



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Sagemcom XMediusFAX Service Provider Edition with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Sagemcom XMediusFAX Service Provider (SP) Edition with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the configuration tested, XMediusFAX interoperates with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to send/receive faxes using SIP trunks and the T.38 fax protocol between XMediusFAX and the Avaya SIP infrastructure.

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

1. Introduction

These Application Notes describe the procedures for configuring Sagemcom XMediusFAX Service Provider (SP) Edition with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunks.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the configuration tested, XMediusFAX interoperates with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to send/receive faxes using SIP trunks and the T.38 protocol between XMediusFAX and the Avaya SIP infrastructure. The compliance testing focused on fax calls to and from the XMediusFAX fax server using various page lengths, resolutions, paper sizes, and fax data speeds.

2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of Sagemcom XMediusFAX SP Edition with the Avaya SIP infrastructure (Session Manager and Communication Manager). This section also covers the test results.

The interoperability compliance test included feature and serviceability test. The feature test cases were performed manually. Fax calls to and from XMediusFAX were made. The faxes were sent and received using the XMediusFAX web interface and an analog fax machine at the PSTN.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to XMediusFAX and rebooting the XMediusFAX server.

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 general test approach was to make intra-site and inter-site fax calls to and from the XMediusFAX fax server. The compliance tested configuration contained two sites. Site 1 served as the main enterprise site and Site 2 served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using SIP trunks and ISDN-PRI trunks between the sites. Faxes were sent with various page lengths, resolutions, paper sizes, and at various fax data speeds. For capacity testing, 100 2-page faxes were continuously sent between the two XMediusFAX fax servers. Serviceability testing included verifying proper operation/recovery from network outages, unavailable resources, and Communication Manager and XMediusFAX restarts. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included the TN2302 MedPro circuit pack and the

TN2602 MedPro circuit pack in the Avaya G650 Media Gateway; and the integrated VoIP engine of the Avaya G450 Media Gateway.

The test focused on fax transmission using the T.38 standard. However, a subset of the test cases were also executed using the G.711 pass-through fax mode.

2.2. Test Results

XMediusFAX successfully passed compliance testing with the following observations noted:

- When shuffling is enabled, fax machine to/from fax server calls between two Communication Managers do not work unless the “Initial IP-IP Direct Media” parameter is on for all the signaling groups on the second Communication Manager.
- When shuffling is enabled, fax server to fax server calls between two Communication Managers do not work unless the “Initial IP-IP Direct Media” parameter is also on for all the signaling groups on the call path.

2.3. Support

For technical support on XMediusFAX, contact Sagemcom at:

- Web: <http://xmediusfax.sagemcom.com/support/>
- Phone: (888) 766-1668
- Email: xmediusfax.support.americas@sagemcom.com

3. Reference Configuration

Figure 1 illustrates the reference configuration used during testing. In the reference configuration, the two sites are connected via a direct SIP trunk and an ISDN-PRI trunk. Faxes were sent between the two sites using either of these two trunks, as dictated by each individual test case.

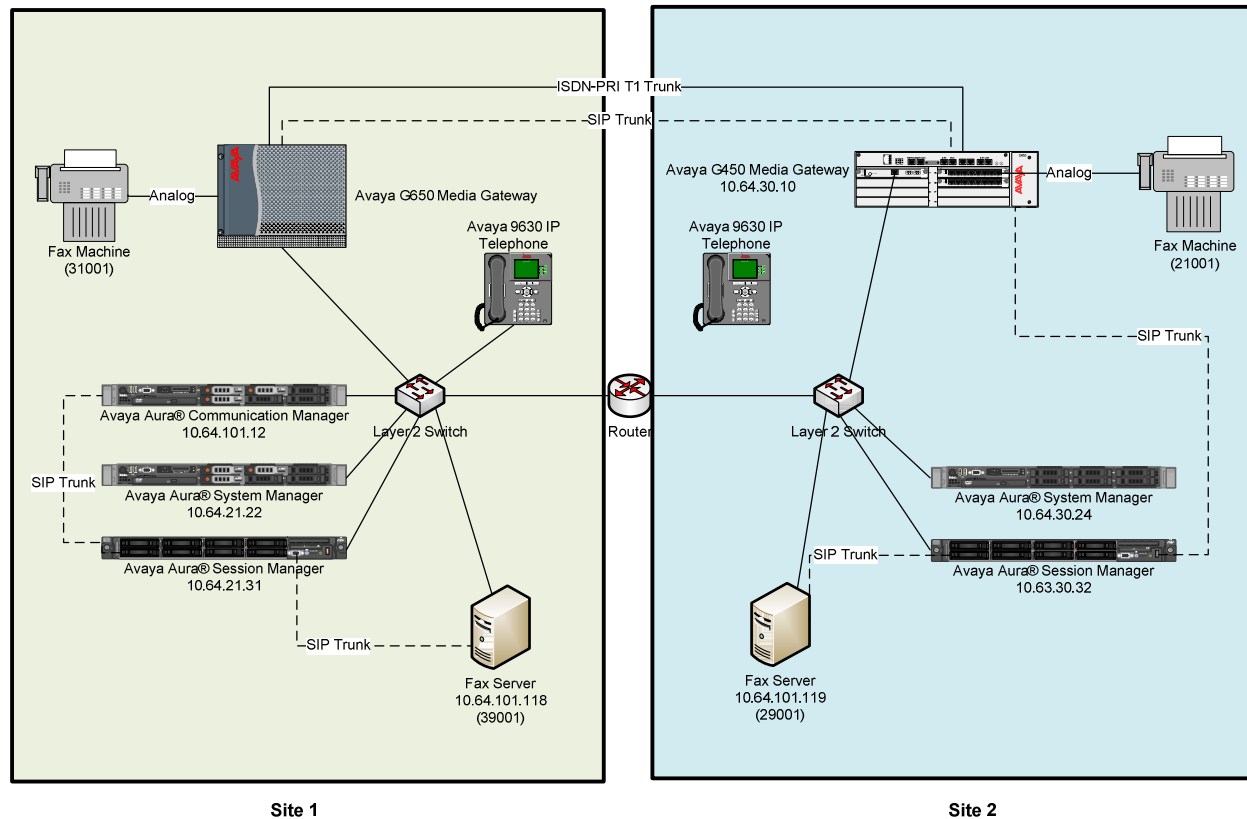


Figure 1: XMediusFAX with Session Manager and Communication Manager

Site 1 consists of the following equipment:

- Communication Manager with Avaya G650 Media Gateway: The media resources required are provided by the IP Media Processor (MedPro) circuit packs. Two versions of the IP MedPro circuit pack were tested in the configuration: the TN2302AP and the TN2602AP.
- System Manager: System Manager provides management functions for Session Manager.
- Session Manager.
- XMediusFAX running on a Windows Server 2008 R2 Enterprise SP1 64-bit.
- Analog fax machine.
- Various Avaya IP endpoints (not all shown).

Site 2 consists of the following equipment:

- Communication Manager in an Avaya G450 Media Gateway: The signaling and media resources needed to support SIP trunks are integrated directly on the media gateway processor.
- System Manager: System Manager provides management functions for Session Manager.
- Session Manager.
- XMediusFAX running on a Windows 2008 R2 Enterprise Server (SP1) 64-bit.
- Analog fax machine
- Various Avaya IP endpoints (not all shown).

Although the IP endpoints (H.323 and SIP telephones) are not involved in the faxing operations, they are present at both sites to verify that VoIP telephone calls are not affected by the FoIP faxing operations and vice versa.

Outbound fax calls originating from the XMediusFAX fax server are sent to Session Manager first, and then from Session Manager to Communication Manager via SIP trunks. Based on the dialed digits, Communication Manager will either direct the calls to the local fax machine, or to the other site via an ISDN-PRI or SIP trunk. Inbound fax calls terminating to the XMediusFAX fax server are sent from the local fax machine or from the remote site are received by Communication Manager. The calls are then directed to Session Manager for onward routing to the XMediusFAX fax server via SIP trunks.

4. Equipment and Software Validated

The following equipment and software were used for the reference configuration:

Equipment/Software	Version
Site 1	
Avaya Aura® Communication Manager running on VMWare virtual machine with Avaya G650 Media Gateway: IP MedPros – TN2302AP IP MedPros – TN2602AP	6.3 SP2 (patch 21106) HW 20, FW 120 HW 04, FW 063
Avaya Aura® System Manager running on Dell PowerEdge R610 Server	6.3.0 FP2
Avaya Aura® Session Manager running on HP ProLiant DL360 G7 Server	6.3.2
XMediusFAX fax server (Windows Server 2008 R2 Enterprise SP1 64-bit)	R7.5
Fax Machine	-
Various Avaya SIP and H.323 endpoints	-
Site 2	
Avaya Aura® Communication Manager Duplex running on Dell PowerEdge R610 Servers with Avaya G450 Media Gateway MGP MM711AP Analog Module MM710AP T1 Module	6.3 SP1 (patch 20850) HW 1 FW 33.13.0 HW 27, FW 073 HW 04 FW 022
Avaya Aura® System Manager running on HP ProLiant DL360 G7 Server	6.3.3
Avaya Aura® Session Manager running on HP ProLiant DL360 G7 Server	6.3.3
XMediusFAX fax server (Windows Server 2008 R2 Enterprise SP1 64-bit)	R7.5
Fax Machine	-
Various Avaya SIP and H.323 endpoints	-

5. Configure Communication Manager

This section describes the Communication Manager configuration at Site 1 to support the network shown in **Figure 1**. Although not shown in this document, a similar Communication Manager configuration would be required at Site 2.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

Step	Description																																		
1.	<p>License</p> <p>Use the display system-parameters customer-options command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to Page 2, and verify that there is sufficient remaining capacity for SIP trunks by comparing the Maximum Administered SIP Trunks field value with the corresponding value in the USED column.</p> <p>The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.</p>																																		
	<div><div>display system-parameters customer-options</div><div>Page 2 of 11</div><div>OPTIONAL FEATURES</div><div><table><thead><tr><th>IP PORT CAPACITIES</th><th>USED</th></tr></thead><tbody><tr><td>Maximum Administered H.323 Trunks: 12000</td><td>0</td></tr><tr><td>Maximum Concurrently Registered IP Stations: 18000</td><td>0</td></tr><tr><td>Maximum Administered Remote Office Trunks: 12000</td><td>0</td></tr><tr><td>Maximum Concurrently Registered Remote Office Stations: 18000</td><td>0</td></tr><tr><td>Maximum Concurrently Registered IP eCons: 414</td><td>0</td></tr><tr><td>Max Concur Registered Unauthenticated H.323 Stations: 100</td><td>0</td></tr><tr><td>Maximum Video Capable Stations: 41000</td><td>0</td></tr><tr><td>Maximum Video Capable IP Softphones: 18000</td><td>0</td></tr><tr><td>Maximum Administered SIP Trunks: 24000</td><td>100</td></tr><tr><td>Maximum Administered Ad-hoc Video Conferencing Ports: 24000</td><td>0</td></tr><tr><td>Maximum Number of DS1 Boards with Echo Cancellation: 522</td><td>0</td></tr><tr><td>Maximum TN2501 VAL Boards: 128</td><td>2</td></tr><tr><td>Maximum Media Gateway VAL Sources: 250</td><td>0</td></tr><tr><td>Maximum TN2602 Boards with 80 VoIP Channels: 128</td><td>0</td></tr><tr><td>Maximum TN2602 Boards with 320 VoIP Channels: 128</td><td>1</td></tr><tr><td>Maximum Number of Expanded Meet-me Conference Ports: 300</td><td>0</td></tr></tbody></table></div></div>	IP PORT CAPACITIES	USED	Maximum Administered H.323 Trunks: 12000	0	Maximum Concurrently Registered IP Stations: 18000	0	Maximum Administered Remote Office Trunks: 12000	0	Maximum Concurrently Registered Remote Office Stations: 18000	0	Maximum Concurrently Registered IP eCons: 414	0	Max Concur Registered Unauthenticated H.323 Stations: 100	0	Maximum Video Capable Stations: 41000	0	Maximum Video Capable IP Softphones: 18000	0	Maximum Administered SIP Trunks: 24000	100	Maximum Administered Ad-hoc Video Conferencing Ports: 24000	0	Maximum Number of DS1 Boards with Echo Cancellation: 522	0	Maximum TN2501 VAL Boards: 128	2	Maximum Media Gateway VAL Sources: 250	0	Maximum TN2602 Boards with 80 VoIP Channels: 128	0	Maximum TN2602 Boards with 320 VoIP Channels: 128	1	Maximum Number of Expanded Meet-me Conference Ports: 300	0
IP PORT CAPACITIES	USED																																		
Maximum Administered H.323 Trunks: 12000	0																																		
Maximum Concurrently Registered IP Stations: 18000	0																																		
Maximum Administered Remote Office Trunks: 12000	0																																		
Maximum Concurrently Registered Remote Office Stations: 18000	0																																		
Maximum Concurrently Registered IP eCons: 414	0																																		
Max Concur Registered Unauthenticated H.323 Stations: 100	0																																		
Maximum Video Capable Stations: 41000	0																																		
Maximum Video Capable IP Softphones: 18000	0																																		
Maximum Administered SIP Trunks: 24000	100																																		
Maximum Administered Ad-hoc Video Conferencing Ports: 24000	0																																		
Maximum Number of DS1 Boards with Echo Cancellation: 522	0																																		
Maximum TN2501 VAL Boards: 128	2																																		
Maximum Media Gateway VAL Sources: 250	0																																		
Maximum TN2602 Boards with 80 VoIP Channels: 128	0																																		
Maximum TN2602 Boards with 320 VoIP Channels: 128	1																																		
Maximum Number of Expanded Meet-me Conference Ports: 300	0																																		

Step	Description
2.	<p>IP network region</p> <p>Use the display ip-network-region command to view the network region settings. The values shown below are the values used during compliance testing.</p> <ul style="list-style-type: none"> ▪ Authoritative Domain: <i>avaya.com</i> This field was configured to match the domain name configured on Session Manager. The domain will appear in the “From” header of SIP messages originating from this IP region. ▪ Name: Any descriptive name may be used (if desired). ▪ Intra-region IP-IP Direct Audio: <i>yes</i> Inter-region IP-IP Direct Audio: <i>yes</i> By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the Signaling Group form. ▪ Codec Set: <i>1</i> The codec set contains the list of codecs available for calls within this IP network region. <pre> display ip-network-region 1 IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: Stub Network Region: n MEDIA PARAMETERS Codec Set: 1 Intra-region IP-IP Direct Audio: yes Inter-region IP-IP Direct Audio: yes IP Audio Hairpinning? n UDP Port Min: 2048 UDP Port Max: 3329 DIFFSERV/TOS PARAMETERS Call Control PHB Value: 46 Audio PHB Value: 46 Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5 H.323 IP ENDPOINTS H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 AUDIO RESOURCE RESERVATION PARAMETERS RSVP Enabled? n </pre>

Step	Description
3.	<p>Codecs</p> <p>IP codec set 1 was used during compliance testing. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing.</p> <pre> display 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 </pre> <p>On Page 2, set the FAX Mode field to <i>t.38-standard</i> and the ECM field to <i>n</i>. The Modem Mode field should be set to <i>off</i>.</p> <p>Leave the FAX Redundancy at its default value of <i>0</i>.</p> <p>A subset of the test cases were also executed with the FAX Mode field set to pass-through.</p> <pre> display ip-codec-set 1 Page 2 of 2 IP Codec Set Allow Direct-IP Multimedia? n FAX Mode Redundancy ECM: n Modem t.38-standard 0 TDD/TTY off 0 Clear-channel US 3 n 0 </pre>
4.	<p>Node Names</p> <p>Use the change node-names ip command to create a node name for the IP address of Session Manager. Enter a descriptive name in the Name column and the IP address assigned to Session Manager in the IP address column.</p> <pre> change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address CM_101_12 10.64.101.12 CM_30_10 10.64.30.10 Gateway 10.64.22.1 SM_21_31 10.64.21.31 default 0.0.0.0 procr 10.64.101.12 procr6 :: </pre>

Step	Description
5.	<p>Signaling Group</p> <p>Signaling group 91 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. The signaling groups and trunk groups between the two sites of the reference configuration is assumed to already be in place and not described in this document. Signaling group 91 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Group Type: <i>sip</i> ▪ Transport Method: <i>tls</i> ▪ Peer Detection Enabled: <i>y</i> ▪ Near-end Node Name: <i>procr</i> This node name maps to the IP address of Communication Manager processor interface. ▪ Near-end Listen Port: <i>5061</i> ▪ Far-end Node Name: <i>SM_21_31</i> This node name maps to the IP address of Session Manager. ▪ Far-end Listen Port: <i>5061</i> ▪ Far-end Network Region: <i>1</i> This defines the IP network region which contains Session Manager. ▪ Far-end Domain: <i>avaya.com</i> This domain is sent in the “To” header of SIP messages of calls using this signaling group. ▪ Direct IP-IP Audio Connections: <i>y</i> This field must be set to <i>y</i> to enable media shuffling on the SIP trunk. ▪ Initial IP-IP Direct Media: <i>y</i> This field must be set to <i>y</i>. See Section 2.2 for more information. <pre> display signaling-group 91 SIGNALING GROUP Page 1 of 2 Group Number: 91 Group Type: sip IMS Enabled? n Transport Method: tls 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 Near-end Node Name: procr Far-end Node Name: SM_21_31 Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: avaya.com Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Bypass If IP Threshold Exceeded? n RFC 3389 Comfort Noise? n Session Establishment Timer(min): 3 Direct IP-IP Audio Connections? y IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? y H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6 </pre>

Step	Description
6.	<p>Trunk Group</p> <p>Trunk group 91 was used for the SIP trunk group between Communication Manager and Session Manager. The signaling groups and trunk groups between the two sites of the reference configuration is assumed to already be in place and not described in this document. Trunk group 91 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Group Type: <i>sip</i> ▪ TAC: <i>191</i> Enter an valid value consistent with the Communication Manager dial plan ▪ Member Assignment Method: <i>auto</i> ▪ Signaling Group: <i>91</i> This field is set to the signaling group shown in the previous step. ▪ Number of Members: <i>50</i> This field represents the number of trunk group members in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. <pre> display trunk-group 91 Page 1 of 21 TRUNK GROUP Group Number: 91 Group Type: sip CDR Reports: y Group Name: to_SM_21_31 COR: 1 TN: 1 TAC: 191 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 91 Number of Members: 50 </pre> <p>On Page 3:</p> <ul style="list-style-type: none"> ▪ The Numbering Format field was set to <i>private</i>. This field specifies the format of the calling party number sent to the far-end. ▪ The default values may be retained for the other fields. <pre> display trunk-group 91 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y Numbering Format: private UUI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Modify Tandem Calling Number: no </pre>

Step	Description																												
7.	<p>Private Numbering</p> <p>Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across any trunk group will be sent as a 5-digit calling number. The calling party number is sent to the far-end in the SIP “From” header.</p> <div><div>display private-numbering 0</div><div>Page 1 of 2</div><div>NUMBERING - PRIVATE FORMAT</div><table><tr><td>Ext</td><td>Ext</td><td>Trk</td><td>Private</td><td>Total</td><td></td></tr><tr><td>Len</td><td>Code</td><td>Grp(s)</td><td>Prefix</td><td>Len</td><td></td></tr><tr><td>5</td><td>3</td><td></td><td></td><td>5</td><td>Total Administered: 1</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>Maximum Entries: 540</td></tr></table></div>	Ext	Ext	Trk	Private	Total		Len	Code	Grp(s)	Prefix	Len		5	3			5	Total Administered: 1						Maximum Entries: 540				
Ext	Ext	Trk	Private	Total																									
Len	Code	Grp(s)	Prefix	Len																									
5	3			5	Total Administered: 1																								
					Maximum Entries: 540																								
8.	<p>Automatic Alternate Routing</p> <p>Automatic Alternate Routing (AAR) was used to route calls either to Session Manager or to the Communication Manager at the other site. Use the change aar analysis command to create an entry in the AAR Digit Analysis Table. The example below shows numbers that begin with 39 and are 5 digits long use route pattern 91 (to Session Manager). Numbers that begin with 2 and are 5 digits long use route pattern 7, which routes calls to Communication Manager at the other site via a SIP trunk (route pattern 3 was also used at times to route calls to Communication Manager at the other site via an ISDN-PRI trunk).</p> <div><div>change aar analysis 2</div><div>Page 1 of 2</div><div>AAR DIGIT ANALYSIS TABLE</div><div>Location: all</div><div>Percent Full: 0</div><table><tr><td></td><td>Dialed</td><td>Total</td><td>Route</td><td>Call</td><td>Node</td><td>ANI</td></tr><tr><td></td><td>String</td><td>Min Max</td><td>Pattern</td><td>Type</td><td>Num</td><td>Reqd</td></tr><tr><td>2</td><td></td><td>5 5</td><td>7</td><td>aar</td><td></td><td>n</td></tr><tr><td>39</td><td></td><td>5 5</td><td>91</td><td>aar</td><td></td><td>n</td></tr></table></div>		Dialed	Total	Route	Call	Node	ANI		String	Min Max	Pattern	Type	Num	Reqd	2		5 5	7	aar		n	39		5 5	91	aar		n
	Dialed	Total	Route	Call	Node	ANI																							
	String	Min Max	Pattern	Type	Num	Reqd																							
2		5 5	7	aar		n																							
39		5 5	91	aar		n																							

Step	Description
9.	<p>Route Pattern</p> <p>Route pattern 91 was used for calls destined for the XMediusFAX fax server through Session Manager. Route patterns 7 and 3 (not shown) were used for calls destined for the other site in the reference configuration. Route pattern 91 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Pattern Name: Any descriptive name. ▪ Grp No: 91 This field is set to the trunk group number defined in Step 6. ▪ FRL: 0 This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive. ▪ Numbering Format: <i>lev0-pvt</i>
	<pre> change route-pattern 91 Pattern Number: 91 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 91 0 2: 3: 4: 5: 6: n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Subaddress Dgts Format 1: y y y y y n n rest lev0-pvt none 2: y y y y y n n rest none 3: y y y y y n n rest none 4: y y y y y n n rest none 5: y y y y y n n rest none 6: y y y y y n n rest none </pre>

6. Configure Avaya Aura® Session Manager

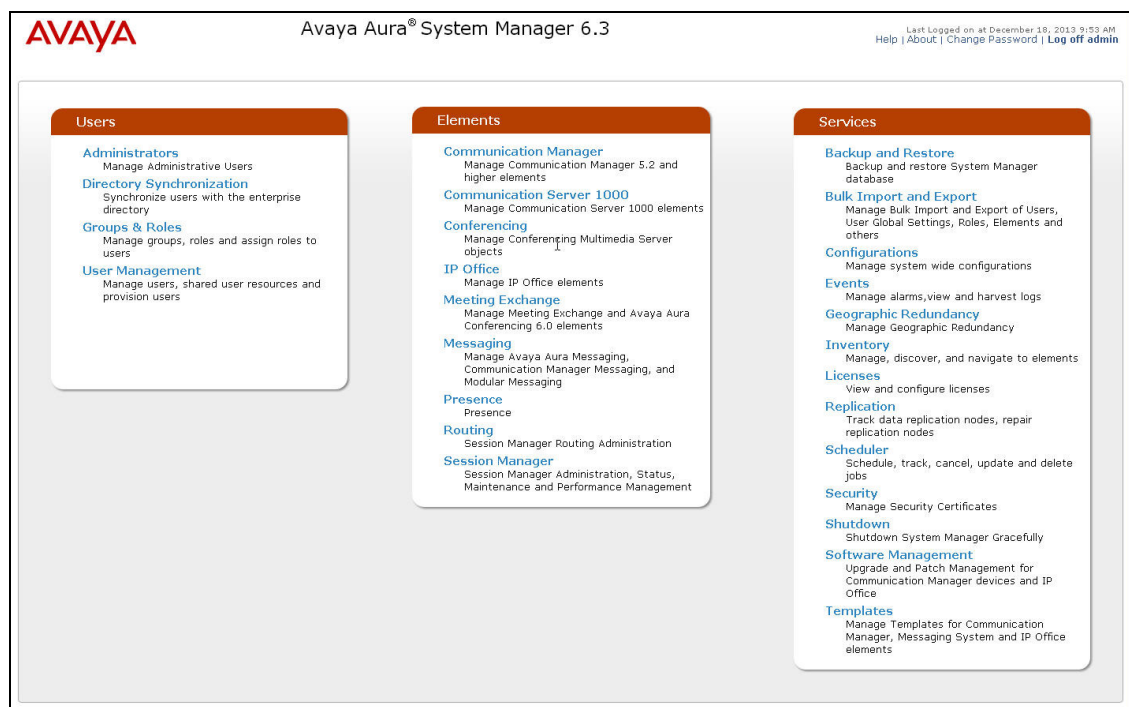
This section provides the procedures for configuring Session Manager as provisioned at Site 1 in the reference configuration. Although not shown in this document, a similar Session Manager configuration would be required at Site 2. All provisioning for Session Manager is performed via the System Manager web interface.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

1. Login

Access the System Manager administration web interface by entering `https://<ip-addr>/SMGR/` as the URL in an Internet browser, where `<ip-addr>` is the IP address of the System Manager server.

Log in with the appropriate credentials. The main page for the administrative interface is shown below.



2.

Add SIP Domain

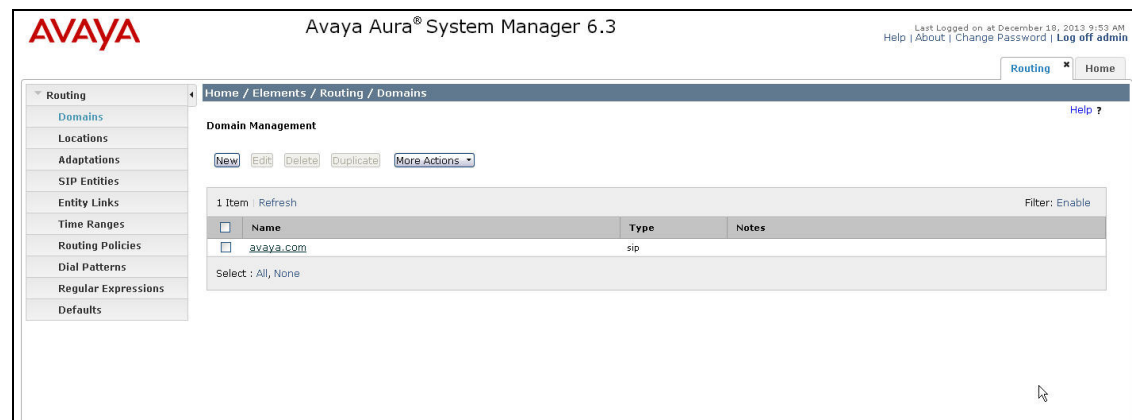
The **Routing** menu contains all the configuration tasks listed at the beginning of this section.

During compliance testing, one SIP Domain was configured.

Navigate to **Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with

- **Name:** *avaya.com* (as set in **Section 5, Step 2**)
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.



3.

Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured at each site for compliance testing.

Navigate to **Routing→Locations** and click the **New** button (not shown) to add the Location.

Under **General**:

- **Name:** a descriptive name
- **Notes:** optional descriptive text

Under **Location Pattern**, click the **Add** button to add a new line:

- **IP Address Pattern:** **10.64.101.*** and **10.64.21.***
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Locations

Location Details [Commit](#) [Cancel](#) [Help ?](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
 See Session Manager -> Session Manager Administration -> Global Settings

General

* **Name:**

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* **Default Audio Bandwidth:**

Alarm Threshold

Audio Alarm Threshold: %

* **Latency before Audio Alarm Trigger:** Minutes

Location Pattern

[Add](#) [Remove](#)

2 Items [Refresh](#) [Filter: Enable](#)

IP Address Pattern	Notes
* 10.64.101.*	
* 10.64.21.*	

Select : All, None

4.

Add Adaptation

An Adaptation was created and applied to the “Fax Server” SIP entity to override the destination domain as shown below.

The ingressOverrideDestinationDomain (**iodstd**) **Module parameter** replaces the domain in the Request-URI, To Header (if administered), and Notify/message-summary body with *avaya.com* for ingress only.

The overrideDestinationDomain (**odstd**) **Module parameter** replaces the domain in the Request-URI, To Header (if administered), Refer-To header, and Notify/message-summary body with the IP address of the fax server *10.64.101.118* for egress only.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptation Details [Commit](#) [Cancel](#) [Help ?](#)

General

* Adaptation name: XMediusFAX Domain 1

Module name: DigitConversionAdapter

Module parameter: iodstd=avaya.com odstd=10.6

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

[Add](#) [Remove](#)

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

[Add](#) [Remove](#)

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

[Commit](#) [Cancel](#)

5.	<p>Add SIP Entities</p> <p>A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP Entity was added for the Session Manager itself, Communication Manager, and the XMediusFAX fax server.</p> <p>Navigate to Routing→SIP Entities, and click the New button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for Session Manager are as follows:</p> <p>Under General:</p> <ul style="list-style-type: none"> ▪ Name: a descriptive name ▪ FQDN or IP Address: <i>10.64.21.31</i> as specified in Figure 1. This is the IP address assigned to the signaling interface of the Session Manager. ▪ Type: select <i>Session Manager</i> <p>Under Port, click Add, then edit the fields in the resulting new row as shown below:</p> <ul style="list-style-type: none"> ▪ Port: <i>5061</i>. This is the port number on which the system listens for SIP requests. ▪ Protocol: <i>TLS</i>. The TLS transport protocol was used between Session Manager and Communication Manager. ▪ Default Domain: select the SIP Domain created in Step 2. ▪ Repeat the three bullets above, but select <i>5060</i> for Port and <i>TCP</i> for Protocol. The TCP protocol was used between Session Manager and the XMediusFAX fax server. <p>Default settings can be used for the remaining fields. Click Commit to save the SIP Entity definition.</p>
----	---

Add SIP Entities (continued) – Session Manager

The screens below show the SIP Entity configuration details for the Session Manager.

AVAYAAvaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
Help | About | Change Password | Log off admin

RoutingHome

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

Home / Elements / Routing / SIP Entities

CommitCancelHelp ?

SIP Entity Details
General
* Name: SM_21_31
* FQDN or IP Address: 10.64.21.31
Type: Session Manager
Notes:
Location: .21 and .101 Subnet
Outbound Proxy:
Time Zone: America/Denver
Credential name:
SIP Link Monitoring: Use Session Manager Configuration

Entity Links
Add Remove
15 Items RefreshFilter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AAM_21_72	* 5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_20_72	* 5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 15060	FT_21_211	* 5063	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TCP	* 5060	iview	* 5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	bambam	* 5061	trusted	<input type="checkbox"/>

Select : All, None< PreviousPage 1 of 3Next >

Port
TCP Failover port:
TLS Failover port:
Add Remove
4 Items RefreshFilter: Enable

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

Add SIP Entities (continued)

The screen below shows the SIP Entity configuration details for the Communication Manager. Note the **CM** selection for **Type**.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:

- Name: CM_101_12
- FQDN or IP Address: 10.64.101.12
- Type: CM (selected in a dropdown)
- Notes: (empty text field)
- Adaptation: (empty dropdown)
- Location: (empty dropdown)
- Time Zone: America/Denver (selected in a dropdown)
- Override Port & Transport with DNS SRV: (unchecked checkbox)
- SIP Timer B/F (in seconds): 4
- Credential name: (empty text field)
- Call Detail Recording: none (selected in a dropdown)
- Loop Detection Mode: Off (selected in a dropdown)
- SIP Link Monitoring: Use Session Manager Configuration (selected in a dropdown)

Links for 'Loop Detection' and 'SIP Link Monitoring' are visible at the bottom left of the configuration area.

The screen below shows the SIP Entity configuration details for the XMediusFAX fax server. Note the **SIP Trunk** selection for **Type**, and the **Adaptation** created in **Step 4** of this section is selected.

The screenshot displays the Avaya Aura System Manager 6.3 interface for a different SIP entity. The configuration fields are as follows:

- Name: Sagemcom XMediusFAX 1
- FQDN or IP Address: 10.64.101.118
- Type: SIP Trunk (selected in a dropdown)
- Notes: (empty text field)
- Adaptation: XMediusFAX Domain 1 (selected in a dropdown)
- Location: (empty dropdown)
- Time Zone: America/Denver (selected in a dropdown)
- Override Port & Transport with DNS SRV: (unchecked checkbox)
- SIP Timer B/F (in seconds): 4
- Credential name: (empty text field)
- Call Detail Recording: egress (selected in a dropdown)
- Loop Detection Mode: Off (selected in a dropdown)
- SIP Link Monitoring: Use Session Manager Configuration (selected in a dropdown)

6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created: one between Session Manager and Communication Manager; the other between Session Manager and the XMediusFAX fax server.

Navigate to **Routing→Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to Communication Manager.

- **Name:** a descriptive name
- **SIP Entity 1:** select the Session Manager SIP Entity.
- **Port:** **5061**. This is the port number to which the other system sends SIP requests.
- **SIP Entity 2:** select the Communication Manager SIP Entity.
- **Port:** **5061**. This is the port number on which the other system receives SIP requests.
- **Trusted:** check this box
- **Protocol:** select **TLS** as the transport protocol.
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation 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 is titled 'Home / Elements / Routing / Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below these is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. The table contains one item: Name: SM_21_31_CM_10, SIP Entity 1: SM_21_31, Protocol: TLS, Port: 5061, SIP Entity 2: CM_101_12, Port: 5061, Connection Policy: trusted, Deny New Service: unchecked, and Notes: empty. A 'Filter: Enable' button is located to the right of the table. Below the table is a 'Select: All, None' option.

The Entity Link for connecting Session Manager to the XMediusFAX fax server was similarly defined as shown in the screen below.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation 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 is titled 'Home / Elements / Routing / Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below these is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. The table contains one item: Name: SM_21_31_Sagem, SIP Entity 1: SM_21_31, Protocol: TCP, Port: 5060, SIP Entity 2: Sagemcom XMediusFAX 1, Port: 5060, Connection Policy: trusted, Deny New Service: unchecked, and Notes: empty. A 'Filter: Enable' button is located to the right of the table. Below the table is a 'Select: All, None' option.

7.

Add Time Ranges

Before adding routing policies (configured in next step), time ranges must be defined during which the policies will be active. One Time Range was defined that would allow routing to occur at anytime.

Navigate to **Routing→Time Ranges**, and click the **New** button to add a new Time Range:

- **Name:** a descriptive name
- **Mo through Su:** check the box under each of these headings
- **Start Time:** enter **00:00**
- **End Time:** enter **23:59**

Click **Commit** to save this time range. The screen below shows the configured Time Range.

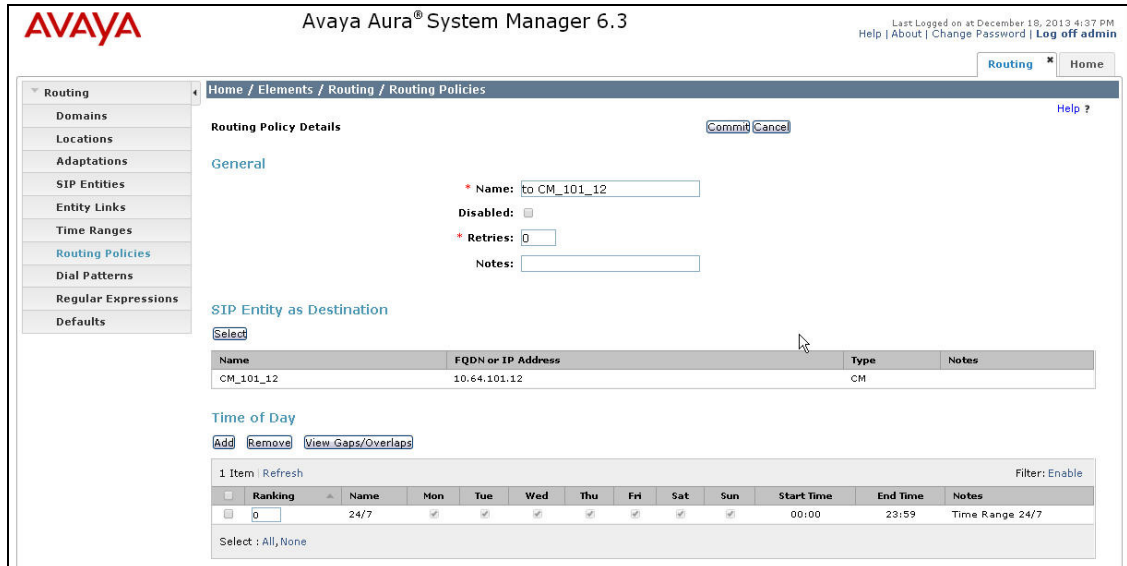
The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges (highlighted), Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Time Ranges' and shows a table with one item, '24/7'. The table has columns for Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The '24/7' item is active for all days of the week (Mo, Tu, We, Th, Fr, Sa, Su) and has a Start Time of 00:00 and an End Time of 23:59. The Notes column contains 'Time Range 24/7'.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
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

8.	<p>Add Routing Policies</p> <p>Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. Two routing policies were added – one for routing calls to Communication Manager, and the other for routing calls to the XMediusFAX fax server.</p> <p>Navigate to Routing→Routing Policies, and click the New button (not shown) to add a new Routing Policy.</p> <p>Under General:</p> <ul style="list-style-type: none"> ▪ Name: a descriptive name ▪ Notes: optional descriptive text <p>Under SIP Entity as Destination</p> <p>Click Select to select the appropriate SIP Entity to which the routing policy applies (not shown).</p> <p>Under Time of Day</p> <p>Click Add to select the Time Range configured in the previous step (not shown).</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>
----	--

Add Routing Policies (continued)

The screens below show the configuration details for the two Routing Policies used during compliance testing, one for Communication Manager and another for the XMediusFAX fax server.



Avaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
Help | About | Change Password | Log off admin

Routing Policy Details

General

* Name: to CM_101_12

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM_101_12	10.64.101.12	CM	

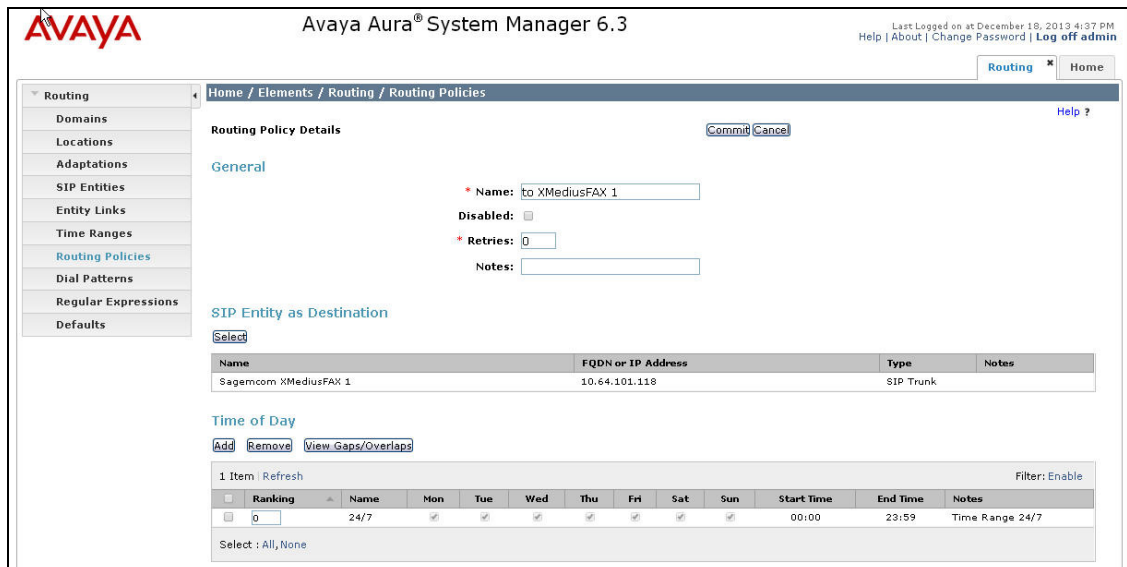
Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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



Avaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
Help | About | Change Password | Log off admin

Routing Policy Details

General

* Name: to XMediusFAX 1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Sagemcom XMediusFAX 1	10.64.101.118	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

9.

Add Dial Patterns

Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 5-digit extensions beginning with “2” were routed to Communication Manager for onward routing to Site 2. 5-digit extensions beginning with “31” were routed to local Communication Manager endpoints at Site 1. 5-digit extensions beginning with “39” were routed to the XMediusFAX fax server at Site 1. Therefore 3 Dial Patterns were created accordingly.

Navigate to **Routing→Dial Patterns**, click the **New** button (not shown) to add a new Dial Pattern.

Under **General**:

- **Pattern**: dialed number or prefix
- **Min**: minimum length of dialed number
- **Max**: maximum length of dialed number
- **SIP Domain**: select the SIP Domain created in **Step 2** (or select **–ALL–** to be less restrictive)
- **Notes**: optional descriptive text

Under **Originating Locations and Routing Policies**

Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown).

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

The screens below shows the configuration details for the Dialed Pattern defined for routing calls to Site 2 via Communication Manager.

Avaya Aura® System Manager 6.3

Last Logged on at December 18, 2013 4:37 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 2

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

Originating Location Name	Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-	to CM_101_12	CM_101_12		<input type="checkbox"/>	CM_101_12	

Select : All, None

Add Dial Patterns (continued)

The screens below show the configuration details for the Dialed Patterns defined for routing calls to local Communication Manager endpoints.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: 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'. Below this, the 'Dial Pattern Details' section is visible, with a 'General' tab selected. The configuration fields include: Pattern (31), Min (5), Max (5), Emergency Call (unchecked), Emergency Priority (1), Emergency Type (empty), SIP Domain (-ALL-), and Notes (empty). Below the configuration fields, there is a section titled 'Originating Locations and Routing Policies' with an 'Add' button and a 'Remove' button. A table shows one item with the following data:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		to CM_101_12		<input type="checkbox"/>	CM_101_12	

At the bottom of the table, it says 'Select : All, None'.

The screen below shows the configuration details for the Dialed Pattern defined for routing calls to the XMediusFAX fax server.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: 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'. Below this, the 'Dial Pattern Details' section is visible, with a 'General' tab selected. The configuration fields include: Pattern (39), Min (5), Max (5), Emergency Call (unchecked), Emergency Priority (1), Emergency Type (empty), SIP Domain (-ALL-), and Notes (empty). Below the configuration fields, there is a section titled 'Originating Locations and Routing Policies' with an 'Add' button and a 'Remove' button. A table shows one item with the following data:

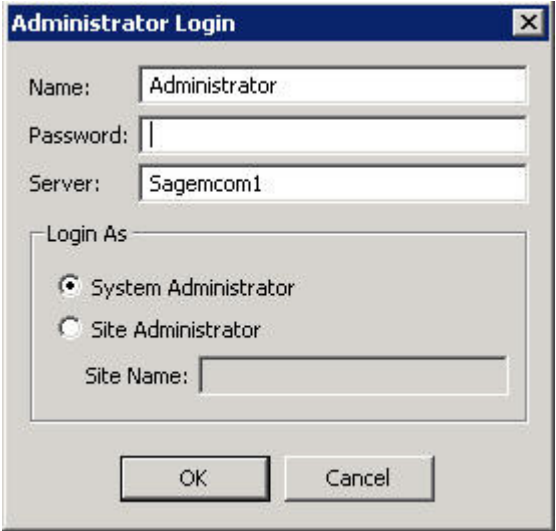
Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		to XMediusFAX 1		<input type="checkbox"/>	Sagemcom XMediusFAX 1	

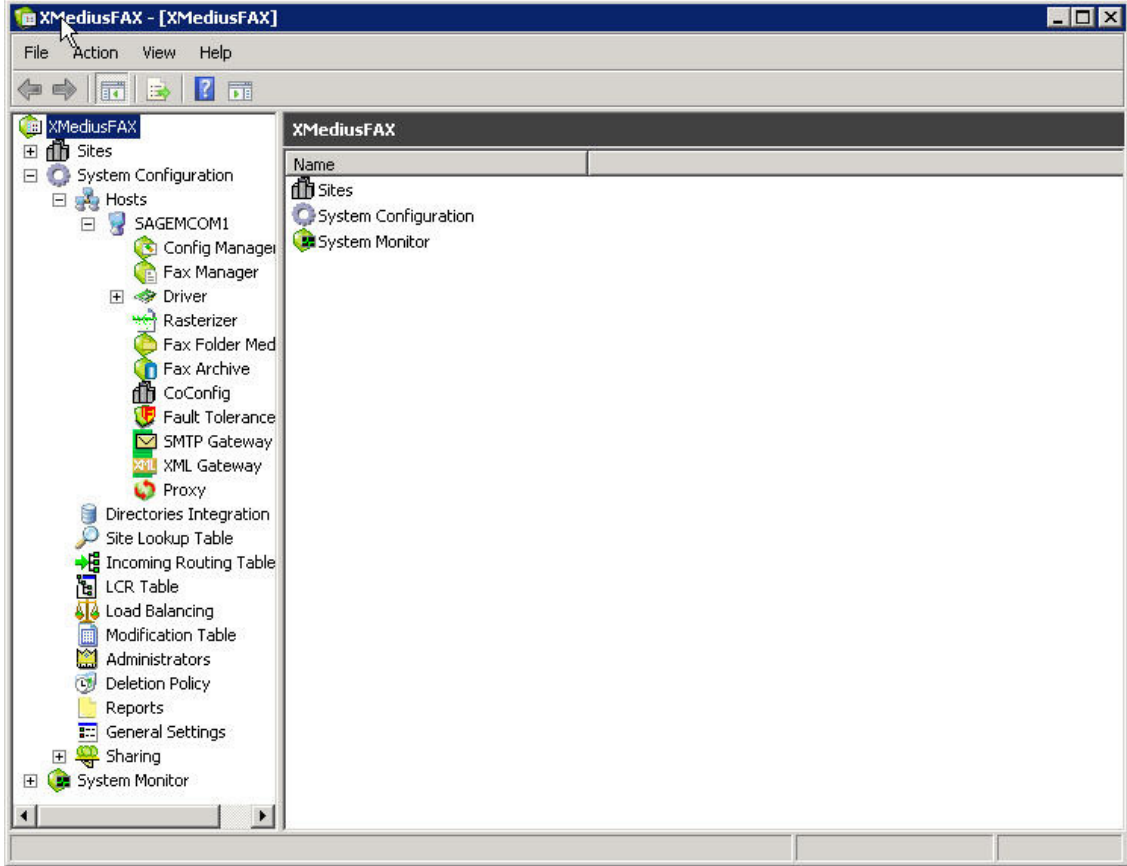
At the bottom of the table, it says 'Select : All, None'.

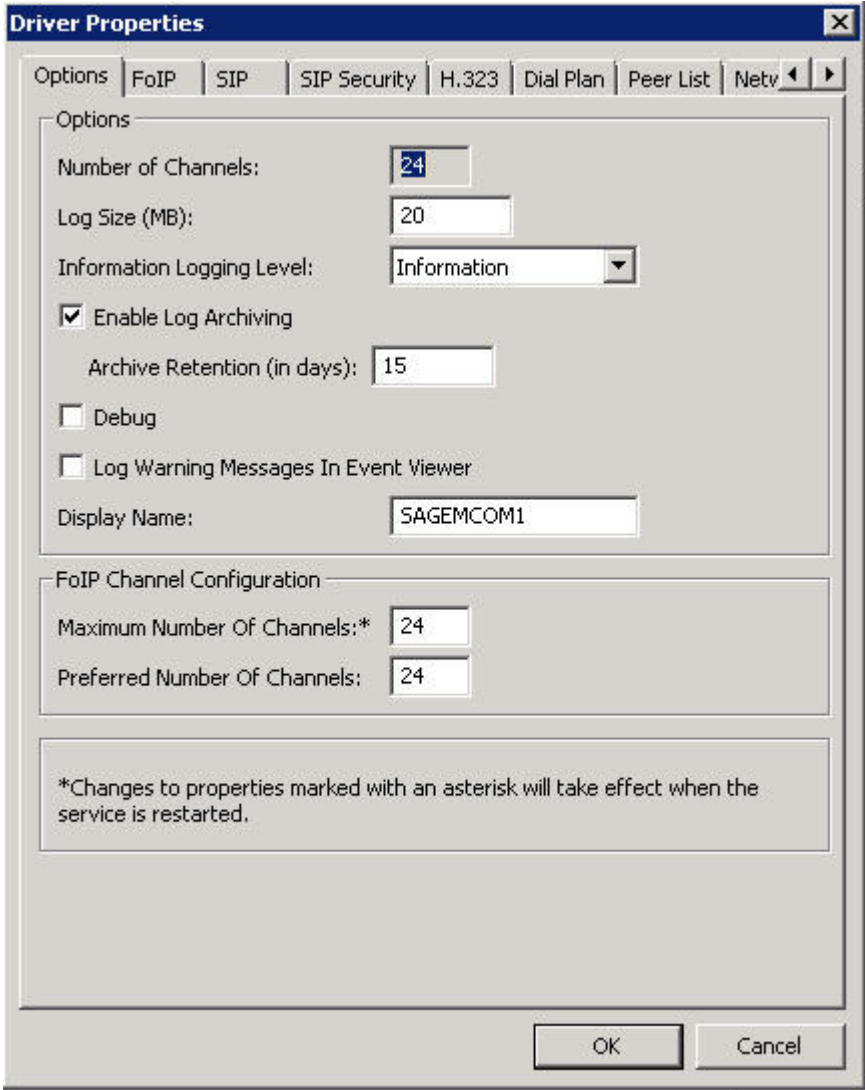
7. Configure Sagemcom XMediusFAX

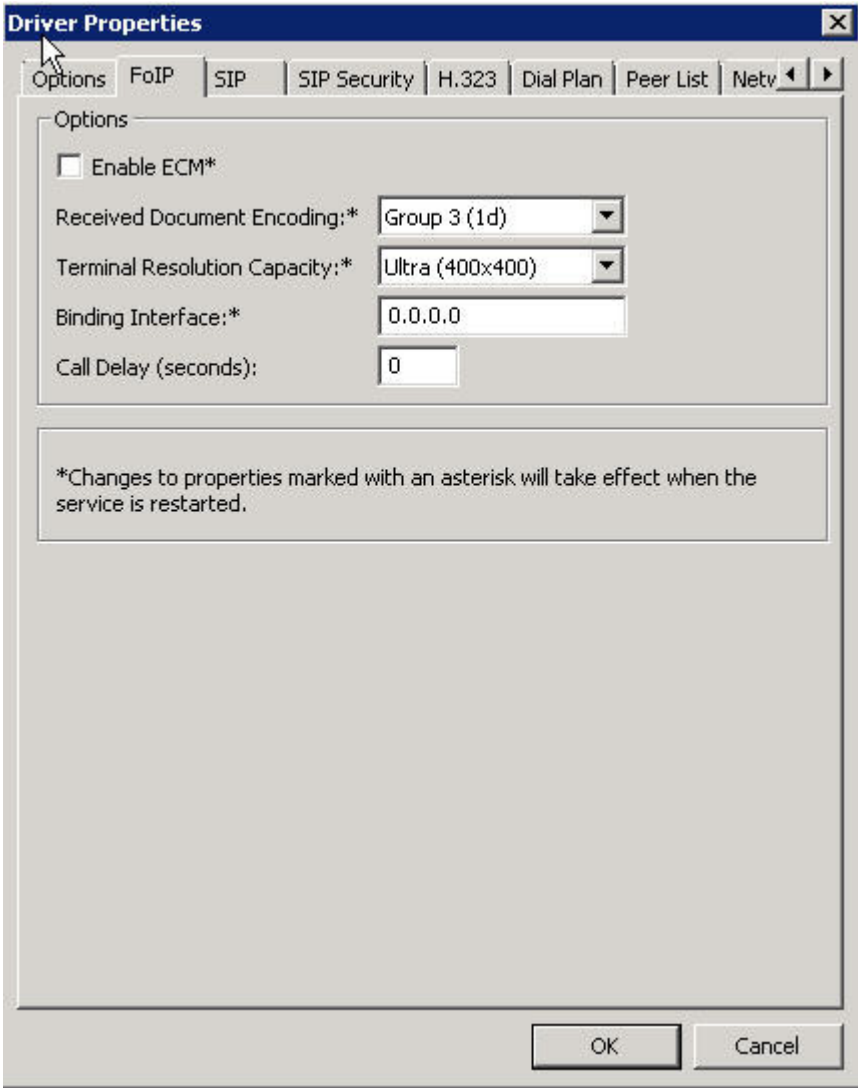
This section describes the configuration of XMediusFAX. It assumes that the application and all required software components have been installed and properly licensed. The number of channels supported by the XMediusFAX server is controlled via an XMediusFAX server license file. For instructions on sending and receiving faxes, consult the XMediusFAX Administrator Guide [3] and User Guide [5].

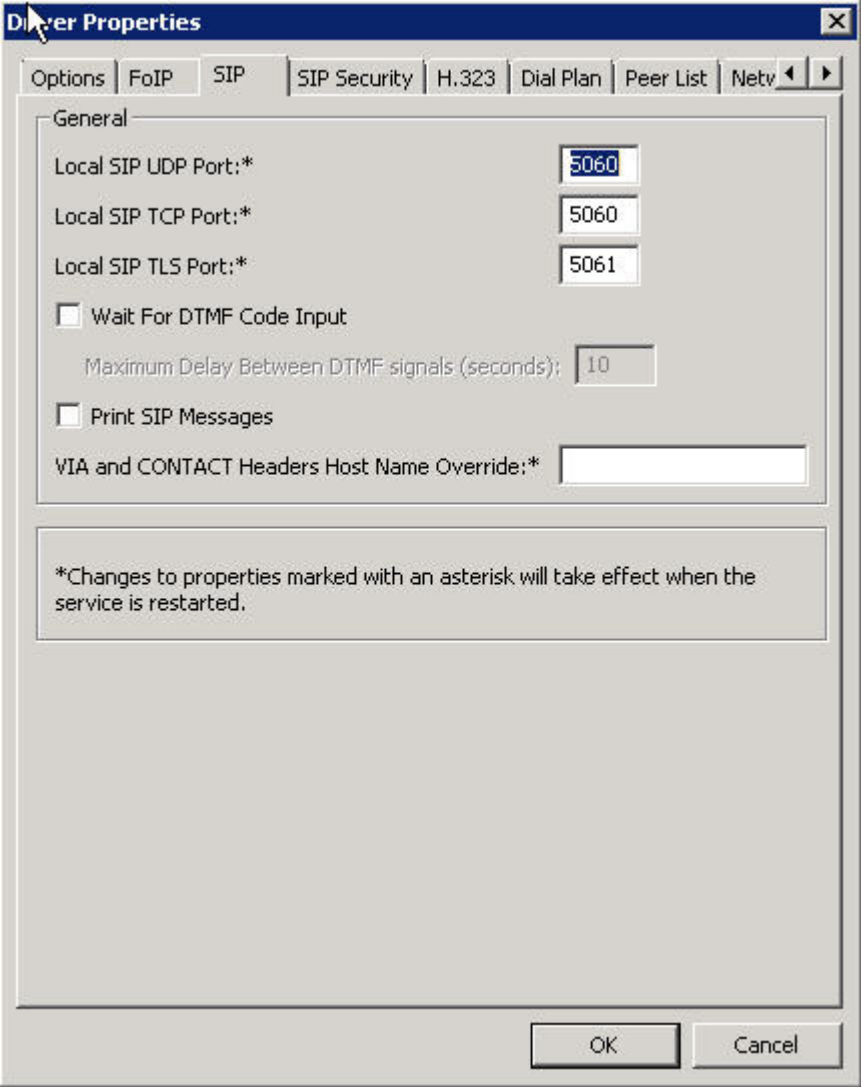
The examples shown in this section refer to Site 1. Unless specified otherwise, the same steps also apply to Site 2 using values appropriate for Site 2 from **Figure 1**.

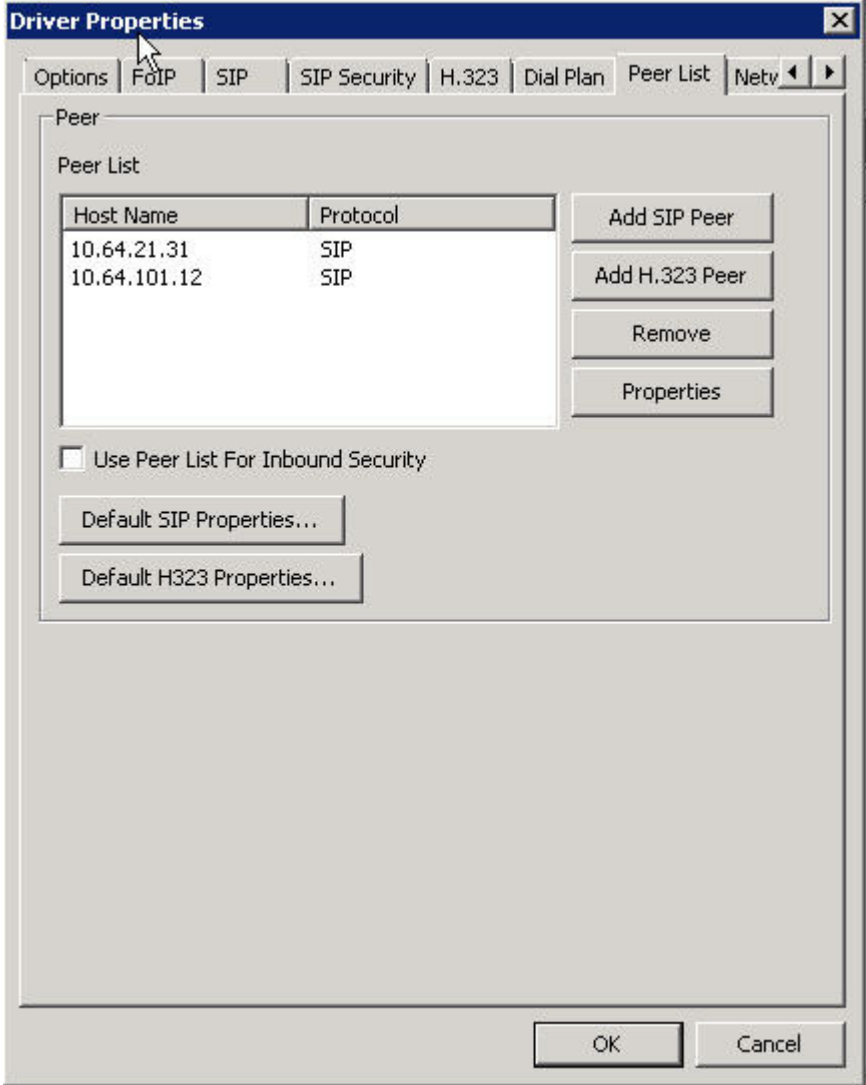
Step	Description
1.	<p>Launch the Application</p> <p>On the XMediusFAX server, launch the XMediusFAX application from the Windows Start Menu. Navigate to Start → All Programs → XMediusFAX → XMediusFAX. A login screen appears. Log in with proper credentials. Click the OK button.</p> 

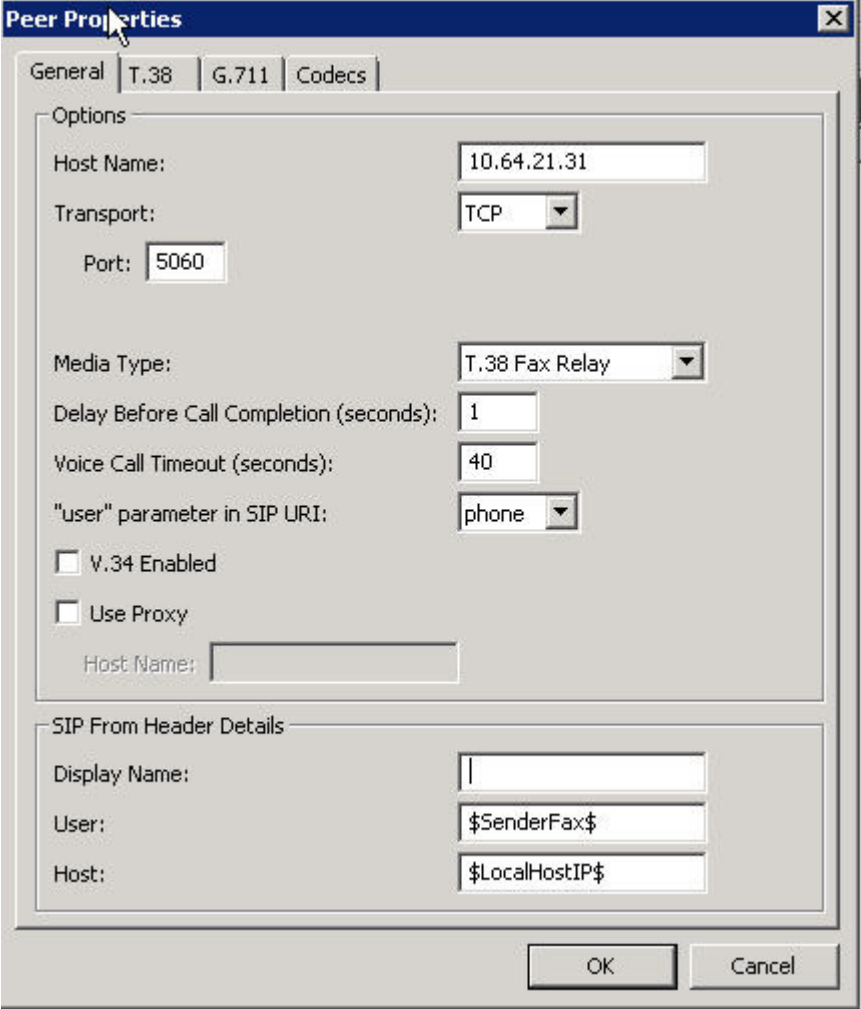
Step	Description
2.	<p>Configure Driver Properties</p> <p>On the main screen, navigate to XMediusFAX → System Configuration → Hosts → SAGENCOM1 → Driver in the left hand tree menu. Right-click on Driver and select Properties (not shown).</p>
	

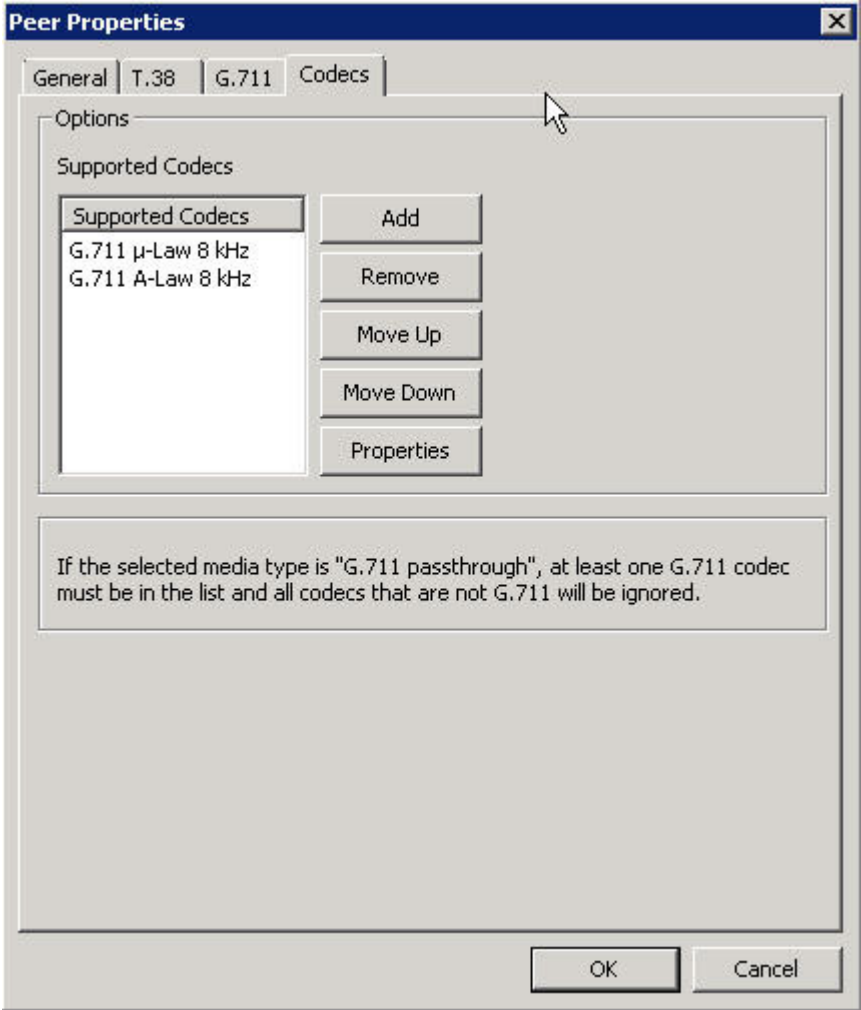
Step	Description
3.	<p>General Options On the Driver Properties screen, select the Options tab. Set the Maximum Number Of Channels and Preferred Number Of Channels fields under FoIP Channel Configuration to the number of simultaneous faxes to be processed.</p> 

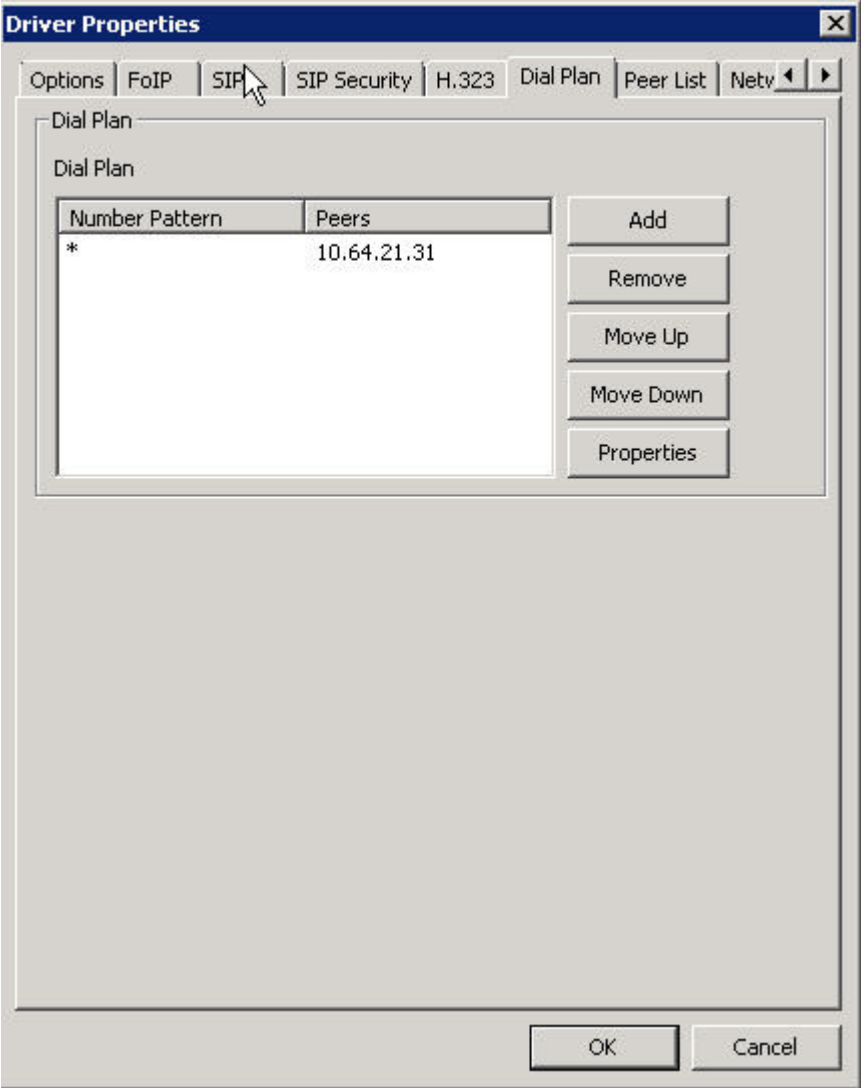
Step	Description
4.	<p>T.38 Parameters</p> <p>On the Driver Properties screen, select the FoIP tab. Configure the fields as follows:</p> <ul style="list-style-type: none"> ▪ Received Document Encoding – Set this field to the highest encoding allowed. For the compliance test, this value was set to <i>Group 3 (1d)</i>. ▪ Terminal Resolution Capacity – Set this field to the highest resolution allowed for incoming calls. For the compliance test, this value was set to <i>Ultra (400x400)</i>. 

Step	Description
5.	<p>SIP Parameters</p> <p>On the Driver Properties screen, select the SIP tab. Configure the Local SIP TCP Port field to match the first Port field of the fax server SIP Entity Link entry configured in Section 6, Step 6. During compliance testing, TCP was used as the transport layer protocol by the XMediusFAX fax server.</p> 

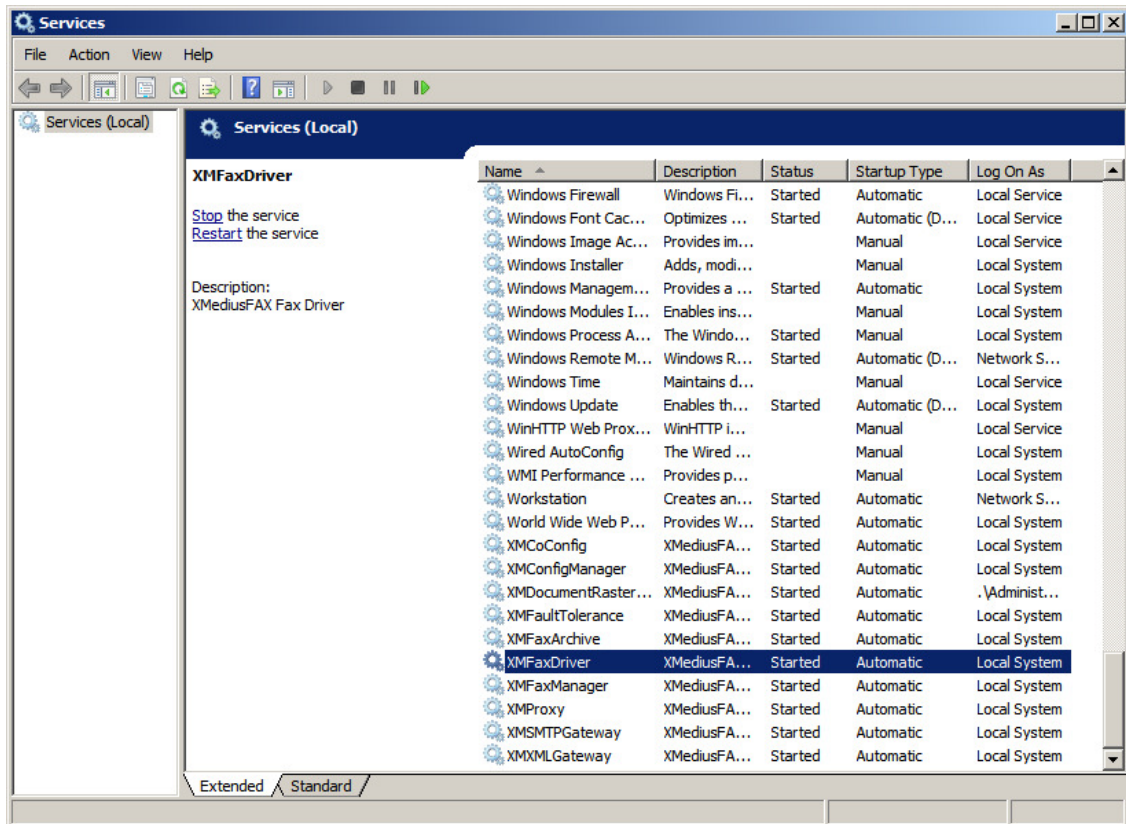
Step	Description
6.	<p>Peer List</p> <p>On the Driver Properties screen, select the Peer List tab. To add a new SIP peer, select the Add SIP Peer button and enter the values shown in Step 7 below. To view an existing peer, highlight the peer in the list and click Properties. The example below shows the peer list after the Session Manager interface, 10.64.21.31, and the Communication Manager processor interface, 10.64.101.12, have been added to the list.</p> <p>Note: The Communication Manager processor interface is needed to support G.711 pass-through fax mode. For T.38 fax mode, the entry is not required.</p> 

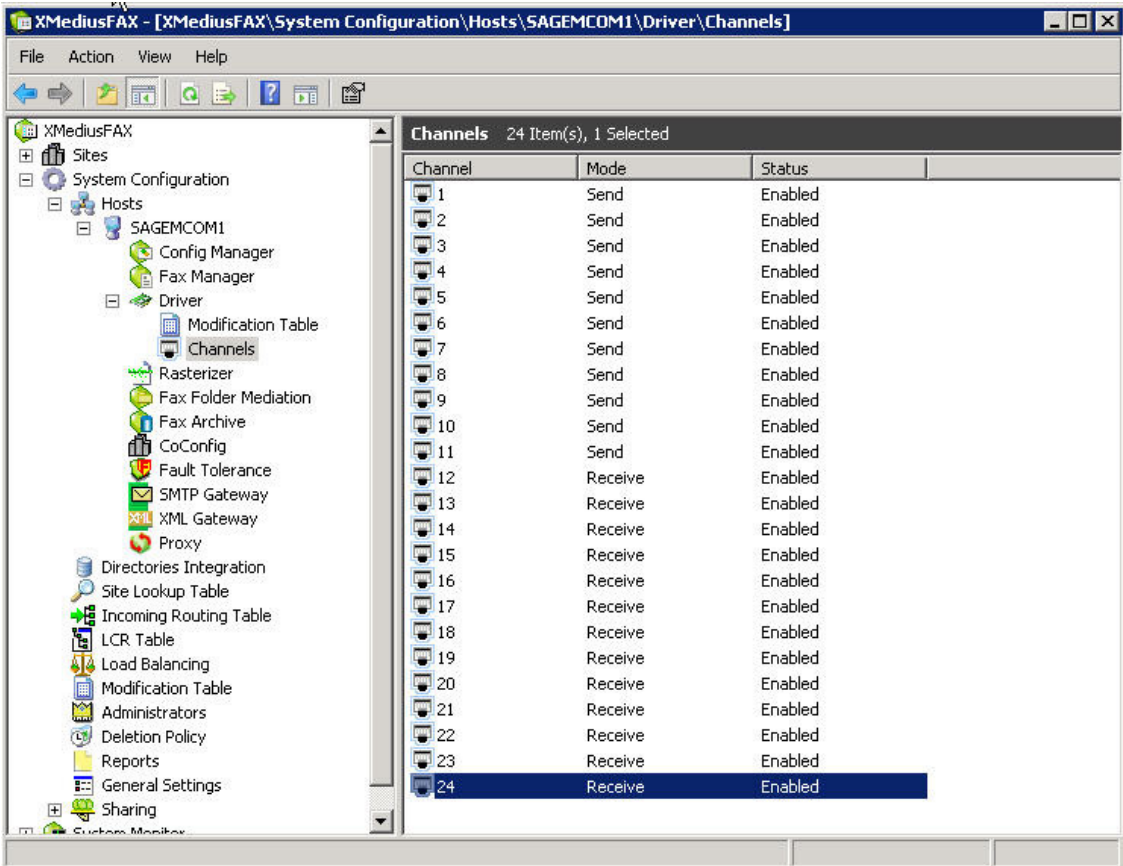
Step	Description
7.	<p>Peer Properties for Session Manager</p> <p>On the Peer Properties screen, configure as follows:</p> <ul style="list-style-type: none"> ▪ Host Name – Set this field to the IP address of Session Manager. ▪ Transport - Set this field to TCP. During compliance testing, TCP was used as the transport layer protocol by the XMediusFAX fax server. ▪ Port - Set this field to 5060. ▪ Media Type – Set this field to T.38 Fax Relay for the T.38 fax mode, or G.711 Passthrough for the pass-through fax mode.  <p>The Peer Properties entry for Communication Manager uses the same values except the Host Name field where the IP address of Communication Manager should be used.</p>

Step	Description
8.	<p>Codec</p> <p>On the Peer Properties screen, select the Codec tab. To add a codec for the SIP peer, select the Add button and select the values from the drop-down menu. To view an existing codec, highlight the codec in the list and click Properties. The example below shows that the default codec list is supported by the newly added SIP peer.</p> 

Step	Description
9.	<p>Dial Plan</p> <p>On the Driver Properties screen, select the Dial Plan tab. To add a new entry to the dial plan, select the Add button and enter the values shown in Step 10. To view an existing entry, highlight the entry in the list and click Properties to get the Number Pattern Properties screen. The example below shows the dial plan after the entry for * (any value) has been added to the list.</p>  <p>Note: no entry is needed for the Communication Manager SIP peer.</p>

Step	Description				
10.	<p>Number Pattern Properties</p> <p>On the Number Pattern Properties screen, configure as follows:</p> <ul style="list-style-type: none"> ▪ Number Pattern – Set this field to the pattern to match. In this example, the value of * indicates any dialed number is acceptable. ▪ Peer – Click the Add button. In the Peer Properties window that appears (not shown), enter the Peer IP Address and Preference value of 1 and click OK. In this example, only one peer is configured. <div data-bbox="492 556 1242 1081" data-label="Image"> <p>The screenshot shows a window titled 'Number Pattern Properties'. It has a 'Dial Plan' tab. Under 'Number Pattern', there is a text field containing an asterisk (*). Below this is a 'Peers' section with a table. The table has two columns: 'Peer' and 'Preference'. It contains one row with the IP address '10.64.21.31' and preference '1 (Higher)'. To the right of the table are three buttons: 'Add', 'Remove', and 'Properties'. At the bottom of the window are 'OK' and 'Cancel' buttons.</p> <table border="1" data-bbox="527 751 1024 989"> <thead> <tr> <th>Peer</th><th>Preference</th></tr> </thead> <tbody> <tr> <td>10.64.21.31</td><td>1 (Higher)</td></tr> </tbody> </table> </div> <p>Lastly, click OK on the Driver Properties screen shown in Step 9, to accept the Driver Configuration.</p>	Peer	Preference	10.64.21.31	1 (Higher)
Peer	Preference				
10.64.21.31	1 (Higher)				

Step	Description																																																																																																																																		
11.	<p>Once all the driver properties have been configured, go to Start → Control Panel → Administrative Tools → Services to stop and start the XMFaxDriver service to make the changes take effect.</p>  <p>The screenshot shows the Windows Services console. The 'Services (Local)' window is open, displaying a list of services. The 'XMFaxDriver' service is highlighted. The 'Description' field shows 'XMediusFAX Fax Driver'. The 'Status' is 'Started', 'Startup Type' is 'Automatic', and 'Log On As' is 'Local System'.</p> <table border="1"><thead><tr><th>Name</th><th>Description</th><th>Status</th><th>Startup Type</th><th>Log On As</th></tr></thead><tbody><tr><td>Windows Firewall</td><td>Windows Fi...</td><td>Started</td><td>Automatic</td><td>Local Service</td></tr><tr><td>Windows Font Cac...</td><td>Optimizes ...</td><td>Started</td><td>Automatic (D...</td><td>Local Service</td></tr><tr><td>Windows Image Ac...</td><td>Provides im...</td><td></td><td>Manual</td><td>Local Service</td></tr><tr><td>Windows Installer</td><td>Adds, modi...</td><td></td><td>Manual</td><td>Local System</td></tr><tr><td>Windows Managem...</td><td>Provides a ...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>Windows Modules I...</td><td>Enables ins...</td><td></td><td>Manual</td><td>Local System</td></tr><tr><td>Windows Process A...</td><td>The Windo...</td><td>Started</td><td>Manual</td><td>Local System</td></tr><tr><td>Windows Remote M...</td><td>Windows R...</td><td>Started</td><td>Automatic (D...</td><td>Network S...</td></tr><tr><td>Windows Time</td><td>Maintains d...</td><td></td><td>Manual</td><td>Local Service</td></tr><tr><td>Windows Update</td><td>Enables th...</td><td>Started</td><td>Automatic (D...</td><td>Local System</td></tr><tr><td>WinHTTP Web Prox...</td><td>WinHTTP i...</td><td></td><td>Manual</td><td>Local Service</td></tr><tr><td>Wired AutoConfig</td><td>The Wired ...</td><td></td><td>Manual</td><td>Local System</td></tr><tr><td>WMI Performance ...</td><td>Provides p...</td><td></td><td>Manual</td><td>Local System</td></tr><tr><td>Workstation</td><td>Creates an...</td><td>Started</td><td>Automatic</td><td>Network S...</td></tr><tr><td>World Wide Web P...</td><td>Provides W...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMCoConfig</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMConfigManager</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMDocumentRaster...</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>. \Administ...</td></tr><tr><td>XMFaultTolerance</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMFaxArchive</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMFaxDriver</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMFaxManager</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMProxy</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMSMTPGateway</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr><tr><td>XMXMLGateway</td><td>XMediusFA...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr></tbody></table>	Name	Description	Status	Startup Type	Log On As	Windows Firewall	Windows Fi...	Started	Automatic	Local Service	Windows Font Cac...	Optimizes ...	Started	Automatic (D...	Local Service	Windows Image Ac...	Provides im...		Manual	Local Service	Windows Installer	Adds, modi...		Manual	Local System	Windows Managem...	Provides a ...	Started	Automatic	Local System	Windows Modules I...	Enables ins...		Manual	Local System	Windows Process A...	The Windo...	Started	Manual	Local System	Windows Remote M...	Windows R...	Started	Automatic (D...	Network S...	Windows Time	Maintains d...		Manual	Local Service	Windows Update	Enables th...	Started	Automatic (D...	Local System	WinHTTP Web Prox...	WinHTTP i...		Manual	Local Service	Wired AutoConfig	The Wired ...		Manual	Local System	WMI Performance ...	Provides p...		Manual	Local System	Workstation	Creates an...	Started	Automatic	Network S...	World Wide Web P...	Provides W...	Started	Automatic	Local System	XMCoConfig	XMediusFA...	Started	Automatic	Local System	XMConfigManager	XMediusFA...	Started	Automatic	Local System	XMDocumentRaster...	XMediusFA...	Started	Automatic	. \Administ...	XMFaultTolerance	XMediusFA...	Started	Automatic	Local System	XMFaxArchive	XMediusFA...	Started	Automatic	Local System	XMFaxDriver	XMediusFA...	Started	Automatic	Local System	XMFaxManager	XMediusFA...	Started	Automatic	Local System	XMProxy	XMediusFA...	Started	Automatic	Local System	XMSMTPGateway	XMediusFA...	Started	Automatic	Local System	XMXMLGateway	XMediusFA...	Started	Automatic	Local System
Name	Description	Status	Startup Type	Log On As																																																																																																																															
Windows Firewall	Windows Fi...	Started	Automatic	Local Service																																																																																																																															
Windows Font Cac...	Optimizes ...	Started	Automatic (D...	Local Service																																																																																																																															
Windows Image Ac...	Provides im...		Manual	Local Service																																																																																																																															
Windows Installer	Adds, modi...		Manual	Local System																																																																																																																															
Windows Managem...	Provides a ...	Started	Automatic	Local System																																																																																																																															
Windows Modules I...	Enables ins...		Manual	Local System																																																																																																																															
Windows Process A...	The Windo...	Started	Manual	Local System																																																																																																																															
Windows Remote M...	Windows R...	Started	Automatic (D...	Network S...																																																																																																																															
Windows Time	Maintains d...		Manual	Local Service																																																																																																																															
Windows Update	Enables th...	Started	Automatic (D...	Local System																																																																																																																															
WinHTTP Web Prox...	WinHTTP i...		Manual	Local Service																																																																																																																															
Wired AutoConfig	The Wired ...		Manual	Local System																																																																																																																															
WMI Performance ...	Provides p...		Manual	Local System																																																																																																																															
Workstation	Creates an...	Started	Automatic	Network S...																																																																																																																															
World Wide Web P...	Provides W...	Started	Automatic	Local System																																																																																																																															
XMCoConfig	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMConfigManager	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMDocumentRaster...	XMediusFA...	Started	Automatic	. \Administ...																																																																																																																															
XMFaultTolerance	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMFaxArchive	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMFaxDriver	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMFaxManager	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMProxy	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMSMTPGateway	XMediusFA...	Started	Automatic	Local System																																																																																																																															
XMXMLGateway	XMediusFA...	Started	Automatic	Local System																																																																																																																															

Step	Description																																																																											
12.	<p>Configure Channels</p> <p>On the main screen, navigate to XMediusFAX → System Configuration → Hosts → SAGEMCOM1 → Driver → Channels in the left hand tree menu. Right-click on each channel in the right pane to set the Mode to <i>Send</i>, <i>Receive</i> or <i>Both</i>. During compliance testing, 11 channels were set to <i>Send</i> and 13 channels were set to <i>Receive</i>.</p>  <table data-bbox="709 598 1424 1245"><thead><tr><th>Channel</th><th>Mode</th><th>Status</th></tr></thead><tbody><tr><td>1</td><td>Send</td><td>Enabled</td></tr><tr><td>2</td><td>Send</td><td>Enabled</td></tr><tr><td>3</td><td>Send</td><td>Enabled</td></tr><tr><td>4</td><td>Send</td><td>Enabled</td></tr><tr><td>5</td><td>Send</td><td>Enabled</td></tr><tr><td>6</td><td>Send</td><td>Enabled</td></tr><tr><td>7</td><td>Send</td><td>Enabled</td></tr><tr><td>8</td><td>Send</td><td>Enabled</td></tr><tr><td>9</td><td>Send</td><td>Enabled</td></tr><tr><td>10</td><td>Send</td><td>Enabled</td></tr><tr><td>11</td><td>Send</td><td>Enabled</td></tr><tr><td>12</td><td>Receive</td><td>Enabled</td></tr><tr><td>13</td><td>Receive</td><td>Enabled</td></tr><tr><td>14</td><td>Receive</td><td>Enabled</td></tr><tr><td>15</td><td>Receive</td><td>Enabled</td></tr><tr><td>16</td><td>Receive</td><td>Enabled</td></tr><tr><td>17</td><td>Receive</td><td>Enabled</td></tr><tr><td>18</td><td>Receive</td><td>Enabled</td></tr><tr><td>19</td><td>Receive</td><td>Enabled</td></tr><tr><td>20</td><td>Receive</td><td>Enabled</td></tr><tr><td>21</td><td>Receive</td><td>Enabled</td></tr><tr><td>22</td><td>Receive</td><td>Enabled</td></tr><tr><td>23</td><td>Receive</td><td>Enabled</td></tr><tr><td>24</td><td>Receive</td><td>Enabled</td></tr></tbody></table>	Channel	Mode	Status	1	Send	Enabled	2	Send	Enabled	3	Send	Enabled	4	Send	Enabled	5	Send	Enabled	6	Send	Enabled	7	Send	Enabled	8	Send	Enabled	9	Send	Enabled	10	Send	Enabled	11	Send	Enabled	12	Receive	Enabled	13	Receive	Enabled	14	Receive	Enabled	15	Receive	Enabled	16	Receive	Enabled	17	Receive	Enabled	18	Receive	Enabled	19	Receive	Enabled	20	Receive	Enabled	21	Receive	Enabled	22	Receive	Enabled	23	Receive	Enabled	24	Receive	Enabled
Channel	Mode	Status																																																																										
1	Send	Enabled																																																																										
2	Send	Enabled																																																																										
3	Send	Enabled																																																																										
4	Send	Enabled																																																																										
5	Send	Enabled																																																																										
6	Send	Enabled																																																																										
7	Send	Enabled																																																																										
8	Send	Enabled																																																																										
9	Send	Enabled																																																																										
10	Send	Enabled																																																																										
11	Send	Enabled																																																																										
12	Receive	Enabled																																																																										
13	Receive	Enabled																																																																										
14	Receive	Enabled																																																																										
15	Receive	Enabled																																																																										
16	Receive	Enabled																																																																										
17	Receive	Enabled																																																																										
18	Receive	Enabled																																																																										
19	Receive	Enabled																																																																										
20	Receive	Enabled																																																																										
21	Receive	Enabled																																																																										
22	Receive	Enabled																																																																										
23	Receive	Enabled																																																																										
24	Receive	Enabled																																																																										

S

8. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager→System Status→SIP Entity Monitoring**, and click on the appropriate SIP Entities to verify that the Entity Links to Communication Manager and the fax server are up.
- From the Communication Manager SAT, use the **status signaling-group x** command to verify that the SIP signaling group is in-service (where **x** is the signaling group number associated with the trunk between Communication Manager and Session Manager).
- From the Communication Manager SAT, use the **status trunk-group y** command to verify that the SIP trunk group is in-service (where **y** is the trunk group number for the trunk between Communication Manager and Session Manager).
- Verify that fax calls can be placed to/from the XMediusFAX fax server at each site.
- From the Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed over the expected trunks.

9. Conclusion

Sagemcom XMediusFAX passed compliance testing with two observations noted in **Section 2.2**. These Application Notes describe the procedures required to configure Sagemcom XMediusFAX to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support the network shown in **Figure 1**.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 9, October 2013, Document 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013

Product documentation for XMediusFAX 7.5 may be obtained from Sagemcom.

- [3] *Sagemcom XMediusFAX Administrator Guide, Version Number 7.5.0.28, October 2013*
- [4] *Sagemcom XMediusFAX Installation Guide, Version Number 7.5.0.28, October 2013*
- [5] *Sagemcom XMediusFAX User Guide, Version Number 7.5.0.28, October 2013*

©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.