



Application Notes for Configuring Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 with Kofax Ltd. Communication Server using Transport Layer Security - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Kofax Communication Server to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. Kofax Communication Server communicates with Avaya Aura® Session Manager via Transport Layer Security. 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 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Kofax Communication Server offers a variety of telephony features. Kofax Communication Server fax features allow sending/receiving of fax messages 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® Communication Manager (Communication 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 Avaya Aura® Session Manager (Session Manager). The Session Manager was configured to connect to both Communication Manager and Kofax Communication Server via SIP trunks using Transport Layer Security (TLS).

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, pass-through mode connection with G.711A and G.711MU codecs
- Basic fax receiving , pass-through mode 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
- 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 with TLS (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

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

Figure 1 illustrates the network configuration used during compliance testing. A SIP trunk was configured between the Kofax Communication Server (using TLS) and the Session Manager SIP Signaling interface. A SIP trunk was also configured between Communication Manager and Session Manager (using TLS). 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.

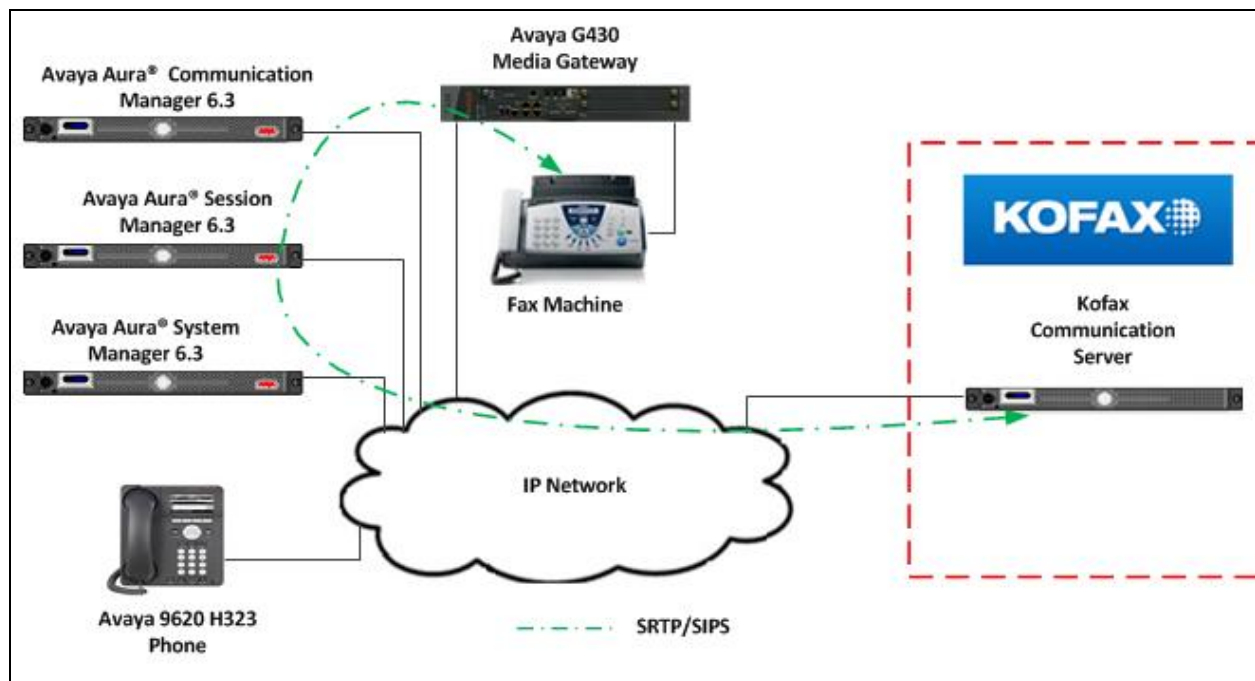


Figure 1: Avaya and Kofax Reference Configuration

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	R6.3 Build R016x.03.0.124.0
Avaya Aura® Session Manager	R6.3.7 Software Update 6.3.7.0.637008
Avaya Aura® System Manager	R6.3.7 Build 6.3.0.8.5682-6.3.8.2826 Update 6.3.5.52017
Avaya G430 Media Gateway Module MM710 (DSP MP20) Module MM714 (ANA)	Version 36.7.0/1 Version HW04 FW021 Version HW03 FW073
Kofax Equipment	Software Version
Kofax Communication Server KCS FoIP Application	Version 10.0 Version 3.22.05

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the 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 the 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 including the configuration of the Session Manager Node, Trunk Group, Signaling Group and Dial Patterns to communicate with the Session Manager. 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
- Configure Trunk Group
- Configure Fax Station
- Configure Codecs

5.1. Configure Session Manager Node

For the Communication Manager to communicate with the Session Manager a node must be configured. The screen shot below shows **SM63RPSIG** with IP address **10.10.16.214** was used.

Note: 10.10.16.214 is the 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	
SM63RPSIG	10.10.16.214	
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 **tls**
- **Enforce SIPS URI for SRTP** Enter **n**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **SM63RPSIG** (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

Configure the remaining inputs as per the screen shots below. Press **F3** to save configuration.

Page 1

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? 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: SM63RPSIG	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	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 SM6.3 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 SM6.3 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**. Press **F3** to save configuration.

Page 3

add 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 the Communication Manager and the **Extension** number used was **1026**. 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. Press **F3** to save configuration.

Page 1

add station 1026		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 1026	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 1026	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 1026		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

All faxes to and from Kofax use Pass-Through. Therefore the **Fax** setting on **Page 2** must be set to **off**. 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 (line 1):** Enter **2-srtp-aescm128-hmac32**
- **Media Encryption (line 2):** Enter **1-srtp-aescm128-hmac80**

Notes: The Media Encryption option is only available if **Media Encryption Over IP** is enabled on the installed license. Also 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: 2-srtp-aescm128-hmac32
2: 1-srtp-aescm128-hmac80
3:
```

On Page 2 enter **off** for **Fax**, 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	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

6. Configuring Avaya Aura® Session Manager

A number of configurations are required to enable the Session Manager to route Faxes between the Communication Manager and the Kofax Server. All configurations of the 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
- Manage Certificates

Note: See **Appendix A** for a screen shot of the Entity Link used between the 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.

AVAYA
Aura System Manager 6.3

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.

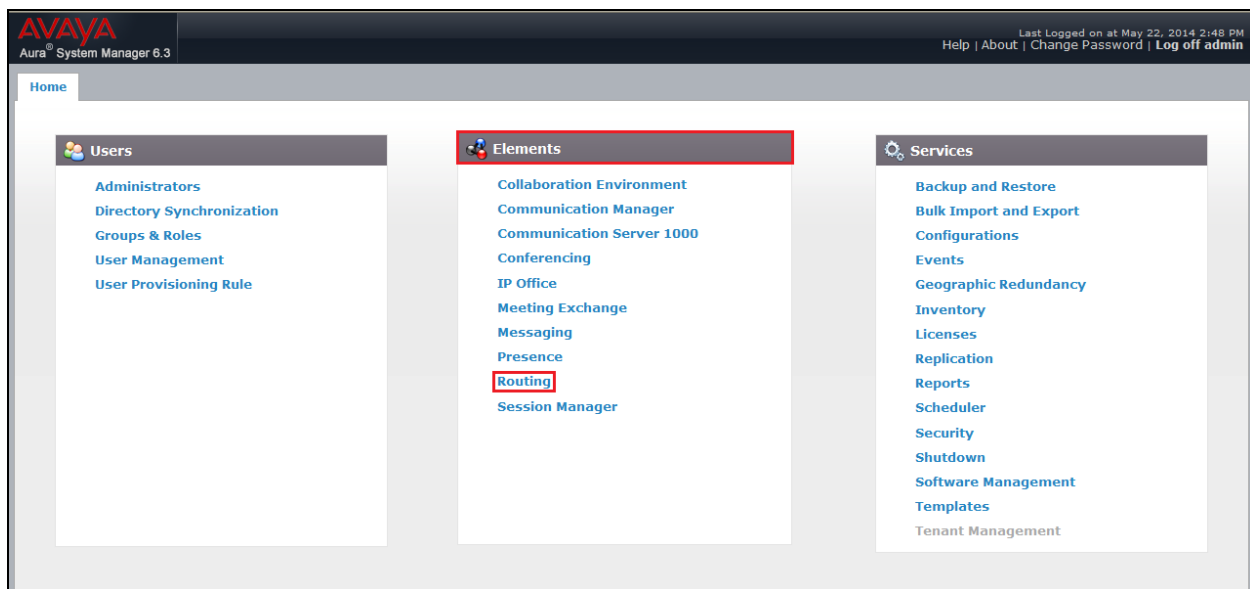
User ID:
Password:

[Change Password](#)

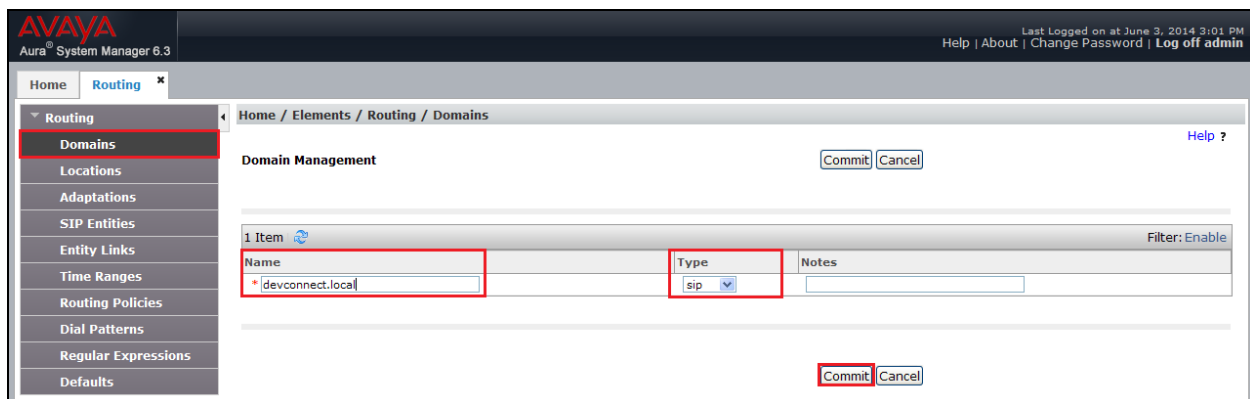
Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

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.



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.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 17, 2014 11:03 AM
Help | About | Change Password | Log off admin

Home Routing * Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* 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

		Notes
<input type="checkbox"/>	IP Address Pattern	
<input type="checkbox"/>	*10.10.16.*	

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 Kofax 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.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** Kofax
- FQDN or IP Address:** 10.10.60.56
- Type:** SIP Trunk (selected from a dropdown)
- Notes:** Trunk to Kofax
- Adaptation:** (empty dropdown)
- Location:** DevConnectRP (selected from a dropdown)
- Time Zone:** America/Fortaleza (selected from a dropdown)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** egress (selected from a dropdown)

At the top right of the form, there are 'Commit' and 'Cancel' buttons. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities'.

6.5. Create an Entity Link for Kofax Communication Server

The SIP trunk between the 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 **TLS** from the Protocol drop down box
- **Port:** Enter **5061**
- **SIP Entity 2:** Select **Kofax** from the **SIP Entity 2** dropdown box (configured in **Section 6.4**)
- **Port:** Enter **5061** 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 Avaya Aura System Manager 6.3 interface. The left sidebar contains a menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The row for 'Kofax Link' shows SIP Entity 1 as 'SM63', Protocol as 'TLS', Port as '5061', SIP Entity 2 as 'Kofax', Port as '5061', and Connection Policy as 'trusted'. A 'Commit' button is visible at the top right of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
*Kofax Link	*SM63	TLS	*5061	*Kofax		*5061	trusted		

6.6. Create a Routing Policy for Kofax Communication Server

Create routing policies to direct calls to the Kofax Server via the 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 the Communication Manager, but is outside the scope of this Application Note.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 17, 2014 11:03 AM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

Name: To Kofax

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

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.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 17, 2014 11:03 AM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

SIP Entities

Select Cancel

SIP Entities

14 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
<input checked="" type="radio"/> Kofax	10.10.60.56	SIP Trunk	Trunk to Kofax
<input type="radio"/> AACC63CMSIP	10.10.16.216	SIP Trunk	

6.7. Create a Dial Pattern for Kofax Communication Server

A dial pattern must be created on the Session Manager to route calls to and from the Kofax Server. During compliance testing a number of 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 the Communication Manager, but is outside the scope of this Application Note.

Under **General** enter out the following:

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

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

AVAYA
Aura® System Manager 6.3

Last Logged on at June 17, 2014 11:03 AM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 1

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: DevConnectRP

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

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 shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and user information: 'Last Logged on at June 17, 2014 11:03 AM', 'Help | About | Change Password | Log off admin'. The left sidebar shows a tree view with 'Routing' selected. The main content area has a breadcrumb 'Home / Elements / Routing / Dial Patterns' and a 'Help ?' link. The 'Originating Location' section has a 'Select' button (highlighted with a red box) and a 'Cancel' button. Below it, the 'Originating Location' table shows one item, 'DevConnectRP', with its checkbox checked (highlighted with a red box). The 'Routing Policies' section shows 13 items in a table. The 'To Kofax' row has its checkbox checked (highlighted with a red box). The table columns are Name, Disabled, Destination, and Notes.

Originating Location			
<input type="checkbox"/> Apply The Selected Routing Policies to All Originating Locations			
1 Item			
✓	Name	Notes	
✓	DevConnectRP		

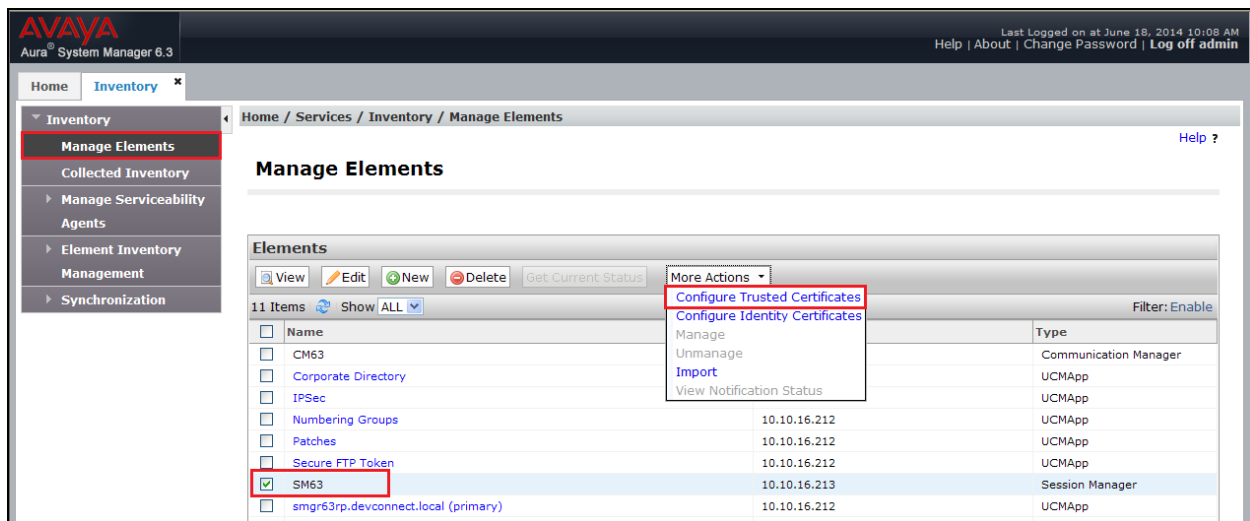
Routing Policies			
13 Items			
<input type="checkbox"/>	Name	Disabled	Notes
<input type="checkbox"/>	To IP office	<input type="checkbox"/>	IP Office
<input checked="" type="checkbox"/>	To Kofax	<input type="checkbox"/>	Kofax

6.8. Manage Certificates

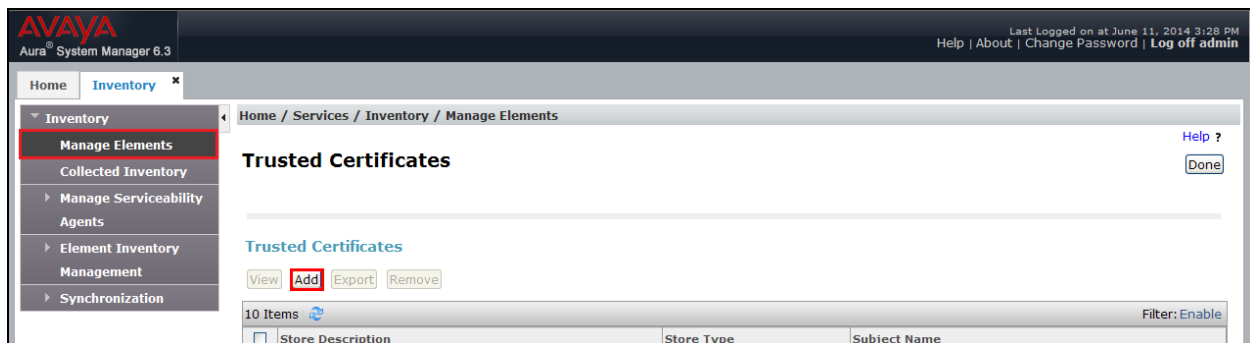
In order for Session Manager and the Kofax Server to successfully negotiate a TLS connection, certificates are exchanged and authenticated during the TLS handshake. For two-way authentication both the Session Manager and Kofax Server need to import each other's certificate. See **Appendix B** for information relating to exporting the Session Manager trusted certificates.

6.8.1. Adding Kofax Server trusted certificate

Before adding the trusted certificate, it must first be placed in a location that is accessible by System Manager. To add the certificate click on **Home** followed by **Inventory** in the **Services** column (not shown). Select **Manage Elements** and click on Session Manager Element (i.e., **SM63**). From the **More Actions** dropdown box select **Configure Trusted Certificates**.



Once the Trusted Certificates screen opens click the **Add** button.



Once the **Add Trusted Certificates** screen opens select **All** from the **Select Store Type** to add **trusted certificate** dropdown box. Check the **Import from file** radio button. At the **Please select a file** box browse to the location of the Kofax Server trusted certificate and click on the **Retrieve Certificate** button.

AVAYA
Aura® System Manager 6.3

Home / Services / Inventory / Manage Elements

Add Trusted Certificate

Select Store Type to add trusted certificate: All

☒ Import from file
☐ Import as PEM certificate
☐ Import from existing certificates
☐ Import using TLS

* Please select a file: C:\Documents and Settings\Administrator\De

You must click the Retrieve certificate button and review the certificate details before you can continue.

Verify the certificate information and then click the **Commit** button to store the certificate.

AVAYA
Aura® System Manager 6.3

Home / Services / Inventory / Manage Elements

Add Trusted Certificate

Select Store Type to add trusted certificate: All

☒ Import from file
☐ Import as PEM certificate
☐ Import from existing certificates
☐ Import using TLS

* Please select a file:

You must click the Retrieve certificate button and review the certificate details before you can continue.

Certificate Details

Subject Details	CN=kic-electronic-documents-test-cert.kofax.	
Valid From	Thu Sep 15 14:17:10 IST 2011	Valid To Wed Sep 10 14:17:10 IST 2031
Key Size	1024	
Issuer Name	CN=kic-electronic-documents-test-cert.kofax.	
Certificate Fingerprint	d6d63da5992d6ae84f71e17fb52d64047b94f	
CA Certificate	No	

7. Configure Kofax Communication Server

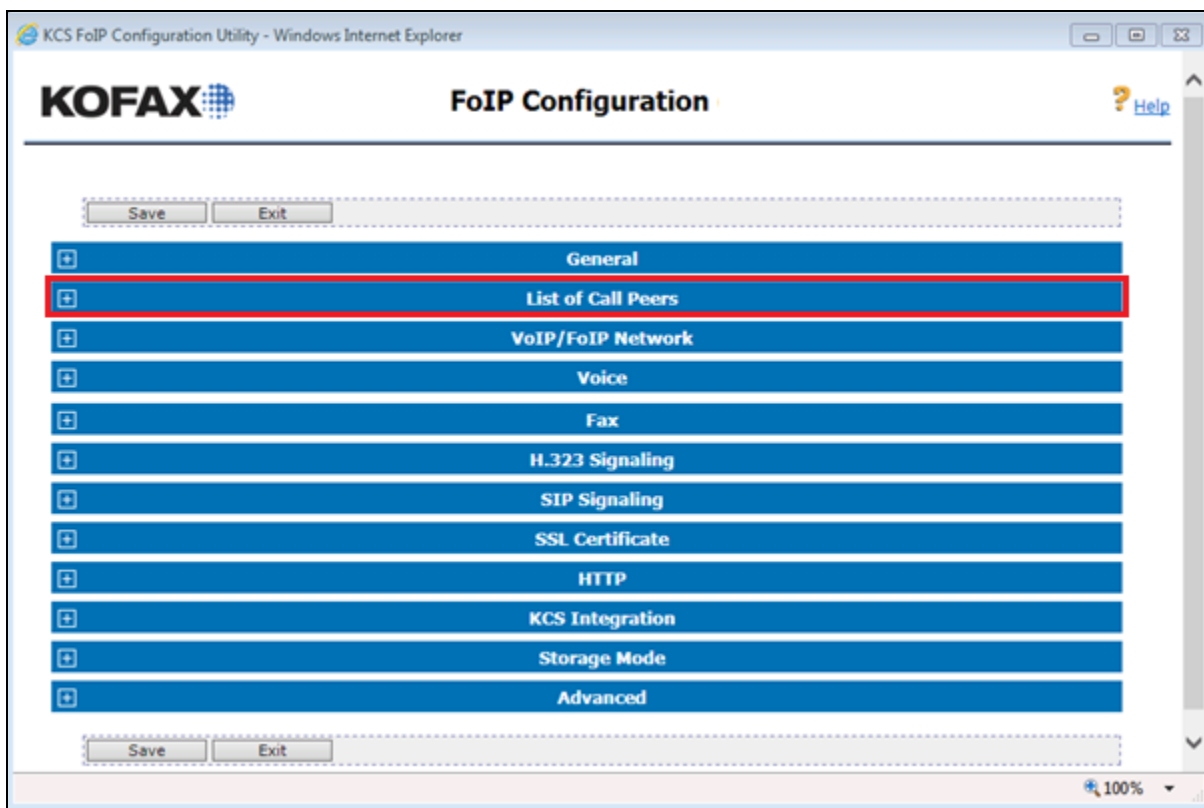
The Kofax Server is provided, installed and implemented by Kofax. Only those configuration details concerning the interface to Avaya are shown within this section. The Web-based Kofax Server FoIP configuration utility was used to configure the interface to Session Manager.

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 Voice
- Configure Fax
- Configure SIP Signaling
- Configure Certificates
- 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 running in a Windows Internet Explorer browser. The interface includes a 'Save' button and an 'Exit' button at the top. Below these are expandable sections for 'General', 'List of Call Peers', 'VoIP/FoIP Network', and 'Voice'. The 'List of Call Peers' section contains a table with the following structure:

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					

The first row of the table is highlighted with a red border. The 'Host' field in the first row contains the IP address '10.10.16.214'. The 'Enabled' checkbox for the first row is checked. The 'Protocol' dropdown for the first row is set to 'SIP'. The 'VoIP/FoIP Network' and 'Voice' sections are currently collapsed.

7.2. Configure Voice

Open the **Voice** menu item and complete the following:

- **MediaSecurity:** Enter **[3] always (use SRTP, reject RTP)** from the dropdown box
- **MediaSecurityUnencryptedSrtp:** Enter **[2] offer only crypto with UNENCRYPTED_SRTP** from the dropdown box

KCS FoIP Configuration Utility - Windows Internet Explorer

KOFAX FoIP Configuration [Help](#)

Save Exit

General

List of Call Peers

VoIP/FoIP Network

Voice

MediaSecurity [3] always (use SRTP, reject RTP)

MediaSecurityCryptoSuites [3] offer crypto suites AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32

MediaSecurityUnencryptedSrtp [2] offer only crypto with UNENCRYPTED_SRTP

Silence Suppression ☒

Nr	Enabled	Codec	Max. Packet Interval
1	<input checked="" type="checkbox"/>	G.711 A-Law <input type="button" value="v"/>	20 ms <input type="button" value="v"/>
2	<input checked="" type="checkbox"/>	G.711 u-Law <input type="button" value="v"/>	20 ms <input type="button" value="v"/>

Fax

H.323 Signaling

SIP Signaling

SSL Certificate

HTTP

KCS Integration

Storage Mode

Advanced

Security option for voice and pass-through fax media data 1

Crypto suites in outgoing SDP offer. All supported suites are accepted when offered by remote side regardless of this configuration parameter. 3

Crypto parameter UNENCRYPTED_SRTP in outgoing SDP offer. Crypto with and without UNENCRYPTED_SRTP is accepted when 3 offered by remote side regardless of this configuration parameter. Enable RTP silence suppression (Voice mode only) true

7.3. Configure Fax

Open the **Fax** menu item and complete the following:

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

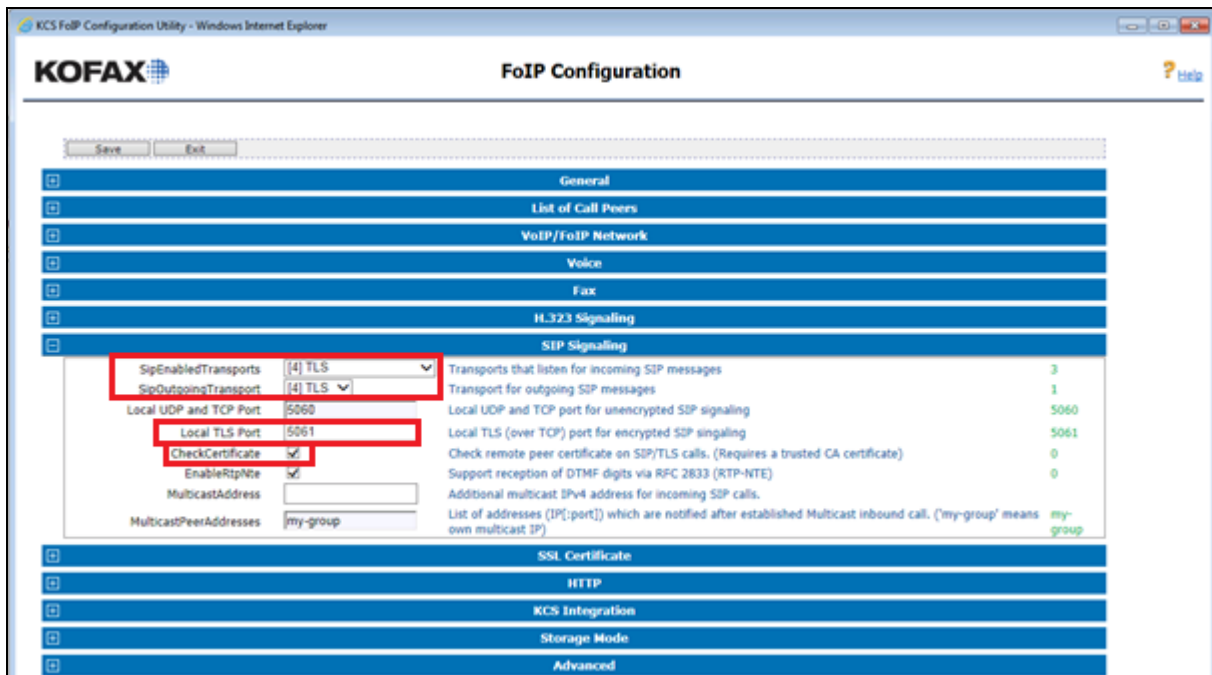
OutboundTdmfMode	0: G.711 audio (default)	Defines how to generated DTMF digits	0
OutboundT38Mode	60: Use G.711 pass-through and prevent switch to T.38	Defines the T.38 mode for outbound calls.	40
InboundT38Mode	60: Use G.711 pass-through and prevent switch to T.38	Defines the T.38 mode for inbound calls.	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

- H.323 Signaling
- SIP Signaling
- SSL Certificate
- HTTP
- KCS Integration
- Storage Mode
- Advanced

7.4. Configure SIP Signaling

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

- **SipEnabledTransport:** Select [4] **TLS** from the dropdown box
- **SipOutgoingTransport:** Select [4] **TLS** from the dropdown box
- **Local TLS Port:** Enter **5061**
- **CheckCertificate:** Check the check box



Parameter	Value	Description	Value
SipEnabledTransports	[4] TLS	Transports that listen for incoming SIP messages	3
SipOutgoingTransport	[4] TLS	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 checked="" type="checkbox"/>	Check remote peer certificate on SIP/TLS calls. (Requires a trusted CA certificate)	0
EnableRtpNte	<input checked="" 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

7.5. Configure Certificates

Open the **SSL Certificate** menu item and complete the following: Locate and open the Session Manager **Trusted** Certificate in a text editor (i.e., Word pad) and copy the contents and paste them in the **SSL Trusted CA Certificates** field between **BEGIN CERTIFICATE** and **END CERTIFICATE**.

KCS FoIP Configuration Utility - Windows Internet Explorer

KOFAX FoIP Configuration

Save Exit

- General
- List of Call Peers
- VoIP/FoIP Network
- Voice
- Fax
- H.323 Signaling
- SIP Signaling
- SSL Certificate

SSL Certificate	hU10ESP+XId/GzwQapMqIxy8vfqRy10IB59doR7a PFkUFbLMucM1vq1/LMkKVjNo wWpruvN2vX/caCWjv4TwSx25/5HjZd6xd1AR8frb vWwC -----END CERTIFICATE-----	Your SSL server certificate in PEM format (Base64 encoded, including -----BEGIN and -----END lines)
SSL Private Key	*****	The private key to the above server certificate, in PEM format (Base64 encoded, including -----BEGIN and -----END lines). The private key entered must not be encrypted, it will be encrypted internally.
SSL Chain Certificate		Optional intermediate certificate in the certificate chain to a well-known root certificate in PEM format (Base64 encoded, including -----BEGIN and -----END lines)
SSL Trusted CA Certificates	-----BEGIN CERTIFICATE----- MIIEHTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUF ADB6HQawCQYDVQQGEwJVUzET MBEGA1UEChMKQXZheWEgSW5jLjEgMCgSA1UECzMh U01QIFByb2R1Y3QgQ2VydGlm aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAg	Optional trusted CA certificates for verifying remote peer certificates. (Base64 encoded, including -----BEGIN and -----END lines)

7.6. 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' web interface in a Windows Internet Explorer browser. The 'KCS Integration' section is expanded, showing various configuration options. The 'Enabled' checkbox is checked. The 'MessageWait' dropdown menu is set to 'RFC3842'. Other visible options include 'Local IP Address', 'Local Port' (5000), 'Password', 'CheckCallPeer' (disabled), 'Call Diversion Mode' ([1] Prefer original called number), 'EnabledVoiceServer' (unchecked), 'Local Port' (5001), 'Call Transfer Mode' ([1] Transfer Into Alerting), and 'Call Transfer with Hold' (unchecked). The interface also includes a 'Save' button and an 'Exit' button at the top left of the configuration area.

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

This screenshot shows the same 'KCS FoIP Configuration Utility' web interface, but with the 'Save' button highlighted by a red rectangle. The 'KCS Integration' section is still expanded, and the configuration values remain the same as in the previous screenshot.

8. Verification Steps

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

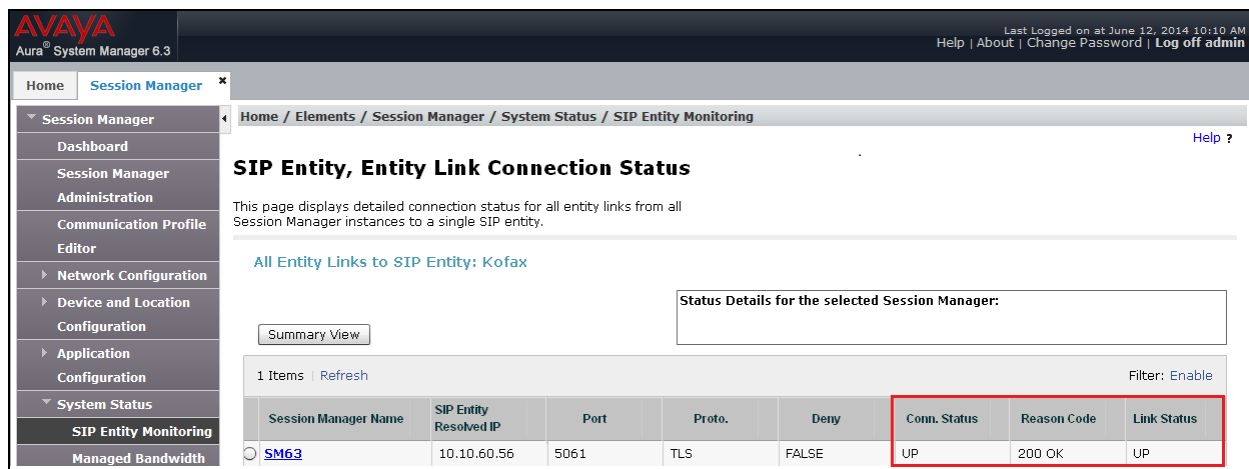
```
status signaling-group 1
                        STATUS SIGNALING GROUP

      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 **200 OK** and the **Link Status** is **Up**.



AVAYA
Aura® System Manager 6.3

Last Logged on at June 12, 2014 10:10 AM
Help | About | Change Password | Log off admin

Home Session Manager x

Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: Kofax

Summary View

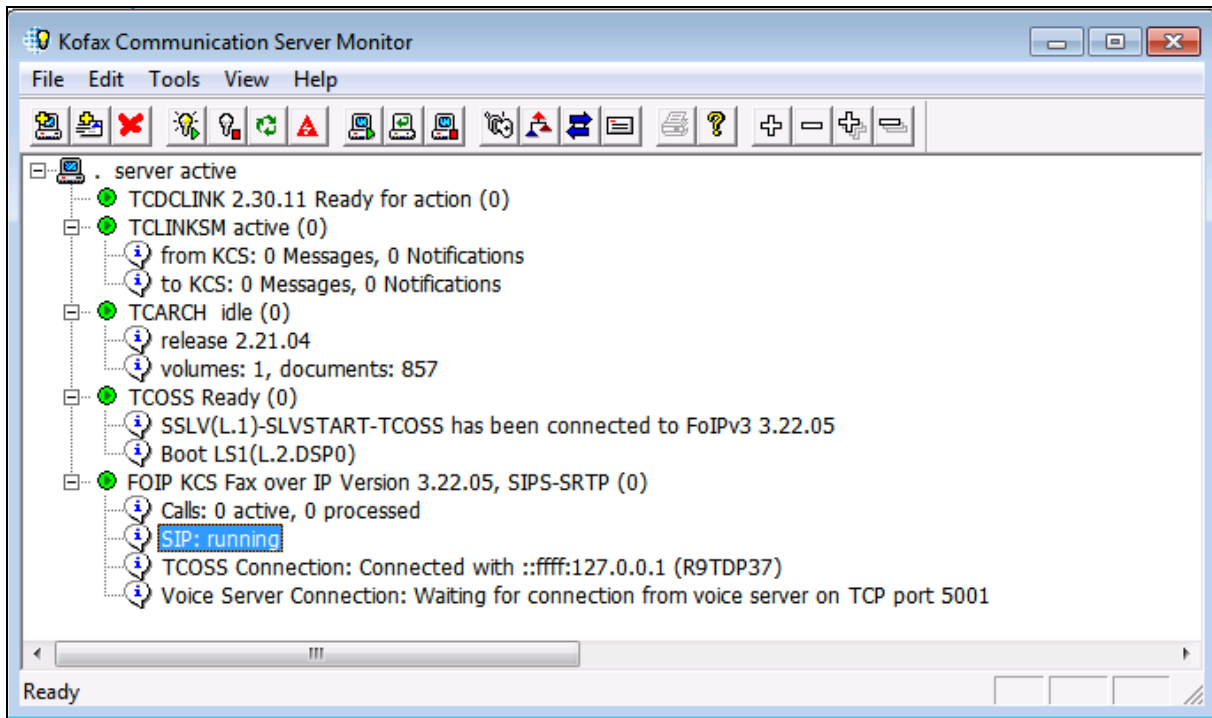
Status Details for the selected Session Manager:

1 Items | Refresh Filter: Enable

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM63	10.10.60.56	5061	TLS	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.



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 6.3 and Avaya Aura® Session Manager 6.3 using TLS. 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 documentations, including the following, are available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager, Release 6.3, Issue 8, May 2013,*
- [2] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013*
- [3] *Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013*

Product Documentation for Kofax can be at the following location:
<http://www.kofax.com/business-communication-software/>

Appendix A

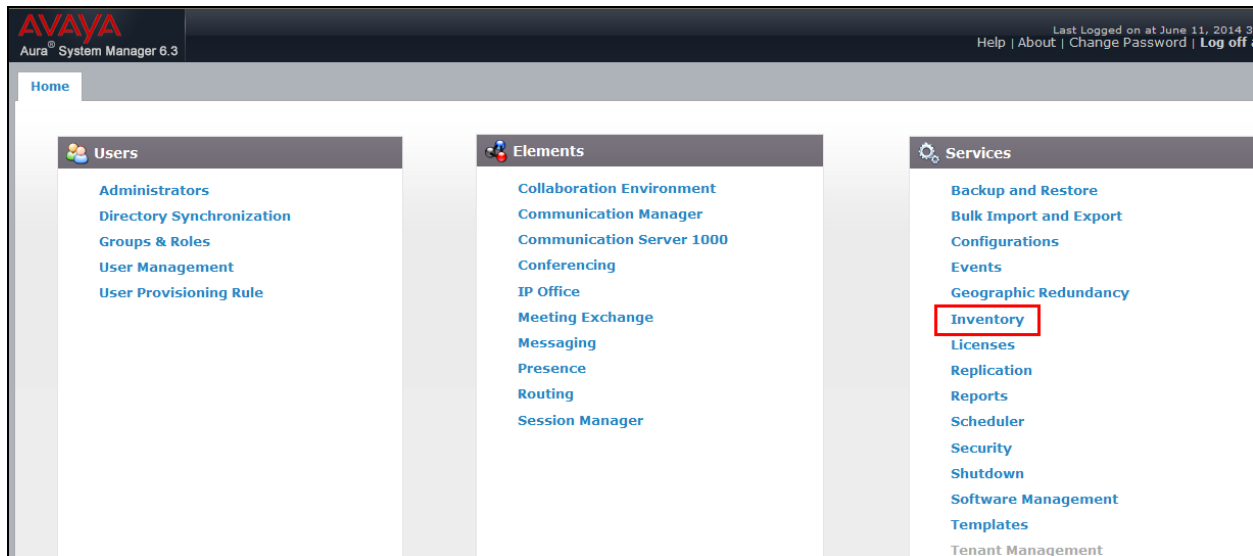
Entity Link between Session Manager and Communication Manager.

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	TLS	* 5061	* CM63	<input type="checkbox"/>	* 5061	trusted	<input type="checkbox"/>	
Select : All, None										

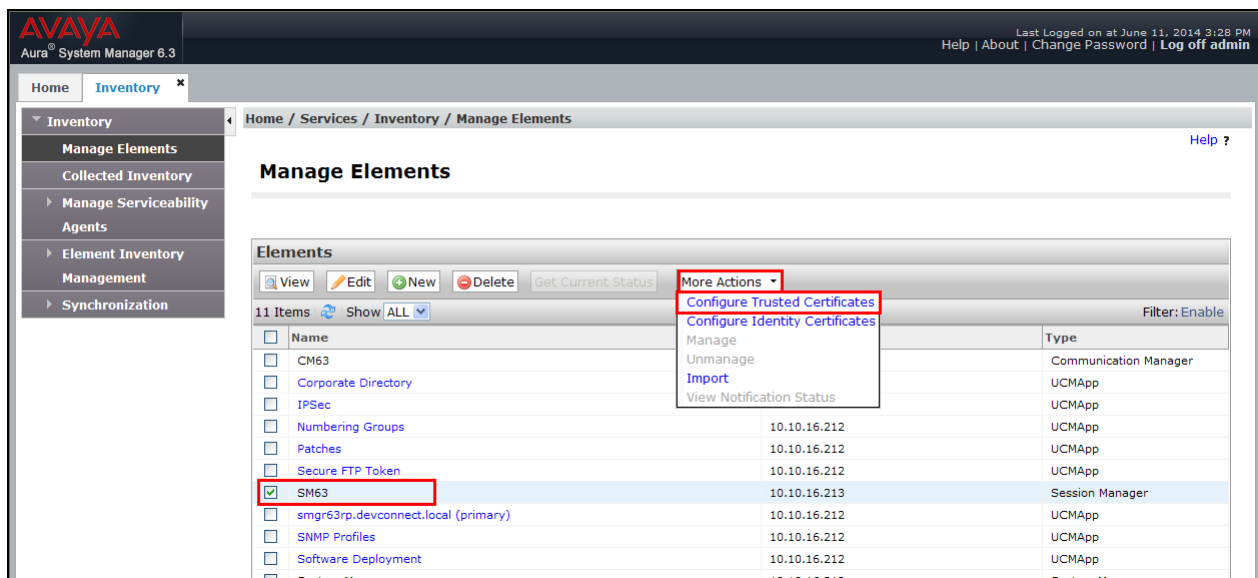
Appendix B

To export the Session Manager trusted certificates follow the steps below.

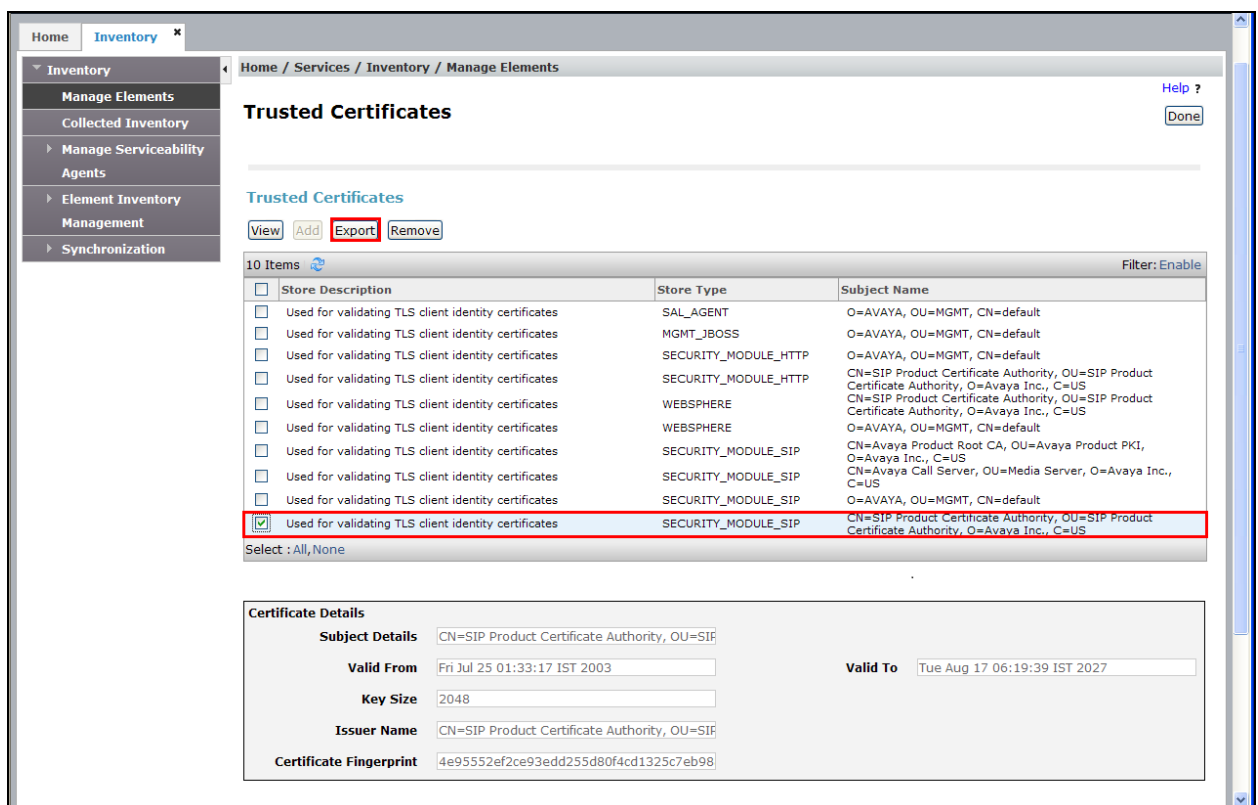
After logging into System Manager go to **Home** → **Services** → **Inventory**.



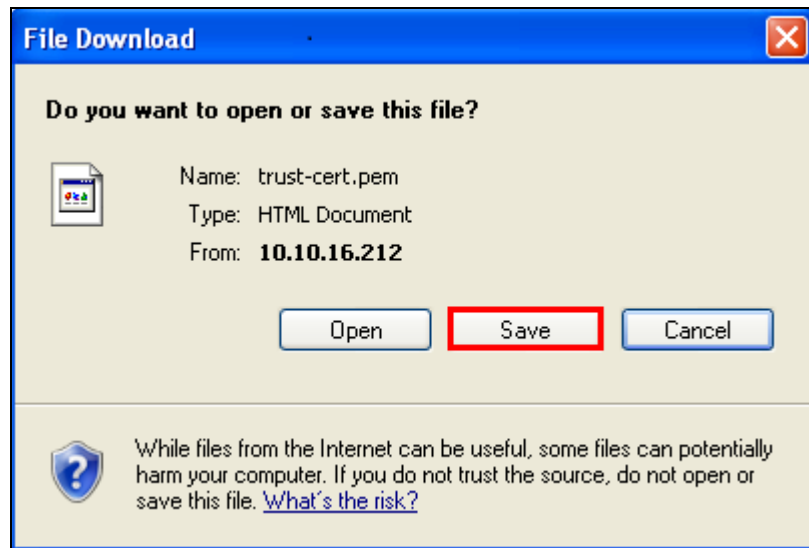
Select **Manage Elements** and click on Session Manager Element (i.e., SM63). From the **More Actions** dropdown box select **Configure Trusted Certificates**



Once the **Trusted Certificates** screen open check the **CN=SIP Product Certificate Authority, OU=SIP Product Certificate, O=Avaya Inc., C=US** check box. Click the **Export** button to export the certificate.



When the **File download** window opens click on the **save** button and chose a location to store the Certificate. The file stored will then be required to be installed on the Kofax Server.



©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.