



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring emFAST FACSys Fax Messaging Suite with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager via a SIP Trunking Interface - Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring the emFAST FACSys Fax Messaging Suite with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager (SM) using a SIP trunk.

The FACSys Fax Messaging Suite includes a software-based fax server that sends and receives fax calls over an IP network. In the tested configuration, the FACSys Fax Messaging Suite interoperates with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager to send/receive faxes using SIP trunks and the T.38 fax protocol between the FACSys Fax Messaging Suite fax server 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 emFAST FACSys Fax Messaging Suite with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager using SIP trunks.

The FACSys Fax Messaging Suite includes a software based fax server that sends and receives fax calls over an IP network. In the tested configuration, the FACSys Fax Messaging Suite interoperates with Communication Manager and Session Manager to send/receive faxes using SIP trunks and the T.38 protocol between the FACSys Fax Messaging Suite fax server and the Avaya SIP infrastructure.

## 1.1. Interoperability Compliance Testing

The compliance test cases that were executed tested the interoperability between the FACSys Fax Messaging Suite, Communication Manager, and Session Manager by making intra-site and inter-site fax calls to and from the FACSys Fax Messaging Suite fax server. The FACSys Fax Messaging Suite fax server connects (at each of the two sites in the test configuration) to Communication Manager and Session Manager via SIP trunks (see **Section 2** for more configuration details). Specifically, the following fax operations were tested:

- Faxes to the FACSys Fax Messaging Suite fax server from a local fax machine
- Faxes from the FACSys Fax Messaging Suite fax server to a local fax machine
- Faxes to the FACSys Fax Messaging Suite fax server from a remote fax machine
- Fax from the FACSys Fax Messaging Suite fax server to a remote fax machine

In the compliance tested configuration, 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. Serviceability testing included verifying proper operation and recovery from cable connection failures, unavailable resources, restarts of the Communication Manager and the Session Manager, as well as reboots of the FACSys Fax Messaging Suite fax server. 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 G450 Media Gateway.

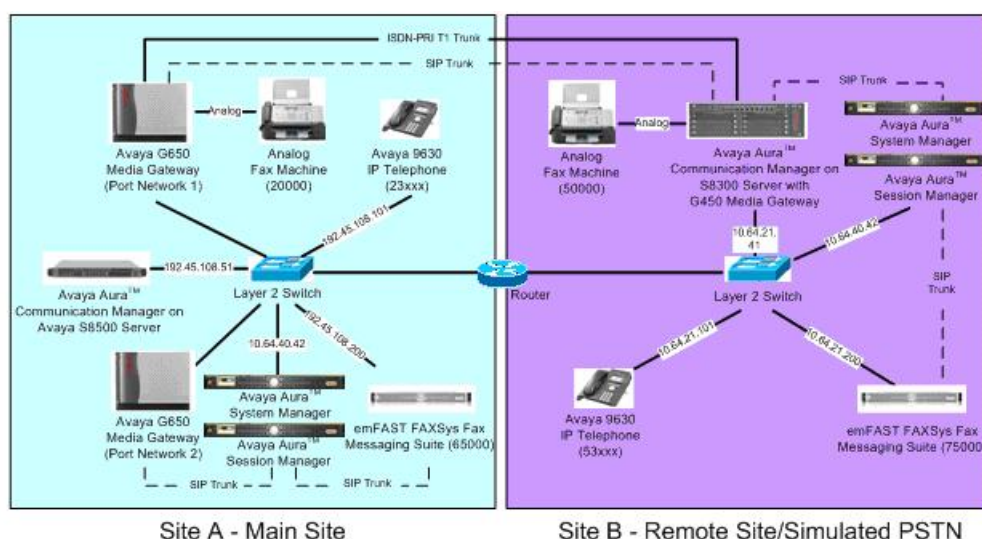
## 1.2. Support

Technical support for the emFAST FACSys Fax Messaging Suite can be obtained through the following:

- **Phone:** (866) 436-3278
- **Web:** <http://www.emfast.com/support.aspx>

## 2. Configuration

**Figure 1** illustrates the configuration used during compliance testing as described in these Application Notes. In the test 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: FACSys Fax Messaging Suite interoperating with Communication Manager and Session Manager**

Site A comprises of a Session Manager (with its companion Avaya Aura™ System Manager) 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. The FACSys Fax Messaging Suite fax server at this site is running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and Session Manager) via SIP trunks. The signaling for the SIP trunk from Session Manager to Communication manager is terminated on a CLAN circuit pack in port network 2. The media resources required by the trunk are provided by an IP Media Processor (MedPro) circuit pack. Two versions of the IP MedPro circuit pack were tested in this configuration: TN2602AP and TN2302AP. Endpoints at this site include Avaya 9600 Series IP Telephones and an analog fax machine.

Site B comprises of a Session Manager (with its companion System Manager) and an Avaya S8300 Server running Communication Manager in an Avaya G450 Media Gateway. Note that the

compliance tested configuration only consisted of a single Session Manager that was shared between the two sites. However, for illustrative purposes only, the Session Manager is shown as a separate entity at each site. The FACSys Fax Messaging Suite fax server at Site B is also running on a Windows 2003 Server and communicates to the Avaya SIP infrastructure (Communication Manager and Session Manager) via SIP trunks. On the Avaya G450 Media Gateway, the signaling and media resources needed to support SIP trunks are integrated directly on the media gateway processor. Endpoints at this site also include Avaya 9600 Series IP Telephones 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 the FACSys Fax Messaging Suite fax server are sent to Session Manager first, and then from Session Manager to Communication Manager via the configured SIP trunks. Based on the dialed digits, the Communication Manager will either direct the calls to the local fax machine, or to the inter-site trunks (ISDN-PRI or SIP) to reach the remote site. Inbound fax calls terminating to the FACSys Fax Messaging Suite fax server from the local fax machine or from the remote site are first received by Communication Manager. Communication Manager then directs the calls to the FACSys Fax Messaging Suite fax server via Session Manager and 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
<b>SITE A</b>	
Avaya S8500 Server	Communication Manager 5.2.1 R015x.02.1.016.4-17959
Avaya G650 Media Gateway - 2 CLANs - 2 IP MedPros – TN2302AP - 2 IP MedPros – TN2602AP	TN799DP - HW01 FW24 TN2302AP - HW20 FW120 TN2602AP - HW02 FW051
Avaya S8800 Server	System Manager 5.2.1.1
Avaya S8800 Server	Session Manager 5.2.1.1
Analog Fax Machine	-
Avaya 9630 IP Telephone (SIP) Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 2.5.0 Avaya one-X® Deskphone Edition 3.0
Windows 2003 Server running emFAST FACSys Fax Messaging Suite	5.1 (emFAST)
<b>SITE B</b>	
Avaya S8300 Server	Communication Manager 5.2.1 R015x.02.1.016.4-17959
Avaya G450 Media Gateway	-
Avaya S8800 Server	System Manager 5.2.1.1
Avaya S8800 Server	Session Manager 5.2.1.1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.0
Analog Fax Machine	-
Windows 2003 Server running emFAST FACSys Fax Messaging Suite	5.1 (emFAST)

## 4. Configure Avaya Aura™ Communication Manager

This section describes the Communication Manager configuration required to interoperate with the FACSys Fax Messaging Suite fax server. It focuses on the configuration of the SIP trunks connecting the FACSys Fax Messaging Suite fax server to the Avaya SIP infrastructure with the following assumptions:

- Procedures necessary to support SIP and connectivity to Session Manager have been performed as described in references [2], [3], and [5].
- All other components are assumed to be in place and previously configured, including the SIP and ISDN-PRI trunks 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 A. Unless specified otherwise, these same steps also apply to Site B using values appropriate for Site B from **Figure 1**.

Step	Description
1.	<p><b>Communication Manager License</b></p> <p>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>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> <pre> change system-parameters customer-options                                 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.	<div><div>IP Interfaces</div><div><ul style="list-style-type: none"><li>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 during compliance testing. All interfaces in cabinet 01 (port network 1), as indicated by the <b>Slot</b> field, are in IP network region 1, as indicated by the <b>Net Rgn</b> field. These interfaces are highlighted below. Testing with the TN2302AP and TN2602AP circuit packs was done separately. When testing with the TN2302AP IP interfaces, the TN2602AP IP interfaces were disabled (turned off) and vice versa as indicated by the <b>ON</b> field. Node Names are defined using the <b>change node-names ip</b> command.</li></ul></div></div> <div><div><div>list ip-interface all</div><div><div>Page1</div><div>IP INTERFACES</div><table><thead><tr><th>ON</th><th>Type</th><th>Slot</th><th>Code/Sfx</th><th>Node Name/ IP-Address</th><th>Mask</th><th>Gateway</th><th>Node</th><th>Net Rgn</th><th>VLAN</th></tr></thead><tbody><tr><td>y</td><td>MEDPRO</td><td>01A02</td><td>TN2302</td><td>MEDPRO1A 192.45.108.54</td><td>/24</td><td>Gateway001</td><td></td><td>1</td><td>n</td></tr><tr><td>y</td><td>C-LAN</td><td>01A03</td><td>TN799 D</td><td>CLAN1A 192.45.108.55</td><td>/24</td><td>Gateway001</td><td></td><td>1</td><td>n</td></tr><tr><td>y</td><td>MEDPRO</td><td>02A02</td><td>TN2302</td><td>MEDPRO2A 192.45.108.56</td><td>/24</td><td>Gateway001</td><td></td><td>2</td><td>n</td></tr><tr><td>y</td><td>C-LAN</td><td>02A03</td><td>TN799 D</td><td>CLAN2A 192.45.108.57</td><td>/24</td><td>Gateway001</td><td></td><td>2</td><td>n</td></tr><tr><td>n</td><td>MEDPRO</td><td>01A04</td><td>TN2602</td><td>MEDPRO1A-2 192.45.108.58</td><td>/24</td><td>Gateway001</td><td></td><td>1</td><td>n</td></tr><tr><td>n</td><td>MEDPRO</td><td>02A04</td><td>TN2602</td><td>MEDPRO2A-2 192.45.108.59</td><td>/24</td><td>Gateway001</td><td></td><td>2</td><td>n</td></tr></tbody></table></div></div></div> <div><div><div>change node-names ip</div><div><div>Page1 of 2</div><div>IP NODE NAMES</div><table><thead><tr><th>Name</th><th>IP Address</th></tr></thead><tbody><tr><td>CLAN1A</td><td>192.45.108.55</td></tr><tr><td>CLAN2A</td><td>192.45.108.57</td></tr><tr><td>CM-Remote</td><td>10.64.21.41</td></tr><tr><td>MEDPRO1A</td><td>192.45.108.54</td></tr><tr><td>MEDPRO1A-2</td><td>192.45.108.58</td></tr><tr><td>MEDPRO2A</td><td>192.45.108.56</td></tr><tr><td>MEDPRO2A-2</td><td>192.45.108.59</td></tr><tr><td>SM1</td><td>10.64.40.42</td></tr></tbody></table></div></div></div>	ON	Type	Slot	Code/Sfx	Node Name/ IP-Address	Mask	Gateway	Node	Net Rgn	VLAN	y	MEDPRO	01A02	TN2302	MEDPRO1A 192.45.108.54	/24	Gateway001		1	n	y	C-LAN	01A03	TN799 D	CLAN1A 192.45.108.55	/24	Gateway001		1	n	y	MEDPRO	02A02	TN2302	MEDPRO2A 192.45.108.56	/24	Gateway001		2	n	y	C-LAN	02A03	TN799 D	CLAN2A 192.45.108.57	/24	Gateway001		2	n	n	MEDPRO	01A04	TN2602	MEDPRO1A-2 192.45.108.58	/24	Gateway001		1	n	n	MEDPRO	02A04	TN2602	MEDPRO2A-2 192.45.108.59	/24	Gateway001		2	n	Name	IP Address	CLAN1A	192.45.108.55	CLAN2A	192.45.108.57	CM-Remote	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	SM1	10.64.40.42
ON	Type	Slot	Code/Sfx	Node Name/ IP-Address	Mask	Gateway	Node	Net Rgn	VLAN																																																																																
y	MEDPRO	01A02	TN2302	MEDPRO1A 192.45.108.54	/24	Gateway001		1	n																																																																																
y	C-LAN	01A03	TN799 D	CLAN1A 192.45.108.55	/24	Gateway001		1	n																																																																																
y	MEDPRO	02A02	TN2302	MEDPRO2A 192.45.108.56	/24	Gateway001		2	n																																																																																
y	C-LAN	02A03	TN799 D	CLAN2A 192.45.108.57	/24	Gateway001		2	n																																																																																
n	MEDPRO	01A04	TN2602	MEDPRO1A-2 192.45.108.58	/24	Gateway001		1	n																																																																																
n	MEDPRO	02A04	TN2602	MEDPRO2A-2 192.45.108.59	/24	Gateway001		2	n																																																																																
Name	IP Address																																																																																								
CLAN1A	192.45.108.55																																																																																								
CLAN2A	192.45.108.57																																																																																								
CM-Remote	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																																																																																								
SM1	10.64.40.42																																																																																								



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 A, the Avaya S8500 Server, Avaya G650 Media Gateway comprising of port network 1, and the IP endpoints were all 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 during compliance testing.</p> <ul style="list-style-type: none"> <li>▪ The <b>Authoritative Domain</b> field was configured to match the domain name configured on Session Manager. In this configuration, the domain name is <b>avaya.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 1 was selected.</li> <li>▪ The default values were used for all other fields.</li> </ul> <p>At Site B, 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> display ip-network-region 1                                     Page 1 of 1                                  IP NETWORK REGION Region: 1 Location:                Authoritative Domain: avaya.com Name: PN1 MEDIA PARAMETERS   Codec Set: 1   Intra-region IP-IP Direct Audio: yes   Inter-region IP-IP Direct Audio: yes   UDP Port Min: 2048   UDP Port Max: 3329   IP Audio Hairpinning? n DIFFSERV/TOS PARAMETERS   Call Control PHB Value: 46   Audio PHB Value: 46   Video PHB Value: 26   RTCP Reporting Enabled? y   RTCP MONITOR SERVER PARAMETERS   Use Default Server Parameters? y 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   H.323 Link Bounce Recovery? y   Idle Traffic Interval (sec): 20   Keep-Alive Interval (sec): 5   Keep-Alive Count: 5   RSVP Enabled? n </pre>

Step	Description
4.	<p><b>IP Network Region 1 – Continued</b></p> <p>On <b>Page 3</b>, codec sets are defined for inter-region calls. For compliance testing at Site A, calls from IP network <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 B, only one IP network region exists so no inter-region settings were required.</p> <pre> 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></p> <p>At Site A, 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> display ip-network-region 2                                     Page 1 of 19  Region: 2 Location:      Authoritative Domain: avaya.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></p> <p>The inter-region codec setting was created similarly to <b>Step 4</b>.</p> <pre> 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></p> <p>Use the <b>change ip-codec-set</b> command to verify that G.711MU or G.711A is contained in the codec list. The example below shows the value used for 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>
8.	<p><b>Fax</b></p> <p>On <b>Page 2</b>, set the <b>FAX Mode</b> field to <b>t.38-standard</b>. 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 0. 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 the IETF RFC-2198 and ITU-T T.38 specifications as a 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> display ip-codec-set 1                                     Page 2 of 2                                  IP Codec Set                                  Allow Direct-IP Multimedia? n                                  Mode      Redundancy                                 FAX      t.38-standard      0                                 Modem     off                0                                 TDD/TTY   US                3                                 Clear-channel n              0 </pre>

Step	Description
9.	<p><b>Signaling Group for Fax Calls</b></p> <p>For compliance testing, the signaling group shown below and the associated SIP trunk (administered in <b>Steps 10-11</b>) are used for routing fax calls to and from the FACSys Fax Messaging Suite fax server via Session Manager. Signaling group 12 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>tls</i>. As a result, the <b>Near-end Listen Port</b> and <b>Far-end Listen Port</b> are automatically set to <b>5061</b>.</li> <li>▪ The <b>Near-end Node Name</b> was set to <b>CLAN2A</b>, the node name that maps to the IP address of the CLAN circuit pack used to connect to Session Manager. 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 <b>SM1</b>. This node name maps to the IP address of the Session Manager 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 CLAN circuit pack for connectivity to the FACSys Fax Messaging Suite fax server via Session Manager.</li> <li>▪ The <b>Far-end Domain</b> was set to the IP address assigned to FACSys Fax Messaging Suite fax server. 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 <b>y</b>. This field must be set to <b>y</b> 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 data-bbox="316 1060 1401 1623"> <pre> display signaling-group 12                                 SIGNALING GROUP  Group Number: 12                Group Type: sip                                 Transport Method: tls IMS Enabled? n  Near-end Node Name: CLAN2A      Far-end Node Name: SM1 Near-end Listen Port: 5061      Far-end Listen Port: 5061 Far-end Network Region: 2 Far-end Domain: 192.45.108.200  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                                 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 compliance testing, trunk group 12 was used for the SIP trunk group for routing fax calls to and from the FACSys Fax Messaging Suite fax server via Session Manager. Trunk group 12 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="316 840 1432 1184" style="border: 1px solid black; padding: 10px;"> <pre> display trunk-group 12                                     Page 1 of 21                                      TRUNK GROUP Group Number: 12                Group Type: sip           CDR Reports: y   Group Name: PN2 to SM          COR: 1                   TN: 1       TAC: *012     Direction: two-way          Outgoing Display? n     Dial Access? n     Queue Length: 0     Service Type: tie           Auth Code? n                                      Signaling Group: 12                                      Number of Members: 50 </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 1480 1416 1827" style="border: 1px solid black; padding: 10px;"> <pre> display trunk-group 12                                     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></p> <p>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 group 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> display public-unknown-numbering 0 NUMBERING - PUBLIC/UNKNOWN FORMAT Page 1 of 1  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></p> <p>Use the <b>change route-pattern</b> command to create a route pattern that will route fax calls to the SIP trunk that connects Communication Manager to Session Manager.</p> <p>The example below shows the route pattern used during compliance testing at Site A. 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> display route-pattern 12 Pattern Number: 12 Pattern Name: To SM SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No      Mrk Lmt List Del Digits  QSIG 1: 12 0 2: 3: 4: 5: 6: Intw 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 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 </pre>

Step	Description																																																																																																																																									
14.	<p><b>Routing Calls to Session Manager</b></p> <p>Automatic Alternate Routing (AAR) was used to route calls to Session Manager. Two places need to be changed to support this routing. 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 A using the <b>display dialplan analysis</b> command. The 4th entry specifies that numbers that begin with 6 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 A using the <b>display aar analysis 0</b> command. The 5th entry specifies that numbers that begin with 6 and are 5 digits long use route pattern 12. Route pattern 12 routes calls to Session Manager at Site A.</p> <div><pre>display dialplan analysis</pre><div><div></div><div>Page1 of 12</div></div><div>DIAL PLAN ANALYSIS TABLE</div><div>Location:allPercent Full:1</div><table><tr><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th></tr><tr><td>0</td><td>3</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>2</td><td>5</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>5</td><td>5</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>6</td><td>5</td><td>aar</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>7</td><td>5</td><td>aar</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>8</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>9</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>*</td><td>4</td><td>dac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></div> <div><pre>display aar analysis 0</pre><div><div></div><div>Page1 of 2</div></div><div>AAR DIGIT ANALYSIS TABLE</div><div>Location:allPercent Full:1</div><table><tr><th>Dialed String</th><th>Total Min</th><th>Total Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr><tr><td>2</td><td>7</td><td>7</td><td>999</td><td>aar</td><td></td><td>n</td></tr><tr><td>3</td><td>7</td><td>7</td><td>999</td><td>aar</td><td></td><td>n</td></tr><tr><td>4</td><td>7</td><td>7</td><td>999</td><td>aar</td><td></td><td>n</td></tr><tr><td>5</td><td>5</td><td>5</td><td>4</td><td>aar</td><td></td><td>n</td></tr><tr><td>6</td><td>5</td><td>5</td><td>12</td><td>aar</td><td></td><td>n</td></tr><tr><td>7</td><td>5</td><td>5</td><td>4</td><td>aar</td><td></td><td>n</td></tr><tr><td>~</td><td>-</td><td>-</td><td>---</td><td></td><td></td><td></td></tr></table></div>	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	0	3	fac							2	5	ext							5	5	ext							6	5	aar							7	5	aar							8	1	fac							9	1	fac							*	4	dac							Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	2	7	7	999	aar		n	3	7	7	999	aar		n	4	7	7	999	aar		n	5	5	5	4	aar		n	6	5	5	12	aar		n	7	5	5	4	aar		n	~	-	-	---			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type																																																																																																																																		
0	3	fac																																																																																																																																								
2	5	ext																																																																																																																																								
5	5	ext																																																																																																																																								
6	5	aar																																																																																																																																								
7	5	aar																																																																																																																																								
8	1	fac																																																																																																																																								
9	1	fac																																																																																																																																								
*	4	dac																																																																																																																																								
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd																																																																																																																																				
2	7	7	999	aar		n																																																																																																																																				
3	7	7	999	aar		n																																																																																																																																				
4	7	7	999	aar		n																																																																																																																																				
5	5	5	4	aar		n																																																																																																																																				
6	5	5	12	aar		n																																																																																																																																				
7	5	5	4	aar		n																																																																																																																																				
~	-	-	---																																																																																																																																							

Step	Description
15.	<p><b>Routing Calls From Site A to Site B</b></p> <p>The AAR Digit Analysis Table in <b>Step 14</b> also shows that a 5-digit dialed number starting with 5 or 7 will use route pattern 4 by AAR. The previously created route pattern 4, as displayed below, specifies that a call from Site A to the fax machine (extension 50000) or the FACSys Fax Messaging Suite fax server (extension 75000) at Site B will be routed to trunk group 4 which is an administered ISDN-PRI trunk. In the same way, this trunk group number can be changed to a SIP trunk group number for fax calls from Site A to Site B to go over a SIP trunk.</p> <pre> display route-pattern 4 Pattern Number: 4    Pattern Name: to G450 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:  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      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 trunk between Site A and Site B. Note that the Far-end Node Name is CM-Remote. This trunk was set up between the two Communication Managers directly without going through Session Manager.</p> <div data-bbox="316 401 1401 976" style="border: 1px solid black; padding: 10px;"> <pre> 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-Remote Near-end Listen Port: 5060                Far-end Listen Port: 5060 Far-end Network Region: 1 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> </div>

## 5. Configure Session Manager

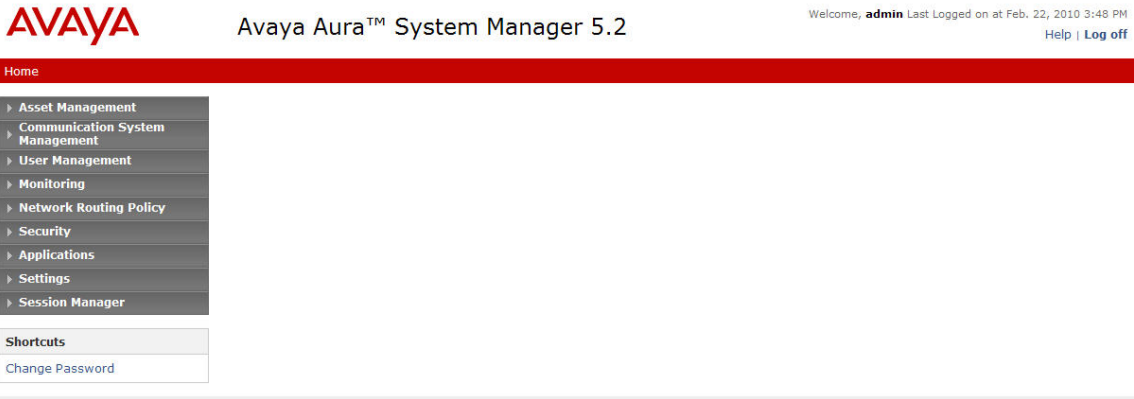
This section provides the procedures for configuring Session Manager. Session Manager must be administered via System Manager.

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

The procedures described in this section include configurations in the following areas:

- **SIP domain**
- Logical/physical **Locations** where SIP Entities may reside
- **SIP Entities** corresponding to the SIP telephony systems including Communication Manager, the FACSys Fax Messaging Suite fax servers, and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed
- **Session Manager** corresponding to the Session Manager Servers managed by System Manager

The documented procedures must be repeated for the Session Manager at Site B using values appropriate for Site B from **Figure 1**.

Step	Description
1.	<p><b>Log in</b></p> <p>Access the administration web interface by entering the URL “https://&lt;ip-address&gt;/SMGR”, where “&lt;ip-address&gt;” is the IP address of System Manager. Log in with the appropriate credentials. The page below will be displayed.</p>  <p>Expand the <b>Network Routing Policy</b> link on the left side as shown in <b>Step 2</b>. The sub-menus displayed in the left column will be used to configure the items in Steps 2-7.</p>

## 2. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

- **Name:** Enter the domain name specified to be the **Authoritative Domain** on the **IP Network Region** form on Communication Manager (see **Section 4, Step 5**)
- **Notes:** Descriptive text (optional)

Click **Commit**.

The screenshot shows the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status bar indicating 'Welcome, admin' and 'Last Logged on at Feb. 18, 2010 11:33 AM'. Below the navigation bar, a red breadcrumb trail reads 'Home / Network Routing Policy / SIP Domains'. On the left, a sidebar menu lists various management categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under 'Network Routing Policy', sub-items include Adaptations, Dial Patterns, Entity Links, Locations, SIP Domains (highlighted in blue), SIP Entities, Time Ranges, and Personal Settings. The main content area is titled 'Domain Management' and contains a table with columns for Name, Type, Default, and Notes. A single row is visible with the name 'avaya.com', type 'sip', and a default checkbox. Below the table, a red asterisk indicates 'Input Required'. 'Commit' and 'Cancel' buttons are present at the top right and bottom right of the form area.

## 3. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of routing and bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)

The remaining fields under *General* can be filled in to specify bandwidth management parameters between Session Manager and this location. The default values were used for compliance testing.

Next, Fill in the following:

Under *Location Pattern*:

- **IP Address Pattern:** An IP address pattern used to logically identify the location
- **Notes:** Descriptive text (optional)

The screen below shows addition of the “192.45.108.0/24” Location which includes the Communication Manager and the FACSys Fax Messaging Suite fax server at Site A. Note that a second Location, “10.64.x.x/24”, was created for Site B (not shown). Since a single Session Manager was shared between Sites A and B during compliance testing, one of the Locations had to be chosen for the logical location of Session Manager. In the compliance tested configuration, Site B was chosen for the logical location.

Click **Commit** to save the Location definition.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM Help | Log off

Home / Network Routing Policy / Locations / Location Details

**Location Details** Commit Cancel

**General**

\* Name: 192.45.108.0/24

Notes:

Managed Bandwidth:

\* Average Bandwidth per Call: 80 Kbit/sec

\* Time to Live (secs): 3600

**Location Pattern**

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
* 192.45.108.*	

Select : All, None ( 0 of 1 Selected )

\* Input Required Commit Cancel

#### 4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the compliance test configuration, a SIP Entity was added for the Session Manager itself, the C-LAN board in the Avaya G650 Media Gateway (Port Network 2), and the FACSys Fax Messaging Suite fax server.

Select **SIP Entities** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Name** A descriptive name
- **FQDN or IP Address:** FQDN or IP address of the signaling interface for the entity
- **Type:** “Session Manager” for Session Manager, “CM” for Communication Manager, or “Other” for the fax server
- **Adaptation:** Leave blank
- **Location:** Select the appropriate Location configured in previous step
- **Time Zone:** Select the proper time zone for this installation

When adding a SIP Entity for Session Manager, Under *Port*, click **Add**, then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests
- **Protocol:** Transport protocol to be used to send SIP requests
- **Default Domain:** Select the SIP Domain configured in **Step 2** of this section

Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

The following screen shows the addition of Session Manager. Two **Port** entries are added. TLS (well-known port 5061) is used for communication with Communication Manager. UDP (well-known port 5060) is used for communication with the FACSys Fax Messaging Suite fax server.

Note: since a single Session Manager was shared between Sites A and B during compliance testing, one of the two configured Locations had to be chosen for the logical location of Session Manager. In this case, the “10.64.x.x/24” **Location** for Site B was chosen. The administration for Site B is not shown in this document.

Also note that the entries under *Entity Links* are populated automatically after the Entity Links are administered (**Step 5** below).

Avaya Aura™ System Manager 5.2
Welcome, **admin** Last Logged on at Mar. 18, 2010 9:29 AM
[Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

Asset Management
Communication System Management
User Management
Monitoring
**Network Routing Policy**
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
**SIP Entities**
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager

Shortcuts
Change Password
Help for SIP Entity Details fields
Help for Committing configuration changes

**SIP Entity Details**
Commit Cancel

General

Name: SM1
FQDN or IP Address: 10.64.40.42
Type: Session Manager
Notes:
Location: 10.64.x.x/24
Outbound Proxy:
Time Zone: America/Denver
Credential name:

SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration

Entity Links
Add Remove

7 Items Refresh							Filter: Enable
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	
<input type="checkbox"/>	SM1	TLS	* 5061	MainCM_PN2	* 5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	UDP	* 5060	MainWin2003Srvr	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TLS	* 5061	RemoteCM	* 5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	UDP	* 5060	RemoteWin2003Srvr	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TLS	* 5061	S8300-G430-FS-Sample	* 5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TLS	* 5061	S8300G450	* 5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TLS	* 5061	S8720G650	* 5061	<input checked="" type="checkbox"/>	

Select : All, None ( 0 of 7 Selected )

Port
Add Remove

3 Items Refresh					Filter: Enable
<input type="checkbox"/>	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		

Select : All, None ( 0 of 3 Selected )

\* Input Required
Commit Cancel

The following screen shows the results of adding Communication Manager. In this case, the **FQDN or IP Address** is the IP address of the C-LAN board in the Avaya G650 Media Gateway, Port Network 2. Note the “CM” selection for **Type**.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM  
[Help](#) | [Log off](#)

[Home](#) / [Network Routing Policy](#) / [SIP Entities](#) / [SIP Entity Details](#)

**SIP Entity Details** Commit Cancel

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording:

**SIP Link Monitoring**

SIP Link Monitoring:

\* Proactive Monitoring Interval (in seconds):

\* Reactive Monitoring Interval (in seconds):

\* Number of Retries:



The following screen shows the results of adding the FACSys Fax Messaging Suite fax server. In this case, **FQDN or IP Address** is the IP address assigned to the fax server. Note the “Other” selection for **Type**.

## 5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the compliance tested configuration, 2 Entity Links were configured; one for Session Manager to Communication Manager and one for Session Manager to the FACSys Fax Messaging Suite fax server.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. For the link to Communication Manager, fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager SIP Entity configured in previous Step
- **Protocol:** Select “TLS”
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the Communication Manager SIP Entity configured in previous section
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box

Click **Commit** to save the configuration.

The screen below shows the first **Entity Link** configured between Session Manager and Communication Manager.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM  
[Help](#) | [Log off](#)

Home / Network Routing Policy / Entity Links

Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager

Entity Links

Commit

Cancel

1 Item Refresh								Filter: Enable
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes	
* SM1_MainCM_PN2_T	* SM1	TLS	* 5061	* MainCM_PN2	* 5061	<input checked="" type="checkbox"/>		

\* Input Required

Commit

Cancel

The second **Entity Link** between Session Manager and the FACSys Fax Messaging Suite fax server is similarly configured. The screen below shows the configured Entity Link. Select “UDP” for the **Protocol**, 5060 for each **Port**, and the FACSys Fax Messaging Suite fax server SIP Entity for **SIP Entity 2**.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM  
[Help](#) | [Log off](#)

Home / Network Routing Policy / Entity Links

Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager

Entity Links

Commit

Cancel

1 Item Refresh								Filter: Enable
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes	
* SM1_MainWin2003Sr	* SM1	UDP	* 5060	* MainWin2003Srvr	* 5060	<input checked="" type="checkbox"/>		

\* Input Required

Commit

Cancel

## 6. Add Routing Policy

A routing policy should be created for each “Routing Destination”. A routing policy must be added for routing calls to Communication Manager (from the fax server). Likewise, a routing policy must be added for routing calls to the fax server (from Communication Manager).

To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name** and optional text in **Notes**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies.

Under *Time of Day*:

Click **Add**, and select the default “24/7” time range.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy used for routing fax calls from the fax server to Communication Manager.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The top header shows the Avaya logo, the system name "Avaya Aura™ System Manager 5.2", and a welcome message for user "admin" last logged on at Feb. 18, 2010 11:33 AM. The breadcrumb trail indicates the current location: Home / Network Routing Policy / Routing Policies / Routing Policy Details. The left sidebar contains a tree view of system management options, with "Network Routing Policy" expanded and "Routing Policies" selected. The main content area is titled "Routing Policy Details" and includes "Commit" and "Cancel" buttons. It is divided into three sections: "General" with fields for Name (To\_MainCM\_PN2), Disabled (unchecked), and Notes; "SIP Entity as Destination" with a "Select" button and a table listing available entities (MainCM\_PN2, 192.45.108.57, CM); and "Time of Day" with "Add", "Remove", and "View Gaps/Overlaps" buttons. Below these is a table showing the selected time range "24/7" with checkboxes for each day of the week (all checked) and the time range "00:00" to "23:59".

Name	FQDN or IP Address	Type	Notes
MainCM_PN2	192.45.108.57	CM	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

The following screen shows the Routing Policy used for routing fax calls from Communication Manager to the fax server.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left sidebar shows a navigation menu with categories like Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, and Settings. The 'Network Routing Policy' section is expanded, showing sub-items like Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges, and Personal Settings. The 'Routing Policies' item is selected.

The main content area is titled 'Routing Policy Details' and includes a 'General' tab. The 'General' tab shows the following fields:

- Name:** To\_MainWin2003Srvr
- Disabled:** ☐
- Notes:** (empty text box)

Below the 'General' tab is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
MainWin2003Srvr	192.45.108.200	Other	

Below the 'SIP Entity as Destination' section is the 'Time of Day' section, which includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It also shows a table with the following data:

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

## 7. Add Dial Patterns

A Dial Pattern is associated with a Routing Policy to direct calls to a destination based on dialed digits.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **SIP Domain:** SIP domain specified in **Step 2** of this section.
- **Notes:** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate Location (or “ALL”) for **Originating Location Name** field and select the appropriate Routing Policy from the list.

Defaults can be used for the remaining fields. Click **Commit** to save the Dial Pattern.

The second entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to the FACSys Fax Messaging Suite fax server. Any call made from Location “192.45.108.0/24” to a 5 digit number starting with “65” will be routed to the fax server.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM  
[Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Asset Management
Communication System Management
User Management
Monitoring
**Network Routing Policy**
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager

Shortcuts
Change Password
Help for Dial Pattern Details fields
Help for Location and Routing Policy Lists
Help for Denied Location fields
Help for Committing configuration changes

Dial Pattern Details
Commit Cancel

General

\* Pattern:

65

\* Min:

5

\* Max:

5

Emergency Call:

☐

SIP Domain:

avaya.com

Notes:

Originating Locations and Routing Policies
Add Remove
2 Items Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	10.64.x.x/24		To_RemoteCM	0	<input type="checkbox"/>	RemoteCM	
<input type="checkbox"/>	192.45.108.0/24		To_MainWin2003Srvr	0	<input type="checkbox"/>	MainWin2003Srvr	

Select : All, None ( 0 of 2 Selected )

Denied Originating Locations
Add Remove
0 Items Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

\* Input Required

Commit Cancel

The second entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to Communication Manager. Any call made from Location “192.45.108.0/24” to a 5 digit number starting with “2” will be routed to the Communication Manager. Similar Dial Patterns were added to route any calls to a 5 digit number starting with “5” or “75” to Communication Manager (not shown).

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 25, 2010 4:22 PM  
Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove 2 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	10.64.x.x/24		To RemoteCM	0	<input type="checkbox"/>	RemoteCM	
<input type="checkbox"/>	192.45.108.0/24		To MainCM_PN2	0	<input type="checkbox"/>	MainCM_PN2	

Select : All, None ( 0 of 2 Selected )

**Denied Originating Locations**

Add Remove 0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>		

\* Input Required Commit Cancel

## 8. Add Session Manager

Adding the Session Manager provides the linkage between System Manager and Session Manager. This configuration procedure should have already been properly executed if the Session Manager used has been set up for other purposes. This configuration step is included here for reference and completeness. To add Session Manager, expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen (note that the screen below is for **Edit Session Manager** since it was already administered):

Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity created for Session Manager
- **Description:** Any descriptive text
- **Management Access**  
**Point Host Name/IP:** IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the proper network mask for Session Manager.
- **Default Gateway:** Enter the default gateway IP address for Session Manager

Accept default settings for the remaining fields.

**AVAYA** Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 18, 2010 11:33 AM  
[Help](#) [Log off](#)

Home / Session Manager / Session Manager Administration / Edit Session Manager

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System Tools

Shortcuts

Change Password

Help for Session Manager Administration

Help for Page Fields

**Edit Session Manager** [Commit](#) [Cancel](#)

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |  
[Expand All](#) | [Collapse All](#)

**General**

SIP Entity Name

Description

\*Management Access Point Host Name/IP

\*Direct Routing to Endpoints

**Security Module**

SIP Entity IP Address

\*Network Mask

\*Default Gateway

\*Call Control PHB

\*QOS Priority

\*Speed & Duplex

VLAN ID

**Monitoring**

Enable Monitoring ☒

\*Proactive cycle time (secs)

\*Reactive cycle time (secs)

\*Number of Retries

**CDR**

Enable CDR ☐

User

Password

Confirm Password

**Personal Profile Manager (PPM) - Connection Settings**

Limited PPM client connection ☒

\*Maximum Connection per PPM client

\*PPM Connection Timeout (mins)

PPM Packet Rate Limiting ☒

\*PPM Packet Rate Limiting Threshold

**Event Server**

Clear Subscription on Notification Failure

\*Required [Commit](#) [Cancel](#)




## 6. Configure emFAST FACSys Fax Messaging Suite

This section describes the configuration of FACSys Fax Messaging Suite. It assumes that the application and all required software components have been installed and properly licensed. The examples shown in this section refer to Site A. However, unless specified otherwise, these same steps also apply to site B using values appropriate for site B from **Figure 1**.

The configuration of the FACSys Fax Message Suite includes the following steps:

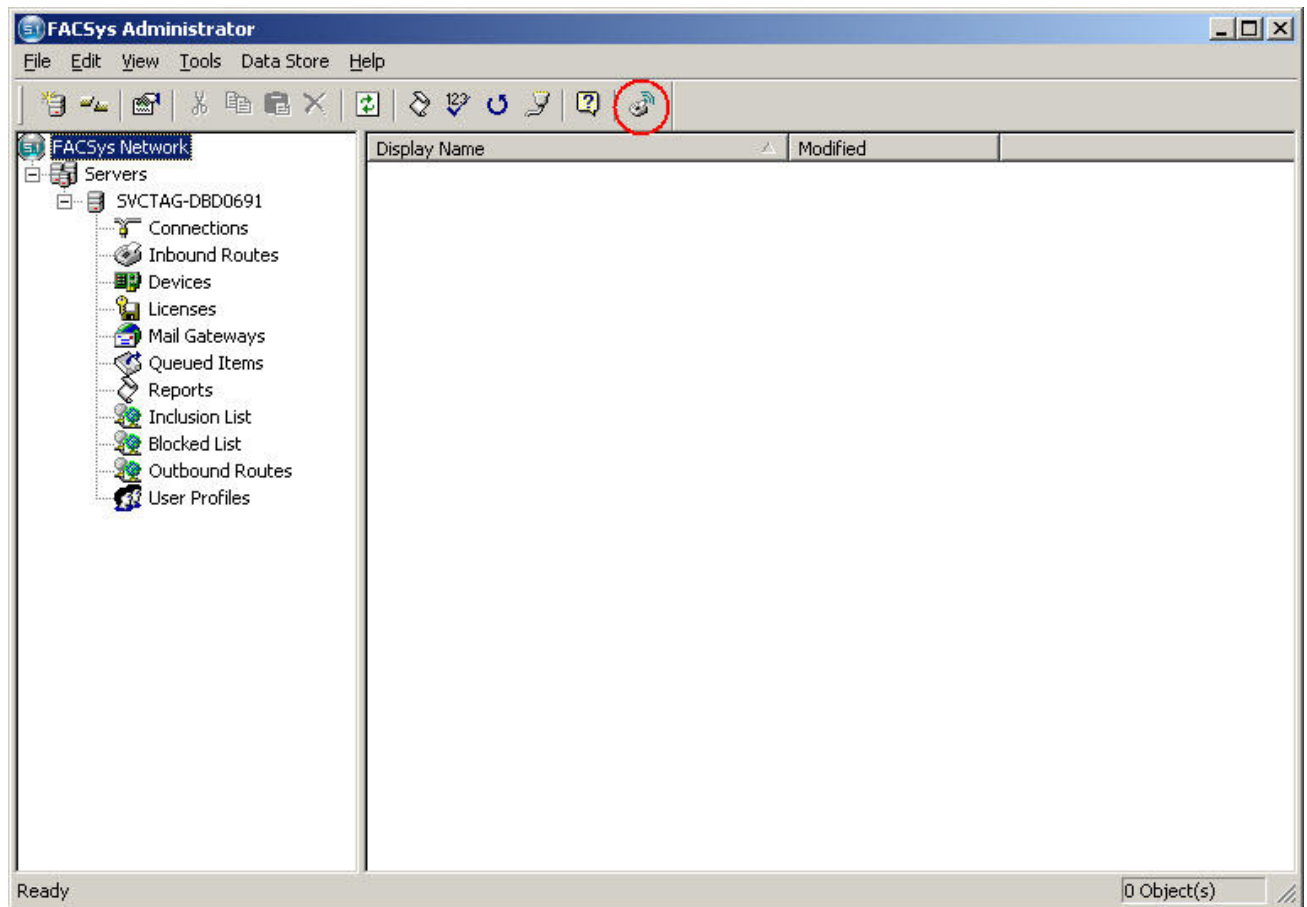
- Launch FACSys Administrator
- Administer IP address
- Administer devices
- Administer user profiles
- Reboot server

Step	Description
1.	<p><b>Launch FACSys Administrator</b></p> <p>From the FACSys Messaging Suite fax server, double-click on the <b>FACSys Administrator</b> icon shown below, which is created as part of installation.</p> 

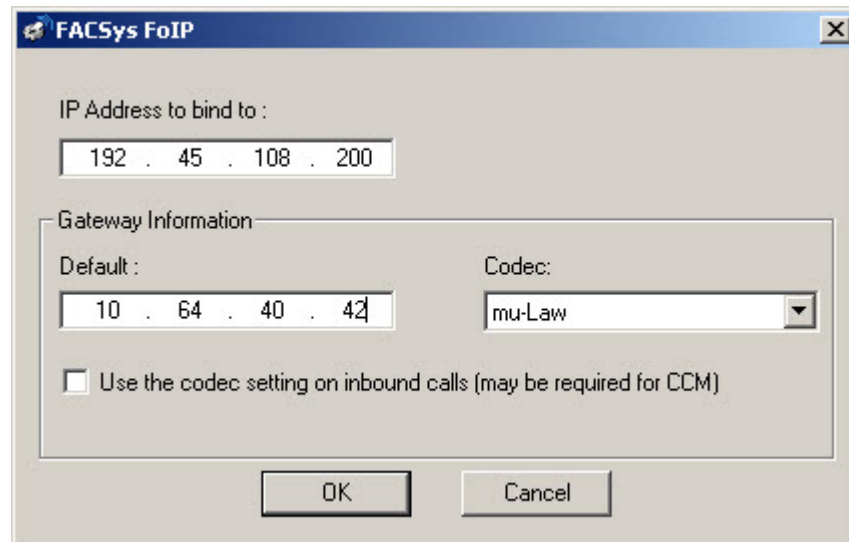


2. **Administer IP Address of Session Manager**

The **FACSys Administrator** screen is displayed. Click on the **Configure FACSys FoIP** icon, as shown below.



The **FACSys FoIP** screen is displayed. In the **Gateway Information Default** field, enter the IP address of Session Manager. Retain the default values in the remaining fields, and click **OK**.



The image shows the FACSys FoIP configuration window. It has a title bar with the text 'FACSys FoIP' and a close button. Inside the window, there is a label 'IP Address to bind to :' followed by a text box containing '192 . 45 . 108 . 200'. Below this is a section titled 'Gateway Information' which contains two text boxes: 'Default :' with '10 . 64 . 40 . 42' and 'Codec:' with a dropdown menu showing 'mu-Law'. There is also a checkbox labeled 'Use the codec setting on inbound calls (may be required for CCM)' which is currently unchecked. At the bottom of the window are 'OK' and 'Cancel' buttons.

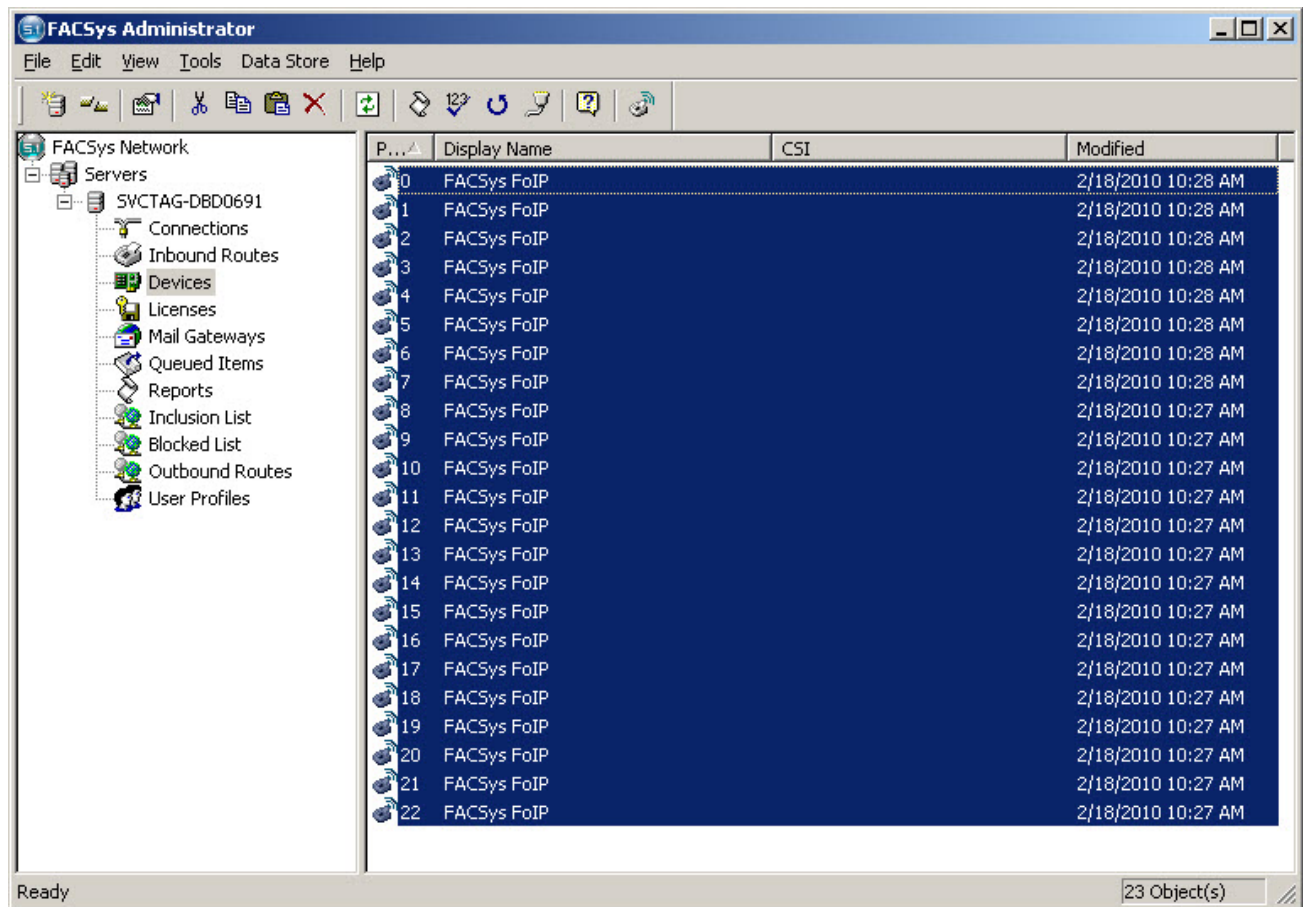
The **FACSys Administrator** dialog box is displayed next. Click **Yes** to restart the server.



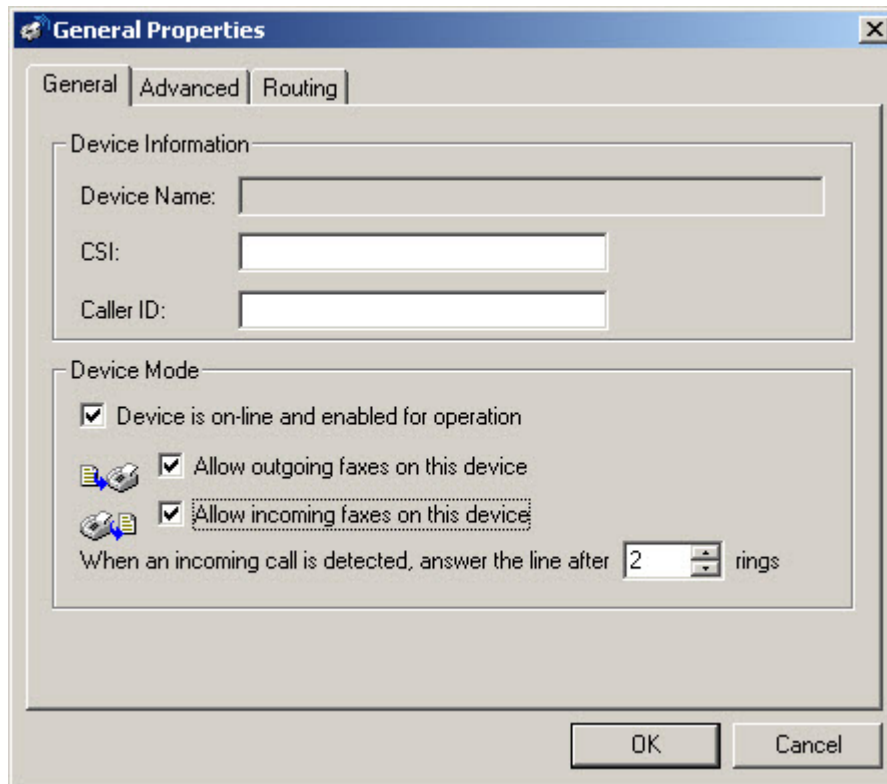
The image shows the FACSys Administrator dialog box. It has a title bar with the text 'FACSys Administrator' and a close button. Inside the window, there is a question mark icon followed by the text: 'Changes have been made to your hardware device configuration which requires that your fax service be restarted. Would you like to restart your fax server now?'. At the bottom of the window are 'Yes' and 'No' buttons.

### 3. Administer Devices

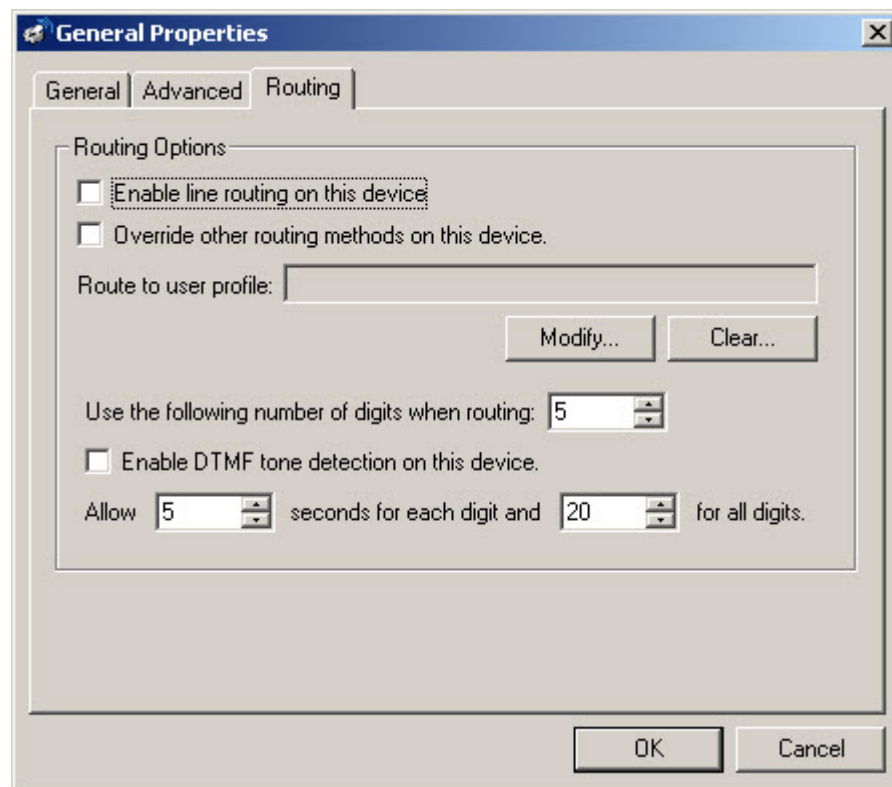
After the server has been restarted, re-launch the FACSys Administrator. In the **FacSys Administrator** screen, select **Devices** from the left pane to display a list of fax ports. Select all fax port entries as shown below, right-click, and select **Properties**.



The **General Properties** screen is displayed. Under the **General** tab, verify that the **Device is on-line and enabled for operation** check box is checked. For compliance testing, each device was enabled for incoming and outgoing faxes via the **Allow outgoing faxes on this device** and **Allow incoming faxes on this device** check-boxes.

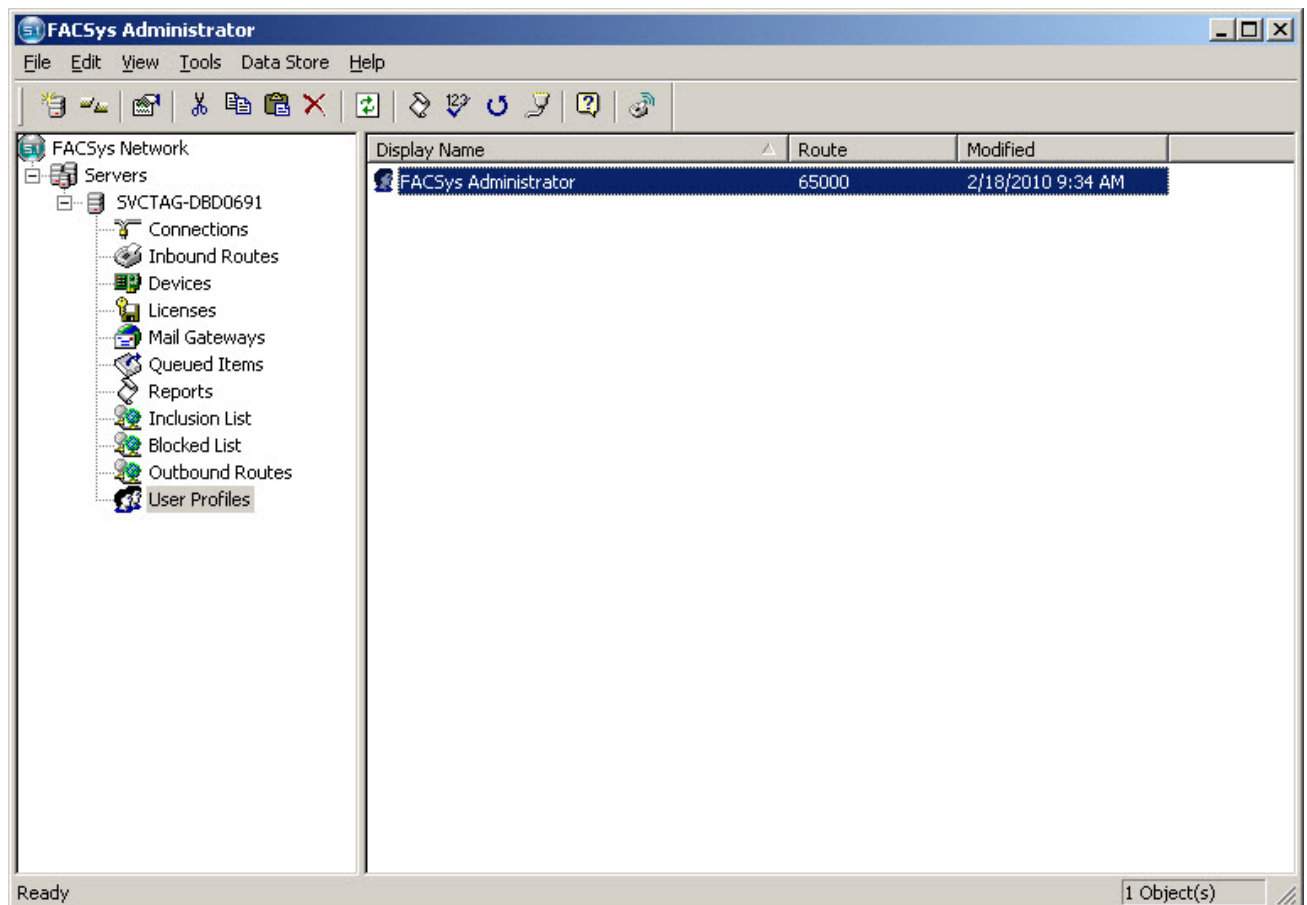


Under the **Routing** tab, set the **Use the following number of digits when routing** field to the proper number of digits used for fax numbers, in this case “5”. Click **OK**.



4. **Administer User Profiles**

From the **FACSys Administrator** screen, select **User Profiles** from the left pane to display a list of users. To add a new user, right-click on **User Profiles** in the left pane, and select **New User Profile** from the pop-up list. To edit an existing user, double-click on the user in the right pane. In this case, the user FACSys Administrator was double-clicked.



The **FACSys Administrator Properties** screen is displayed. In the **Routing** field, enter the fax number shown in **Figure 1** for site A, in this case “65000”. Click **OK**.

The screenshot shows the 'FACSys Administrator Properties' dialog box with the 'Routing' tab selected. The 'User Information' section contains the following fields: 'First Name' (empty), 'Last' (empty), 'Display As' (FACSys Administrator), 'Alias' (Admin), 'Password' (masked with 'xxxx'), 'Department' (empty), and 'Manager' (empty). There are 'Modify...' and 'Clear...' buttons next to the 'Manager' field. Below these fields is a checked checkbox labeled 'Enable inbound routing services for this user account.' and a 'Routing' field containing the value '65000'. At the bottom right are 'OK' and 'Cancel' buttons.

5. **Reboot fax server**

Manually reboot the FACSys Messaging Suite server.

## 7. General Test Approach and Test Results

This section describes the testing used to verify the interoperability of emFAST FACSys Fax Messaging Suite with the Avaya SIP infrastructure (Communication Manager and Session Manager). 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 the FACSys Fax Messaging Suite fax server. In the compliance test configuration, one site served as the main enterprise site and a second site served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using a SIP trunk or an ISDN-PRI trunk between the two sites. By using two Communication Managers and two port networks with one of the Communication Managers, fax calls across multiple TDM/IP hops were tested. Faxes were sent with various page lengths, resolutions, and at various fax data speeds. Serviceability testing included verifying proper operation/recovery from cable connection failures, unavailable resources, and Communication Manager and FACSys Fax Messaging Suite fax server 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 G450 Media Gateway.

### 7.2. Test Results

FACSys Fax Messaging Suite successfully passed compliance testing. The following observations were made during the compliance test:

- All the fax calls were established successfully with or without shuffling enabled. However, for inter-site calls that had shuffling enabled and a SIP trunk was 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.

## 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 group configured in **Step 9 of Section 4** is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Steps 10 - 11 of Section 4** is in-service.
- Verify that fax calls can be placed to/from the FACSys Fax Messaging Suite server to/from a fax machine at each site.
- From the Avaya Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed over 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 emFAST FACSys Fax Messaging Suite to interoperate with Avaya SIP infrastructure (Communication Manager and Session Manager). The emFAST FACSys Fax Messaging Suite successfully passed compliance testing with the observations documented in **Section 7.2**.

## 10. Additional References

- [1] *Feature Description and Implementation for Avaya Communication Manager*, Document 555-245-205, Issue 7, Release 5.2, May 2009.
- [2] *Administrator Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009.
- [3] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Document 555-245-206, Issue 9, May 2009.
- [4] *Installing Avaya Aura™ Session Manager*, Document 03-603437, Issue 1.3, Release 5.2, January 2010.
- [5] *Administering Avaya Aura™ Session Manager*, Document 03-603324, Issue 2, Release 5.2, November 2009.
- [6] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Document 03-603325, Issue 1.3, Release 5.2, January 2010.

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

*FACSys 5.1 Enterprise Administrator Program Manual*, available on the FACSys installation CD.

---

**©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).