



## Avaya Solution & Interoperability Test Lab

---

# **Application Notes for Configuring Sagem-Interstar XMediusFAX SP Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services via SIP Trunking Interface - Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring the Sagem-Interstar XMediusFAX SP Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services (SES) using a SIP trunk.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, XMediusFAX interoperates with the Avaya Aura™ Communication Manager and the Avaya Aura™ SIP Enablement Services to send/receive faxes using SIP trunks and 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 the Sagem-Interstar XMediusFAX Service Provider (SP) Edition with Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services (SES) using SIP trunks.

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

## 1.1. Interoperability Compliance Testing

The compliance test tested interoperability between XMediusFAX and the Communication Manager and the SIP Enablement Services by making intra-site and inter-site fax calls to and from XMediusFAX. The XMediusFAX server connects (at each of the two sites in the test configuration) to the Communication Manager and the SIP Enablement Services via SIP trunks (see **Section 2** for detailed configuration). Specifically, the following fax operations were tested in the setup for the compliance test:

- Fax from/to XMediusFAX to/from fax machine at local site
- Fax from/to XMediusFAX to/from fax machine at remote site
- Fax from/to XMediusFAX to/from XMediusFAX server at remote site

In the compliance test, Site A and Site B were connected by both ISDN-PRI trunks and SIP trunks. The inter-site calls were tested by using either of these 2 types of trunks between sites.

Faxes were sent with various page lengths, resolutions and at various fax data speeds. For capacity, a large number of 2-page faxes were continuously sent between the two XMediusFAX servers across sites. Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources, restarts of the Communication Manager and the SIP Enablement Services as well as XMediusFAX reboots. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included the TN2302AP IP Media Processor (MedPro) circuit pack and the TN2602AP IP Media Processor circuit pack in the Avaya G650 Media Gateway, as well as the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G350 Media Gateway.

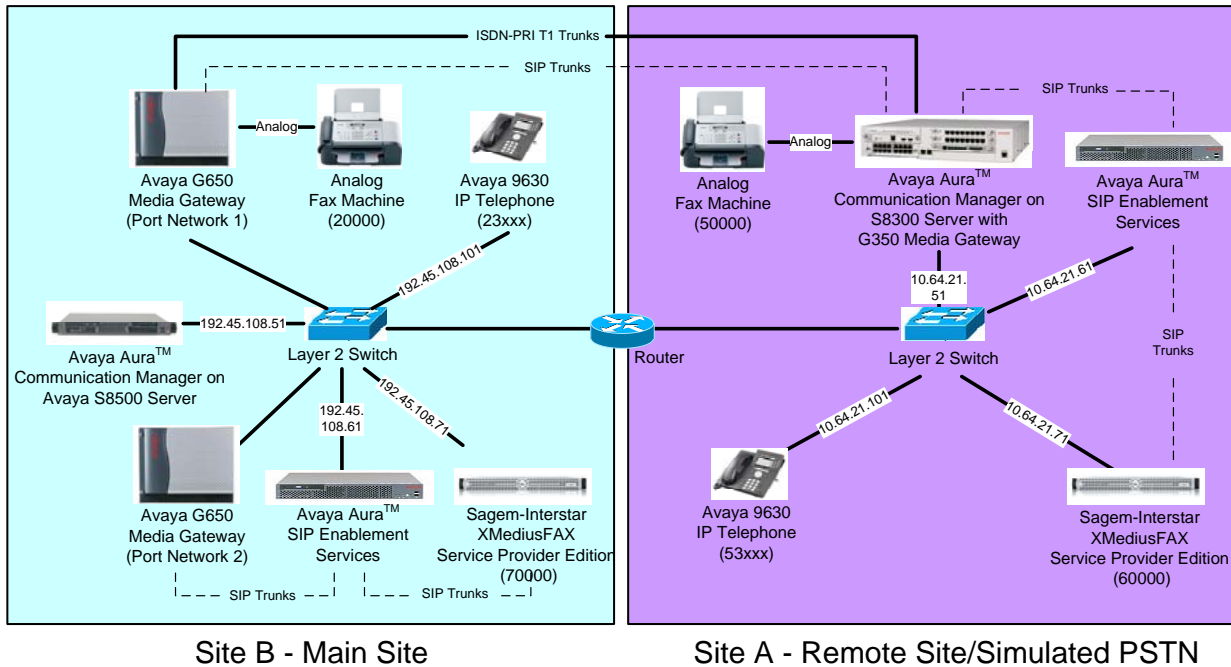
## 1.2. Support

For technical support on XMediusFAX, contact Sagem-Interstar at:

- Phone: (888) 766-1668
- Email: support@sagem-interstar.com

## 2. Configuration

**Figure 1** illustrates the configuration used in these Application Notes. In the sample configuration, two sites are connected via direct SIP trunks and ISDN-PRI trunks. Faxes can be sent between the two sites using either of these two trunk groups.



**Figure 1: XMediusFAX interoperating with Communication Manager and SIP Enablement Services**

Located at Site B is a SIP Enablement Services server and an Avaya S8500 Server running Communication Manager with two Avaya G650 Media Gateways. Each media gateway is configured as a separate port network in separate IP network regions. XMediusFAX at this site is running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services) via SIP trunks whose signaling is terminated on a CLAN circuit pack in port network 2. The media resources required by the trunk are provided by the IP Media Processor (MedPro) circuit pack. Two versions of the IP MedPro circuit pack were tested in this configuration: TN2302AP and TN2602AP. Endpoints at this site include Avaya 9600 Series IP Telephones (with SIP and H.323 firmware) and an analog fax machine.

Located at Site A is an SIP Enablement Services server and an Avaya S8300 Server running Communication Manager in an Avaya G350 Media Gateway. XMediusFAX at this site is also running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services) via SIP trunks. On the Avaya G350 Media Gateway, the signaling and media resources needed to support SIP trunks are integrated directly on the media gateway processor. Endpoints at this site include an Avaya 1600 Series IP Telephone

(with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware and SIP firmware), and an analog fax machine.

Although the IP telephones are not involved in the faxing operations, they are present in the configuration to verify that VoIP telephone calls are not affected by the FoIP faxing operations and vice versa.

Outbound fax calls originating from XMediusFAX are sent to the SIP Enablement Services server first, then from the SIP Enablement Services to the Communication Manager, via the configured SIP trunks. Based on the dialed digits, the Communication Manager will direct the calls to the local fax machine, or the inter-site trunks (ISDN-PRI or SIP) to reach the remote site. Inbound fax calls terminating to XMediusFAX from the local fax machine or from the remote site are first received by the Communication Manager. The Communication Manager then directs the calls to XMediusFAX via the configured SIP trunks.

### 3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8500 Server running Avaya Aura™ Communication Manager (Site B)	R5.2.1 SP1 (R015x.02.1.016.4-17959)
Avaya G650 Media Gateway (Site B) <ul style="list-style-type: none"> <li>- 2 CLANs</li> <li>- 2 IP MedPros – TN2302AP</li> <li>- 2 IP MedPros – TN2602AP</li> </ul>	TN799DP - HW01 FW24 TN2302AP - HW20 FW120 TN2602AP - HW02 FW051
Avaya Aura™ SIP Enablement Services (Site B)	5.2.1.016.4
Avaya S8300 Server running Avaya Aura™ Communication Manager (Site A)	R5.2.1 SP1 (R015x.02.1.016.4-17959)
Avaya G350 Media Gateway (Site A)	30.10.4
Avaya Aura™ SIP Enablement Services (Site A)	5.2.1.016.4
Avaya 1608 IP Telephone (H.323)	1.100
Avaya 9620 IP Telephone (SIP) Avaya 9630 IP Telephone (SIP) Avaya 9630 IP Telephone (H.323)	2.2 2.2 & 2.0 3.0
Analog Fax Machines	-
Sagem-Interstar XMediusFAX SP Edition Fax Server running on Windows 2003 Server	6.5 with patch XMFSP_6.5.0.127

## 4. Configure Avaya Aura™ Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with XMediusFAX. It focuses on the configuration of the SIP trunks connecting XMediusFAX to the Avaya SIP infrastructure with the following assumptions:

- Procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3], including all SIP phones at each site.
- All other components are assumed to be in place and previously configured, including the SIP and ISDN-PRI trunk groups that connect both sites.

The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager license (Step 1)
- Identify IP Interfaces (Step 2)
- Administer IP network regions (Steps 3 – 6)
- Administer IP codec set (Steps 7 – 8)
- Administer SIP signaling group (Step 9)
- Administer SIP trunk group (Steps 10 – 11)
- Administer public unknown numbering (Step 12)
- Administer route pattern (Step 13)
- Administer AAR analysis (Steps 14 – 15)
- Turn on Media Shuffling on cross-site SIP trunks (Step 16)

The configuration of the 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.

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

Step	Description
1.	<p data-bbox="315 222 779 254"><b>Communication Manager License</b></p> <p data-bbox="315 260 1437 436">Use the <b>display system-parameters customer-options</b> command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to <b>Page 2</b>, and verify that there is sufficient remaining capacity for SIP trunks by comparing the <b>Maximum Administered SIP Trunks</b> field value with the corresponding value in the <b>USED</b> column.</p> <p data-bbox="315 478 1383 583">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 data-bbox="315 621 1399 1136" style="border: 1px solid black; padding: 5px;"> <pre data-bbox="334 632 1344 1108"> change system-parameters customer-options                               Page  2 of 11                                 OPTIONAL FEATURES  IP PORT CAPACITIES  USED       Maximum Administered H.323 Trunks: 800 100       Maximum Concurrently Registered IP Stations: 18000 1       Maximum Administered Remote Office Trunks: 0 0 Maximum Concurrently Registered Remote Office Stations: 0 0       Maximum Concurrently Registered IP eCons: 0 0       Max Concur Registered Unauthenticated H.323 Stations: 0 0       Maximum Video Capable H.323 Stations: 0 0       Maximum Video Capable IP Softphones: 0 0       <b>Maximum Administered SIP Trunks: 800 232</b>       Maximum Administered Ad-hoc Video Conferencing Ports: 0 0       Maximum Number of DS1 Boards with Echo Cancellation: 0 0       Maximum TN2501 VAL Boards: 10 1       Maximum Media Gateway VAL Sources: 0 0       Maximum TN2602 Boards with 80 VoIP Channels: 128 0       Maximum TN2602 Boards with 320 VoIP Channels: 128 2       Maximum Number of Expanded Meet-me Conference Ports: 0 0 </pre> </div>

Step	Description
2.	<p data-bbox="316 184 495 220"><b>IP Interfaces</b></p> <ul data-bbox="316 220 1445 514" style="list-style-type: none"> <li data-bbox="316 220 1445 514">Use the <b>list ip-interface all</b> command to identify which IP interfaces are located in which network region. The example below shows the IP interfaces used in the compliance test. All interfaces in cabinet 01 (port network 1) as indicated in the <b>Slot</b> field are in IP network region 1 as indicated in the <b>Net Rgn</b> field. These interfaces are highlighted below. Testing with the TN2302AP and TN2602AP circuit packs were done separately. When testing with the TN2302AP, the TN2602AP was disabled (turned off) and vice versa as indicated in the <b>ON</b> field. Node Names are defined using the <b>change node-names ip</b> command.</li> </ul> <div data-bbox="316 546 1396 1039" style="border: 1px solid black; padding: 5px;"> <pre data-bbox="332 556 1380 1018"> list ip-interface all                                      IP INTERFACES                                      Page 1 ----- ON Type  Slot  Code/Sfx  Node Name/  Mask  Gateway Node  Net  VLAN                            IP-Address                          Rgn   ----- ---- ----- ----- ----- ----- ----  y MEDPRO 01A02 TN2302  MEDPRO1A   /24  Gateway001    1   n                            192.45.108.54 y C-LAN  01A03 TN799  D  CLAN1A     /24  Gateway001    1   n                            192.45.108.55 y MEDPRO 02A02 TN2302  MEDPRO2A   /24  Gateway001    2   n                            192.45.108.56 y C-LAN  02A03 TN799  D  CLAN2A     /24  Gateway001    2   n                            192.45.108.57 n MEDPRO 01A04 TN2602  MEDPRO1A-2 /24  Gateway001    1   n                            192.45.108.58 n MEDPRO 02A04 TN2602  MEDPRO2A-2 /24  Gateway001    2   n                            192.45.108.59 </pre> </div> <ul data-bbox="316 1081 1372 1155" style="list-style-type: none"> <li data-bbox="316 1081 1372 1155">Node Names in the above screen are defined using the <b>change node-names ip</b> command.</li> </ul> <div data-bbox="316 1186 1396 1480" style="border: 1px solid black; padding: 5px;"> <pre data-bbox="332 1197 1380 1459"> change node-names ip                                      IP NODE NAMES                                      Page 1 of 2 Name          IP Address CLAN1A       192.45.108.55 CLAN2A       192.45.108.57 CM-A         10.64.21.41 MEDPRO1A     192.45.108.54 MEDPRO1A-2   192.45.108.58 MEDPRO2A     192.45.108.56 MEDPRO2A-2   192.45.108.59 SES-B        192.45.108.61 </pre> </div>



Step	Description
3.	<p><b>IP Network Region – Region 1</b></p> <p>The configuration of the IP network regions (<b>Steps 3 – 6</b>) is assumed to be already in place and is included here for clarity. At Site B, the Avaya S8500 Server, the Avaya G650 Media Gateway comprising port network 1, and all IP endpoints were located in IP network region 1 using the parameters described below. Use the <b>display ip-network-region</b> command to view these settings. The example below shows the values used for the compliance test.</p> <ul style="list-style-type: none"> <li>▪ The <b>Authoritative Domain</b> field was configured to match the domain name configured on Avaya SES. In this configuration, the domain name is <b>business.com</b>. This name appears in the “From” header of SIP messages originating from this IP region.</li> <li>▪ A descriptive name was entered for the <b>Name</b> field.</li> <li>▪ <b>IP-IP Direct Audio</b> (Media Shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Media Shuffling can be further restricted at the trunk level on the <b>Signaling Group</b> form.</li> <li>▪ The <b>Codec Set</b> field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set <b>I</b> was selected.</li> <li>▪ The default values were used for all other fields.</li> </ul> <p>At Site A, all IP components were located in IP network region 1 and the IP network region was configured in the same manner as shown below.</p> <pre data-bbox="316 1060 1399 1621"> display ip-network-region 1                                     Page 1 of   IP NETWORK REGION Region: 1 Location:                Authoritative Domain: business.com Name: PN1 MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes Codec Set: 1                Inter-region IP-IP Direct Audio: yes UDP Port Min: 2048                IP Audio Hairpinning? n UDP Port Max: 3329 DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y Call Control PHB Value: 46                RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46                Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5                AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS                RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 </pre>

Step	Description
4.	<p><b>IP Network Region 1 – Continued</b>  <b>On Page 3</b>, codec sets are defined for inter-region calls. In the case of the compliance test at Site B, calls from IP network region 1, <b>Source Region 1</b>, to IP network region 2, <b>dst rgn 2</b>, used <b>codec set 1</b>. The default values were used for all other fields. At Site A, only one IP network region exists so no inter-region settings were required.</p> <pre data-bbox="316 403 1399 621"> display ip-network-region 1                                     Page 3 of 19  Source Region: 1      Inter Network Region Connection Management  I      M   G      A      e dst codec direct  WAN-BW-limits  Video      Intervening  Dyn  A  G  a rgn set  WAN  Units  Total Norm  Prio Shr Regions  CAC  R  L  s 1  1 2  1  y  NoLimit                                     n </pre>
5.	<p><b>IP Network Region – Region 2</b>  At Site B, IP network region 2 was created for port network 2 in a similar manner as IP network region 1 shown in <b>Step 3</b> but with a different name.</p> <pre data-bbox="316 808 1399 1360"> display ip-network-region 2                                     Page 1 of 19  Region: 2 Location:      Authoritative Domain: business.com Name: PN2 MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes Codec Set: 1          Inter-region IP-IP Direct Audio: yes UDP Port Min: 2048    IP Audio Hairpinning? n UDP Port Max: 3329 DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y Call Control PHB Value: 46    RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46          Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS      RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 </pre>
6.	<p><b>IP Network Region 2 – Continued</b>  The inter-region codec setting was created similarly to <b>Step 4</b>.</p> <pre data-bbox="316 1512 1399 1730"> display ip-network-region 2                                     Page 3 of 19  Source Region: 2      Inter Network Region Connection Management  I      M   G      A      e dst codec direct  WAN-BW-limits  Video      Intervening  Dyn  A  G  a rgn set  WAN  Units  Total Norm  Prio Shr Regions  CAC  R  L  s 1  1 2  1  y  NoLimit                                     n all </pre>

Step	Description
7.	<p><b>Codecs</b> Use the <b>change ip-codec-set</b> command to verify the codec used for the testing. The example below shows that <b>G.711MU</b> is used in the compliance test.</p> <pre data-bbox="318 327 1414 573"> 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>
8.	<p><b>Codecs - Continued</b> On <b>Page 2</b>, set the <b>FAX Mode</b> field to <b>t.38-standard</b>. This is necessary to support the XMediusFAX server assigned to IP network region 2. The <b>Modem Mode</b> field should be set to <b>off</b>.</p> <p>Leave the <b>FAX Redundancy</b> setting at its default value of <b>0</b>. A packet redundancy level can be assigned to improve packet delivery and robustness of FAX transport over the network (with increased bandwidth as trade-off). Avaya uses IETF RFC-2198 and ITU-T T.38 specifications as redundancy standard. With this standard, each Fax over IP packet is sent with additional (redundant) 0 to 3 previous fax packets based on the redundancy setting. A setting of 0 (no redundancy) is suited for networks where packet loss is not a problem.</p> <pre data-bbox="318 1087 1414 1436"> display ip-codec-set 1                                     Page 2 of 2                                  IP Codec Set                                  Allow Direct-IP Multimedia? n  FAX          Mode          Redundancy <b>FAX</b>          <b>t.38-standard</b>      0 <b>Modem</b>        <b>off</b>              0 TDD/TTY      US              3 Clear-channel n              0 </pre>

Step	Description
9.	<p><b>Signaling Group for Fax Calls</b></p> <p>For the compliance test, this signaling group and the associated SIP trunk group are used for routing fax calls to/from the XMediusFAX server. For the compliance test at Site B, signaling group 7 was configured using the parameters highlighted below. All other fields were set as described in [3].</p> <ul style="list-style-type: none"> <li>▪ The <b>Group Type</b> was set to <i>sip</i>.</li> <li>▪ The <b>Transport Method</b> was set to <i>tcp</i>. As a result, the <b>Near-end Listen Port</b> and <b>Far-end Listen Port</b> are automatically set to <b>5060</b>.</li> <li>▪ The <b>Near-end Node Name</b> was set to <i>CLAN2A</i>, the node name that maps to the IP address of the CLAN circuit pack used to connect to XMediusFAX. Node names are defined using the <b>change node-names ip</b> command (see <b>Step 2</b> above).</li> <li>▪ The <b>Far-end Node Name</b> was set to <i>SES-B</i>. This node name maps to the IP address of the SIP Enablement Services server as defined using the <b>change node-names ip</b> command.</li> <li>▪ The <b>Far-end Network Region</b> was set to <b>2</b>. This is the IP network region which contains XMediusFAX.</li> <li>▪ The <b>Far-end Domain</b> was set to the IP address assigned to XMediusFAX. This domain is sent in the headers of SIP INVITE messages for calls originating from and terminating to the fax server using this signaling group.</li> <li>▪ <b>Direct IP-IP Audio Connections</b> was set to <i>y</i>. This field must be set to <i>y</i> to enable Media Shuffling on the trunk level (see <b>Step 3</b> on <b>IP-IP Direct Audio</b>).</li> <li>▪ The default values were used for all other fields.</li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> display signaling-group 7                                 SIGNALING GROUP  Group Number: 7                Group Type: sip                                 Transport Method: tcp  IMS Enabled? n  Near-end Node Name: CLAN2A      Far-end Node Name: SES-B Near-end Listen Port: 5060      Far-end Listen Port: 5060 Far-end Network Region: 2  Far-end Domain: 192.45.108.100  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? n                                 Direct IP-IP Early Media? n H.323 Station Outgoing Direct Media? n                                 Alternate Route Timer(sec): 6 </pre> </div>

Step	Description
10.	<p><b>Trunk Group for Fax Calls</b></p> <p>For the compliance test, trunk group 7 was used for the SIP trunk group for routing fax calls to/from XMediusFAX. Trunk group 7 was configured using the parameters highlighted below. All other fields were set as described in [3].</p> <p><b>On Page 1:</b></p> <ul style="list-style-type: none"> <li>▪ The <b>Group Type</b> field was set to <i>sip</i>.</li> <li>▪ A descriptive name was entered for the <b>Group Name</b>.</li> <li>▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the <b>TAC</b> field.</li> <li>▪ The <b>Service Type</b> field was set to <i>tie</i>.</li> <li>▪ The <b>Signaling Group</b> was set to the signaling group shown in the previous step.</li> <li>▪ The <b>Number of Members</b> field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration.</li> <li>▪ The default values were used for all other fields.</li> </ul> <div data-bbox="316 804 1399 1146" style="border: 1px solid black; padding: 5px;"> <pre> display trunk-group 7                                     Page 1 of 21                                      TRUNK GROUP  Group Number: 7                Group Type: sip                CDR Reports: y   Group Name: FaxServer-SIP        COR: 1                TN: 1                TAC: *007   Direction: two-way              Outgoing Display? n   Dial Access? n                  Night Service:   Queue Length: 0   Service Type: tie                Auth Code? n                                       Signaling Group: 7                                      Number of Members: 24 </pre> </div>
11.	<p><b>Trunk Group for Fax Calls – continued</b></p> <p><b>On Page 3:</b></p> <ul style="list-style-type: none"> <li>▪ Set the <b>Numbering Format</b> field to <i>public</i>. This field specifies the format of the calling party number sent to the far-end.</li> <li>▪ Default values may be used for all other fields.</li> </ul> <div data-bbox="316 1444 1414 1791" style="border: 1px solid black; padding: 5px;"> <pre> display trunk-group 7                                     Page 3 of 21 TRUNK FEATURES   ACA Assignment? n                Measured: none                                      Maintenance Tests? y                                       Numbering Format: public                                      UUI Treatment: service-provider                                      Replace Restricted Numbers? n                                      Replace Unavailable Numbers? n </pre> </div>

Step	Description
12.	<p><b>Public Unknown Numbering</b>  Public unknown numbering defines the calling party number to be sent to the far-end. Use the <b>change public-unknown-numbering</b> command to create an entry that will be used by the trunk groups defined in <b>Steps 10-11</b>. In the example shown below, all calls originating from a 5-digit extension beginning with 2, 6, or 7 and routed across any trunk group (<b>Trk Grp</b> column is blank) will be sent as a 5-digit calling number.</p> <pre data-bbox="316 436 1416 688"> display public-unknown-numbering 0 NUMBERING - PUBLIC/UNKNOWN FORMAT Page 1 of Ext Ext          Trk      CPN          Total Len Code        Grp(s)   Prefix      CPN 5 2              5 5 6              5 5 7              5 Total Administered: 3 Maximum Entries: 9999 </pre>
13.	<p><b>Route Pattern</b>  Use the <b>change route-pattern</b> command to create a route pattern that will route fax calls to the SIP trunk that connects to the XMediusFAX server.</p> <p>The example below shows the route pattern used for the compliance test at Site B. A descriptive name was entered for the <b>Pattern Name</b> field. The <b>Grp No</b> field was set to the trunk group created in <b>Steps 10–11</b>. The Facility Restriction Level (<b>FRL</b>) field was set to a level that allows access to this trunk for all users that require it. The value of <b>0</b> is the least restrictive level. The default values were used for all other fields.</p> <pre data-bbox="316 1094 1399 1570"> display route-pattern 7 Pattern Number: 7  Pattern Name: ToFaxServer Page 1 of 3           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: 7    0 2: 3: 4: 5: 6:           BCC VALUE  TSC CA-TSC  ITC BCIE Service/Feature PARM No. Numbering LAR           0 1 2 M 4 W      Request      Dgts Format 1: y y y y y n  n          rest          none 2: y y y y y n  n          rest          none 3: y y y y y n  n          rest          none </pre>

Step	Description
14.	<p><b>Routing Calls to XMediusFAX</b></p> <p>Automatic Alternate Routing (AAR) was used to route calls to XMediusFAX. Two places need to be changed to support this routing. At first use the <b>change dialplan analysis</b> command to create an entry in the dial plan. The example below shows entries previously created for Site B using the <b>display dialplan analysis</b> command. The 5th highlighted entry specifies that numbers that begin with 7 are of Call Type <b>aar</b>. Second use the <b>change aar analysis</b> command to create an entry in the AAR Digit Analysis Table. The example below shows entries previously created for Site B using the <b>display aar analysis 0</b> command. The 4th highlighted entry specifies that numbers that begin with 7 and are 5 digits long use route pattern 7. Route pattern 7 routes calls to the XMediusFAX fax server at Site B.</p> <pre data-bbox="316 619 1396 976"> display dialplan analysis                                 DIAL PLAN ANALYSIS TABLE                                 Location: all           Percent Full: 1      Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call     String   Length Type   String   Length Type   String   Length Type     0                3   fac   0                3   fac     2                5   ext   2                5   ext     5                5   ext   5                5   ext     6                5   aar   6                5   aar     7                5   aar   7                5   aar     8                1   fac   8                1   fac     9                1   fac   9                1   fac     *                4   dac   *                4   dac </pre> <pre data-bbox="316 1018 1396 1281"> display aar analysis 0                                 AAR DIGIT ANALYSIS TABLE                                 Location: all           Percent Full: 1      Dialed   Total   Route   Call   Node   ANI     String   Min   Max   Pattern   Type   Num   Reqd     50                5   5   4         aar   n     53                5   5   4         aar   n     6                5   5   4         aar   n     7                5   5   7         aar   n </pre>

Step	Description
15.	<p><b>Routing Calls From Site B to Site A</b></p> <p>The AAR Digit Analysis Table in <b>Step 14</b> also shows that a 5-digit dialed number starting with 50 or 6 will use route pattern 4 by AAR. The previously created route pattern <b>4</b> as displayed below specifies that a call from Site B to the fax machine 50000 or the XMediusFAX server 60000 at Site A will be routed to trunk group 4 which is an administered ISDN-PRI trunk. In the same way, this trunk group can be changed to a SIP trunk group for fax calls from Site B to Site A to go over a SIP trunk.</p> <pre data-bbox="316 478 1399 1050"> display route-pattern 4 Pattern Number: 4   Pattern Name: CMnorth RP SCCAN? n          Secure SIP? n  Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/  IXC No   Mrk Lmt List Del  Digits      QSIG                                 Intw 1:  4    0 2: 3: 4: 5: 6:            BCC VALUE  TSC CA-TSC   ITC BCIE Service/Feature PARM  No.  Numbering LAR           0 1 2 M 4 W      Request          Dgts Format                                 Subaddress 1:  y y y y y n  n          rest          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>



Step	Description
16.	<p><b>Turn On Media Shuffling on SIP Trunk between Sites</b></p> <p>Use the <b>change signaling-group</b> command to turn on Media Shuffling on the previously administered SIP trunks between Site B and Site A (in this compliance test, trunk group 1 was used at Site B). Note that the <b>Far-end Node Name</b> is <b>CM-A</b> which indicates that the trunk is set up between two Communication Managers directly without going through an SES.</p> <pre data-bbox="316 436 1399 1012"> change signaling-group 1                               Page 1 of 1                 SIGNALING GROUP  Group Number: 1          Group Type: sip                 Transport Method: tcp  IMS Enabled? n  Near-end Node Name: CLAN1A          Far-end Node Name: CM-A Near-end Listen Port: 5060          Far-end Listen Port: 5060 Far-end Network Region: 2 Far-end Domain:  Incoming Dialog Loopbacks: eliminate          Bypass If IP Threshold Exceeded? n DTMF over IP: rtp-payload                    RFC 3389 Comfort Noise? n Session Establishment Timer(min): 3           Direct IP-IP Audio Connections? y Enable Layer 3 Test? n                       IP Audio Hairpinning? n H.323 Station Outgoing Direct Media? n      Direct IP-IP Early Media? n  Alternate Route Timer(sec): 6 </pre>

## 5. Configure Avaya Aura™ SIP Enablement Services

This section covers the configuration of the SIP Enablement Services at Site B. The SIP Enablement Services are configured via an Internet browser using the administration web interface. It is assumed that the SIP Enablement Services software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used for initial configurations. For additional information on these installation tasks, refer to [4].

Each SIP endpoint used in the compliance test that registers with the SIP Enablement Services requires that a user and media server extension be created in the SIP Enablement Services. This configuration is not directly related to the interoperability between XMediusFAX and the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services), so it is not included here. These procedures are covered in [4].

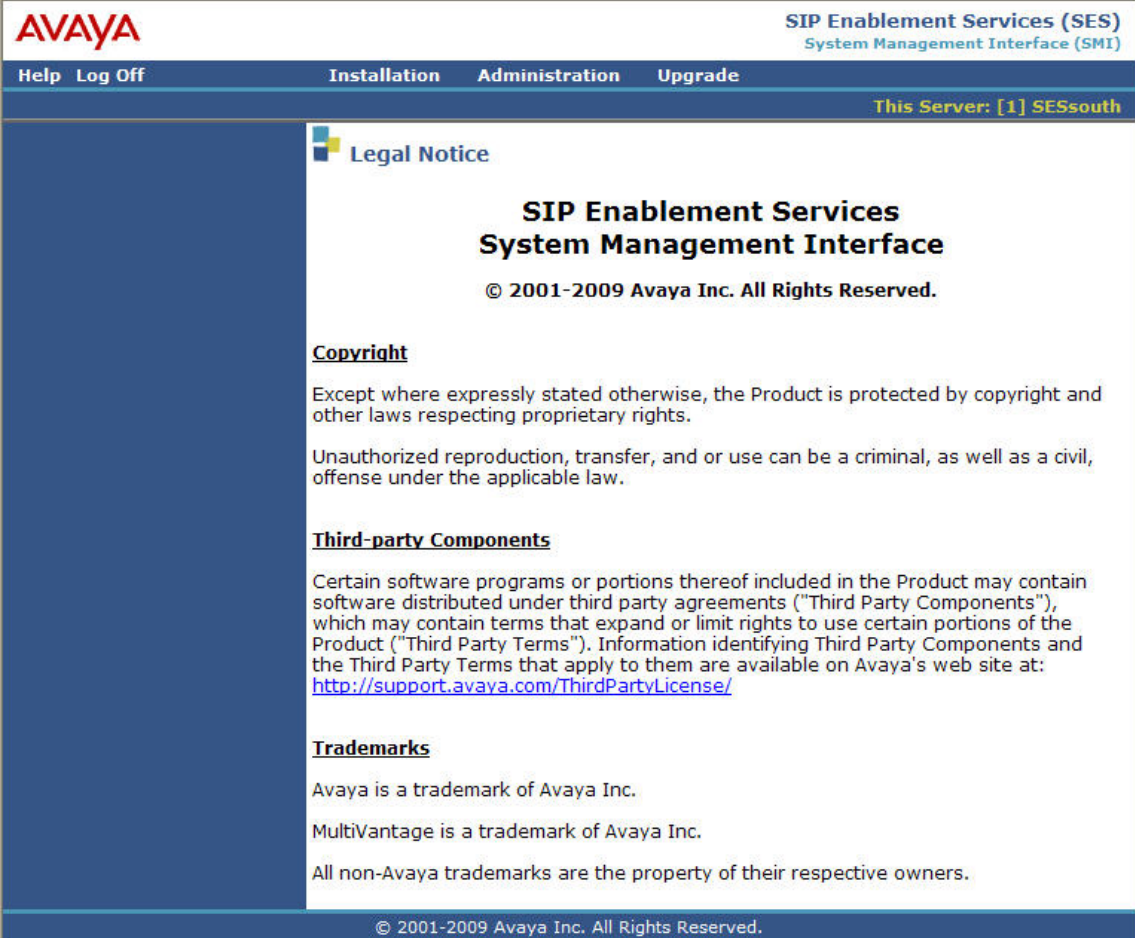
This section is divided into two parts. **Section 5.1** summarizes the user-defined parameters used in the SIP Enablement Services installation procedures that are important for the understanding of the solution as a whole. It does not attempt to show the installation procedures in their entirety. It also describes any deviations from the standard procedures, if any.


**Section 5.2** describes configurations beyond those covered in **Section 5.1** that are necessary for interoperating with XMediusFAX.

The documented configurations must be repeated for the SIP Enablement Services at Site A using values appropriate for Site A from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

## 5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	<p><b>Login</b></p> <p>Access the Avaya SES administration web interface by entering <a href="http://&lt;ip-addr&gt;/admin">http://&lt;ip-addr&gt;/admin</a> as the URL in an Internet browser, where &lt;ip-addr&gt; is the IP address of the Avaya SES server. Log in with the appropriate credentials and the page below will be displayed.</p> 


Step	Description																								
2.	<p><b>Top Page</b>            Select <b>Administration</b> → <b>SIP Enablement Services</b> from the top menu (not shown).            The Avaya SES <b>Top</b> page will be displayed as shown below.</p>  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. At the top left is the Avaya logo. To the right, it says 'Integrated Management SIP Server Management' and 'This Server: [1] SESSouth'. Below the header is a navigation menu with 'Help' and 'Exit'. The main content area is titled 'Top' and contains a list of management tasks:</p> <table border="1"> <thead> <tr> <th>Task</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Manage Users</td> <td>Add and delete Users.</td> </tr> <tr> <td>Manage Address Map Priorities</td> <td>Adjust Address Map Priorities.</td> </tr> <tr> <td>Manage Adjunct Systems</td> <td>Add and delete Adjunct Systems.</td> </tr> <tr> <td>Manage Event Aggregators</td> <td>Add/Delete Event Aggregators.</td> </tr> <tr> <td>Certificate Management</td> <td>Manage Certificates.</td> </tr> <tr> <td>Manage Conferencing</td> <td>Add and delete Conference Extensions.</td> </tr> <tr> <td>Manage Emergency Contacts</td> <td>Add and delete Emergency Contacts.</td> </tr> <tr> <td>Export Import to ProVision</td> <td>Export and import data using ProVision on this host.</td> </tr> <tr> <td>Manage Hosts</td> <td>Add and delete Hosts.</td> </tr> <tr> <td>IM logs</td> <td>Download IM Logs.</td> </tr> <tr> <td>Manage Communication Manager Servers</td> <td>Add and delete Communication Manager Servers.</td> </tr> </tbody> </table>	Task	Description	Manage Users	Add and delete Users.	Manage Address Map Priorities	Adjust Address Map Priorities.	Manage Adjunct Systems	Add and delete Adjunct Systems.	Manage Event Aggregators	Add/Delete Event Aggregators.	Certificate Management	Manage Certificates.	Manage Conferencing	Add and delete Conference Extensions.	Manage Emergency Contacts	Add and delete Emergency Contacts.	Export Import to ProVision	Export and import data using ProVision on this host.	Manage Hosts	Add and delete Hosts.	IM logs	Download IM Logs.	Manage Communication Manager Servers	Add and delete Communication Manager Servers.
Task	Description																								
Manage Users	Add and delete Users.																								
Manage Address Map Priorities	Adjust Address Map Priorities.																								
Manage Adjunct Systems	Add and delete Adjunct Systems.																								
Manage Event Aggregators	Add/Delete Event Aggregators.																								
Certificate Management	Manage Certificates.																								
Manage Conferencing	Add and delete Conference Extensions.																								
Manage Emergency Contacts	Add and delete Emergency Contacts.																								
Export Import to ProVision	Export and import data using ProVision on this host.																								
Manage Hosts	Add and delete Hosts.																								
IM logs	Download IM Logs.																								
Manage Communication Manager Servers	Add and delete Communication Manager Servers.																								


Step	Description
3.	<p data-bbox="298 186 751 218"><b>Initial Configuration Parameters</b></p> <p data-bbox="298 222 1430 510">As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of the required steps to view the values for that group from the Avaya SES administration home page shown in the previous step. Note that for Site A, the <b>SIP Trunk IP Address</b> should be set to the IP assigned to the Avaya Communication Manager (<i>procr</i>) since there is no separate CLAN circuit pack in the Avaya G350 Media Gateway.</p> <ul data-bbox="347 554 1365 961" style="list-style-type: none"> <li data-bbox="347 554 1256 625">• <b>SIP Domain:</b> <i>business.com</i> (To view, navigate to <b>Server Configuration</b>→<b>System Properties</b>)</li> <li data-bbox="347 663 1040 695">• <b>Host IP Address</b> (SES IP address): <i>192.45.108.61</i></li> <li data-bbox="347 703 992 774">• <b>Host Type:</b> <i>SES combined home-edge</i> (To view, navigate to <b>Hosts</b>→<b>List</b>; click <b>Edit</b>)</li> <li data-bbox="347 816 1062 848">• <b>Communication Manager Interface Name:</b> <i>CM-B</i></li> <li data-bbox="347 856 769 888">• <b>SIP Trunk Link Type:</b> <i>TCP</i></li> <li data-bbox="347 896 1365 961">• <b>SIP Trunk IP Address</b> (CLAN2A IP address): <i>192.45.108.57</i> (To view, navigate to <b>Communication Manger Servers</b>→<b>List</b>; click <b>Edit</b>)</li> </ul>

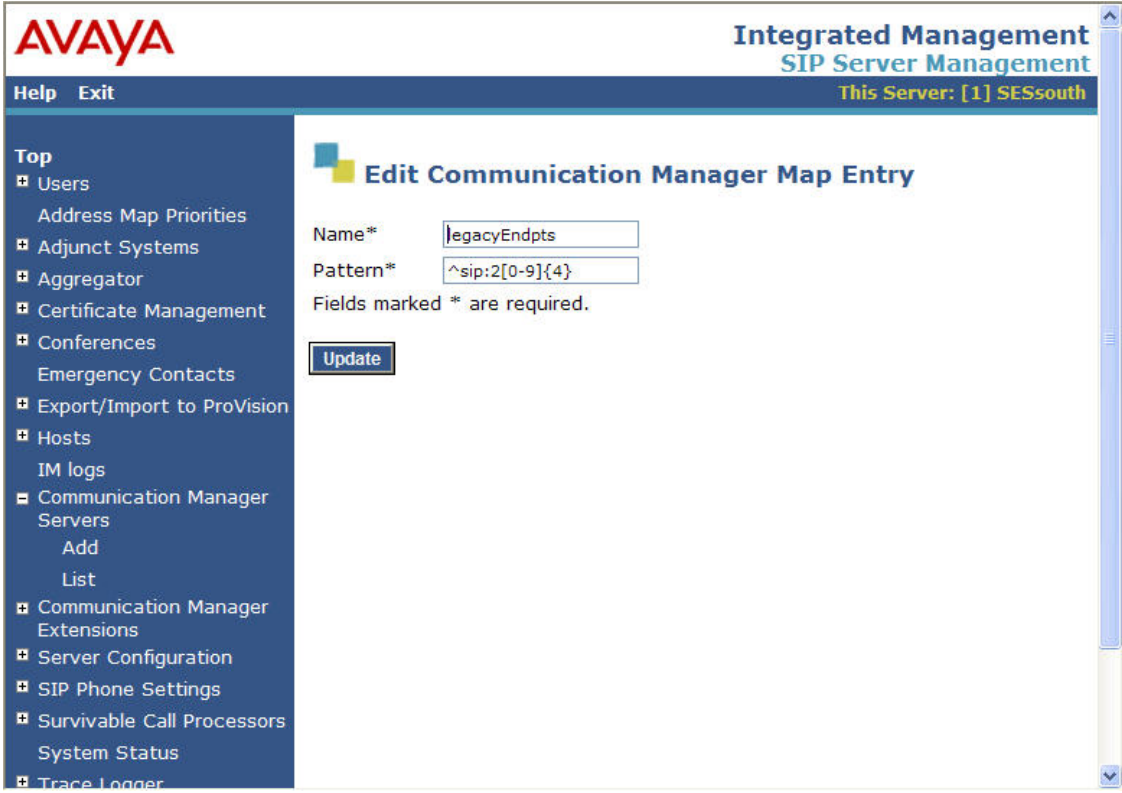
## 5.2. XMediusFAX Specific Configuration

This section describes additional SIP Enablement Services configurations necessary for interoperating with XMediusFAX. These specific configurations include the following:

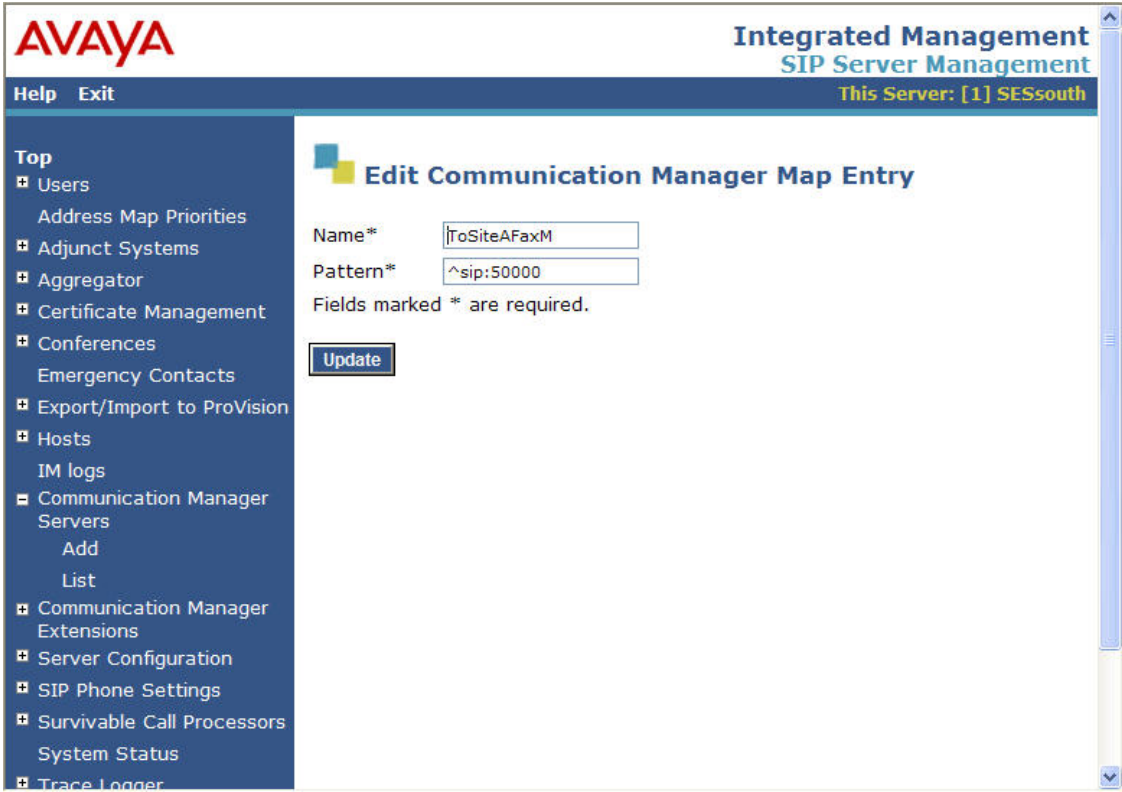
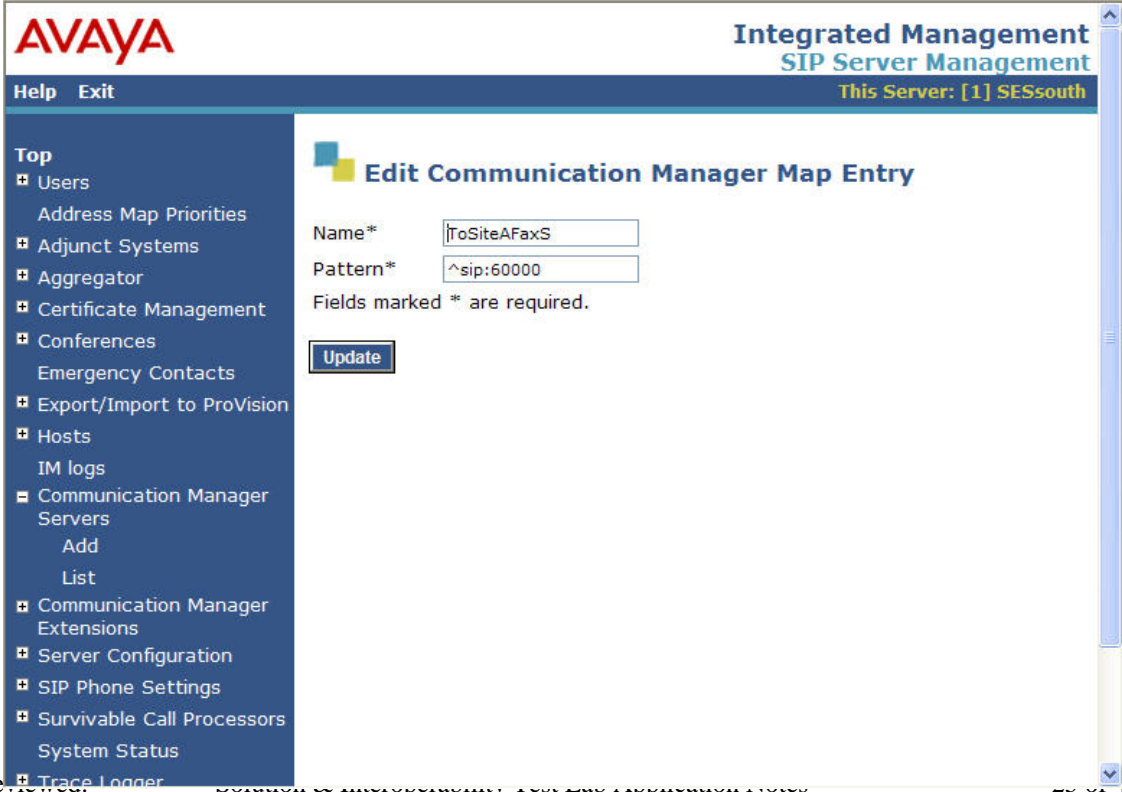
- Administer Communication Manager Server Address Map (Steps 1 – 4)
- Administer trusted host (Step 5)

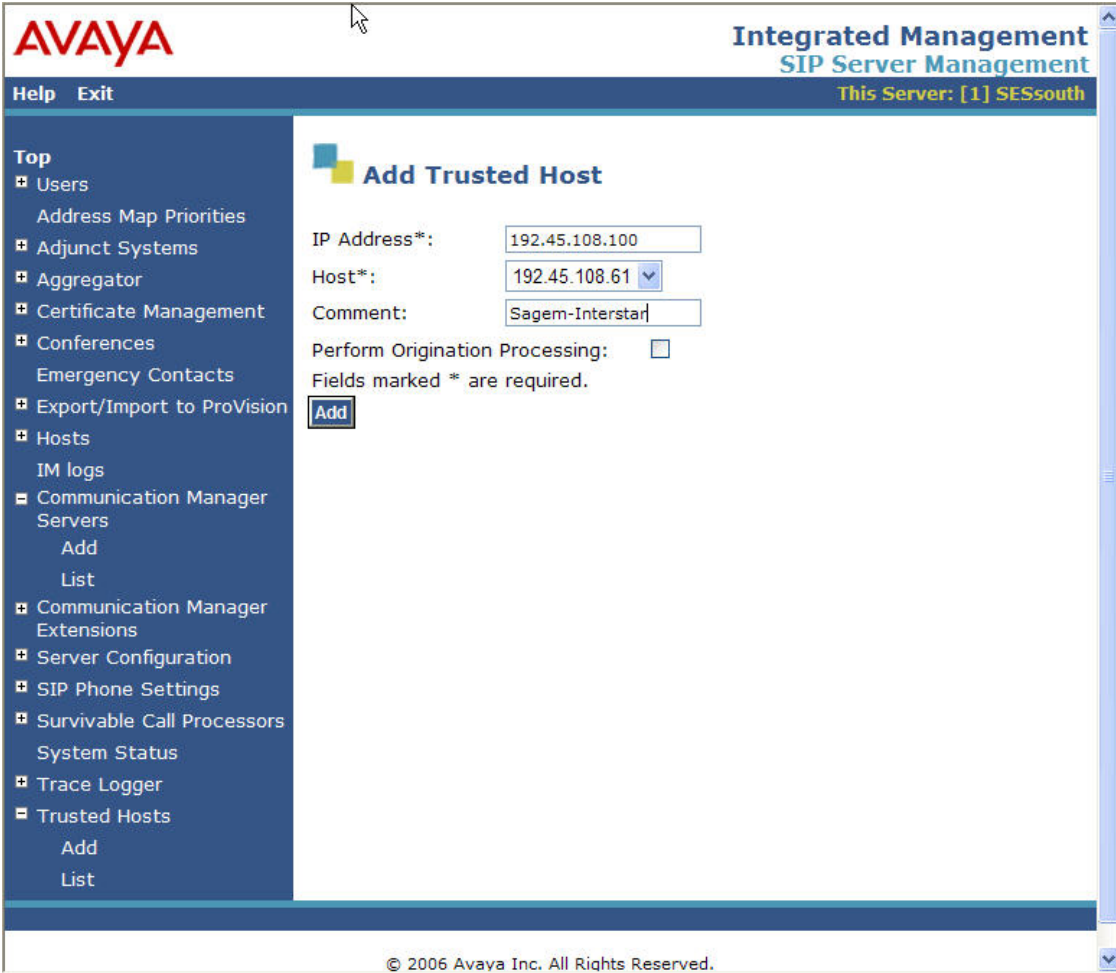
Step	Description
1.	<p><b>Communication Manager Server Address Map</b></p> <p>A Communication Manager Server Address Map is needed to route calls to the fax machines (local or remote) or the XMediusFAX fax server at the remote site. This is because neither the caller nor the called party is a registered user on the local Avaya SES with a media server extension assigned to it. Thus, Avaya SES does not know how to route this call to Avaya Communication Manager. To accomplish this task, a Communication Manager Server Address Map is needed.</p> <p>To view the Communication Manager Server Address Maps, navigate to <b>Communication Manager Servers → List</b> in the left pane.</p> 

Step	Description																				
2.	<p><b>Communication Manager Servers Address Map – Continued</b></p> <p>In the displayed window above, click the <b>Map</b> link in the <b>CM-B</b> interface entry. The list of Communication Manager Server Address Maps will appear as shown below. Each map defines criteria for matching calls to the Avaya SES based on the contents of the SIP Request-URI of the call</p> <p>In the example below, three configured maps are shown for the compliance test:</p> <ul style="list-style-type: none"> <li>– <i>legacyEndpts</i> was used for mapping calls to the fax machine at local site</li> <li>– <i>ToSiteAFaxM</i> was used for mapping calls to the fax machine at remote site</li> <li>– <i>ToSiteAFaxS</i> was used for mapping calls to the XMediusFAX fax server at remote site</li> </ul> <p>All 3 maps were associated to a <b>Contact</b> that directs the calls to the IP address of the <b>CLAN2A</b> interface, <b>192.45.108.57</b>, using port <b>5060</b> and <b>TCP</b> as the transport protocol. The user portion in the original request URI is substituted for <b>\$(user)</b> in the <b>Contact</b> expression shown below and in the screenshot:</p> <p style="text-align: center;"><code>sip:\$(user)@192.45.108.57:5060;transport=tcp</code></p>  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. The main content area displays a table titled "List Communication Manager Server Address Map". The table has four columns: "Commands", "Name", "Commands", and "Contact". The data rows are as follows:</p> <table border="1"> <thead> <tr> <th>Commands</th> <th>Name</th> <th>Commands</th> <th>Contact</th> </tr> </thead> <tbody> <tr> <td>Edit Delete</td> <td>ToSiteAFaxM</td> <td></td> <td></td> </tr> <tr> <td>Edit Delete</td> <td>ToSiteAFaxS</td> <td></td> <td></td> </tr> <tr> <td>Edit Delete</td> <td>legacyEndpts</td> <td></td> <td></td> </tr> <tr> <td>Edit Delete</td> <td></td> <td></td> <td>sip:\$(user) @192.45.108.57:5060;transport=tcp</td> </tr> </tbody> </table> <p>Below the table, there are buttons for "Add Another Map", "Add Another Contact", "Delete Group", and "Add Map In New Group". A left-hand navigation menu is visible with various system management options.</p>	Commands	Name	Commands	Contact	Edit Delete	ToSiteAFaxM			Edit Delete	ToSiteAFaxS			Edit Delete	legacyEndpts			Edit Delete			sip:\$(user) @192.45.108.57:5060;transport=tcp
Commands	Name	Commands	Contact																		
Edit Delete	ToSiteAFaxM																				
Edit Delete	ToSiteAFaxS																				
Edit Delete	legacyEndpts																				
Edit Delete			sip:\$(user) @192.45.108.57:5060;transport=tcp																		

Step	Description
3.	<p data-bbox="315 186 1000 218"><b>Communication Server Address Map – Continued</b></p> <p data-bbox="315 222 1430 291">To view or edit the call matching criteria of the map, click the <b>Edit</b> link next to the map name. The content of the Communication Server Address Map is described below.</p> <ul data-bbox="363 331 1427 548" style="list-style-type: none"> <li data-bbox="363 331 899 363">▪ <b>Name:</b> Contains any descriptive name</li> <li data-bbox="363 367 1427 548">▪ <b>Pattern:</b> Contains an expression to define the matching criteria for calls to be routed to this Avaya Communication Manager. For the address map named <i>legacyEndpts</i>, the expression will match any URI that begins with <i>sip:2</i> followed by any digit between <i>0-9</i> for the next <i>4</i> digits. Additional information on the syntax used for address map patterns can be found in [4].</li> </ul> <p data-bbox="315 588 818 619">If any changes are made, click <b>Update</b>.</p> <div data-bbox="315 657 1430 1444" style="border: 1px solid black; padding: 5px;">  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server name 'This Server: [1] SESsouth'. A navigation menu on the left lists various system components, with 'Communication Manager Servers' expanded to show 'Add' and 'List' options. The main content area is titled 'Edit Communication Manager Map Entry' and contains two text input fields: 'Name*' with the value 'legacyEndpts' and 'Pattern*' with the value '^sip:2[0-9]{4}'. Below the fields is a note 'Fields marked * are required.' and an 'Update' button.</p> </div>



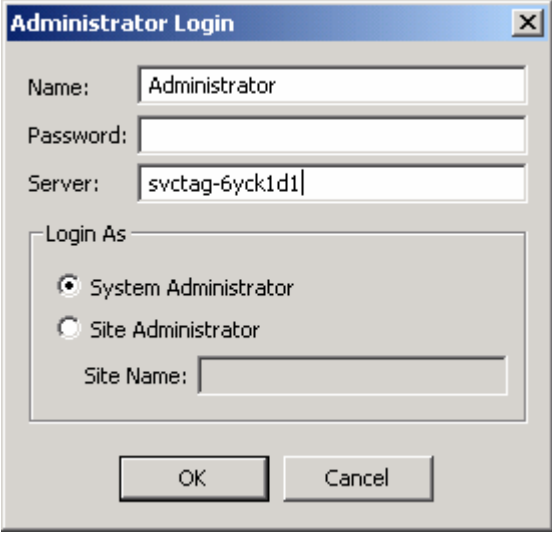
Step	Description
4.	<p data-bbox="315 184 1382 289"><b>Communication Server Address Map – Continued</b> Displayed below are the address maps configured in the compliance test for routing calls to the fax machine and fax server at remote site.</p> <div data-bbox="315 327 1430 1113">  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. The title bar indicates 'This Server: [ 1 ] SESsouth'. The main heading is 'Edit Communication Manager Map Entry'. There are two input fields: 'Name*' with the value 'ToSiteAFaxM' and 'Pattern*' with the value '^sip:50000'. Below the fields is the text 'Fields marked * are required.' and an 'Update' button. A navigation menu on the left lists various system components, with 'Communication Manager Servers' expanded to show 'Add' and 'List' options.</p> </div> <div data-bbox="315 1150 1430 1936">  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. The title bar indicates 'This Server: [ 1 ] SESsouth'. The main heading is 'Edit Communication Manager Map Entry'. There are two input fields: 'Name*' with the value 'ToSiteAFaxS' and 'Pattern*' with the value '^sip:60000'. Below the fields is the text 'Fields marked * are required.' and an 'Update' button. A navigation menu on the left lists various system components, with 'Communication Manager Servers' expanded to show 'Add' and 'List' options.</p> </div>

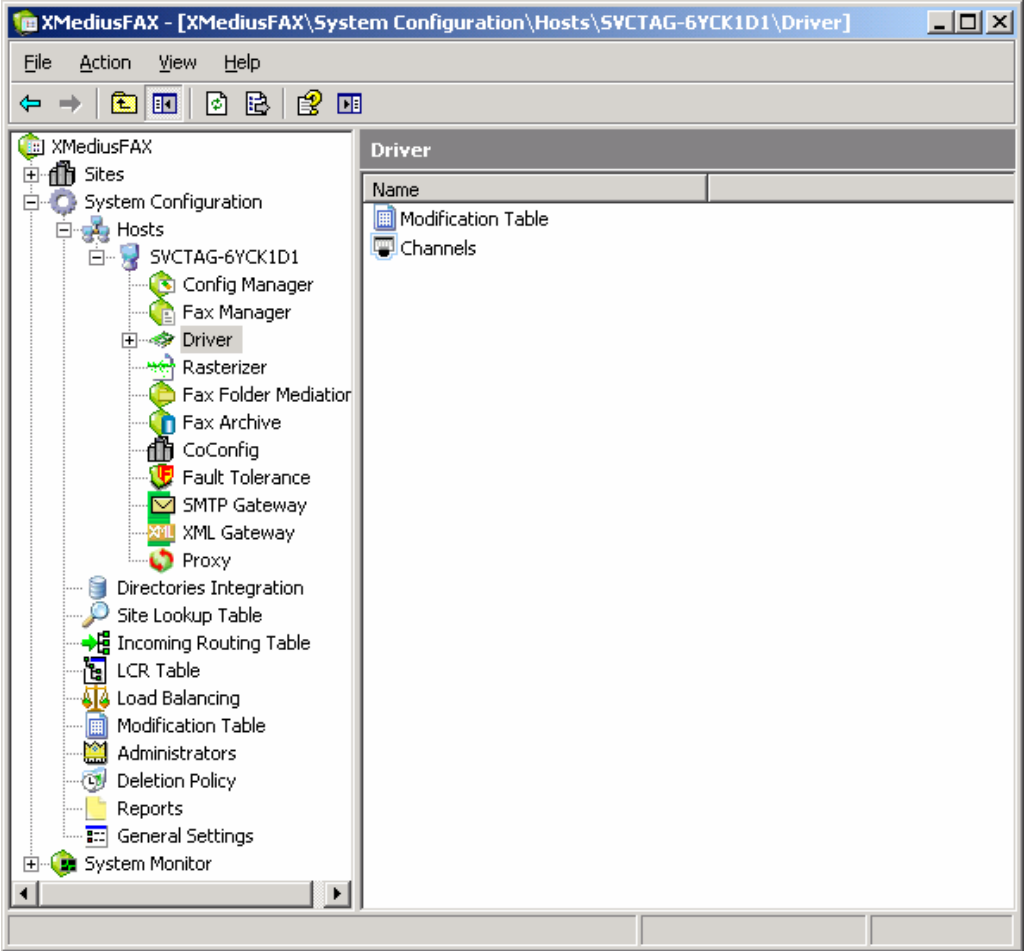
Step	Description
5.	<p><b>Trusted Host</b>  XMediusFAX fax server must be added as a Trusted Host (to the SIP Enablement Services). To add a new Trusted Host, navigate to <b>Trusted Hosts → Add Trusted Host</b> in the left pane. In the displayed window, configure the following fields:</p> <ul style="list-style-type: none"> <li>▪ <b>IP Address:</b> Enter IP address assigned to the XMediusFAX server</li> <li>▪ <b>Host:</b> Select the IP address for the Avaya SES</li> <li>▪ <b>Comments:</b> Enter a descriptive text</li> </ul> <p>After the fields are properly set, click <b>Add</b>.</p> 

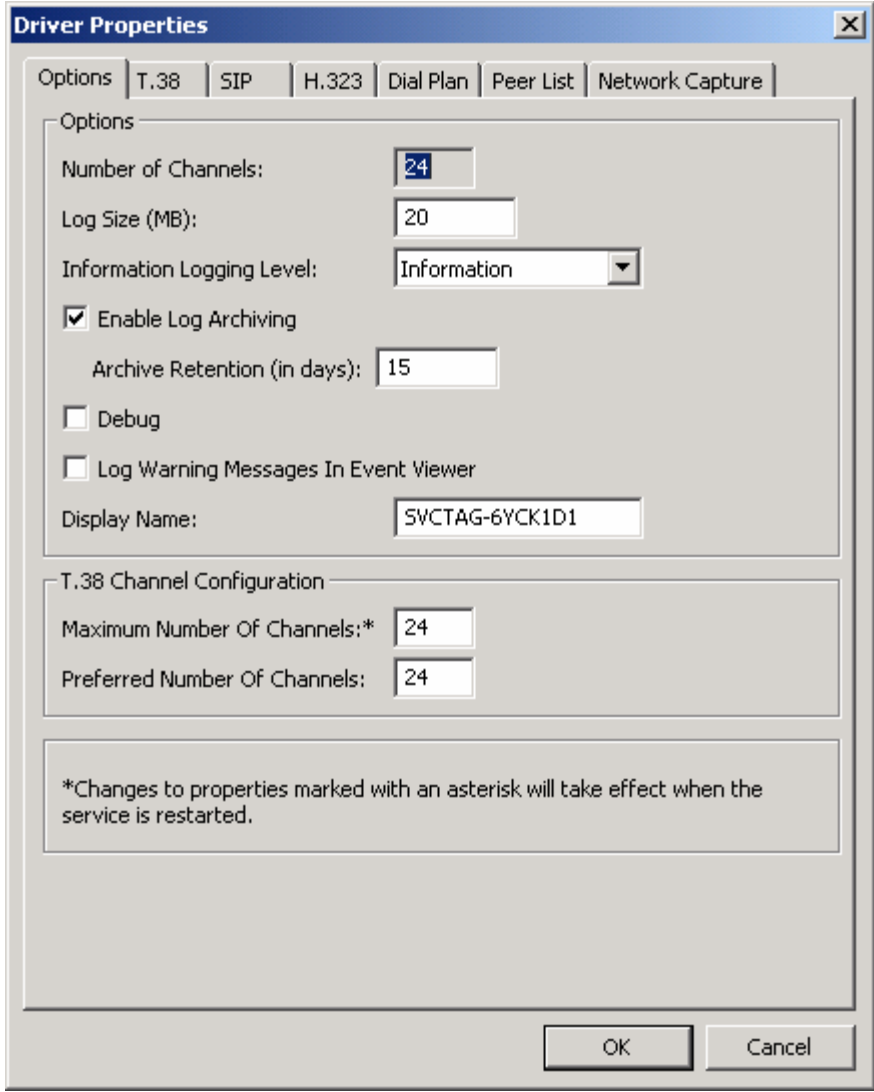
## 6. Configure Sagem-Interstar XMediusFAX

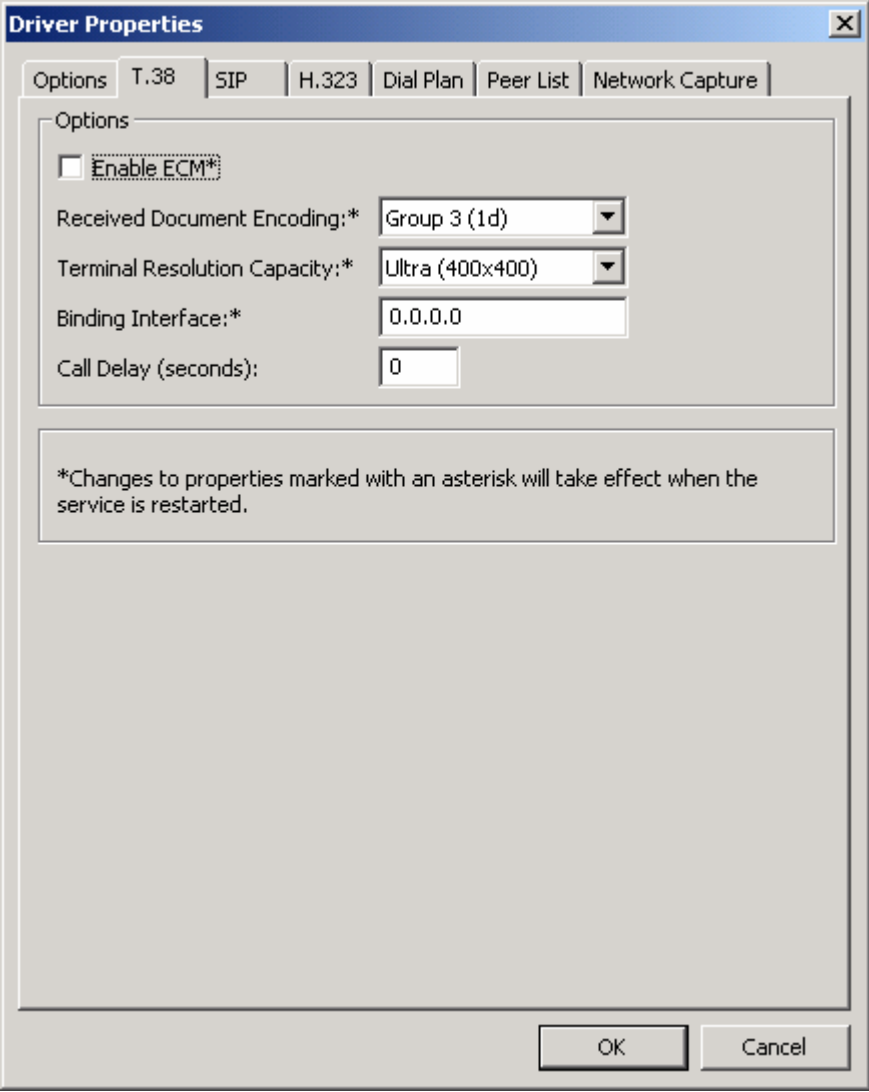
This section describes the configuration of XMediusFAX. It assumes that the application and all required software components have been installed and properly licensed. The number of channels supported by the XMediusFAX server is controlled via an XMediusFAX server license file. For instructions on sending and receiving faxes, consult the XMediusFAX Administrator Guide [5] and User Guide [7].

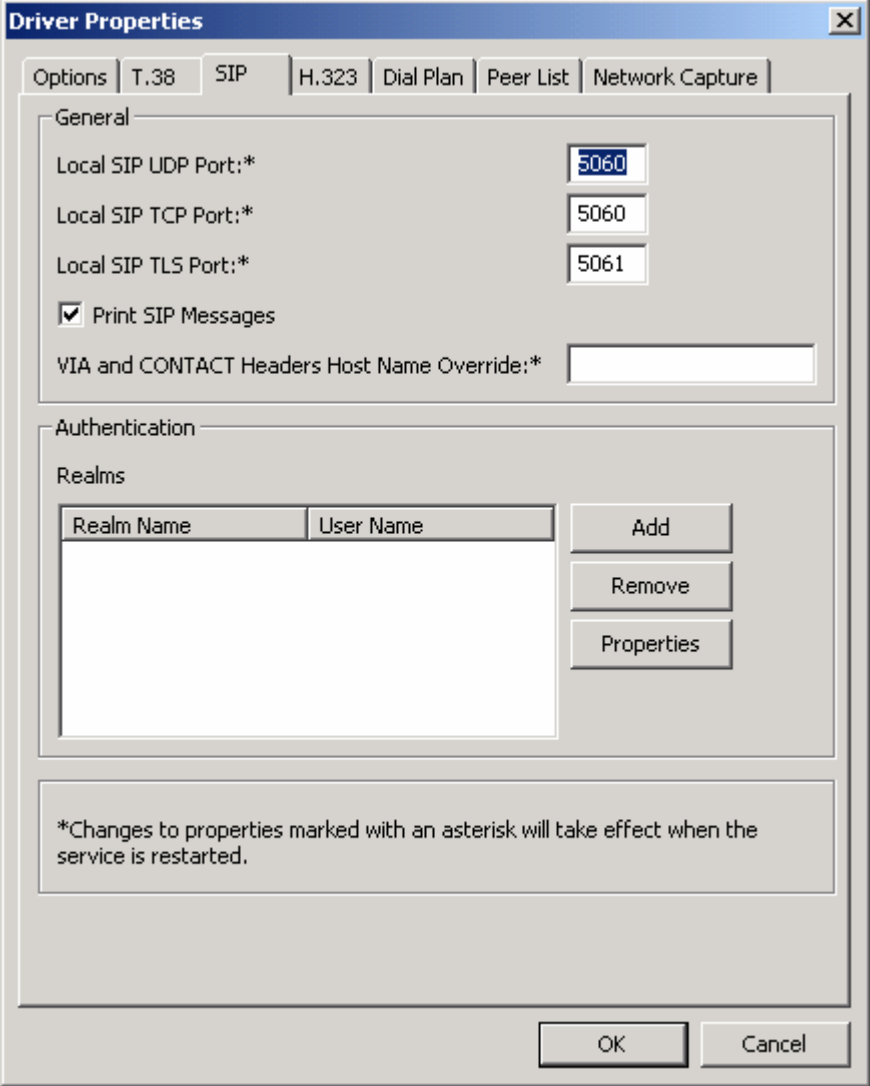
The examples shown in this section refer to Site B. Unless specified otherwise, the same steps also apply to Site A using values appropriate for Site A from **Figure 1**.

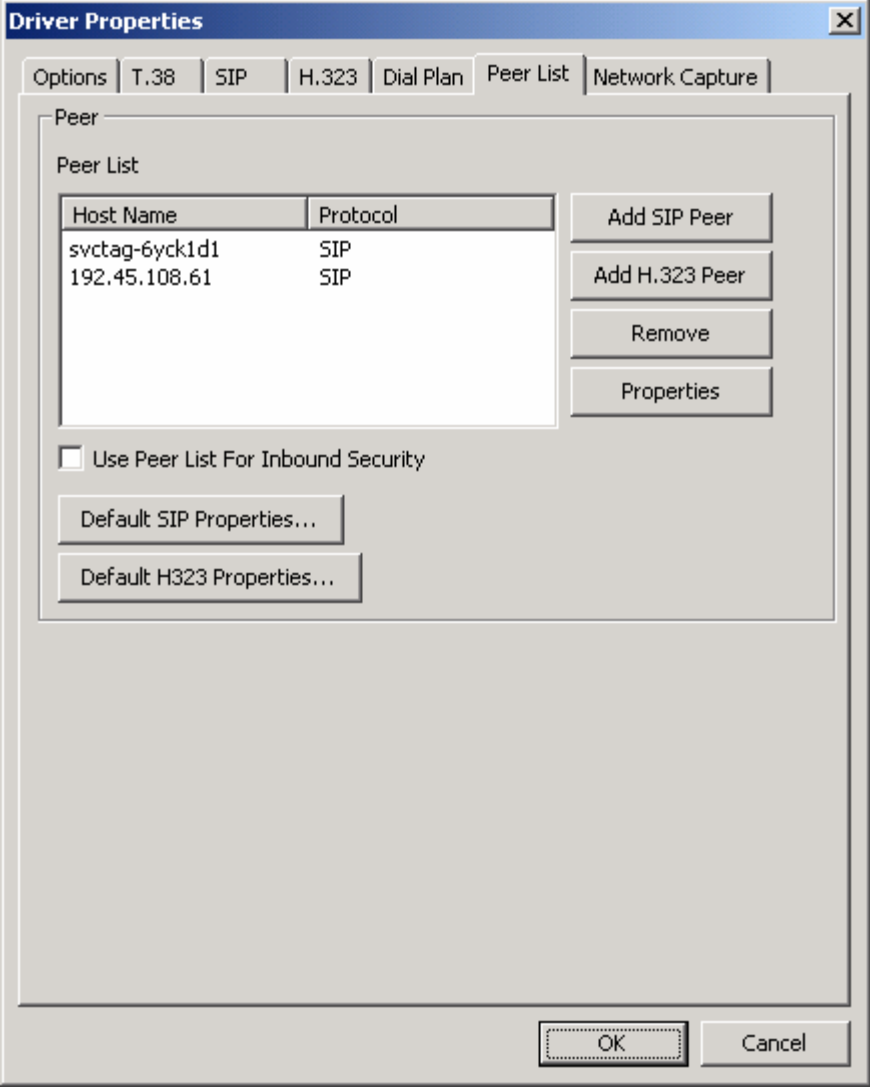
Step	Description
1.	<p><b>Prepare Windows 2003 Server for XMediusFAX launch</b></p> <p>To function properly XMediusFAX needs to have read/write privileges to the C:\Windows\temp folder. If McAfee VirusScan Enterprise is running on the Windows 2003 server, the C:\Windows\temp folder needs to be excluded from the scan list. Consult Sagem-Interstar for instructions.</p>
2.	<p><b>Launch the Application</b></p> <p>On the XMediusFAX server, launch the XMediusFAX application from the Windows Start Menu. Navigate to <b>Start → All Programs → XMediusFAX → XMediusFAX</b>. A login screen appears. Log in with proper credentials. Click the <b>OK</b> button.</p> <div data-bbox="662 1041 1211 1570" style="text-align: center;"></div>

Step	Description
3.	<p><b>Configure Driver Properties</b></p> <p>On the main screen, navigate to <b>XMediusFAX</b> → <b>System Configuration</b> → <b>Hosts</b> → <b>SVCTAG-6YCK1D1</b> → <b>Driver</b> in the left hand tree menu. Right-click on <b>Driver</b> and select <b>Properties</b> (not shown).</p>  <p>The screenshot shows the XMediusFAX application window. The title bar reads 'XMediusFAX - [XMediusFAX\System Configuration\Hosts\SVCTAG-6YCK1D1\Driver]'. The menu bar includes 'File', 'Action', 'View', and 'Help'. Below the menu bar is a toolbar with navigation icons. The main area is split into two panes. The left pane is a tree view showing the following structure: XMediusFAX (expanded) -&gt; Sites -&gt; System Configuration (expanded) -&gt; Hosts (expanded) -&gt; SVCTAG-6YCK1D1 (expanded) -&gt; Driver (selected). Other items under SVCTAG-6YCK1D1 include Config Manager, Fax Manager, Rasterizer, Fax Folder Mediation, Fax Archive, CoConfig, Fault Tolerance, SMTP Gateway, XML Gateway, and Proxy. Other items under Hosts include Directories Integration, Site Lookup Table, Incoming Routing Table, LCR Table, Load Balancing, Modification Table, Administrators, Deletion Policy, Reports, and General Settings. Under System Configuration, there is also a System Monitor icon. The right pane is titled 'Driver' and contains a table with a 'Name' header and two rows: 'Modification Table' and 'Channels'.</p>

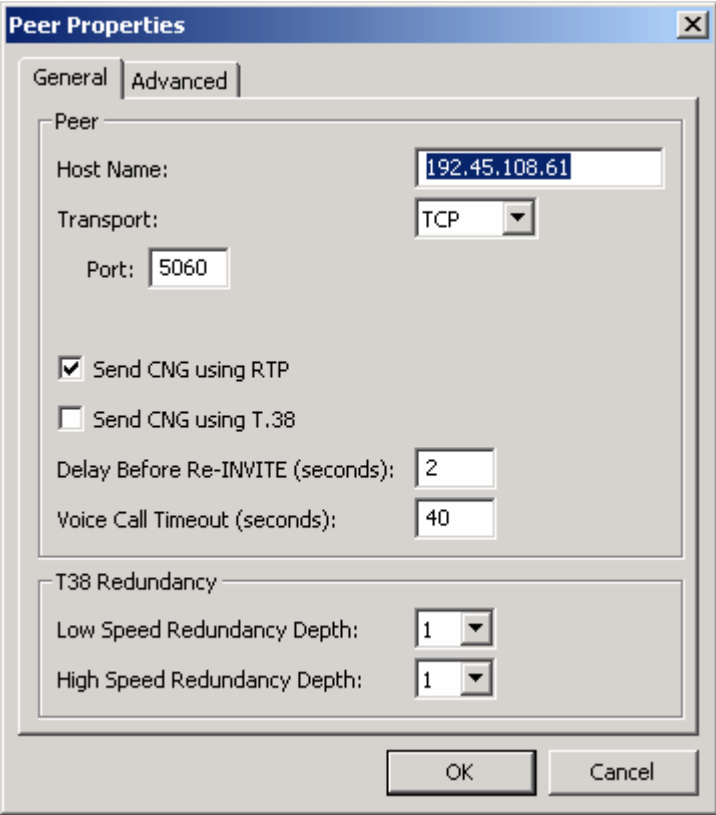
Step	Description
4.	<p><b>General Options</b></p> <p>On the <b>Driver Properties</b> screen, select the <b>Options</b> tab. Set the <b>Maximum Number Of Channels</b> and <b>Preferred Number Of Channels</b> fields under <b>T.38 Channel Configuration</b> to the number of simultaneous faxes to be processed. This number should be consistent with the <b>Number of Members</b> field specified in <b>Section 4, Step 10</b>.</p>  <p>The screenshot shows the 'Driver Properties' dialog box with the 'Options' tab selected. The 'T.38 Channel Configuration' section is expanded, showing 'Maximum Number Of Channels:*' and 'Preferred Number Of Channels' both set to 24. Other settings include 'Log Size (MB): 20', 'Information Logging Level: Information', and 'Enable Log Archiving' checked. A note at the bottom states: '*Changes to properties marked with an asterisk will take effect when the service is restarted.'</p>

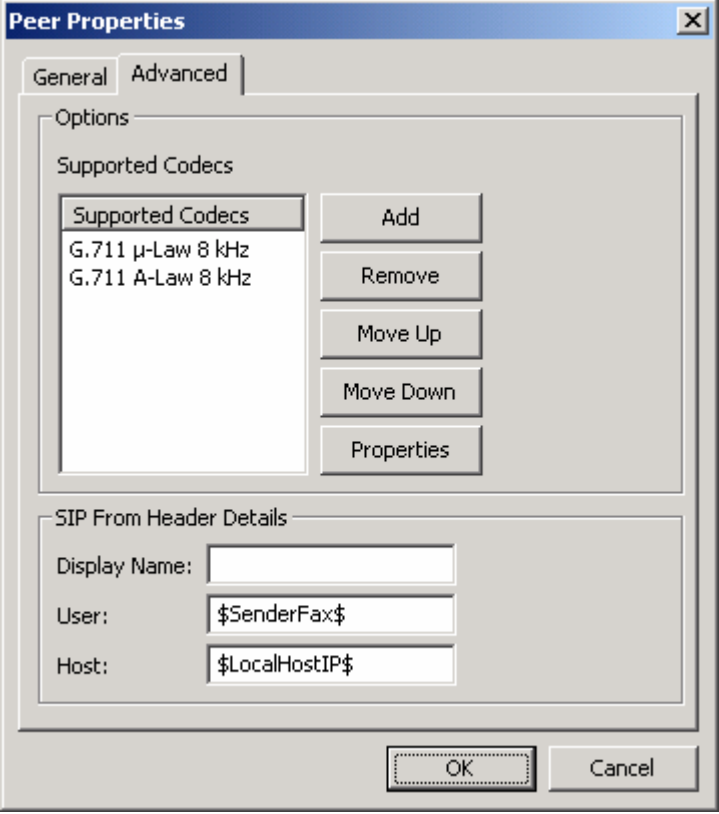
Step	Description
5.	<p><b>T.38 Parameters</b></p> <p>On the <b>Driver Properties</b> screen, select the <b>T.38</b> tab. Configure the fields as follows:</p> <ul style="list-style-type: none"> <li>• <b>Received Document Encoding</b> – Set this field to the highest encoding allowed. For the compliance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

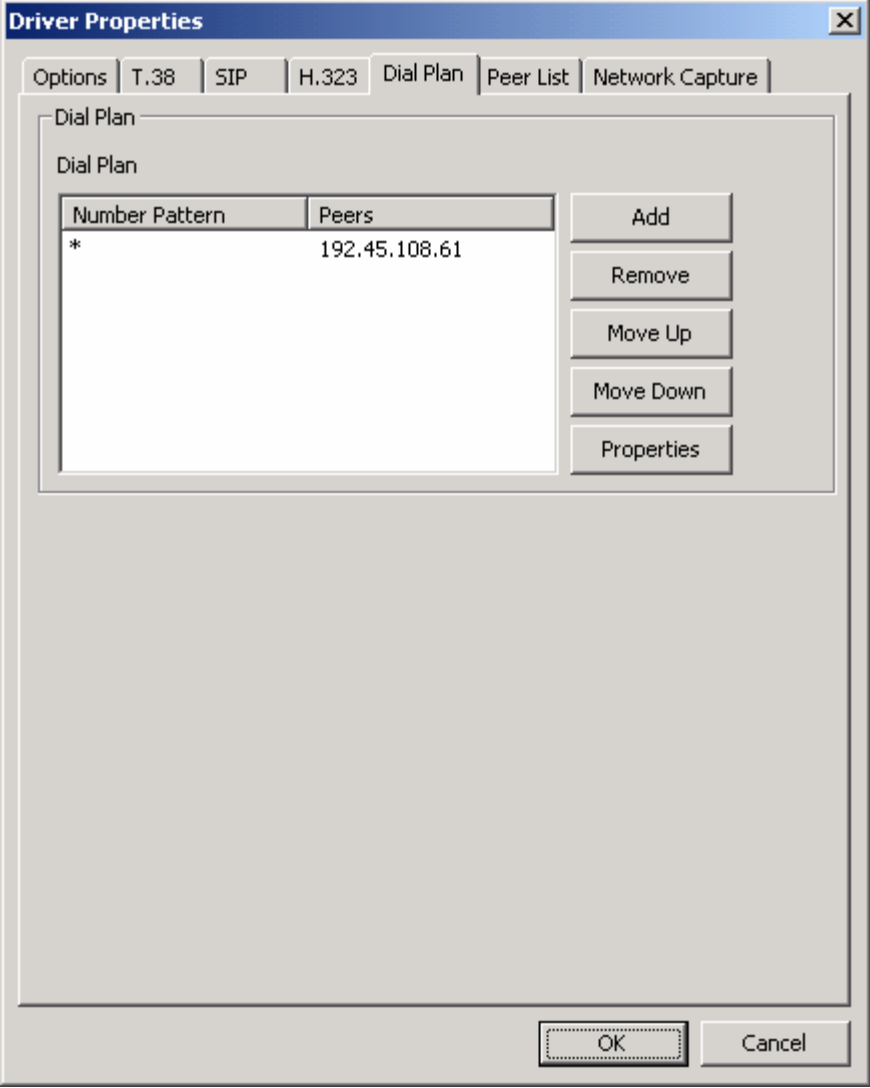
Step	Description
6.	<p><b>SIP Parameters</b></p> <p>On the <b>Driver Properties</b> screen, select the <b>SIP</b> tab. Configure the fields as follows:</p> <ul style="list-style-type: none"> <li>• <b>Local SIP TCP port</b> – Set this field to match the <b>Far-end Listen Port</b> field in <b>Section 4, Step 9</b>. For the compliance test, TCP was used as the transport layer protocol by the XMediusFAX.</li> </ul> 

Step	Description						
7.	<p><b>Peer List</b></p> <p>On the <b>Driver Properties</b> screen, select the <b>Peer List</b> tab. To add a new SIP peer, select the <b>Add SIP Peer</b> button and enter the values shown in <b>Step 8</b>. To view an existing peer in the list and click <b>Properties</b>. The example below shows the peer list after the Avaya SIP Enablement Services interface, <b>192.45.108.61</b>, has been added to the list.</p>  <p>The screenshot shows the 'Driver Properties' dialog box with the 'Peer List' tab selected. The 'Peer List' section contains a table with the following data:</p> <table border="1" data-bbox="561 600 1057 831"> <thead> <tr> <th>Host Name</th> <th>Protocol</th> </tr> </thead> <tbody> <tr> <td>svctag-6yck1d1</td> <td>SIP</td> </tr> <tr> <td>192.45.108.61</td> <td>SIP</td> </tr> </tbody> </table> <p>Buttons for 'Add SIP Peer', 'Add H.323 Peer', 'Remove', and 'Properties' are located to the right of the table. Below the table, there is a checkbox for 'Use Peer List For Inbound Security' (unchecked), and buttons for 'Default SIP Properties...' and 'Default H323 Properties...'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.</p>	Host Name	Protocol	svctag-6yck1d1	SIP	192.45.108.61	SIP
Host Name	Protocol						
svctag-6yck1d1	SIP						
192.45.108.61	SIP						

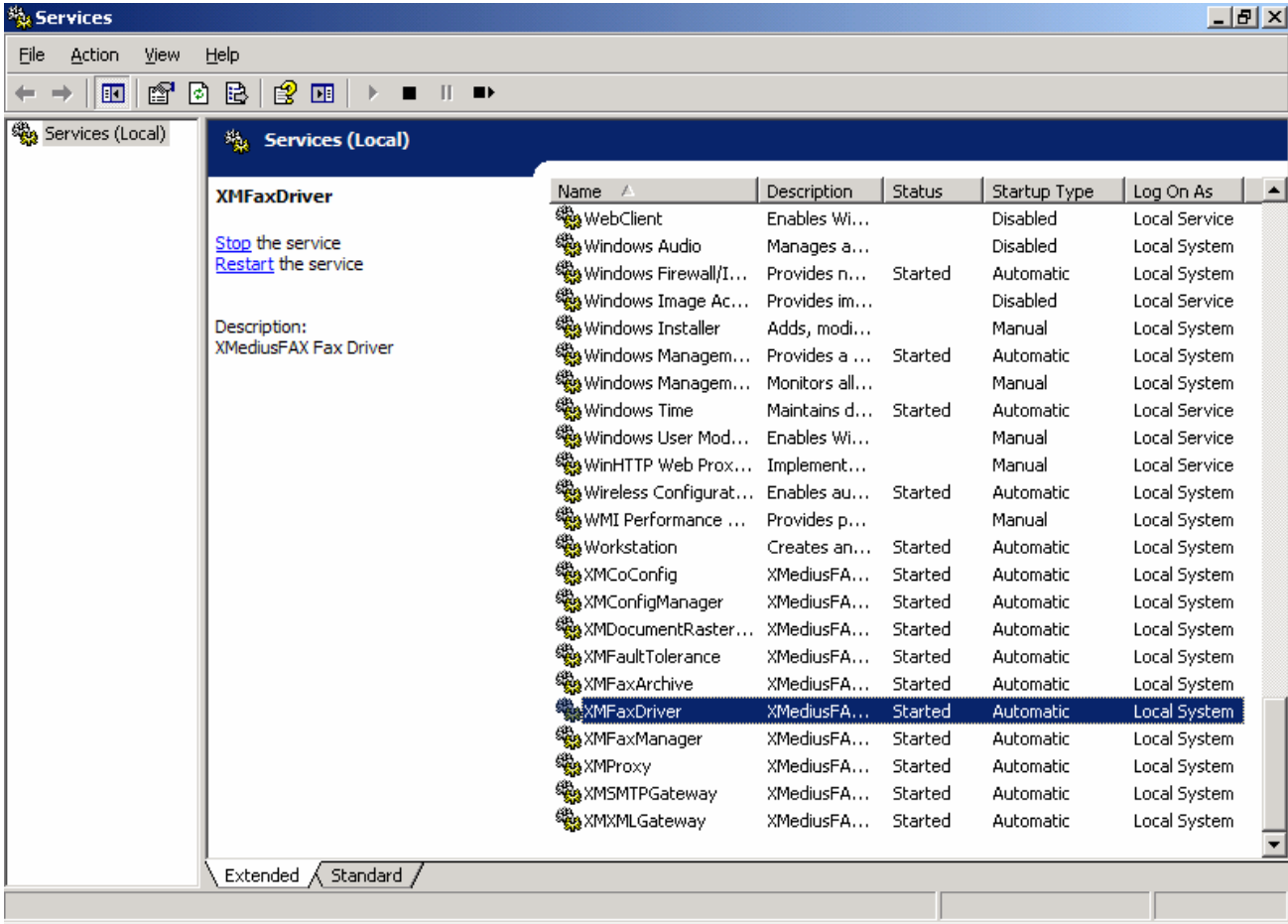


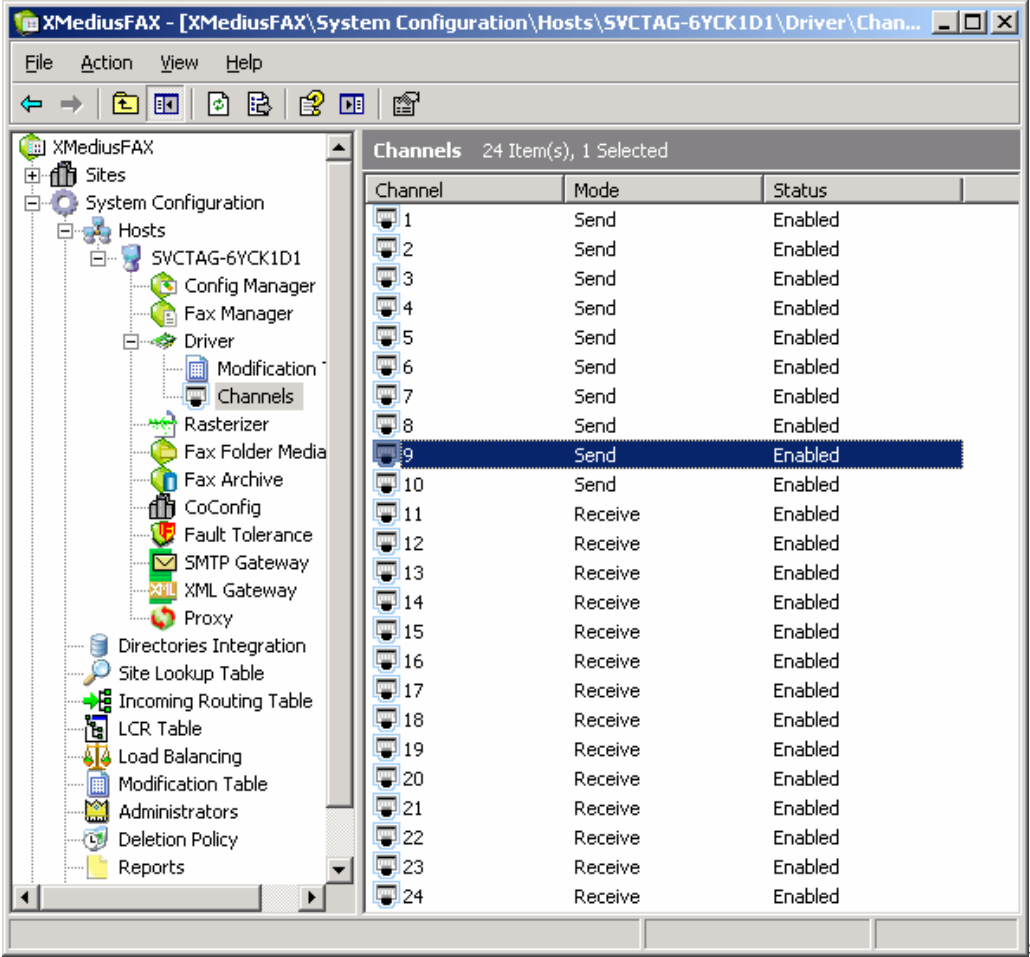
Step	Description
8.	<p><b>Peer Properties</b></p> <p>On the <b>Peer Properties</b> screen, configure as follows:</p> <ul style="list-style-type: none"> <li>• <b>Host Name</b> – Set this field to the IP address of the Avaya SIP Enablement Services server in <b>Section 5.1, Step 3</b>.</li> <li>• <b>Transport:</b> Set this field to <b>TCP</b>. For the compliance test, TCP was used as the transport layer protocol by the XMediusFAX.</li> <li>• <b>Port</b> - Set this field to <b>5060</b>.</li> <li>• Check the <b>Send CNG using RTP</b> field.</li> </ul> 

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

Step	Description				
10.	<p><b>Dial Plan</b></p> <p>On the <b>Driver Properties</b> screen, select the <b>Dial Plan</b> tab. To add a new entry to the dial plan, select the <b>Add</b> button and enter the values shown in <b>Step 11</b>. To view an existing entry, highlight the entry in the list and click <b>Properties</b> to get the <b>Number Pattern Properties</b> screen. The example below shows the dial plan after the entry for * (any value) has been added to the list.</p>  <p>The screenshot shows the 'Driver Properties' dialog box with the 'Dial Plan' tab selected. The dialog contains a table with the following data:</p> <table border="1" data-bbox="561 600 1057 877"> <thead> <tr> <th>Number Pattern</th> <th>Peers</th> </tr> </thead> <tbody> <tr> <td>*</td> <td>192.45.108.61</td> </tr> </tbody> </table> <p>Buttons for 'Add', 'Remove', 'Move Up', 'Move Down', and 'Properties' are located to the right of the table. The 'OK' and 'Cancel' buttons are at the bottom of the dialog.</p>	Number Pattern	Peers	*	192.45.108.61
Number Pattern	Peers				
*	192.45.108.61				

Step	Description				
11.	<p><b>Number Pattern Properties</b></p> <p>On the <b>Number Pattern Properties</b> screen, configure as follows:</p> <ul style="list-style-type: none"> <li>• <b>Number Pattern</b> – Set this field to the pattern to match. In this example, the value of * indicates any dialed number is acceptable.</li> <li>• <b>Peer</b> – Click the <b>Add</b> button. In the <b>Peer Properties</b> window that appears (not shown), enter the <b>Peer IP Address</b> and <b>Preference</b> value of <i>1</i> and click <b>OK</b>. In this example, only one peer is configured.</li> </ul> <div data-bbox="565 516 1312 1045" data-label="Image"> <table border="1" data-bbox="597 709 1096 961"> <thead> <tr> <th>Peer</th> <th>Preference</th> </tr> </thead> <tbody> <tr> <td>192.45.108.61</td> <td>1 (Higher)</td> </tr> </tbody> </table> </div> <p>Lastly, click OK on the <b>Driver Properties</b> screen shown in <b>Step 10</b>, to accept the Driver Configuration.</p>	Peer	Preference	192.45.108.61	1 (Higher)
Peer	Preference				
192.45.108.61	1 (Higher)				

Step	Description																																																																																																																								
12.	<p>Once all the driver properties have been configured, go to <b>Start → Control Panel → Administrative Tools → Services</b> to stop and start the <b>XMFaxDriver</b> service to effect the changes.</p>  <p>The screenshot shows the Windows Services console window. The 'Services (Local)' list is displayed, and the 'XMFaxDriver' service is selected and highlighted. The service details on the left show it is a description of the XMMediusFAX Fax Driver. The table below lists the services visible in the console.</p> <table border="1" data-bbox="495 466 1580 1144"> <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>WebClient</td><td>Enables Wi...</td><td>Disabled</td><td>Disabled</td><td>Local Service</td></tr> <tr><td>Windows Audio</td><td>Manages a...</td><td>Disabled</td><td>Disabled</td><td>Local System</td></tr> <tr><td>Windows Firewall/I...</td><td>Provides n...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr> <tr><td>Windows Image Ac...</td><td>Provides im...</td><td>Disabled</td><td>Disabled</td><td>Local Service</td></tr> <tr><td>Windows Installer</td><td>Adds, modi...</td><td>Manual</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 Managem...</td><td>Monitors all...</td><td>Manual</td><td>Manual</td><td>Local System</td></tr> <tr><td>Windows Time</td><td>Maintains d...</td><td>Started</td><td>Automatic</td><td>Local Service</td></tr> <tr><td>Windows User Mod...</td><td>Enables Wi...</td><td>Manual</td><td>Manual</td><td>Local Service</td></tr> <tr><td>WinHTTP Web Prox...</td><td>Implement...</td><td>Manual</td><td>Manual</td><td>Local Service</td></tr> <tr><td>Wireless Configur...</td><td>Enables au...</td><td>Started</td><td>Automatic</td><td>Local System</td></tr> <tr><td>WMI Performance ...</td><td>Provides p...</td><td>Manual</td><td>Manual</td><td>Local System</td></tr> <tr><td>Workstation</td><td>Creates an...</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>Local System</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><b>XMFaxDriver</b></td><td><b>XMediusFA...</b></td><td><b>Started</b></td><td><b>Automatic</b></td><td><b>Local System</b></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	WebClient	Enables Wi...	Disabled	Disabled	Local Service	Windows Audio	Manages a...	Disabled	Disabled	Local System	Windows Firewall/I...	Provides n...	Started	Automatic	Local System	Windows Image Ac...	Provides im...	Disabled	Disabled	Local Service	Windows Installer	Adds, modi...	Manual	Manual	Local System	Windows Managem...	Provides a ...	Started	Automatic	Local System	Windows Managem...	Monitors all...	Manual	Manual	Local System	Windows Time	Maintains d...	Started	Automatic	Local Service	Windows User Mod...	Enables Wi...	Manual	Manual	Local Service	WinHTTP Web Prox...	Implement...	Manual	Manual	Local Service	Wireless Configur...	Enables au...	Started	Automatic	Local System	WMI Performance ...	Provides p...	Manual	Manual	Local System	Workstation	Creates an...	Started	Automatic	Local System	XMCoConfig	XMediusFA...	Started	Automatic	Local System	XMConfigManager	XMediusFA...	Started	Automatic	Local System	XMDocumentRaster...	XMediusFA...	Started	Automatic	Local System	XMFaultTolerance	XMediusFA...	Started	Automatic	Local System	XMFaxArchive	XMediusFA...	Started	Automatic	Local System	<b>XMFaxDriver</b>	<b>XMediusFA...</b>	<b>Started</b>	<b>Automatic</b>	<b>Local System</b>	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																																																																																																																					
WebClient	Enables Wi...	Disabled	Disabled	Local Service																																																																																																																					
Windows Audio	Manages a...	Disabled	Disabled	Local System																																																																																																																					
Windows Firewall/I...	Provides n...	Started	Automatic	Local System																																																																																																																					
Windows Image Ac...	Provides im...	Disabled	Disabled	Local Service																																																																																																																					
Windows Installer	Adds, modi...	Manual	Manual	Local System																																																																																																																					
Windows Managem...	Provides a ...	Started	Automatic	Local System																																																																																																																					
Windows Managem...	Monitors all...	Manual	Manual	Local System																																																																																																																					
Windows Time	Maintains d...	Started	Automatic	Local Service																																																																																																																					
Windows User Mod...	Enables Wi...	Manual	Manual	Local Service																																																																																																																					
WinHTTP Web Prox...	Implement...	Manual	Manual	Local Service																																																																																																																					
Wireless Configur...	Enables au...	Started	Automatic	Local System																																																																																																																					
WMI Performance ...	Provides p...	Manual	Manual	Local System																																																																																																																					
Workstation	Creates an...	Started	Automatic	Local System																																																																																																																					
XMCoConfig	XMediusFA...	Started	Automatic	Local System																																																																																																																					
XMConfigManager	XMediusFA...	Started	Automatic	Local System																																																																																																																					
XMDocumentRaster...	XMediusFA...	Started	Automatic	Local System																																																																																																																					
XMFaultTolerance	XMediusFA...	Started	Automatic	Local System																																																																																																																					
XMFaxArchive	XMediusFA...	Started	Automatic	Local System																																																																																																																					
<b>XMFaxDriver</b>	<b>XMediusFA...</b>	<b>Started</b>	<b>Automatic</b>	<b>Local System</b>																																																																																																																					
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																																																																											
13.	<p><b>Configure Channels</b></p> <p>On the main screen, navigate to <b>XMediusFAX → System Configuration → Hosts → SVCTAG-6YCK1D1 → Driver → Channels</b> in the left hand tree menu. Right-click on each channel in the right pane to set the <b>Mode</b> to <i>Send</i>, <i>Receive</i> or <i>Both</i>. In the compliance test, 10 channels were set to <i>Send</i> and 14 channels were set to <i>Receive</i>.</p>  <table border="1" data-bbox="779 577 1429 1312"> <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 style="background-color: #000080; color: white;"><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>Receive</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	Receive	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	Receive	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																																																																										

## 7. General Test Approach and Test Results

This section describes the compliance testing used to verify the interoperability of Sagem-Interstar XMediusFAX SP Edition with the Avaya SIP infrastructure (Communication Manager and SIP Enablement Services). This section covers the general test approach and the test results.

### 7.1. General Test Approach

The general test approach was to make intra-site and inter-site fax calls to and from XMediusFAX. In the compliance test configuration Site B served as the main enterprise site and Site A served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using SIP trunks or ISDN-PRI trunks between the sites. By using two Communication Managers and two port networks with one of the Communication Managers, fax calls across multiple TDM/IP hops were able to be tested. Faxes were sent with various page lengths, resolutions, and at various fax data speeds. For capacity testing, a 100 2-page faxes were continuously sent between the two XMediusFAX servers. Because the G350 has a limited DSP capacity, a G450 with the same configuration was used for the capacity testing. Serviceability testing included verifying proper operation/recovery from failed cables, 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, the TN2602 MedPro circuit pack in the Avaya G650 Media Gateway; and the integrated VoIP engine of the Avaya G350 Media Gateway.

### 7.2. Test Results

XMediusFAX successfully passed compliance testing. The following observations were made during the compliance test:

- All the fax calls were established successfully with or without shuffling on. However, for those inter-site calls that have shuffling on and SIP trunks used between the two sites, the audio was not shuffled from end-to-end. Instead, Port Network 1 Medpro media resources were used in the audio path for those calls.
- To function properly XMediusFAX needs to have read/write privileges to the C:\Windows\temp folder. If McAfee VirusScan Enterprise is running on the Windows 2003 server, the C:\Windows\temp folder needs to be excluded from the scan list to make the folder readable and writeable by XMediusFAX.
- During the serviceability testing, the cable between the router and the Layer 2 switch that connected the XMediusFAX server was unplugged to simulate a network disruption. When the cable was plugged back in, inbound calls to the XMediusFAX were working. But outbound calls from the XMediusFAX server did not work any more. This was because the Windows 2003 server, the XMediusFAX server ran on, still kept the old TCP socket. The XMediusFAX server can go back to normal by stopping and starting the XMediusFAX Driver service manually.

## 8. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling groups configured in **Step 9** of **Section 4** are in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Section 4, Steps 10 - 11** is in-service.
- Verify that fax calls can be placed to/from XMediusFAX server at each site.
- From the Avaya Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed to the expected trunks.
- From the Avaya Communication Manager SAT, use the **status trunk group** command to identify the trunk used for a particular call and then use the **status trunk group/member** command to verify the audio path of the call.

## 9. Conclusion

These Application Notes describe the procedures required to configure the Sagem-Interstar XMediusFAX Service Provider (SP) Edition to interoperate with Avaya SIP infrastructure (Communication Manager and SIP Enablement Services). The Sagem-Interstar XMediusFAX SP Edition successfully passed compliance testing with the observations documented in **Section 7.2**.

## 10. Additional References

- [1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Doc # 555-245-205, May 2009.
- [2] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, May 2009.
- [3] *SIP support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers*, Doc # 555-245-206, May 2009.
- [4] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server*, Doc # 03-602508, May 2009.
- [5] *Sagem-Interstar XMediusFAX Administrator Guide*, November 2009
- [6] *Sagem-Interstar XMediusFAX Installation and Maintenance Guide*, November 2009
- [7] *Sagem-Interstar XMediusFAX User Guide*, November 2009

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

Documentation for XMediusFAX version 6.5 may be found at [www.sagem-interstar.com](http://www.sagem-interstar.com).



---

**©2010 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](mailto:devconnect@avaya.com).