RTP parameters (Steps 13 – 14)
- ◆ Administer RightFax dialing rules (Steps 15 – 16)
- ◆ Administer RightFax users (Steps 17 – 20)

The examples shown in this section refer to Site 1 from **Figure 1**.

1.

Launch RightFax Enterprise Fax Manager

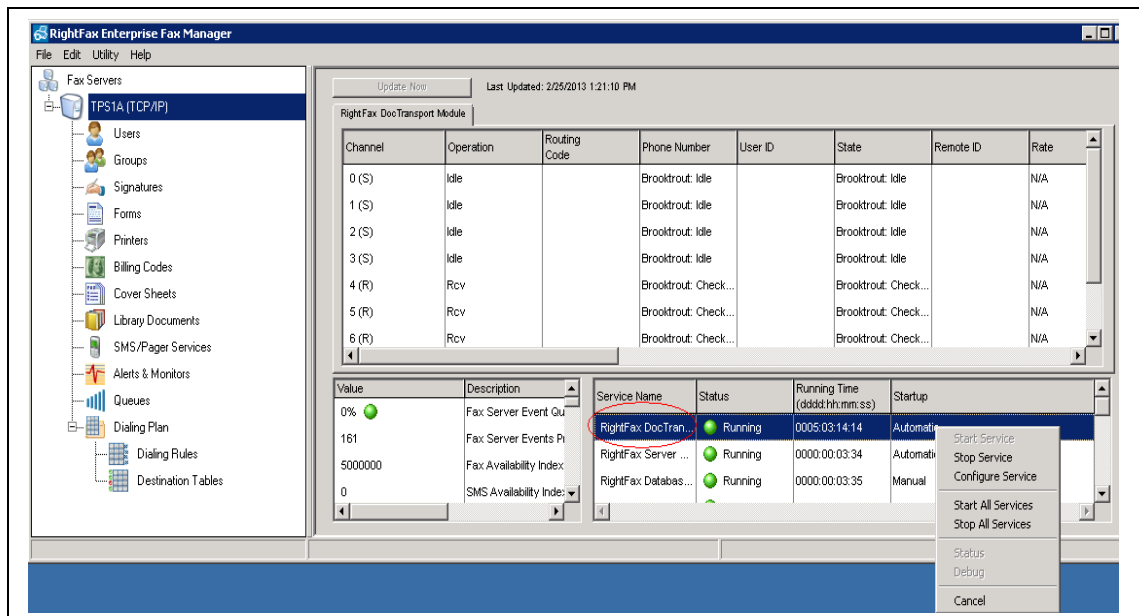
The RightFax configuration is performed using the RightFax Enterprise Fax Manager. Launch the RightFax Enterprise Fax Manager from the Windows Start menu. At the main window, highlight the host name of the fax server (created during the installation process) from the navigation menu in the left pane:



2.

RightFax DocTransport Module

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**.



3.

RightFax DocTransport Module - Continued

In the **DocTransport Configuration** 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
Channel #4
Channel #5
Channel #6
Channel #7

Board module number: [Dropdown]
Number from the rotary switch on the board: [Text]
DID Settings
Number of digits for routing: 4 [Dropdown]

☒ Set Fax ID for all channels: TPS1A [Text]
☐ Set Capability for all channels: Both [Dropdown]

Configure Brooktrout Board
Configure Brooktrout [Button]
Number of SR140 channels: 8 [Dropdown]

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 [Text]
Domain: ExchangeServerDomain [Text]
User Account: ... [Text]
ValidSmtAccount [Text]
Password: [Text]

SQL Connections
Driver={SQL Server};server=WIN-LGYU4RV79VL\RIGHTFAX;database=RightFax ... [Text]

Delete Device [Button] Add Transport [Button] Select Service Account... [Button] OK [Button] Cancel [Button]

4.

Account Access Information

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.

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: TPS1A\administrator

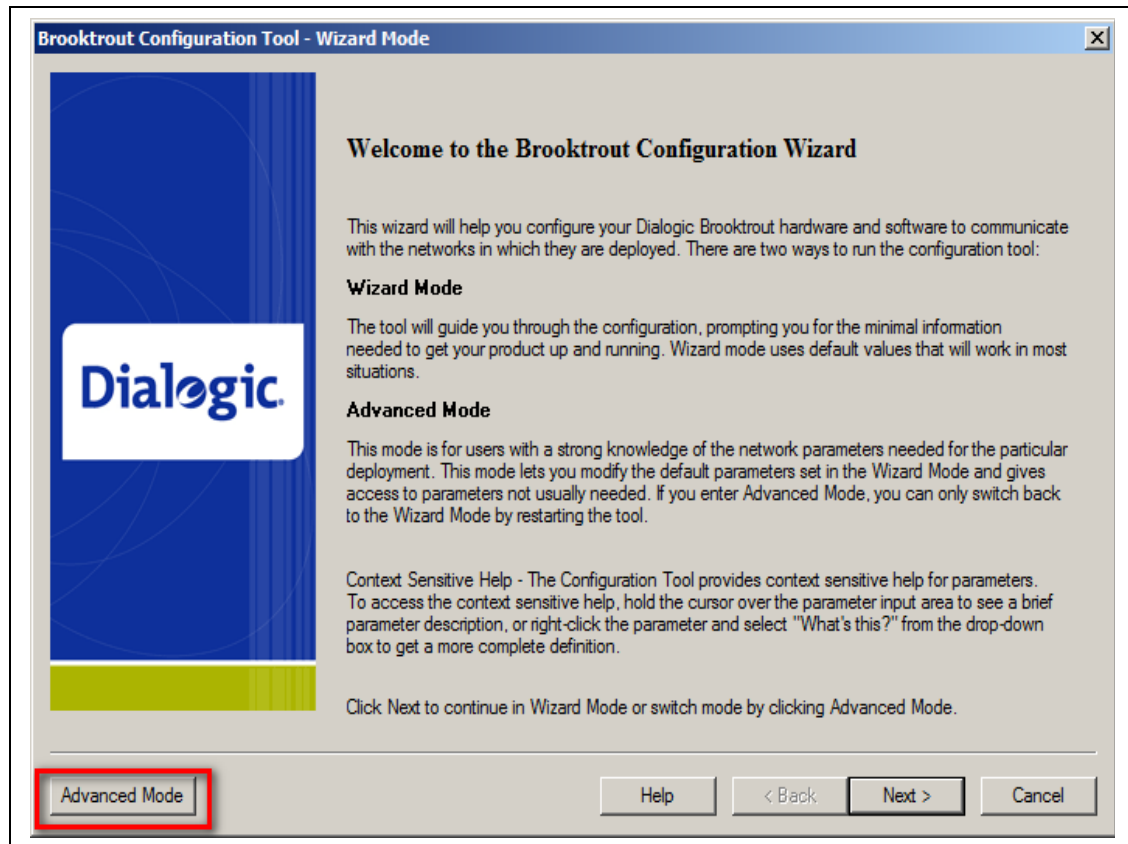
Password: ●●●●●●●●

OK Cancel

5.

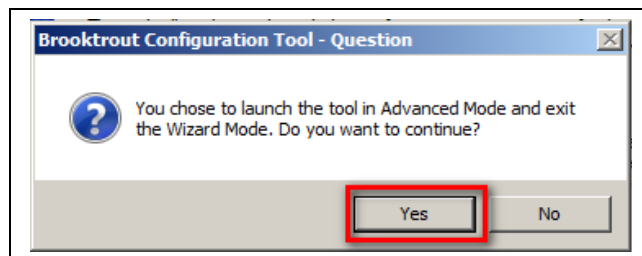
Brooktrout Configuration Tool

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



6.

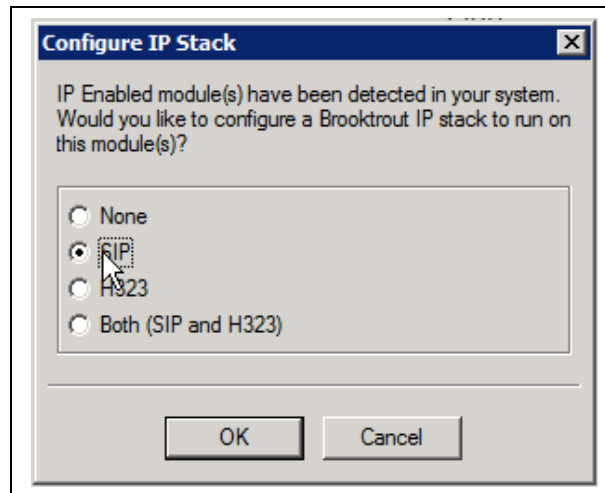
Click **Yes** when prompted to launch the Configuration Tool in Advanced mode.



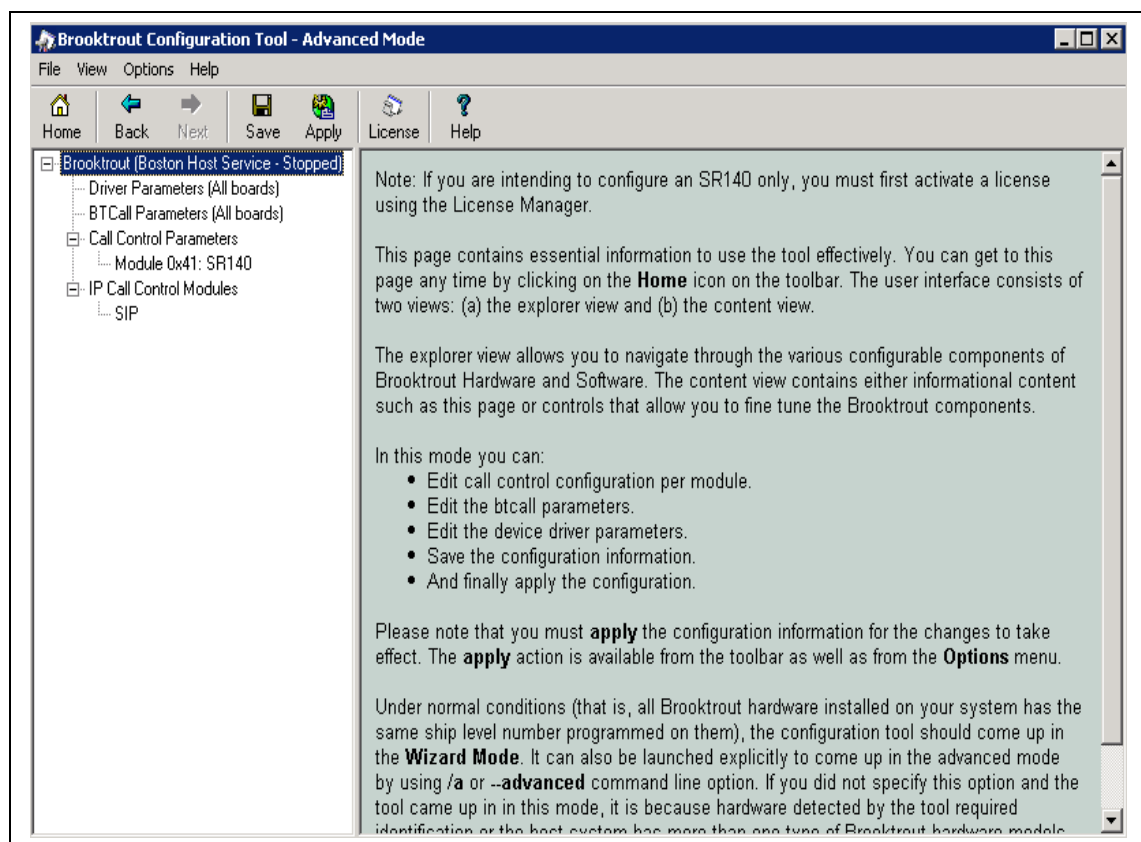
7.

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.

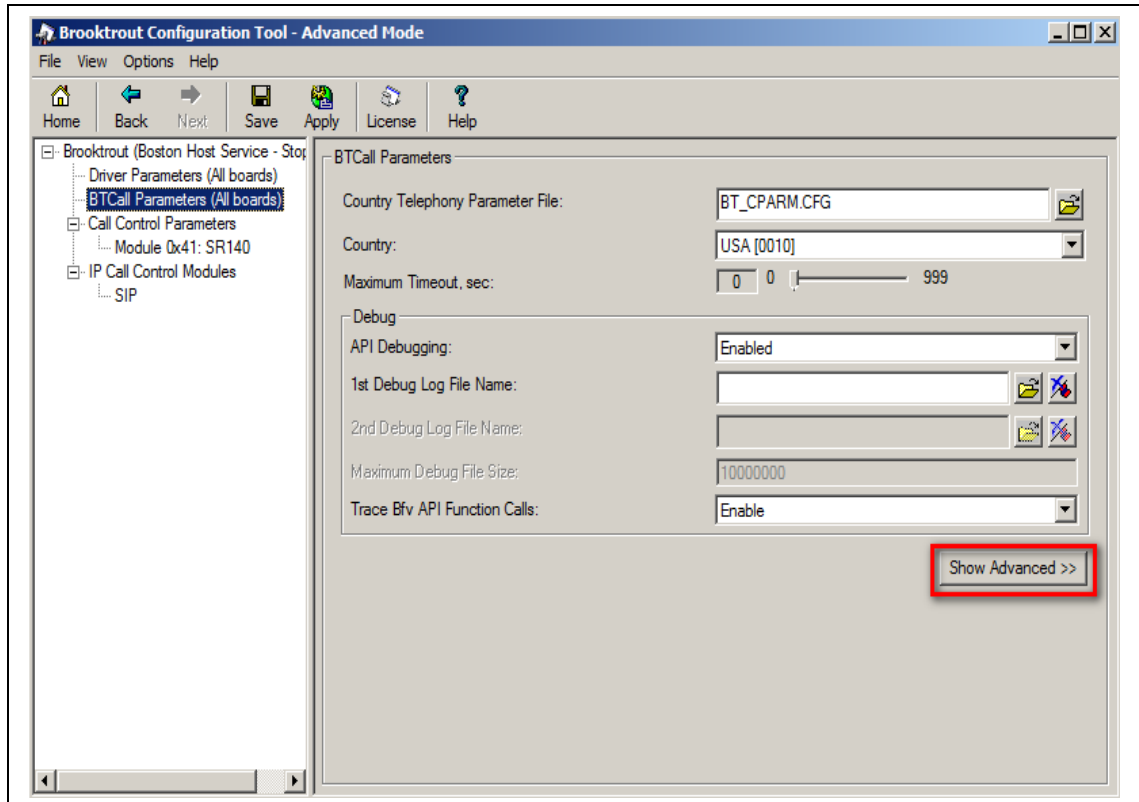


Note that IP Stack can be viewed/reconfigured from the Brooktrout Configuration Tool menu **Options** → **Configure IP Stack**.

8. Configure BtCall Parameters

***Note:** During the compliance testing, the following settings were configured differently than 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.

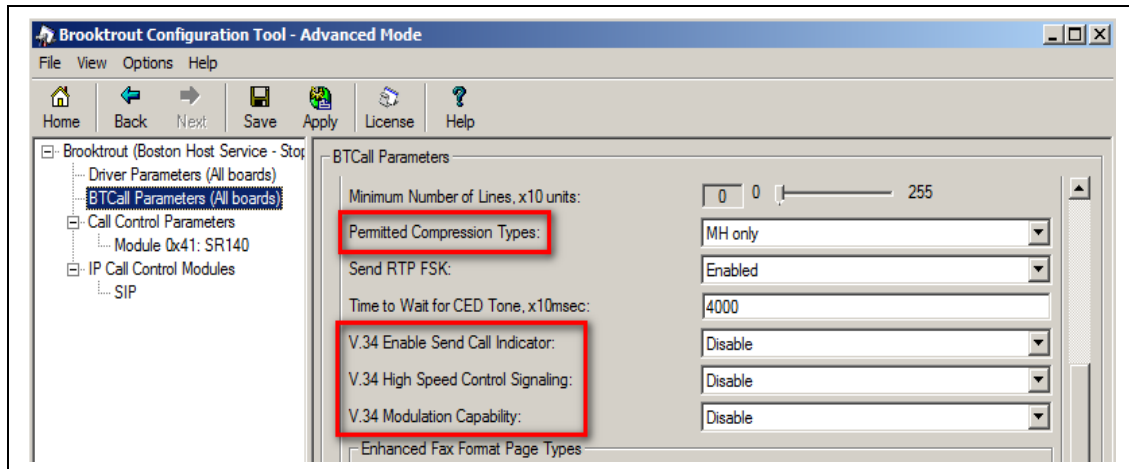
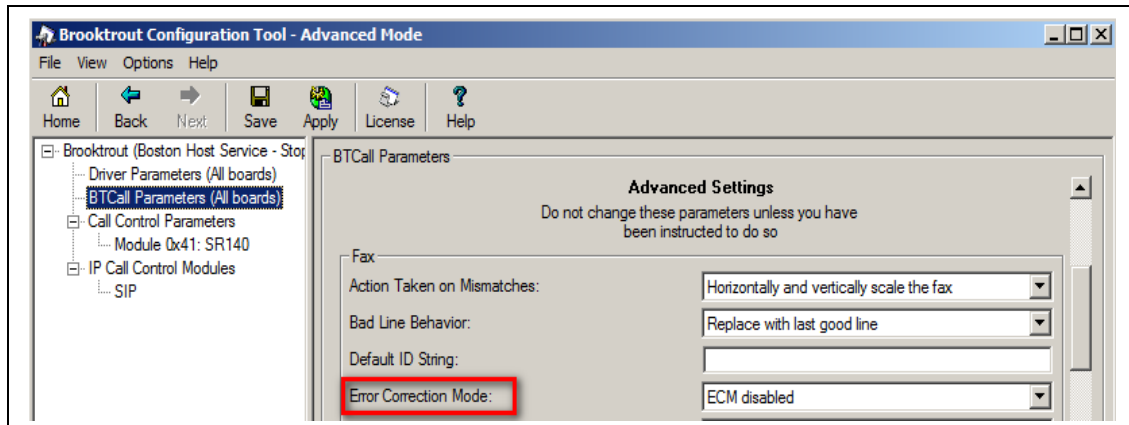


9. Configure BtCall Parameters (continued)

Under Advanced Settings, configure the fields as follows:

- ◆ **Error Correction Mode:** ECM Disabled
- ◆ **Permitted Compression Types:** MH only
- ◆ **V.34 Enable Send Call Indicator:** Disable
- ◆ **V.34 High Speed Control Signaling:** Disable
- ◆ **V.34 Modulation Capability:** Disable

Use default values for other fields.

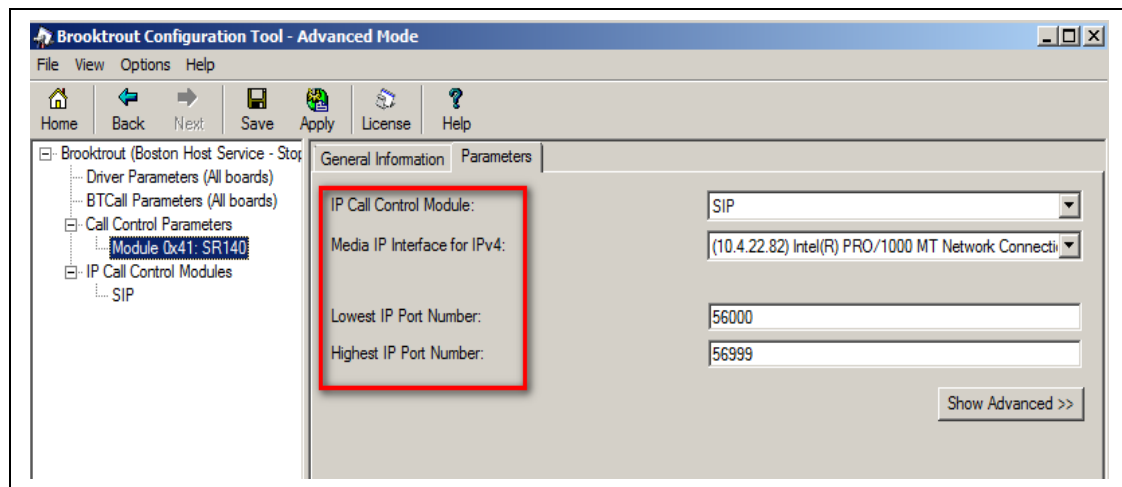


10.

Configure Call Control Parameters

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



11.

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:

- ◆ **From Value** – If required by the Avaya environment, set this to an appropriate *UserInfo@DomainName*. The *DomainName* should be set to the authoritative domain as configured in Session Manager. During compliance testing this value was left at default.
- ◆ **Contact Address** – If required by the Avaya environment, set 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 pane shows the navigation tree with 'SIP' selected under 'IP Call Control Modules'. The right pane shows the 'IP Parameters' tab. The 'From Value' field is highlighted with a red box. The 'Contact IPv4 Address' field is also highlighted with a red box. The 'Username' field is highlighted with a red box. The 'Session Name' field is highlighted with a red box. The 'Session Description' field is highlighted with a red box. The 'Description URI' field is highlighted with a red box. The 'Email Address' field is highlighted with a red box. The 'Phone Number' field is highlighted with a red box. The 'Show Advanced >>' button is visible at the bottom right.

Field	Value
Maximum SIP Sessions:	256
Primary Gateway:	
Primary Proxy Server:	
Additional Proxy Server #2:	
Additional Proxy Server #3:	
Additional Proxy Server #4:	
Primary Registrar Server URL:	
Additional Registrar Server #2:	
Additional Registrar Server #3:	
Additional Registrar Server #4:	
From Value:	Anonymous <sip.no_from_info@anonymous.invalid>
Contact IPv4 Address:	0 . 0 . 0 . 0 :0
Username:	-
Session Name:	no_session_name
Session Description:	
Description URI:	
Email Address:	
Phone Number:	

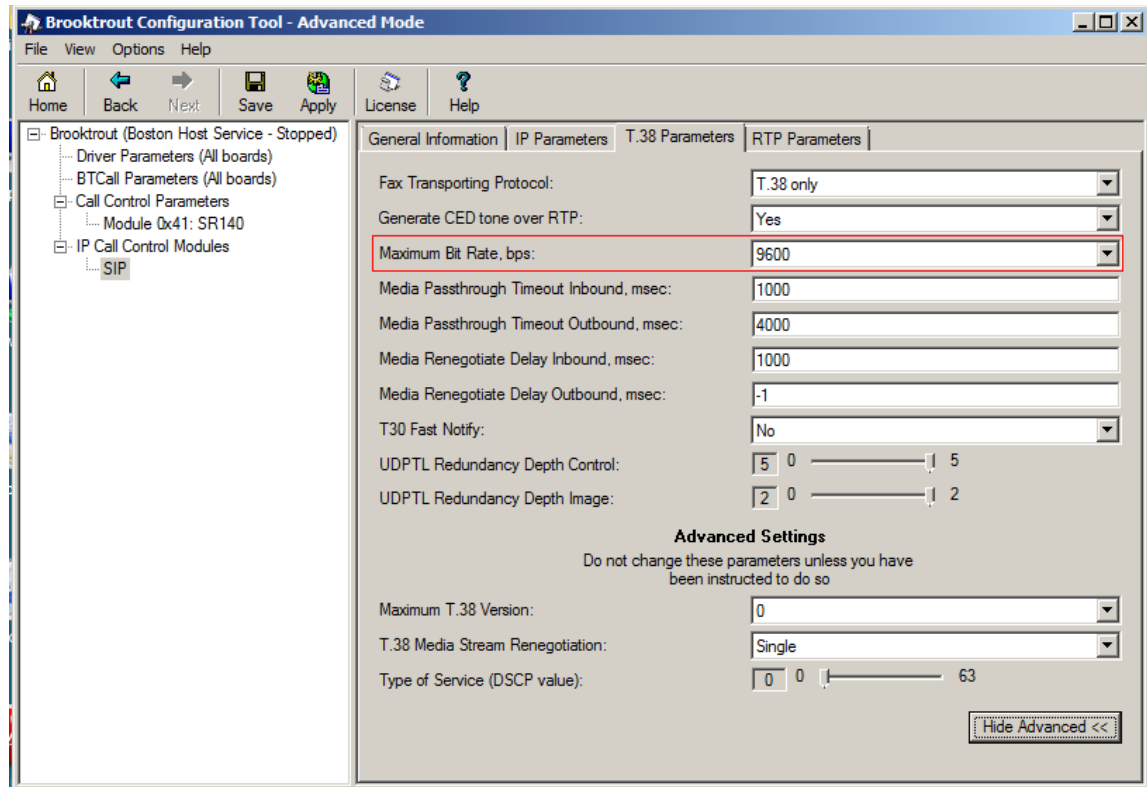
12.

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 differently than the default settings. In practice, these settings may not be required for full functionality.*

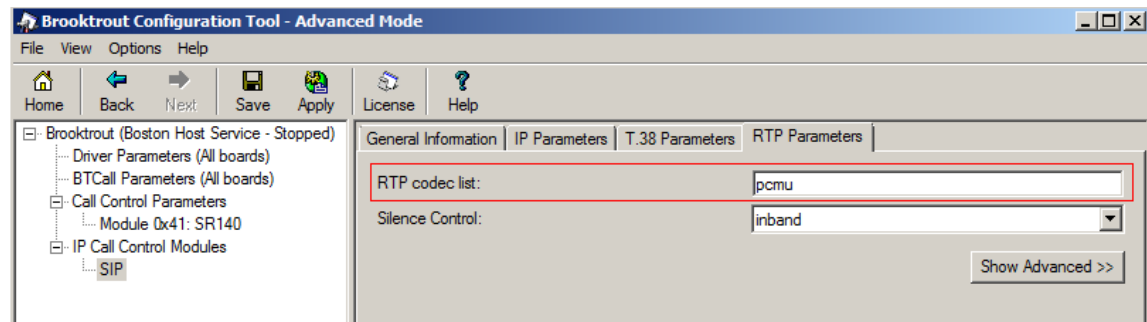
- ◆ “Maximum Bit Rate, bps” is set to maximum, 9600 (default is 14400).



13.

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.



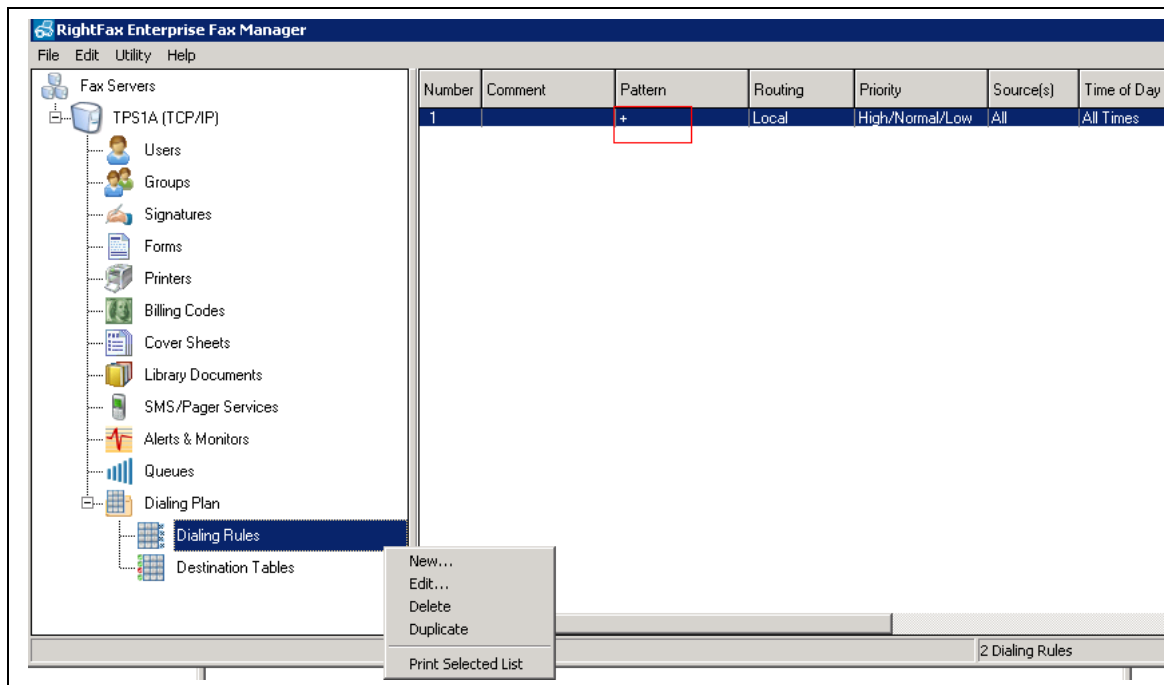
14.	<p>Complete Brooktrout SR140 Configuration</p> <p>After verifying all the above parameters are properly set, click Save in the button menu (not shown).</p> <p>Exit the Brooktrout Configuration Tool.</p> <p>In the DocTransport Configuration screen, click the OK button (See screen shot in Step 3 above).</p> <p>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 Step 2 above).</p>
-----	---

15. Configure Dialing Rules

Dialing Rules are used by RightFax to route calls. In the compliance test, a dialing rule was created to route outbound fax calls to the Session Manager.

In the left navigation menu under the host name of the fax server, navigate to **Dialing Plan**, right-click **Dialing Rules** and select **New** to create a new rule.

The example below shows the single rule created for the compliance test at site 1. The + in the **Pattern** field indicates that this rule applies to all dialed numbers. To view the details, double click on the rule in the right pane.



16.

Configure Dialing Rules - Continued

The **Rule Edit** window will appear as shown below. The **Number Adjustments** tab shows the digit string manipulation that is done to each dialed number. In the example below, each outbound fax phone number is appended with **@110.10.10.198** as indicated in the **Append this** field. This IP address is for the Session Manager server at Site 1.

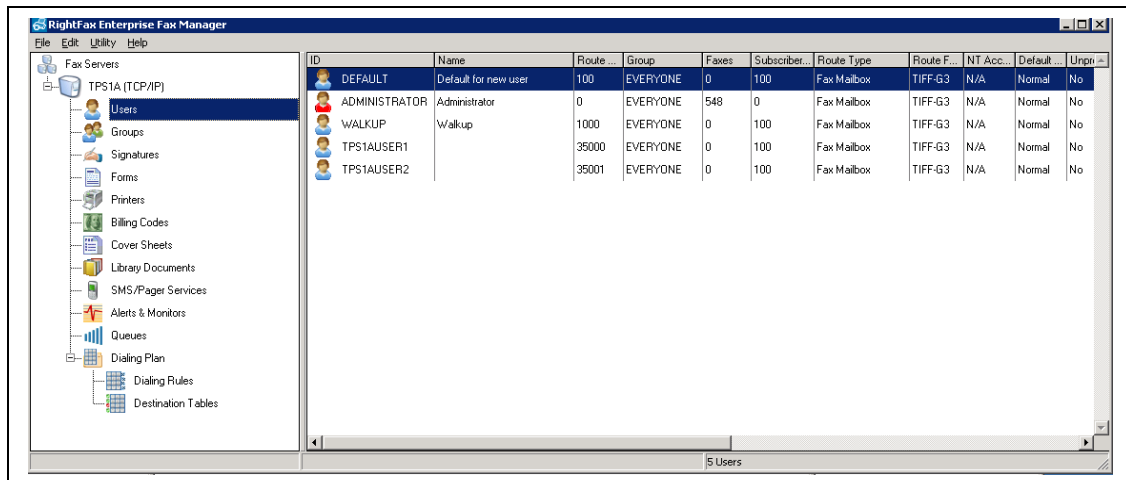
The screenshot shows the 'Rule Edit' window with the 'Number Adjustments' tab selected. The 'Pattern' field contains a plus sign (+). Below it, a legend explains the symbols: '+' matches zero or more digits (must be at end), '~' matches zero or one digit, '?' matches exactly one digit, and '%[tbl#]' matches digits against a destination table. The 'Priorities' section has three checked options: 'Applies to High priority faxes', 'Applies to Normal priority faxes', and 'Applies to Low priority faxes'. The 'Fax Traffic Type' section has four radio buttons, with 'Rule applies to all traffic' selected. The 'Other' section has two spinners: 'Minimum Queue Depth (in pages)' set to 0 and 'Minimum Fax Size (in pages)' set to 0. 'OK' and 'Cancel' buttons are at the bottom right.

This screenshot shows the 'Rule Edit' window with the 'Number Adjustments' tab selected. The 'Strip beginning digits' spinner is set to 0. The 'Prepend this' field is empty. The 'Strip ending digits' spinner is set to 0. The 'Append this' field contains '@110.10.10.198' and is highlighted with a red rectangle. 'OK' and 'Cancel' buttons are at the bottom right.

17.

Configure 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 five users. To view the details of a user, double-click on the user entry in the right pane.



18.

Configure Users – Identification

The **User Edit** window will appear as shown below. Select the **Identification** tab. The example below shows the settings used for the compliance test at Site 1. The **User ID** field is set to a descriptive name. Appropriate values should be entered or selected for other fields.

The screenshot shows the 'User Edit' window with the 'Identification' tab selected. The 'User ID' field is highlighted with a red box and contains the text 'TPS1AUSER1'. Below it is a checkbox for 'Use Integrated Windows NT Security?' which is unchecked, and a 'Select NT Account' button. The 'User Name' field is empty. The 'Password' field is empty, with a 'Change Password' button to its right. The 'Distinguished Name' field is empty. The 'Group ID' dropdown menu is set to 'EVERYONE'. The 'Voice Mail Subscriber ID' field contains the number '100'. The 'E-mail address' and 'SMS/Mobile Address' fields are empty. At the bottom left is a 'Compute Disk Usage' button, and to its right is the text 'May take several seconds on a server with many faxes'. The 'OK' and 'Cancel' buttons are at the bottom right.

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

User ID:

☐ Use Integrated Windows NT Security?

User Name:

Password:

Distinguished Name:

Group ID:

Voice Mail Subscriber ID:

E-mail address:

SMS/Mobile Address:

May take several seconds on a server with many faxes

19.

Configure Users – Inbound Routing

On the **Inbound Routing** tab, the **Routing Code** field is set to the fax number of the recipient. In the case of the compliance test, this was extension **35000** for Site 1 as shown below. Default values may be used for all other fields.

The screenshot shows the 'User Edit' dialog box with the 'Inbound Routing' tab selected. The 'Routing Code (DID/DNIS number):' field is highlighted with a red box and contains the value '35000'. Below it, the 'Routing Type:' dropdown is set to 'Fax Mailbox', and the 'File Format:' dropdown is set to 'TIFF (G3-1D)'. The 'Routing Info:' field is empty. Below that, the 'Received Fax Routing Form:' dropdown is set to 'Advanced Outlook Form'. At the bottom, there is a checkbox labeled 'Delete after routing?' which is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

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

Routing Code (DID/DNIS number):
35000

Routing Type:
Fax Mailbox

File Format:
TIFF (G3-1D)

Routing Info:

When routing to a Fax Mailbox, no additional information is necessary. If notifications occur through e-mail, the e-mail address should be specified in the Routing Info field.

Received Fax Routing Form:
Advanced Outlook Form

☐ Delete after routing?

OK Cancel

20.

Configure Users – Outbound Settings

The **Default Outbound Settings** tab configures various outbound fax call settings. Configure these settings as appropriate.

The image shows a 'User Edit' dialog box with a tabbed interface. The 'Default Outbound Settings' tab is selected. The dialog contains the following elements:

- Default Fax Resolution:** A dropdown menu set to 'Fine (200 x 200)'.
- Default Priority:** A dropdown menu set to 'Normal'.
- Auto-Delete Setting:** A dropdown menu set to 'Never'.
- Use Smart-Resume?** An unchecked checkbox.
- Cover Sheet Defaults:** A section containing:
 - Send Cover Sheets?** A checked checkbox.
 - Cover Sheet Model:** A dropdown menu set to '{System Default}'.
 - Cover Sheet Resolution:** A dropdown menu set to 'Fine (200 x 200)'.
- Private Fax Number:** A text input field.
- General Fax Number:** A text input field.
- General Voice Number:** A text input field.
- From Name:** A text input field.
- Voice Number:** A text input field.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Verification Steps

The following steps may be used to verify the configuration:

- ◆ From Communication Server 1000 command line (CLI) use **LD 32** to find the status of the trunks for both SIP (Site 1) and ISDN (between Site 1 and 2) are up and in service.
- ◆ From Communication Server 1000 CLI use **LD 96** to check the status of D-channel (DCH) for both the SIP and ISDN configured and make sure they are active and in service with no alarms.
- ◆ Verify that fax calls can be placed to/from OpenText RightFax server to an analog fax machine at both Sites 1 and 2.
- ◆ From Communication Server 1000 CLI use **LD 96** to capture DCH messages and verify that the fax calls are routed through the correct DCH and trunks.
- ◆ From System Manager, confirm that the Entity Link between Session Manager and the OpenText RightFax server is in service.

Conclusion

These Application Notes describe the procedures required to configure OpenText RightFax to interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager. OpenText RightFax successfully passed compliance testing.

Additional References

- ◆ *Software Input Output Reference — Administration Avaya Communication Server 1000 7.5 NN43001-611, Standard 05.13 September 2012.*
- ◆ *Element Manager System Reference – Administration Avaya Communication Server 1000 7.5 NN43001-632, Standard 05.15 August 2012.*
- ◆ *Unified Communications Management Common Services Fundamentals Avaya Communication Server 1000 7.5 NN43001-116, 05.17 January 2012.*
- ◆ *ISDN Primary Rate Interface Installation and Commissioning Avaya Communication Server 1000 7.5 NN43001-301, 05.08 February 2012.*
- ◆ *Administering Avaya Aura® Session Manager, Doc # 03-603324, Release 6.2, July, 2012.*
- ◆ *Administering Avaya Aura® System Manager, Release 6.2, Issue 2.0, July 2012*
- ◆ *OpenText RightFax 10.5 Administrator's Guide, July, 2012.*
- ◆ *OpenText RightFax 10.5 Installation Guide, June, 2012.*

Documentation for:

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

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

©2013 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.