



Application Notes for configuring Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 with Kofax Communication Server from Kofax Ltd. using a SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Kofax Communication Server to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0. Kofax Communication Server communicates with Avaya Aura® Session Manager via a SIP trunk. This document provides configuration steps related to faxing capabilities of Kofax Communication Server.

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

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

1. Introduction

These Application Notes describe the configuration used to enable Kofax Communication Server, from Kofax Ltd., to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0. Kofax Communication Server offers a variety of telephony features. Kofax Communication Server fax features allow fax messages to be sent/received to/from both local and PSTN fax endpoints, and can subsequently be printed or archived. During compliance testing the fax feature and functionality was the sole focus.

2. General Test Approach and Test results

The general test approach was to simulate the configuration as implemented on a customer premises. Compliance testing was between the Kofax Communication Server (Kofax Server) and Avaya Aura® Session Manager (Session Manager), and was performed manually. The tests were all functional in nature, and no performance testing was done. The test method employed can be described as follows, Communication Manager was configured to support various local IP (H.323) telephones and an analogue Fax Machine, as well as a SIP connection to Session Manager. Session Manager was configured to connect to both Communication Manager and Kofax Communication Server via SIP trunks.

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 following tests were performed as part of the compliance testing:

- Basic fax sending in T.38 ECM mode and pass-through connection with G.711A and G.711MU codecs
- Basic fax receiving in T.38 ECM mode and pass-through connection with G.711A and G.711MU codecs
- Forwarding of a fax from a local Fax Machine to the Kofax Server via a local extension
- Forwarding of a fax from the Kofax Server to a local Fax Machine via a local extension
- Supervised and Blind transfer of a fax from a local Fax Machine to the Kofax Server via a local extension (pass-through mode only)
- Supervised and Blind transfer of a fax from the Kofax Server to a local Fax Machine via a local extension (pass-through mode only)
- Verification of correct status and Caller ID for sent and received fax messages
- Verification that Message Waiting Indication is sent to the correct phone extensions when faxes are received and subsequently turned off when the fax is accessed
- Successful recovery from network or power failure

2.2. Test Results

Tests were performed to insure full interoperability of a Kofax Communication Server when configured for SIP (using Session Manager). The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

Support for Kofax Ltd. is available at: <http://www.kofax.com/support/>

3. Reference Configuration

Figure 1 illustrates the network configuration used during compliance testing. A SIP trunk was configured between the Kofax Communication Server (using UDP) and the Session Manager SIP Signaling interface. A SIP trunk was also configured between Communication Manager and Session Manager (using TCP). An analogue Fax Machine was connected to an MM714 Analog card on the G430 Media Gateway. An Avaya 9620 (H323) telephone was also configured on the communication Manager so as to test faxes sent to phone extensions which had Call Forward enabled and also to transfer faxes to alternative Fax Machines, including to the Kofax Communication Server. An Avaya Aura® System Manager was used to manage the Session Manager.

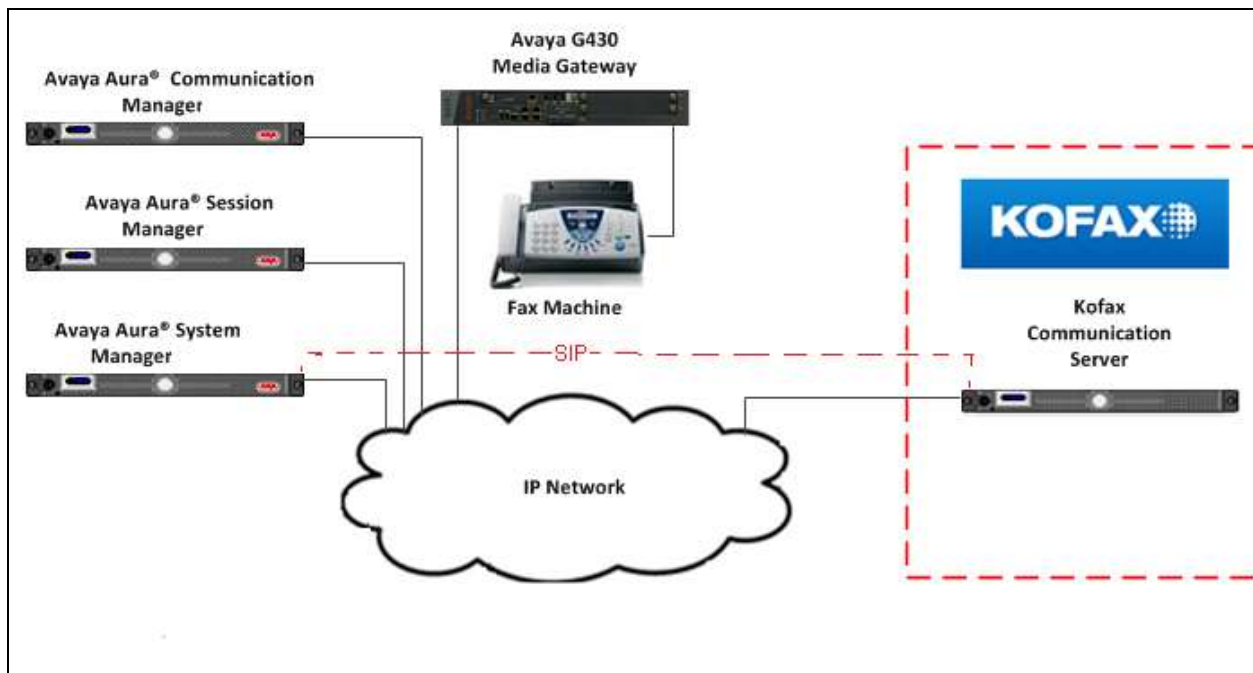


Figure 1: Avaya and Kofax Reference Configuration

4. Equipment and Software Validated

The hardware and associated software used in the compliance testing is listed below.

Avaya Equipment	Software Version
Avaya Aura® Communication Manager	R7.0 Build R017x.00.0.441.0 Update: 00.0.441.0-22856
Avaya Aura® Session Manager	R7.0.0.1.700102
Avaya Aura® System Manager	R7.0.0.1 Build 7.0.0.0.16266-7.0.9.7001011 Update 7.0.0.1.4212
Avaya G430 Media Gateway Module MM714 (ANA)	Version 37.20.0 Version HW03 FW073
Kofax Equipment	Software Version
Kofax Communication Server KCS FoIP Application	Version 10.0.1 Version 3.24.22

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (**Note:** during Compliance Testing all inputs not highlighted in bold were left as default).

- Configure Session Manager Node
- Configure Signaling-Group (for information only)
- Configure Trunk Group (for information only)
- Configure Fax Station
- Configure Codecs

5.1. Configure Session Manager Node

For Communication Manager to communicate with Session Manager a node must be configured. The screen shot below shows **SM71676** with IP address **10.10.16.77** was used.

Note: 10.10.16.77 IP address of the Session Manager SIP Signaling interface.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AES63RP	10.10.60.210	
SM71676	10.10.16.77	
default	0.0.0.0	
procr	10.10.16.211	
procr6	::	

5.2. Configure Signaling Group

A signaling group is required before a trunk-group can be configured. Use the **add signaling-group** command followed by next available signaling-group number to configure the following:

- **Group Type:** Enter **SIP**
- **Transport Method** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **SM71676** (Session Manager Node as configured in **Section 5.1**)
- **Far-end Network Region:** Enter the appropriate Network Region (i.e. 1)
- **Far End Domain:** Enter the appropriate Domain

When the configuration is complete, press **F3** to save.

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? 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		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM71676	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain: devconnect.local		
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

5.3. Configure Trunk Group

This section describes the Trunk Group configuration used during compliance testing. Use the **add trunk-group** command followed by next available Group number and configure the following:

- **Group Type:** Enter **sip**
- **Group Name:** Enter an informative name for the trunk (i.e. **To SM7.0 SIP**)
- **TAC** Enter a TAC number (i.e. **701**)
- **Service Type:** Enter **public-ntwrk**
- **Signaling Group:** Enter the Signaling Group number as configured in **Section 5.2**
- **Number of Members:** Enter the number of channels required to connect to the Session Manger (during compliance testing 30 channels were used)

Page 1

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: To SM7.0 SIP	COR: 1	TN: 1	TAC: 701
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 30		

Go to **Page 3** and enter **private** for **Numbering format**. When the configuration is complete, press **F3** to save.

display trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UII Treatment: service-provider	
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

5.4. Configure Fax Station

The Fax Machine is configured as an analog station **Type 2500** on Communication Manager and the **Extension** number used was **8270501**. The port used was an available port on a MM714 card on the G430 Media Gateway. Use the **add station** command to add the Fax Machine. The screen shots below show the configuration used during compliance testing. When the configuration is complete, press **F3** to save.

Page 1

add station 8270501		Page 1 of 4
STATION		
Extension: 1026	Lock Messages? n	BCC: 0
Type: 2500	Security Code: 1026	TN: 1
Port: 002V301	Coverage Path 1:	COR: 1
Name: Fax Machine 1026	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
XOIP Endpoint type: auto	Time of Day Lock Table:	
Loss Group: 1	Message Waiting Indicator: none	
Off Premises Station? n		
Survivable COR: internal		
Survivable Trunk Dest? y	Remote Office Phone? n	
Passive Signalling Station? N		

Page 2

add station 8270501	Page 2 of 4
STATION	
FEATURE OPTIONS	
LWC Reception: spe	
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Call Waiting Indication: y
Per Button Ring Control? n	Att. Call Waiting Indication: y
Bridged Call Alerting? n	Distinctive Audible Alert? y
Switchhook Flash? y	Adjunct Supervision? y
Ignore Rotary Digits? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	
Multimedia Mode: basic	Audible Message Waiting? n
MWI Served User Type:	
AUDIX Name:	
	Coverage After Forwarding? s
	Multimedia Early Answer? n
	Direct IP-IP Audio Connections? Y
Emergency Location Ext: 1026	IP Audio Hairpinning? n

Page 3

add station 8270501	Page 3 of 4
STATION	
Bridged Appearance Origination Restriction? n	
ENHANCED CALL FORWARDING	
Forwarded Destination	Active
Unconditional For Internal Calls To:	n
External Calls To:	n
Busy For Internal Calls To:	n
External Calls To:	n
No Reply For Internal Calls To:	n
External Calls To:	n
SAC/CF Override: n	

Page 4

add station 8270501		Page 4 of 4
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
HOT LINE DESTINATION		
Abbreviated Dialing List Number (From above 1, 2 or 3):		
Dial Code:		
Line Appearance: call-appr		

5.5. Configure Codecs

During compliance testing T.38 Fax was used. If using Pass-through Fax configuration see **Appendix A**. To configure T.38 Fax, use the **change ip-codec-set x** command where x is the ip-codec-set being used. Configure the following on page 1:

- **Audio Codec (line 1)** Enter **G.711MU**
- **Silence Suppression** Enter **n**
- **Frames Per Pkt** Enter **2**
- **Audio Codec (line 2)** Enter **G.711A**
- **Silence Suppression** Enter **n**
- **Frames Per Pkt** Enter **2**
- **Media Encryption** Enter **None** (note: the Media Encryption option is only displayed if Media Encryption Over IP is enabled on the installed license)

Note: The max baud rate is 9600 bits per second.

Page 1

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

                                IP CODEC SET

Codec Set: 1

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

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

On **Page 2** configure the following:

- **Fax** Enter **t.38-standard**
- **ECM** Enter **y**

All other inputs may be left at default. When the configuration is complete, press **F3** to save.

Page 2

change ip-codec-set 1		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	Packet Size (ms)
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Alternatively if using Pass-through Fax configuration see **Appendix A**.

6. Configuring Avaya Aura® Session Manager

A number of configurations are required to enable the Session Manager to route faxes between Communication Manager and the Kofax Communication Server. All configurations of Session Manager are performed using System Manager. The configuration operations described in this section can be summarized as follows:

- Logging on to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Locations
- Create Kofax Communication Server as a SIP Entity
- Create an Entity Link for Kofax Communication Server
- Create a Routing Policy Kofax Communication Server
- Create a Dial Pattern for Kofax Communication Server

Note: See **Appendix B** for a screen shot of the Entity Link used between Session Manager and Communication Manager.

6.1. Logging on to Avaya Aura® System Manager

Log on by accessing the browser-based GUI of System Manager, using the URL

“http://<fqdn>/SMGR” or “http://<ip-address>/SMGR”, where:

“<fqdn>” is the fully qualified domain name of the Avaya Aura® System Manager or the “<ipaddress>” is the IP address of Avaya Aura® System Manager.

Once the System Manager web page opens log in with the appropriate credentials and click on the **Log on** button.

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

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

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

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

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

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.

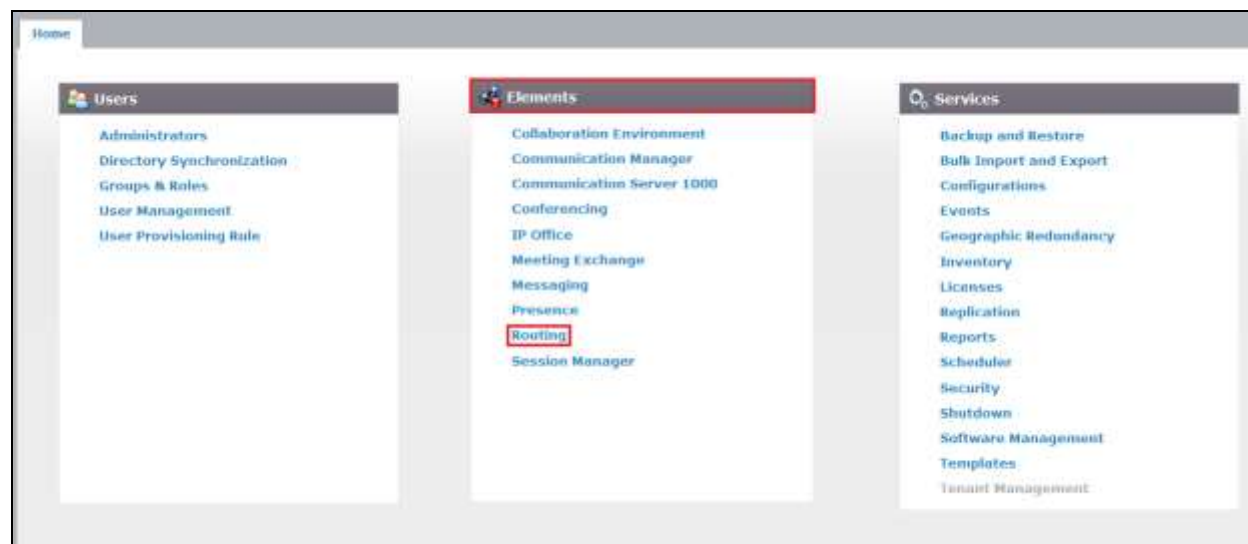
User ID:
Password:

Log On Cancel [Change Password](#)

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

6.2. Administer SIP Domain

Once logged in, select **Routing** from under the **Elements** column.



Select **Domains** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter the domain of the enterprise (i.e. **devconnect.local**) and select **sip** from the dropdown box. Click **Commit** to save changes.

The screenshot shows the 'Domain Management' page. On the left, a sidebar menu has 'Domains' highlighted. The main area shows a table with one item. The 'Name' field contains 'devconnect.local' and the 'Type' dropdown is set to 'sip'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	Type	Notes
* devconnect.local	sip	

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. Select **Locations** on the left panel menu and then click on the **New** button (not shown). In the **Name** field enter an informative name for the location (i.e. **DevConnectRP**). During compliance testing, all other fields were left at default values.

The screenshot shows the 'Location Details' page. On the left, a sidebar menu has 'Locations' highlighted. The main area shows the 'General' tab. The 'Name' field contains 'DevConnectRP'. There are 'Commit' and 'Cancel' buttons at the top right. Below the 'Name' field, there is a 'Notes' field, a 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox, a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' dropdown.

Name: DevConnectRP

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used during compliance testing.

Location Pattern

Add Remove

2 Items Filter: Enable

IP Address Pattern	Notes
10.10.10.	

Select : All, None

Commit Cancel

6.4. Create Kofax Communication Server as a SIP Entity

A SIP Entity must be added for the Kofax Server. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown).

Note: A SIP Entity was already configured for the Communication Manager and was called **CM63**.

Enter the following for the ApplianX SIP Entity:

Under **General** enter the following:

- **Name** Enter an informative name (e.g., **Kofax**)
- **FQDN or IP Address** Enter the IP address of the of the Kofax Server
- **Type** Select **SIP Trunk** from the dropdown box
- **Location** Select the location from the dropdown box that was configured in **Section 6.3**
- **Time Zone** Select Time zone for this location from the dropdown box
- **SIP Timer** Enter **4**

Once the correct information is entered click the **Commit** button.

Note: During compliance testing **Adaptation** was left blank.

Home Routing SIP Entities

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: Kofax

FQDN or IP Address: 10.10.60.56

Type: SIP Trunk

Notes: Trunk to Kofax

Adaptation:

Location: DevConnectRP

Time Zone: America/Fortaleza

SIP Timer B/F (In seconds): 4

Credential name:

Call Detail Recording: egress

Commit Cancel

6.5. Create an Entity Link for Kofax Communication Server

The SIP trunk between Session Manager and the Kofax Server requires an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown) Enter the following:

- **Name** An informative name, (e.g. **Kofax Link**)
- **SIP Entity 1** Select **SM63** from the **SIP Entity 1** dropdown box
- **Protocol** Select **UDP** from the Protocol drop down box
- **Port** Enter **5060**
- **SIP Entity 2** Select **Kofax** from the **SIP Entity 2** dropdown box (configured in **Section 6.4**)
- **Port** Enter **5060** as the Port
- **Connection Policy** Select **trusted** from the dropdown box

Click **Commit** to save changes. The following screen shows the Entity Links used.

The screenshot shows the 'Entity Links' configuration page. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / Entity Links. Below this, there is a 'Commit' button and a 'Cancel' button. A table titled 'Entity Links' shows one item, 'Kofax Link', which is highlighted with a red box. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The values for the 'Kofax Link' row are: Name: Kofax Link, SIP Entity 1: SM63, Protocol: UDP, Port: 5060, SIP Entity 2: Kofax, DNS Override: (empty), Port: 5060, Connection Policy: trusted, Deny New Service: (empty), and Notes: (empty). Below the table, there is a 'Select' dropdown menu with the value 'All/None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
Kofax Link	SM63	UDP	5060	Kofax		5060	trusted		

6.6. Create a Routing Policy for Kofax Communication Server

Create routing policies to direct calls to the Kofax Server via Session Manager. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). In **Routing Policy Details** enter an informative name in the **Name** field (example, **To Kofax**) and enter **0** in the **Retries** field. At **SIP Entity as Destination**, click the **Select** button. A Routing Policy was also configured to direct calls to Communication Manager, but is outside the scope of these Application Notes.

Name	FQDN or IP Address	Type	Notes
Kofax	10.10.60.56	SIP Trunk	Trunk to Kofax

Once the **SIP Entity** List screen opens, check the **Kofax** radio button. Click on the **Select** button to confirm the chosen options and then return to the **Routing Policies Details** screen and select the **Commit** button (not shown) to save.

Name	FQDN or IP Address	Type	Notes
Kofax	10.10.60.56	SIP Trunk	Trunk to Kofax
AACSCMSIP	10.10.16.216	SIP Trunk	

6.7. Create a Dial Pattern for Kofax Communication Server

A dial pattern must be created on Session Manager to route calls to and from the Kofax Server. During compliance testing a number of dial patterns were used. The example below shows **1**. To configure the Dial Pattern to route calls to the Kofax Server, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown). A Dial Pattern was also configured to route calls to Communication Manager, but is outside the scope of these Application Notes.

Under **General** enter out the following:

- **Pattern** Enter **1**
- **Min** Enter **4** as the minimum length of dialed number
- **Max** Enter **4** as the maximum length of dialed number
- **SIP Domain** Select **All** from the drop down box

Click the **Add** button in **Originating Locations and Routing Policies**.

The screenshot displays the 'Dial Pattern Details' configuration page in the Session Manager web interface. The left sidebar shows the 'Routing' menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'General' tab. The 'Pattern' field is set to '1', 'Min' is '4', and 'Max' is '4'. The 'SIP Domain' dropdown is set to 'devconnect.local'. The 'Originating Locations and Routing Policies' section at the bottom has an 'Add' button highlighted with a red box. The 'Add' button is located next to the 'Remove' button and the '1 Item' indicator.

In **Originating Location** check the **DevConnectRP** check box. Under **Routing Policies** check the **To Kofax** check box. Click on the **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save not shown.

The screenshot displays the Avaya SIP Gateway configuration interface. The left sidebar shows a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Dial Patterns'. It features a 'Select' button and a 'Cancel' button. Below this, the 'Originating Location' section includes a checkbox for 'Apply The Selected Routing Policies to All Originating Locations'. A table lists one item, 'DevConnectRP', with a checked checkbox. The 'Routing Policies' section lists 13 items, including 'To IP office' and 'To Kofax', with checkboxes for each. The 'To Kofax' checkbox is checked.

Name	Disabled	Destination	Notes
To IP office	<input type="checkbox"/>	IP Office	
To Kofax	<input checked="" type="checkbox"/>	Kofax	

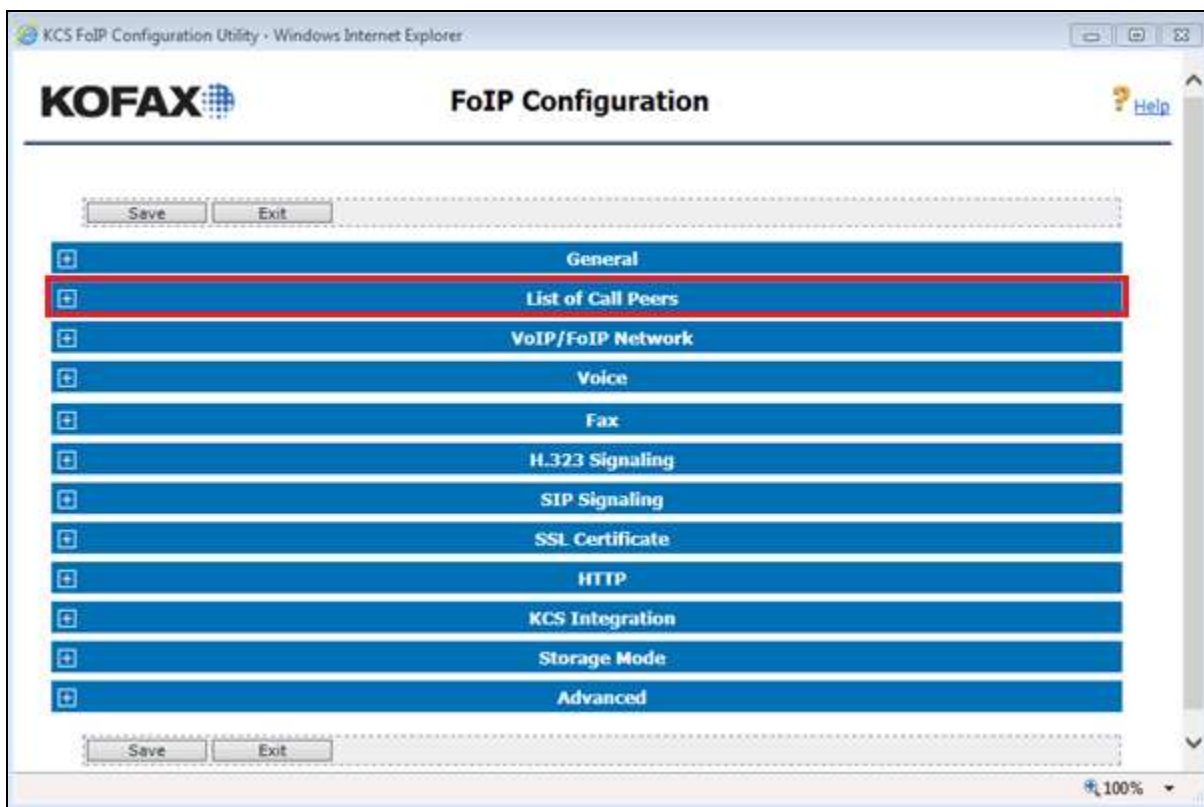
7. Configure Kofax Communication Server

The Kofax Server is provided, installed and implemented by Kofax. Only those configuration details concerning the interface to Avaya are shown within this section. The web-based Kofax Server FoIP configuration utility was used to configure the interface to Session Manager. Open the KCS FoIP configuration utility from the shortcut on the Kofax Server desktop. The configuration operations described in this section can be summarized as follows:

- Configure List of Call Peers
- Configure Fax
- Configure SIP Signaling
- Configure KCS Integration

7.1. Configure List of Call Peers

Once the KCS FoIP configuration utility opens expand List of Call Peers menu item.



Once the **List of Call Peers** menu item opens complete the following for a free **Host**:

- **Enabled** Click on the Check box
- **Protocol** Select **SIP** from the dropdown box
- **Host** Enter the IP address of the Session Manager SIP Signaling Interface (see **Section 5.1**)

The screenshot shows the 'Kofax FoIP Configuration' utility window. The 'List of Call Peers' section is expanded, displaying a table with 8 rows. The first row is highlighted with a red border. The table columns are: Nr, Enabled, Protocol, Remote Address (Host, Port), Authorization (User ID, Password), and Reg. Numbers.

Nr	Enabled	Protocol	Remote Address		Authorization		Reg. Numbers
			Host	Port	User ID	Password	
1	<input checked="" type="checkbox"/>	SIP	10.10.16.214				
2	<input type="checkbox"/>	SIP					
3	<input type="checkbox"/>	SIP					
4	<input type="checkbox"/>	SIP					
5	<input type="checkbox"/>	SIP					
6	<input type="checkbox"/>	SIP					
7	<input type="checkbox"/>	SIP					
8	<input type="checkbox"/>	SIP					

7.2. Configure Fax

Fax can be configured for either **T.38** or **G.711 Pass-through**.

7.2.1. T.38 Fax

If only T.38 Fax support is required, complete the following:

- **OutboundDtmfMode** Select **0: G711 audio (default)** from the dropdown box
- **OutboundT38Mode** Select **10: Switch to T.38 w/o G.711 pass-through support** from the dropdown box
- **InboundT38Mode** Select **10: Switch to T.38 w/o G.711 pass-through support** from the dropdown box

KCS FoIP Configuration Utility - Windows Internet Explorer

KOFAX FoIP Configuration

Save Exit

General

List of Call Peers

VoIP/FoIP Network

Voice

Fax

OutboundDtmfMode: 0: G.711 audio (default) Defines how to generated DTMF digits 0

OutboundT38Mode: 10: Switch to T.38 w/o G.711 pass-through support Defines the T.38 mode for outbound calls. 40

InboundT38Mode: 10: Switch to T.38 w/o G.711 pass-through support Defines the T.38 mode for inbound calls. 40

EnableV34 ☐ Enable support for V.34 (ASN.1 2002) via T.38 false

RedundancyLS: 0 T.38 low-speed redundancy (0..3) 0

RedundancyHS: 0 T.38 high-speed redundancy (0..3) 0

H.323 Signaling

SIP Signaling

100%

7.2.2. G.711 Pass-through

If only G.711 pass-through support is required, complete the following:

- **OutboundDtmfMode** Select **0: G.711 audio (default)** from the dropdown box
- **OutboundT38Mode** Select **60: User G.711 pass-through and prevent switch to T.38** from the dropdown box
- **InboundT38Mode** Select **60: User G.711 pass-through and prevent switch to T.38** from the dropdown box

The screenshot shows the 'Kofax FoIP Configuration Utility' window. The 'Fax' tab is selected, and a red box highlights the 'OutboundDtmfMode', 'OutboundT38Mode', and 'InboundT38Mode' settings. The 'OutboundDtmfMode' is set to '0: G.711 audio (default)'. The 'OutboundT38Mode' and 'InboundT38Mode' are both set to '60: Use G.711 pass-through and prevent switch to T.38'. The 'EnableV34' checkbox is unchecked. The 'RedundancyLS' and 'RedundancyHS' fields are both set to '0'. The 'H.323 Signaling' and 'SIP Signaling' tabs are also visible at the bottom.

Setting	Value	Description	Value
OutboundDtmfMode	0: G.711 audio (default)	Defines how to generated DTMF digits	0
OutboundT38Mode	60: Use G.711 pass-through and prevent switch to T.38	Defines the T.38 mode for outbound calls.	40
InboundT38Mode	60: Use G.711 pass-through and prevent switch to T.38	Defines the T.38 mode for inbound calls.	40
EnableV34	<input type="checkbox"/>	Enable support for V.34 (ASN.1 2002) via T.38	false
RedundancyLS	0	T.38 low-speed redundancy (0..3)	0
RedundancyHS	0	T.38 high-speed redundancy (0..3)	0

7.3. Configure SIP Signaling

Open the **SIP Signaling** menu item and complete the following:

- **SipEnabledTransport** Select [3 **TCP and UDP** from the dropdown box
- **SipOutgoingTransport** Select [1] **sip(UDP)** from the dropdown box
- **Local UDP and TCP Port** Enter **5060**

Configuration Item	Value	Description	Value
SipEnabledTransports	[3] TCP and UDP	Transports that listen for incoming SIP messages	3
SipOutgoingTransport	[1] UDP	Transport for outgoing SIP messages	1
Local UDP and TCP Port	5060	Local UDP and TCP port for unencrypted SIP signaling	5060
Local TLS Port	5061	Local TLS (over TCP) port for encrypted SIP signaling	5061
CheckCertificate	<input type="checkbox"/>	Check remote peer certificate on SIP/TLS calls. (Requires a trusted CA certificate)	0
EnableRtpNte	<input type="checkbox"/>	Support reception of DTMF digits via RFC 2833 (RTP-NTE)	0
MulticastAddress		Additional multicast IPv4 address for incoming SIP calls.	
MulticastPeerAddresses	my-group	List of addresses (IP[:port]) which are notified after established Multicast inbound call. ('my-group' means own multicast IP)	my-group

7.4. Configure KCS Integration

KCS Integration is configured if Message Waiting Indication is used to signal if a fax is in the fax recipient's in-box. Complete the following to configure KCS Integration:

- **Enabled** Check the check box
- **MessageWait** Select **RFC3842** from the dropdown box

The screenshot shows the 'KCS FoIP Configuration Utility' window. The 'KCS Integration' section is expanded, showing the following settings:

Setting	Value	Description
Enabled	<input checked="" type="checkbox"/>	If checked, the component may be controlled by a TCOSS server.
Local IP Address		IP address of local interface used for connection to TCOSS / Voice server. If empty all local interfaces are used.
Local Port	5000	TCP Listener port for connection from TCOSS
Password		Password for connection from TCOSS. (empty means: do not check password)
CheckCallPeer	disabled	If enabled, TCOSS may only connect if Call-peer is OK.
MessageWait	RFC3842	Method of Message Waiting Indication signaling (MWI)
Call Diversion Mode	[1] Prefer original called number	Defines the priority if multiple call diversion numbers are available.
EnabledVoiceServer	<input type="checkbox"/>	If checked, the component may be controlled by a voice server.
Local Port	5001	TCP Listener port for connection from voice server
Call Transfer Mode	[1] Transfer Into Alerting	Consider Call Transfer completed after transfer-to party has reached Alerting or Connected state
Call Transfer with Hold	<input type="checkbox"/>	Execute Call Hold prior to the Call Transfer

Once the configuration is complete click on the **Save** button as shown in the screenshot below.

The screenshot shows the 'KCS FoIP Configuration Utility' window with the 'Save' button highlighted by a red box. The 'KCS Integration' section is still expanded, showing the same settings as the previous screenshot.

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Kofax Communication Server solution.

8.1. Verify the signaling group status

Using the SAT terminal, enter the **status signaling-group <n>** command, where <n> is the number of the SIP signaling group which connects to Session Manager. Verify that the **Group State** is **in-service**.

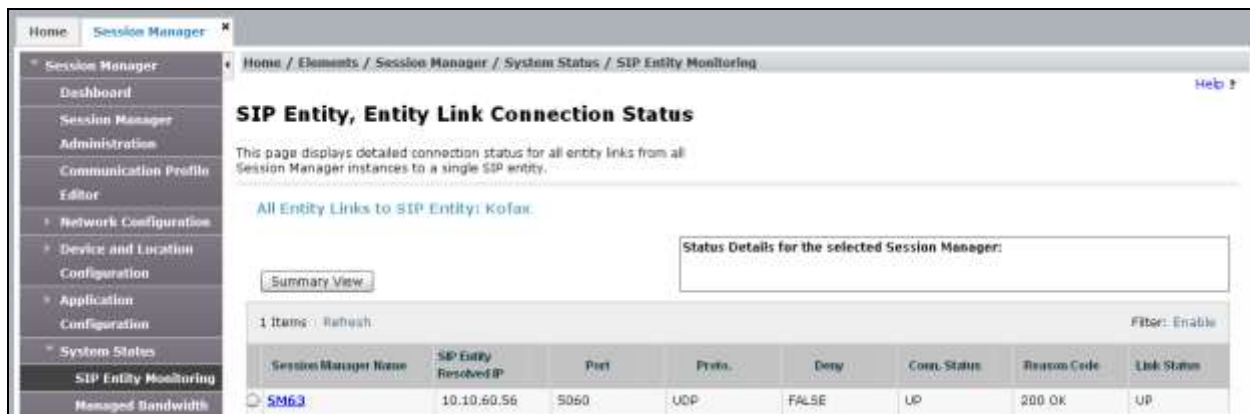
```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

8.2. Verify the SIP Entity Link status for the Kofax Communication server

From System Manager select **Session Manager** from under the **Elements** column, (not shown). When the **Session Manager** tab opens select **System Status** followed by **SIP Entity Monitoring**, then click on Kofax SIP Entity created in **Section 6.4**, ensure that the **Conn. Status** is **Up**, the **Reason Code** is **200OK** and the **Link Status** is **Up**.

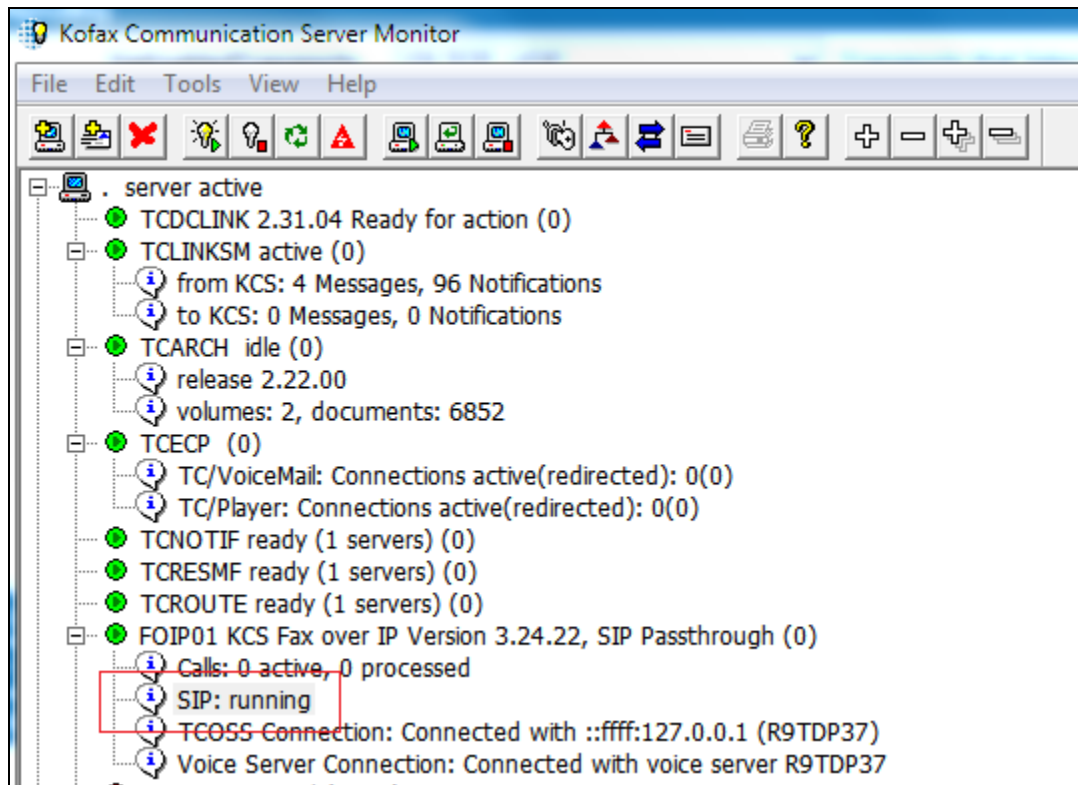


The screenshot shows the Session Manager web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, and Managed Bandwidth. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a breadcrumb trail: Home / Elements / Session Manager / System Status / SIP Entity Monitoring. Below the title, there is a description: 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' A link 'All Entity Links to SIP Entity: Kofax' is visible. A 'Summary View' button is present. Below this, a table displays the connection status for one item, 'SM63'. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The data row shows 'SM63' with IP '10.10.60.56', Port '5060', Proto. 'UDP', Deny 'FALSE', Conn. Status 'UP', Reason Code '200 OK', and Link Status 'UP'.

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM63	10.10.60.56	5060	UDP	FALSE	UP	200 OK	UP

8.3. Verify Kofax Communication Server SIP Status

Start the Kofax Communication Server monitor and verify that **SIP** is in the **running** state.



8.4. Verify that faxes are sent and received from the Kofax Communication Server

Send and receive multipage faxes, ensure the faxes are successfully sent and received and are legible, confirm that the caller ID and fax details are correct.

9. Conclusion

These Application Notes describe the configuration steps required for Kofax Communication Server to interoperate with an Avaya Aura® Communication Manager 7.0 and Avaya Aura® Session Manager 7.0. All test cases have passed and met the objectives outlined in **Section 2.2**.

10. Additional References

This section references the Avaya and Kofax documentation that is relevant to these Application Notes. Avaya product documentation, including the following, are available at:

<http://support.avaya.com>

[1] *Administering Avaya Aura® Communication Manager, Release 7.0, 2015,*

[2] *Administering Avaya Aura® Session Manager, Release 7.0, 2015*

[3] *Administering Avaya Aura® System Manager, Release 7.0, 2015*

Product Documentation for Kofax can be at the following location:

<http://www.kofax.com/business-communication-software/>

Appendix A

Pass-through Fax configuration.

Page 1

change ip-codec-set 1 Page 1 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.711A	n	2	20
3:			
4:			
5:			
6:			
7:			

Media Encryption

1: none

2:

3:

Page 2

change ip-codec-set 1 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size (ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Appendix B

Entity Link between Session Manager and Communication Manager.

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	*SM63_CM63_5060_T	*SM63	TCP	*5060	*CM63	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

Select: All, None

©2016 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*.