



## **Application Notes for Configuring SIP Trunks among Ingate SIParator, Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.1**

### **Abstract**

These Application Notes describe a sample configuration for a network that uses Avaya Aura® Session Manager to connect Ingate SIParator and Avaya Aura® Communication Manager using SIP trunks.

The Ingate SIParator is a SIP Session Border Controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted IP network. The compliance testing focused on telephony scenarios between an enterprise site, where the Ingate SIParator, Session Manager, and Communication Manager were located, and a second site.

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 a sample configuration for a network that uses Avaya Aura® Session Manager to connect Ingate SIParator and Avaya Aura® Communication Manager using SIP trunks.

The compliance testing focused on telephony scenarios between an enterprise site, where the Ingate SIParator, Session Manager, and Communication Manager were located, and a second site.

## 2. General Test Approach and Test Results

The general test approach was to make calls between the main enterprise site and a second site using various codec settings and exercising common PBX features.

### 2.1. Interoperability Compliance Testing

The compliance testing focused on interoperability between Ingate SIParator and Session Manager / Communication Manager by making calls between the enterprise site and a second site simulating a service provide service node that were connected through the SIParator using direct SIP trunks. The following functions and features were tested:

- Calls from both SIP and non-SIP endpoints between sites
- G.711u and G.729A codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus
- Proper operation of voicemail with message waiting indicators (MWI)
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference
- Extended telephony features using Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Automatic Call Back, and Send All Calls.
- Proper system recovery after a SIParator restart and/or re-establishment of broken IP connectivity.

### 2.2. Test Results

The Ingate SIParator passed compliance testing. The following observations were made during testing:

- The caller-ID was incorrectly displayed at the endpoints for calls flowing through Ingate SIParator.
- If a call was placed to a SIP enterprise endpoint via Ingate SIParator while there was a SIParator outage (such as an Ethernet disconnect), the called failed as expected. However, after SIParator recovered from the outage, all calls to the same SIP endpoint continued to fail. The endpoint needed to be restarted in order to successfully terminate calls to the same endpoint again.

## 2.3. Support

Technical support for Ingate SIParator can be obtained by contacting Ingate at

- EMEA Phone: +46-13-21 08 52
- NA Phone: +1-866-809-0002
- Email: [support@ingate.com](mailto:support@ingate.com)
- Web: <http://www.ingate.com>

## 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows two sites connected via a SIP trunk across an untrusted IP network: the main enterprise site and a second site. The Ingate SIParator Session Border Controller (SBC) is at the edge of the main site. The public side of the SIParator is connected to the untrusted network and the private side is connected to the trusted corporate LAN.

All SIP traffic between two sites flows through the SIParator. In this manner, the SIParator can protect the main site's infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over TCP and RTP for the media streams.

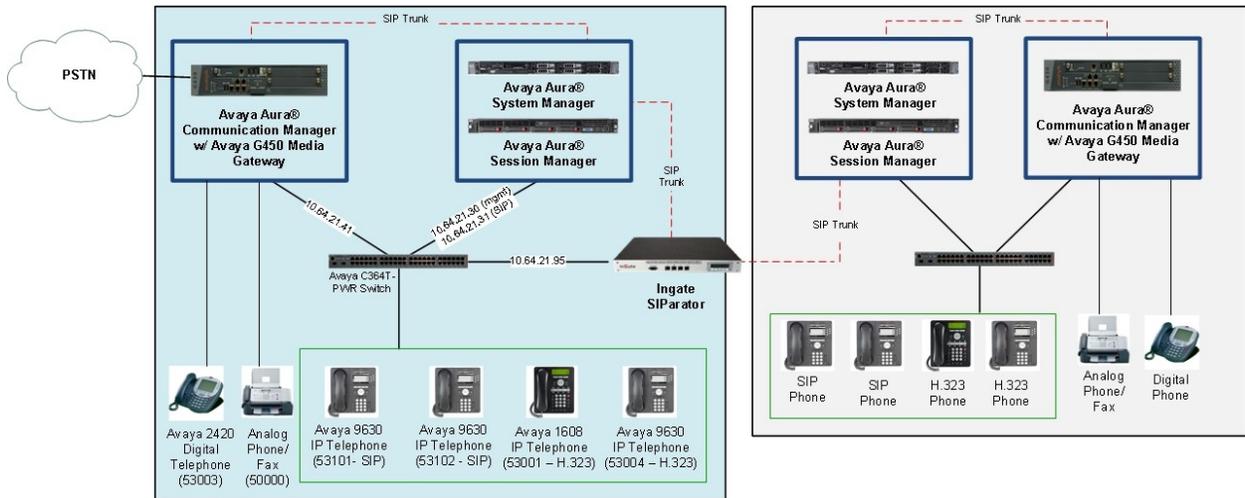
Also connected to the LAN at the main site are:

- An Avaya S8300D Server running Avaya Aura® Communication Manager in an Avaya G450 Media Gateway. Avaya Aura® Communication Manager Messaging is also running on the Avaya S8300D Server to provide voice mail functionality.
- A Dell™ PowerEdge™ R610 Server running Avaya Aura® System Manager. System Manager provides management functions for Session Manager.
- An HP ProLiant DL360 G7 Server running Avaya Aura® Session Manager that provides SIP registrar and proxy server functions for SIP endpoints in the enterprise IP telephony network.

The Session Manager connects the SIParator and Communication Manager using SIP trunks. Endpoints include both SIP and non-SIP endpoints. An ISDN-PRI trunk connects the media gateway to the PSTN.

The 2<sup>nd</sup> site also comprises of a Communication Manager, System Manager, and Session Manager, with both SIP and non-SIP endpoints.

The SIP endpoints located at both sites are registered to the local Session Manager. Each site has a separate SIP domain: *avaya.com* for the main site and *devconnect.com* for the 2<sup>nd</sup> site.



**Figure 1: SIP Parator SIP Trunking Test Configuration**

## 4. Equipment and Software Validated

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

Equipment	Software
Avaya S8300D Server with a Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1, R016x.00.1.510.1, Patch 18621 (Avaya Aura® System Platform: 6.0.2.1.5)
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager: 6.1.0 (Build No. – 6.1.0.4.5072-6.1.4.11) (Avaya Aura® System Platform: 6.0.2.1.5)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1.0 (Build No. – 6.1.0.0.42003-6.1.0.610012)
Avaya 9600 Series IP Telephones <ul style="list-style-type: none"><li>• H.323</li><li>• SIP</li></ul>	3.1. Service Pack 1 2.6.4
Fax Machine	-
Ingate SIParator with installed modules: <ul style="list-style-type: none"><li>• Standard SIP features</li><li>• SIP Trunking</li><li>• Remote SIP Connectivity (NAT Traversal)</li><li>• Failover</li><li>• VPN (IPsec and PPTP)</li></ul>	4.9.1

## 5. Configure Communication Manager

This section describes the Communication Manager configuration at the main enterprise site to support the network shown in **Figure 1**. It assumes station administration (for both SIP and non-SIP endpoints) and the procedures necessary to support SIP and connectivity to Session Manager have been performed as described in [2] and [3].

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

Step	Description
1.	<p><b>IP network region</b>  All equipment at the main site were located in a single IP network region (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>▪ <b>Authoritative Domain: <i>avaya.com</i></b>  This field was configured to match the domain name configured on Session Manager. The domain will appear in the “From” header of SIP messages originating from this IP region.</li> <li>▪ <b>Name:</b> Any descriptive name may be used (if desired).</li> <li>▪ <b>Intra-region IP-IP Direct Audio: <i>yes</i></b>  <b>Inter-region IP-IP Direct Audio: <i>yes</i></b>  By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the <b>Signaling Group</b> form.</li> <li>▪ <b>Codec Set: <i>1</i></b>  The codec set contains the list of codecs available for calls within this IP network region.</li> </ul>
	<pre> display ip-network-region 1                                     Page 1 of 20                                 IP NETWORK REGION Region: 1 Location:                               Authoritative Domain: avaya.com Name: 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 Call Control PHB Value: 46 Audio PHB Value: 46 Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5                               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
2.	<p><b>Codecs</b>  IP codec set 1 was used during compliance testing. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing. It should be noted that when testing the use of each individual codec, only the single codec under test was included in the list.</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: <b>G.711MU</b>      n            2           20 2: <b>G.729AB</b>      n            2           20 3: 4: 5: 6: 7: </pre>

Step	Description
3.	<p data-bbox="313 235 1414 378"><b>Node Names</b> Use the <b>change node-names ip</b> command to create a node name for the IP address of Session Manager. Enter a descriptive name in the <b>Name</b> column and the IP address assigned to Session Manager in the <b>IP address</b> column.</p> <pre data-bbox="313 420 1323 661"> change node-names ip                                     Page 1 of 2                                      IP NODE NAMES Name                                IP Address CM_20_40                            10.64.20.40 SM_20_31                            10.64.20.31 <b>SM_21_31</b>                          <b>10.64.21.31</b> default                             0.0.0.0 msgserver                           10.64.21.41 procr                                10.64.21.41 procr6                              :: </pre>

Step	Description
4.	<p><b>Signaling Group</b>            Signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. Signaling group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> <li>▪ <b>Near-end Node Name: <i>procr</i></b> This node name maps to the IP address of the Avaya S8300D Server. Node names are defined using the <b>change node-names ip</b> command.</li> <li>▪ <b>Far-end Node Name: <i>SM_21_31</i></b> This node name maps to the IP address of Session Manager.</li> <li>▪ <b>Far-end Network Region: <i>1</i></b> This defines the IP network region which contains Session Manager.</li> <li>▪ <b>Far-end Domain: <i>avaya.com</i></b> This domain is sent in the “To” header of SIP messages of calls using this signaling group.</li> <li>▪ <b>Direct IP-IP Audio Connections: <i>y</i></b> This field must be set to <i>y</i> to enable media shuffling on the SIP trunk.</li> </ul> <pre> display signaling-group 1                                 SIGNALING GROUP  Group Number: 1                Group Type: sip IMS Enabled? n                Transport Method: tls     Q-SIP? n                                SIP Enabled LSP? n     IP Video? n                    Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM      <b>Near-end Node Name: procr</b>                <b>Far-end Node Name: SM_21_31</b> <b>Near-end Listen Port: 5061</b>                <b>Far-end Listen Port: 5061</b>                                 <b>Far-end Network Region: 1</b>  <b>Far-end Domain: avaya.com</b>  Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload                Bypass If IP Threshold Exceeded? n                                 RFC 3389 Comfort Noise? n <b>Direct IP-IP Audio Connections? y</b> Session Establishment Timer(min): 3                IP Audio Hairpinning? n     Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n                Alternate Route Timer(sec): 6           </pre>

Step	Description
5.	<p><b>Trunk Group</b></p> <p>Trunk group 1 was used for the SIP trunk group between Communication Manager and Session Manager. Trunk group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> <li>▪ <b>Group Type: sip</b> This field sets the type of the trunk group.</li> <li>▪ <b>TAC: 101</b> Enter an valid value consistent with the Communication Manager dial plan</li> <li>▪ <b>Service Type: tie</b> Set to tie.</li> <li>▪ <b>Member Assignment Method: auto</b> Set to Auto.</li> <li>▪ <b>Signaling Group: 1</b> This field is set to the signaling group shown in the previous step.</li> <li>▪ <b>Number of Members: 10</b> This field represents the number of trunk group members in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.</li> </ul>
	<pre> display trunk-group 1                                     Page 1 of 21                                      TRUNK GROUP Group Number: 1                Group Type: sip          CDR Reports: y   Group Name: to SM_21_31      COR: 1              TN: 1          TAC: 101   Direction: two-way          Outgoing Display? n   Dial Access? n              Night Service:   Queue Length: 0   Service Type: tie           Auth Code? n                                      Member Assignment Method: auto                                      Signaling Group: 1                                      Number of Members: 10 </pre>

Step	Description
	<p><b>Trunk Group – continued</b>  <b>On Page 3:</b></p> <ul style="list-style-type: none"> <li>▪ The <b>Numbering Format</b> field was set to <i>unk-pvt</i>. This field specifies the format of the calling party number sent to the far-end.</li> <li>▪ The default values may be retained for the other fields.</li> </ul> <pre> display trunk-group 1                               Page 3 of 21 TRUNK FEATURES   ACA Assignment? n                               Measured: none   Maintenance Tests? y                                  <b>Numbering Format: unk-pvt</b>                                 UUI Treatment: service-provider                                 Replace Restricted Numbers? n                                 Replace Unavailable Numbers? n                                  Modify Tandem Calling Number: no  Show ANSWERED BY on Display? y </pre>
6.	<p><b>Private Numbering</b>  Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed across any trunk group will be sent as a 5 digit calling number. The calling party number is sent to the far-end in the SIP “From” header.</p> <pre> display private-numbering 0                           Page 1 of 2                                 NUMBERING - PRIVATE FORMAT  Ext Ext      Trk      Private      Total Len Code     Grp(s)    Prefix      Len  5  5                                 Total Administered: 1                                 Maximum Entries: 540 </pre>

Step	Description																																																																																																																																																								
7.	<p><b>Automatic Alternate Routing</b> Automatic Alternate Routing (AAR) was used to route calls to Session Manager. In the example shown, dialed numbers that begin with 3 and are 5 digits long use route pattern 1. Route pattern 1 routes calls to the trunk group defined in <b>Step 5</b>.</p> <pre>display aar analysis 3</pre> <p style="text-align: right;">Page 1 of 2</p> <p style="text-align: center;">AAR DIGIT ANALYSIS TABLE Location: all                      Percent Full: 1</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Dialed String</th> <th style="text-align: center;">Total Min</th> <th style="text-align: center;">Total Max</th> <th style="text-align: center;">Route Pattern</th> <th style="text-align: center;">Call Type</th> <th style="text-align: center;">Node Num</th> <th style="text-align: center;">ANI Reqd</th> </tr> </thead> <tbody> <tr> <td>3</td> <td style="text-align: center;">5</td> <td style="text-align: center;">5</td> <td style="text-align: center;">1</td> <td style="text-align: center;">aar</td> <td></td> <td style="text-align: center;">n</td> </tr> <tr> <td>4</td> <td></td> <td style="text-align: center;">7</td> <td style="text-align: center;">7</td> <td style="text-align: center;">999</td> <td style="text-align: center;">aar</td> <td style="text-align: center;">n</td> </tr> <tr> <td>531</td> <td style="text-align: center;">5</td> <td style="text-align: center;">5</td> <td style="text-align: center;">1</td> <td style="text-align: center;">unku</td> <td></td> <td style="text-align: center;">n</td> </tr> <tr> <td>532</td> <td style="text-align: center;">5</td> <td style="text-align: center;">5</td> <td style="text-align: center;">1</td> <td style="text-align: center;">unku</td> <td></td> <td style="text-align: center;">n</td> </tr> <tr> <td>59997</td> <td style="text-align: center;">5</td> <td style="text-align: center;">5</td> <td style="text-align: center;">99</td> <td style="text-align: center;">aar</td> <td></td> <td style="text-align: center;">n</td> </tr> </tbody> </table>	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	3	5	5	1	aar		n	4		7	7	999	aar	n	531	5	5	1	unku		n	532	5	5	1	unku		n	59997	5	5	99	aar		n																																																																																																														
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd																																																																																																																																																			
3	5	5	1	aar		n																																																																																																																																																			
4		7	7	999	aar	n																																																																																																																																																			
531	5	5	1	unku		n																																																																																																																																																			
532	5	5	1	unku		n																																																																																																																																																			
59997	5	5	99	aar		n																																																																																																																																																			
8.	<p><b>Route Pattern</b> Route pattern 1 was used for calls destined for the 2nd site through Session Manager and the SIParator. Route pattern 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> <li>▪ <b>Pattern Name:</b> Any descriptive name.</li> <li>▪ <b>Grp No: 1</b> This field is set to the trunk group number defined in <b>Step 5</b>.</li> <li>▪ <b>FRL: 0</b> This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.</li> </ul> <pre>display route-pattern 1</pre> <p style="text-align: right;">Page 1 of 3</p> <p style="text-align: center;">Pattern Number: 1    <b>Pattern Name: to SM_21_31</b> SCCAN? n    Secure SIP? n</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Grp No</th> <th style="text-align: center;">FRL</th> <th style="text-align: center;">NPA</th> <th style="text-align: center;">Pfx</th> <th style="text-align: center;">Hop</th> <th style="text-align: center;">Toll</th> <th style="text-align: center;">No.</th> <th style="text-align: center;">Inserted</th> <th style="text-align: center;">DCS/ IXC</th> </tr> <tr> <th style="text-align: left;">No</th> <th style="text-align: center;">Mrk</th> <th style="text-align: center;">Lmt</th> <th style="text-align: center;">List</th> <th style="text-align: center;">Del</th> <th style="text-align: center;">Digits</th> <th style="text-align: center;">Dgts</th> <th style="text-align: center;">Intw</th> <th style="text-align: center;">QSIG</th> </tr> </thead> <tbody> <tr> <td>1:</td> <td style="text-align: center;">1</td> <td style="text-align: center;">0</td> <td></td> <td></td> <td></td> <td style="text-align: center;">0</td> <td></td> <td style="text-align: center;">n user</td> </tr> <tr> <td>2:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">n user</td> </tr> <tr> <td>3:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">n user</td> </tr> <tr> <td>4:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">n user</td> </tr> <tr> <td>5:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">n user</td> </tr> <tr> <td>6:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">n user</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">BCC VALUE</th> <th style="text-align: center;">TSC</th> <th style="text-align: center;">CA-TSC</th> <th style="text-align: center;">ITC</th> <th style="text-align: center;">BCIE</th> <th style="text-align: center;">Service/Feature</th> <th style="text-align: center;">PARM</th> <th style="text-align: center;">No.</th> <th style="text-align: center;">Numbering</th> <th style="text-align: center;">LAR</th> </tr> <tr> <th style="text-align: left;">0 1 2 M 4 W</th> <th style="text-align: center;">Request</th> <th style="text-align: center;">Dgts</th> <th style="text-align: center;">Format</th> <th style="text-align: center;">Subaddress</th> </tr> </thead> <tbody> <tr> <td>1:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">lev0-pvt none</td> </tr> <tr> <td>2:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">none</td> </tr> <tr> <td>3:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">none</td> </tr> <tr> <td>4:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">none</td> </tr> <tr> <td>5:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">none</td> </tr> <tr> <td>6:</td> <td style="text-align: center;">y</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n</td> <td style="text-align: center;">rest</td> <td style="text-align: center;">none</td> </tr> </tbody> </table>	Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC	No	Mrk	Lmt	List	Del	Digits	Dgts	Intw	QSIG	1:	1	0				0		n user	2:								n user	3:								n user	4:								n user	5:								n user	6:								n user	BCC VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR	0 1 2 M 4 W	Request	Request	Request	Request	Request	Request	Dgts	Format	Subaddress	1:	y	y	y	y	y	n	n	rest	lev0-pvt none	2:	y	y	y	y	y	n	n	rest	none	3:	y	y	y	y	y	n	n	rest	none	4:	y	y	y	y	y	n	n	rest	none	5:	y	y	y	y	y	n	n	rest	none	6:	y	y	y	y	y	n	n	rest	none
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC																																																																																																																																																	
No	Mrk	Lmt	List	Del	Digits	Dgts	Intw	QSIG																																																																																																																																																	
1:	1	0				0		n user																																																																																																																																																	
2:								n user																																																																																																																																																	
3:								n user																																																																																																																																																	
4:								n user																																																																																																																																																	
5:								n user																																																																																																																																																	
6:								n user																																																																																																																																																	
BCC VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR																																																																																																																																																
0 1 2 M 4 W	Request	Request	Request	Request	Request	Request	Dgts	Format	Subaddress																																																																																																																																																
1:	y	y	y	y	y	n	n	rest	lev0-pvt none																																																																																																																																																
2:	y	y	y	y	y	n	n	rest	none																																																																																																																																																
3:	y	y	y	y	y	n	n	rest	none																																																																																																																																																
4:	y	y	y	y	y	n	n	rest	none																																																																																																																																																
5:	y	y	y	y	y	n	n	rest	none																																																																																																																																																
6:	y	y	y	y	y	n	n	rest	none																																																																																																																																																
9.	<p><b>Save Translation</b> Use the <b>save translation</b> command to make the Communication Manager changes permanent.</p>																																																																																																																																																								

## 6. Configure Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms. . During compliance testing, the IP address assigned to Session Manager is 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a separate network interface used for connectivity to System Manager for provisioning Session Manager. The IP address assigned to the Session Manager management interface is 10.64.21.30.

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

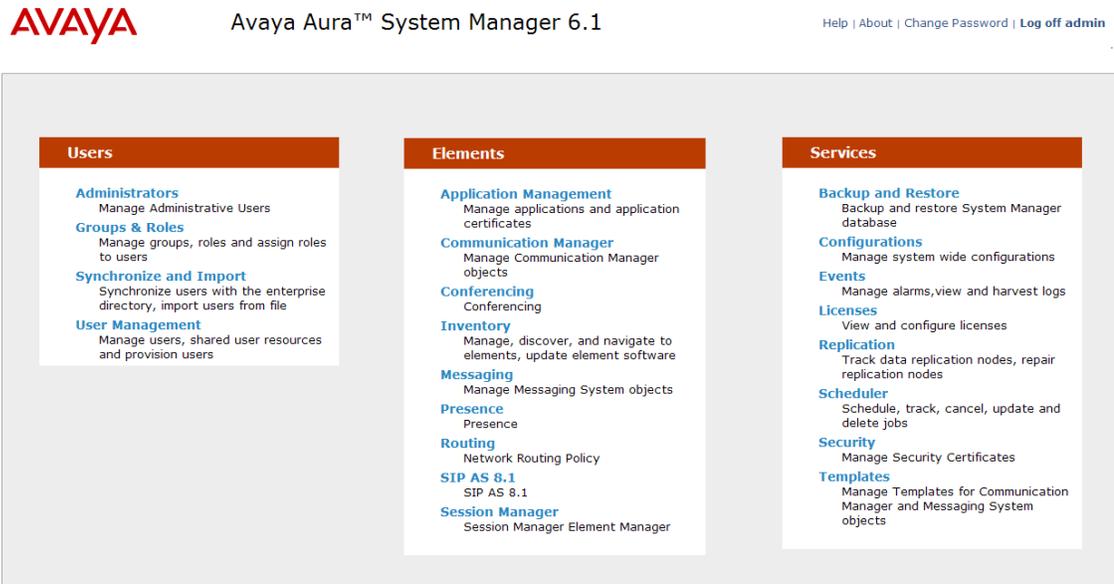
- **SIP domain**
- Logical/physical **Locations** that can be occupied by SIP Entities
- **SIP Entities** corresponding to the SIP telephony systems (including Communication Manager and Session Border Controller) and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Time Ranges** during which routing policies are active
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed

1.

## Login

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

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



2.

### Add SIP Domain

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

During compliance testing, one SIP Domain was configured on each Session Manager since all SIP entities were located within the same authoritative domain.

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

- **Name:** *avaya.com* (as set in **Section 5, Step 1**)
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. The main content area is titled 'Domain Management' and features a table with one item. The table has columns for Name, Type, Default, and Notes. The item 'avaya.com' is listed with a type of 'sip' and a default checkbox that is unchecked. A 'Filter: Enable' option is visible on the right side of the table. Below the table, there is a red asterisk indicating 'Input Required' and 'Commit' and 'Cancel' buttons.

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

3.

### Add Location

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

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

Under **General**:

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

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

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

Click **Commit** to save the configuration.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / Locations- Location Details

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

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

**General**

\* **Name**:   
**Notes**:

**Overall Managed Bandwidth**

**Managed Bandwidth Units**:   
**Total Bandwidth**:

**Per-Call Bandwidth Parameters**

\* **Default Audio Bandwidth**:

**Location Pattern**

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

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.21.*	<input type="text"/>

Select : All, None

\* **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. During compliance testing, a SIP Entity was added for the Session Manager itself, Communication Manager, and the Ingate SIParator.

Navigate to **Routing**→**SIP Entities**, and click the **New** button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for Session Manager are as follows:

Under **General**:

- **Name**: a descriptive name
- **FQDN or IP Address**: *10.64.21.31* as specified in **Figure 1**. This is the IP address assigned to the SM-100 security module installed in the Session Manager.
- **Type**: select *Session Manager*

Under **Port**, click **Add**, then edit the fields in the resulting new row as shown below:

- **Port**: *5060*. This is the port number on which the system listens for SIP requests.
- **Protocol**: *TCP*. The TCP transport protocol was used in the compliance test to send SIP requests.
- **Default Domain**: select the SIP Domain created in **Step 2**.

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

## Add SIP Entities (continued) – Session Manager

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



Avaya Aura™ System Manager  
6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing x Home

Home / Elements / Routing / SIP Entities- SIP Entity Details

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

Help ?
Commit
Cancel

### SIP Entity Details

#### General

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

#### SIP Link Monitoring

SIP Link Monitoring:

#### Entity Links

Add
Remove

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_20_40	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_41	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	RedSky	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TCP	* 5060	IngateRmtEndpt	* 5060	<input type="checkbox"/>

#### Port

Add
Remove

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.com	<input style="width: 100%;" type="text"/>
<input type="checkbox"/>	5060	TCP	avaya.com	<input style="width: 100%;" type="text"/>
<input type="checkbox"/>	5061	TLS	avaya.com	<input style="width: 100%;" type="text"/>

Select : All, None

## Add SIP Entities (continued) – Communication Manager

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

The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and utility links for 'Help | About | Change Password | Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. A left-hand menu lists various configuration categories, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' section with the following fields: Name (CM\_21\_41), FQDN or IP Address (10.64.21.41), Type (CM), Notes, Adaptation, Location, and Time Zone (America/Denver). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV', a SIP Timer B/F (in seconds) field set to 4, a Credential name field, and a Call Detail Recording dropdown set to 'none'. Below this is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. An 'Entity Links' section includes 'Add' and 'Remove' buttons and a table with one entry. The table has columns for SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The entry shows SM\_21\_31 linked to CM\_21\_41 via TLS on port 5061, with the 'Trusted' checkbox checked.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing \* Home

Home / Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details [Help ?](#)  
Commit Cancel

**General**

\* Name: CM\_21\_41

\* FQDN or IP Address: 10.64.21.41

Type: CM

Notes:

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV:

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Entity Links**

Add Remove

1 Item Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_41	* 5061	<input checked="" type="checkbox"/>

## Add SIP Entities (continued) – Ingate SIParator

The screen below shows the SIP Entity configuration details for the Ingate SIParator. Note the *Other* selection for **Type**.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. A left-hand menu lists various configuration categories, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' section with the following fields: 'Name' (IngateSIParator), 'FQDN or IP Address' (10.64.21.99), 'Type' (Other), 'Notes' (empty), 'Adaptation' (dropdown), 'Location' (.21 Subnet), and 'Time Zone' (America/Denver). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV'. The 'SIP Timer B/F (in seconds)' is set to 4. The 'Credential name' field is empty. 'Call Detail Recording' is set to 'none'. Below this is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. At the bottom, the 'Entity Links' section has 'Add' and 'Remove' buttons and a table with one entry. The table has columns for 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', and 'Trusted'. The entry shows 'SM\_21\_31' as SIP Entity 1, 'TCP' as Protocol, '\* 5060' as Port, 'IngateSIParator' as SIP Entity 2, '\* 5060' as Port, and a checked 'Trusted' checkbox.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing \* Home

Home / Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details [Help ?](#)  
Commit Cancel

**General**

\* Name: IngateSIParator

\* FQDN or IP Address: 10.64.21.99

Type: Other

Notes:

Adaptation:

Location: .21 Subnet

Time Zone: America/Denver

Override Port & Transport with DNS SRV:

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Entity Links**  
Add Remove

1 Item Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	IngateSIParator	* 5060	<input checked="" type="checkbox"/>

5.

### Add Entity Links

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

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

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

Click **Commit** to save the configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 6.1", and links for "Help | About | Change Password | Log off admin". The main content area is titled "Entity Links" and contains a table with one row of configuration data. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The values in the table are: Name: CM\_21\_41, SIP Entity 1: SM\_21\_31, Protocol: TLS, Port: 5061, SIP Entity 2: CM\_21\_41, Port: 5061, Trusted: checked, and Notes: empty. There are "Commit" and "Cancel" buttons at the top right and bottom right of the configuration area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	<input checked="" type="checkbox"/>	

**Add Entity Links (continued)**

The Entity Link for connecting Session Manager to Ingate SIParator was similarly defined as shown in the screen below.

AVAYA Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Entity Links- Entity Links

Entity Links [Help ?](#)

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* to IngateSIParator	* SM_21_31	TCP	* 5060	* IngateSIParator	* 5060	<input checked="" type="checkbox"/>	

\* Input Required

6.

### Add Time Ranges

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

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

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

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and user options like 'Help | About | Change Password | Log off admin'. The breadcrumb trail is 'Home / Elements / Routing / Time Ranges- Time Ranges'. A left-hand menu lists various configuration categories, with 'Time Ranges' selected. The main content area shows a 'Time Ranges' section with buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below this is a table with one item, '24/7', which is active for all days of the week (Mo-Su) from 00:00 to 23:59. The table has columns for Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The 'Notes' column for the '24/7' entry contains 'Time Range 24/7'.

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

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

## Add Routing Policies (continued)

The screens below show the configuration details for the two Routing Policies used during compliance testing.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × Home

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details [Help ?](#)  
Commit Cancel

**General**

\* Name:

Disabled:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM_21_41	10.64.21.41	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Select : All, None

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × Home

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details [Help ?](#)  
Commit Cancel

**General**

\* Name:

Disabled:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
IngateSIParator	10.64.21.99	Other	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Select : All, None

8.

### **Add Dial Patterns**

Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 5-digit extensions beginning with “5” resided on Communication Manager at the main enterprise site. 5-digit extensions beginning with “3” should were routed to Ingate SIParator for onward routing to the 2<sup>nd</sup> site. Therefore two Dial Patterns were created accordingly.

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

#### **Under General:**

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

#### **Under Originating Locations and Routing Policies**

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

#### **Under Time of Day**

Click **Add** to select the time range configured in **Step 6**.

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

## Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing calls to Communication Manager at the main enterprise site.

The screenshot displays the Avaya Aura System Manager 6.1 interface for configuring a Dial Pattern. The breadcrumb trail is Home / Elements / Routing / Dial Patterns - Dial Pattern Details. The left sidebar shows a navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Help ?' link, 'Commit', and 'Cancel' buttons. The 'General' section contains the following fields: '\* Pattern: 5', '\* Min: 5', '\* Max: 5', 'Emergency Call: ', 'SIP Domain: avaya.com', and 'Notes: to CM\_21\_41'. Below this is the 'Originating Locations and Routing Policies' section, which has 'Add' and 'Remove' buttons. It shows '1 Item' and a 'Filter: Enable' option. A table lists the configuration details for the single item.

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to CM_21_41	0	<input type="checkbox"/>	CM_21_41	

Select : All, None

Denied Originating Locations

## Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing calls to Ingate SIParator (for onward routing to the 2<sup>nd</sup> site).

The screenshot displays the Avaya Aura™ System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The breadcrumb trail is Home / Elements / Routing / Dial Patterns - Dial Pattern Details. The left sidebar shows a tree view with 'Routing' expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the following fields are visible: '\* Pattern:' with a value of 3, '\* Min:' with a value of 5, '\* Max:' with a value of 5, 'Emergency Call:' with an unchecked checkbox, 'SIP Domain:' with a dropdown menu set to '-ALL-', and 'Notes:' with an empty text box. Below this is the 'Originating Locations and Routing Policies' section, which has 'Add' and 'Remove' buttons. It shows a table with 1 item, a 'Refresh' button, and a 'Filter: Enable' option. The table columns are: checkbox, Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single row contains: checkbox, -ALL-, Any Locations, to IngateSIParator, 0, unchecked, IngateSIParator. At the bottom of the table area, it says 'Select : All, None'.

**Avaya Aura™ System Manager 6.1**

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

**Dial Pattern Details** [Help ?](#)

Commit Cancel

**General**

\* Pattern: 3

\* Min: 5

\* Max: 5

Emergency Call:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

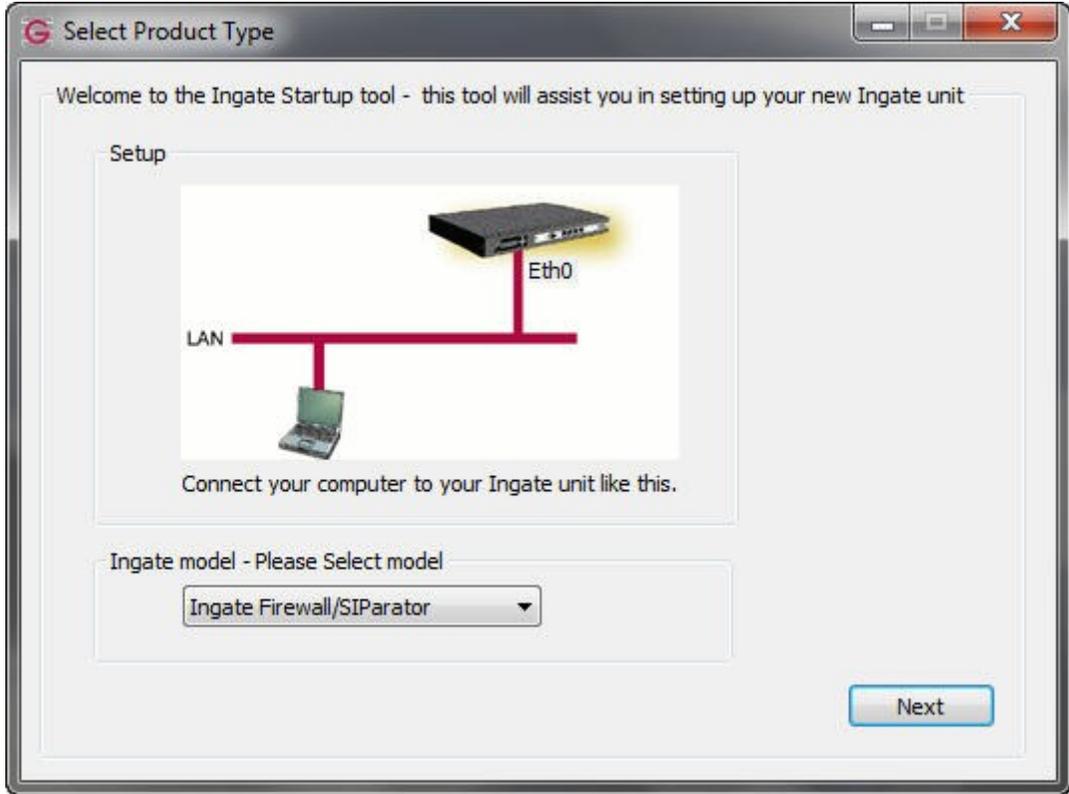
1 Item Refresh Filter: Enable

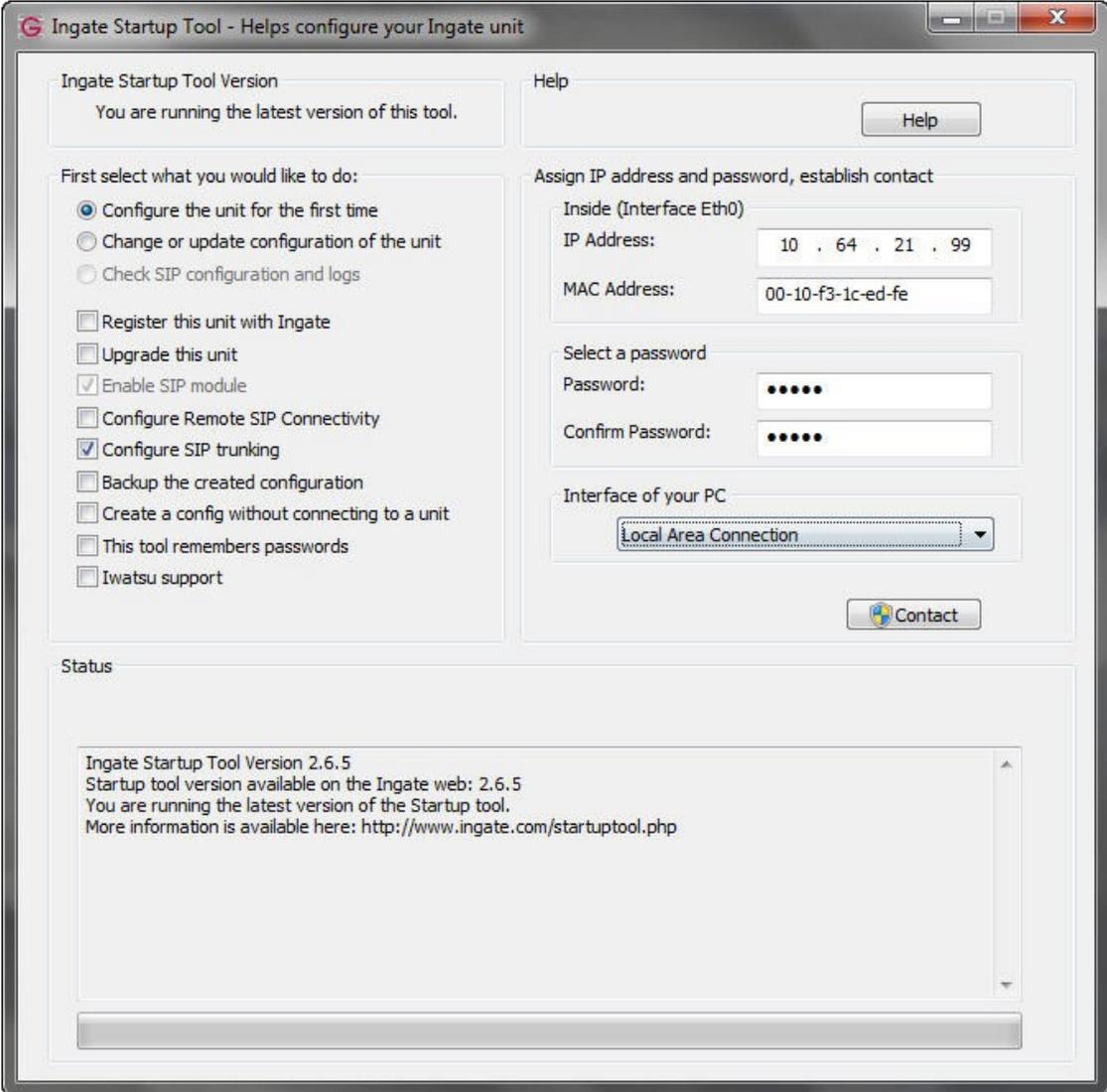
<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to IngateSIParator	0	<input type="checkbox"/>	IngateSIParator	

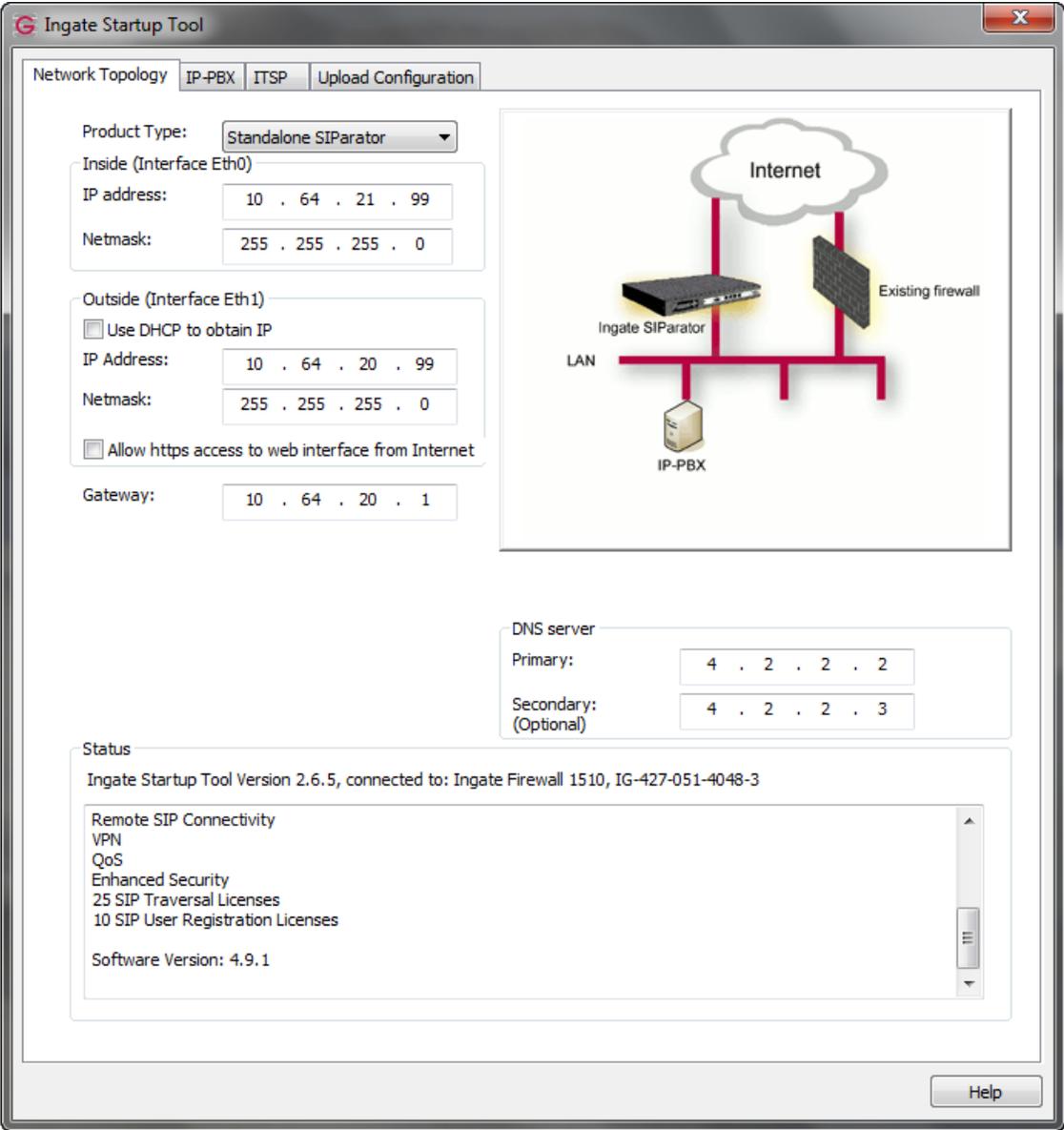
Select : All, None

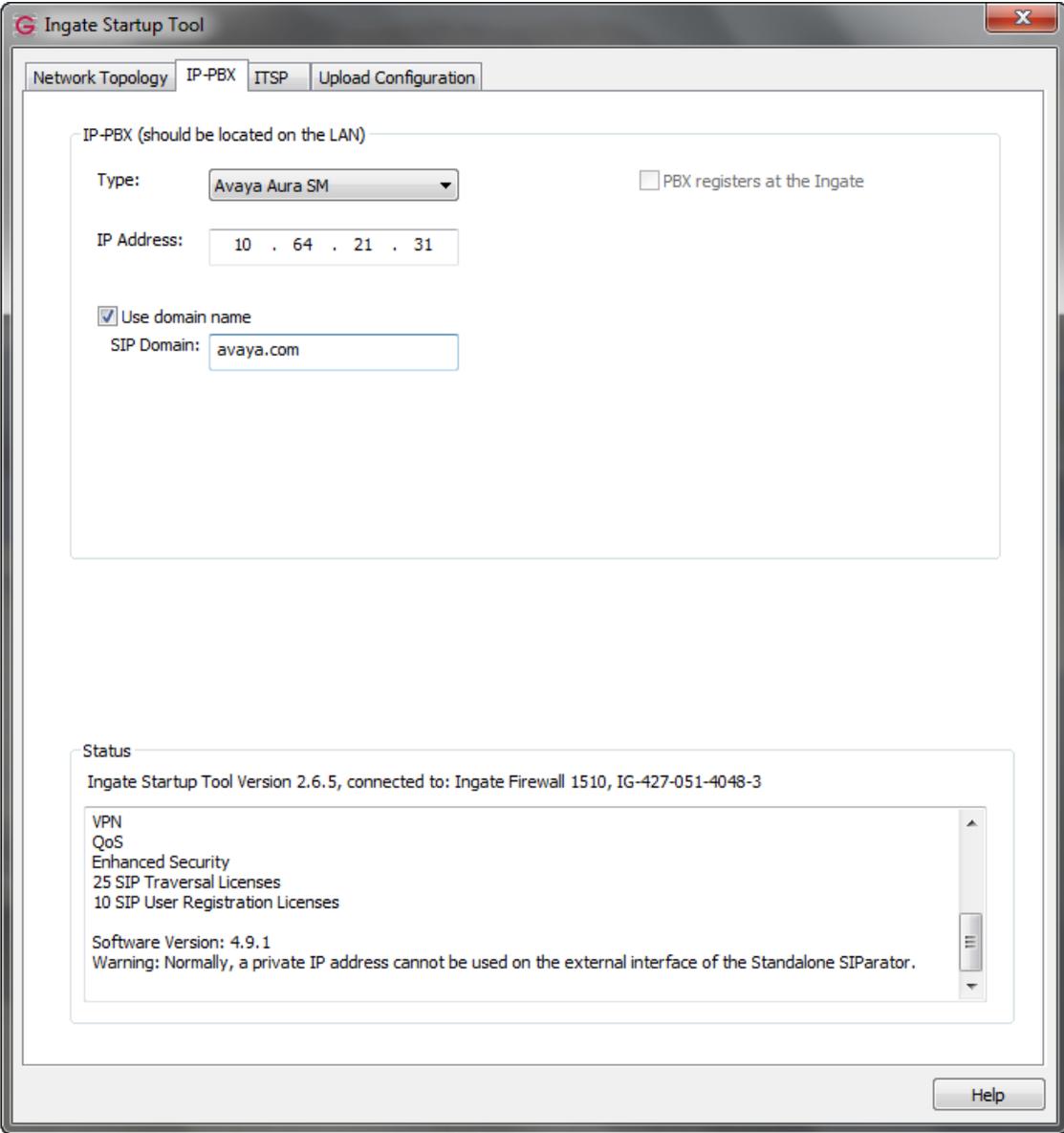
## 7. Configure Ingate SIParator

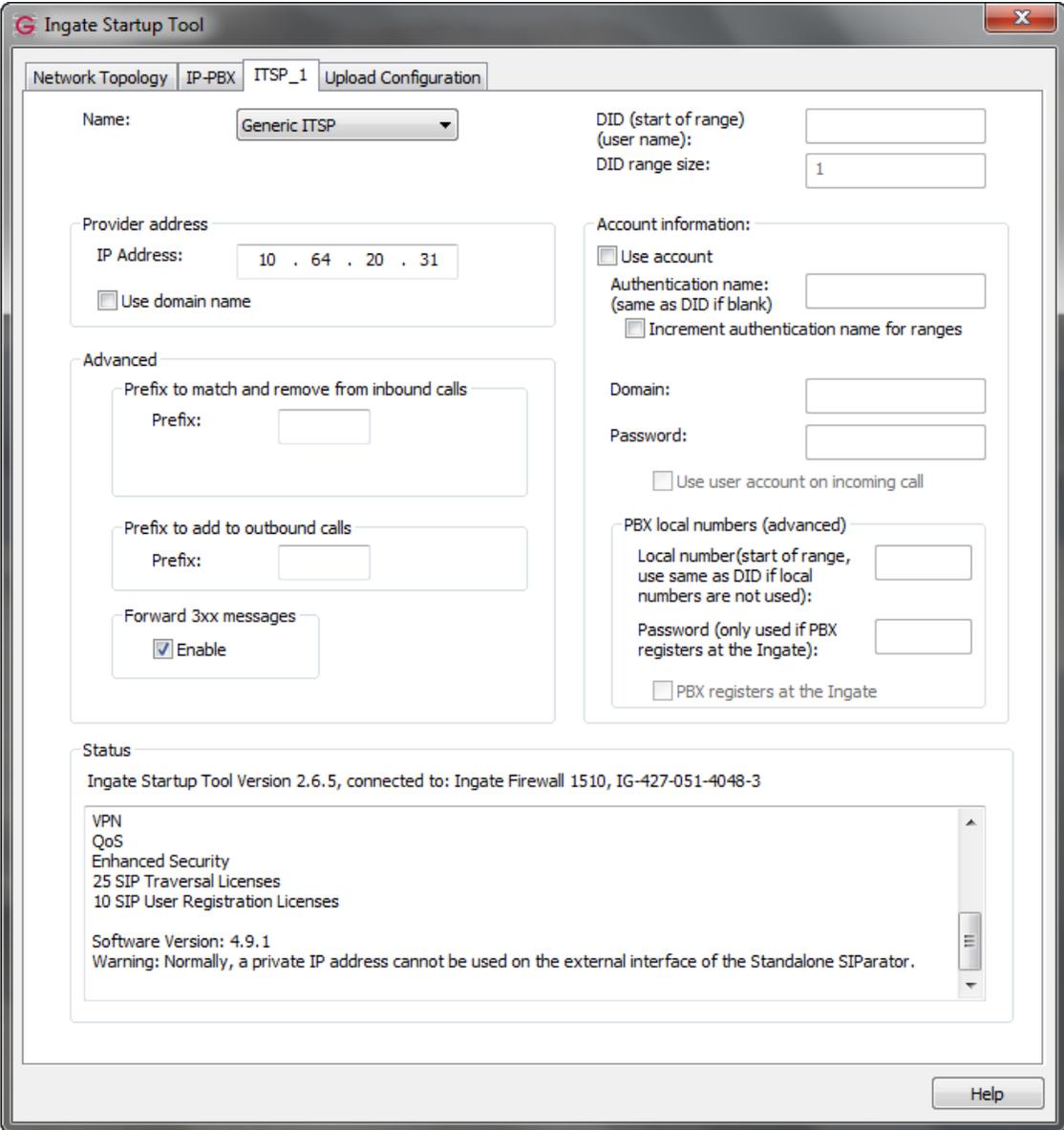
The Ingate SIParator is configured initially with the Ingate Startup Tool. Based on the provided input, the Startup Tool will create an initial configuration that can be uploaded to the SIParator. The results of this configuration can then be viewed or expanded using the SIParator web interface. To access the web interface, enter the IP address of the SIParator as the destination address in a web browser. When prompted for login credentials, enter an appropriate user name and password.

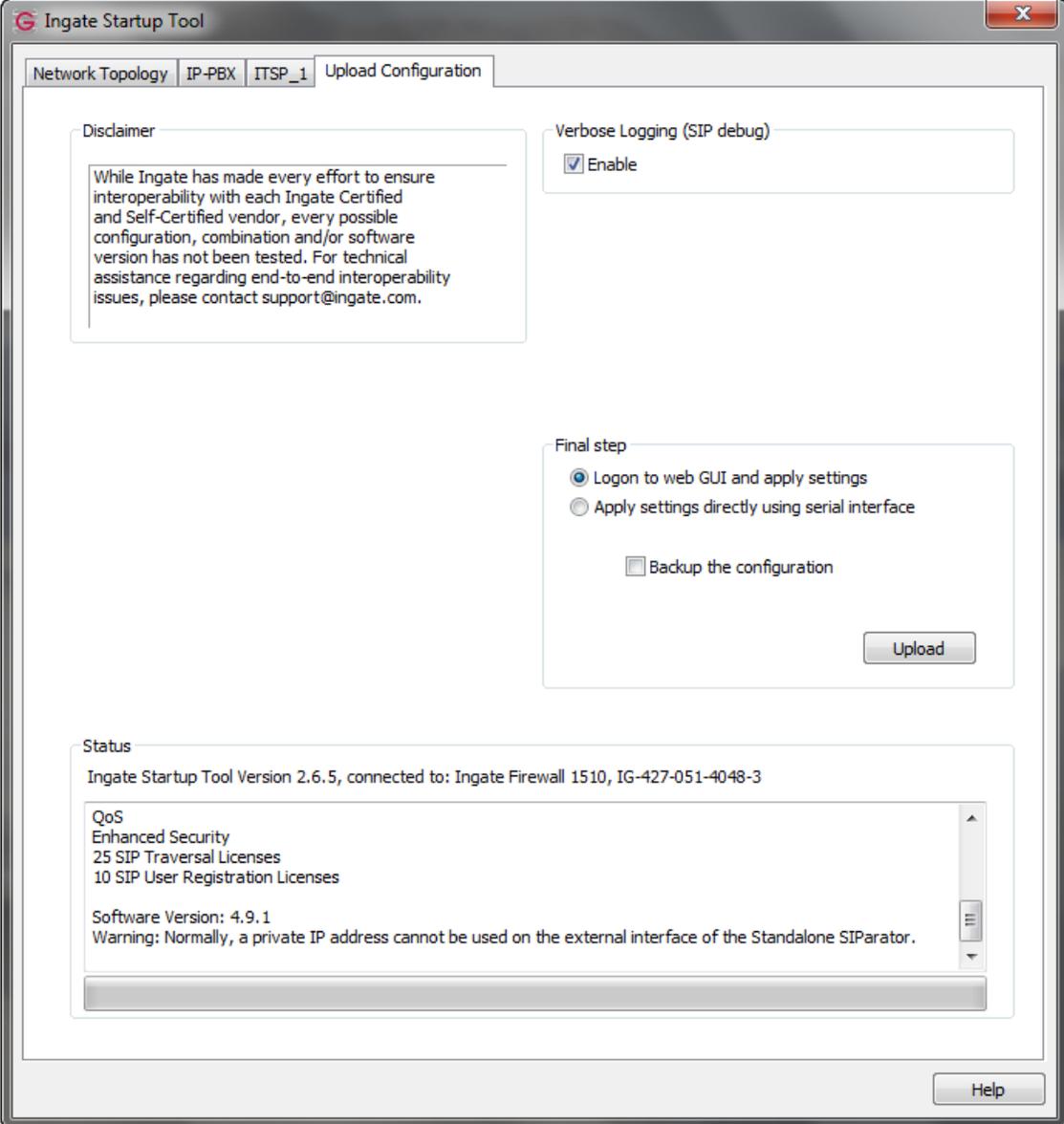
Step	Description
1.	<b>Launch Startup Tool</b> The Ingate Startup Tool is a windows application which is launched from the Windows Start Menu by navigating to <b>Start→All Programs→Shortcut to StartupTool.exe</b> .
2.	<b>Select Product Type</b> The initial Ingate Startup Tool screen is shown below. Verify the PC is running on the same LAN subnet as the SIParator as shown in the diagram. This is necessary in order to assign the initial IP address to the SIParator from the Startup Tool. Select the SIParator model from the <b>Ingate model</b> drop-down menu. Click the <b>Next</b> button. 

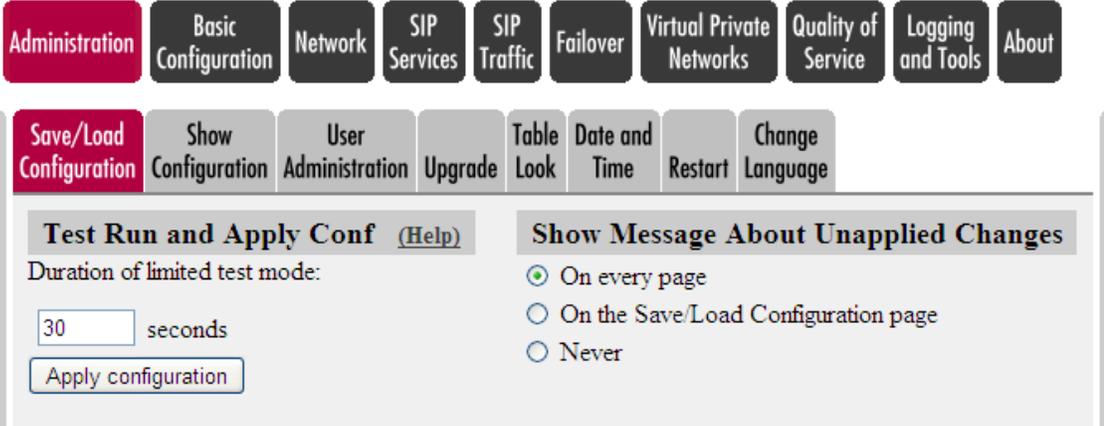
Step	Description
3.	<p><b>Select Configuration Options and Assign Private IP</b>            Select <b>Configure the unit for the first time</b> and the <b>Configure SIP trunking</b> option. Enter the <b>Inside (Interface Eth0) IP address, MAC Address</b> and <b>Password</b> fields. Click the <b>Contact</b> button to establish a connection to the SIParator. For future updates, click the option - <b>Change or update configuration of the unit</b></p> 

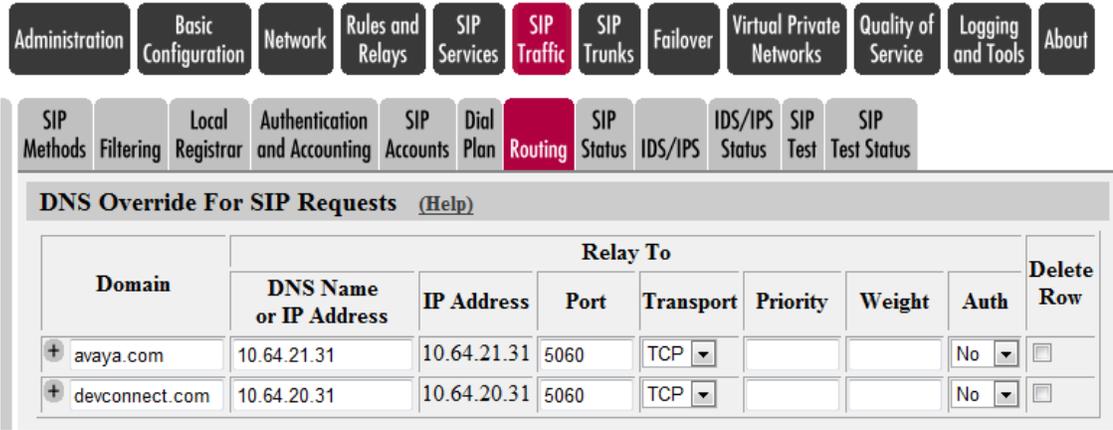
Step	Description
4.	<p><b>Network Topology</b></p> <p>After connecting to the SIParator, the following page appears. Select the <b>Network Topology</b> tab. Select <i>Standalone SIParator</i> from the <b>Product Type</b> drop-down menu. Enter an IP address and subnet mask for both the inside and outside interfaces as shown in <b>Figure 1</b>. The <b>Gateway</b> field is set to the IP address of the default gateway on the public side of the SIParator. A DNS server was not used during compliance testing.</p>  <p>The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'Standalone SIParator'. The 'Inside (Interface Eth0)' section has an IP address of 10.64.21.99 and a netmask of 255.255.255.0. The 'Outside (Interface Eth1)' section has an IP address of 10.64.20.99, a netmask of 255.255.255.0, and a gateway of 10.64.20.1. The 'DNS server' section has a primary of 4.2.2.2 and a secondary of 4.2.2.3. The 'Status' section shows 'Ingate Startup Tool Version 2.6.5, connected to: Ingate Firewall 1510, IG-427-051-4048-3' and lists features like Remote SIP Connectivity, VPN, QoS, Enhanced Security, 25 SIP Traversal Licenses, 10 SIP User Registration Licenses, and Software Version: 4.9.1. A network diagram on the right shows the 'Ingate SIParator' connected to a 'LAN' with an 'IP-PBX' and an 'Existing firewall', both connected to the 'Internet' cloud.</p>

Step	Description
5.	<p><b>IP-PBX Settings</b></p> <p>Select the <b>IP-PBX</b> tab. Select <i>Avaya Aura SM</i> from the <b>Type</b> drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the internal interface to be compatible with the Avaya component (Session Manager in this case) connected to it through a direct SIP trunking interface. Enter the Session Manager IP address in the <b>IP Address</b> field. Also check the option to <b>Use domain name</b>, then specify the domain name as set on Session Manager (see <b>Section 6 Step 2</b>).</p> 

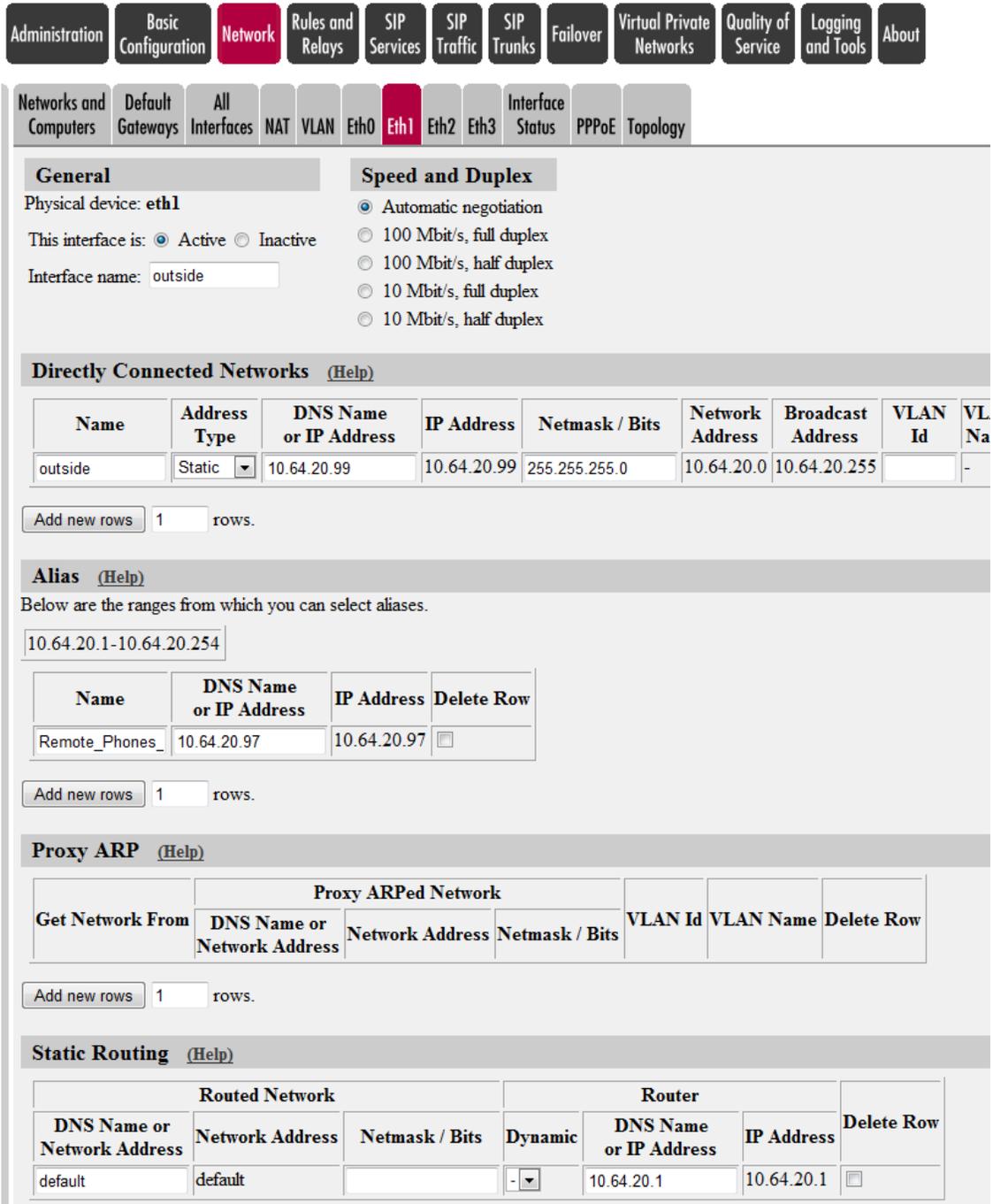
Step	Description
6.	<p><b>Service Provider Settings</b></p> <p>Select the <b>ITSP_1</b> tab. Select <b>Generic ITSP</b> from the <b>Name</b> drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the external interface to be compatible with a generic SIP service provider. In the <b>IP Address</b> field in the <b>Provider address</b> section, enter the IP address for the node to route calls to at the 2<sup>nd</sup> site. During compliance testing, when calls were routed to the 2<sup>nd</sup> site, they were routed to a Session Manager (not shown in <b>Figure 1</b>), with an IP address 10.64.20.31.</p> 

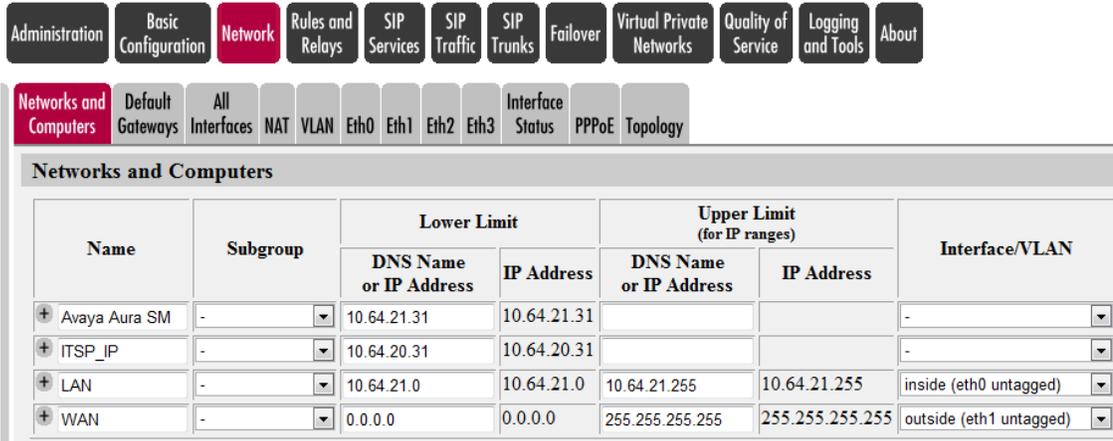
Step	Description
7.	<p><b>Upload Configuration</b>            Select the <b>Upload Configuration</b> tab to upload the configuration to the SIParator.            Click the <b>Upload</b> button to begin the upload.</p> 

Step	Description
8.	<p><b>Apply Configuration</b></p> <p>After uploading the configuration, the Startup Tool opens a web browser to the <b>Administration</b>→<b>Save/Load Configuration</b> page of the SIParator. Click the <b>Apply configuration</b> button to apply the configuration. The Startup Tool configuration is complete at this point. However, additional configuration was required to support all the test cases in the compliance test. This configuration is performed using the SIParator web interface and is covered in the remaining steps.</p> 

Step	Description																																		
9.	<p><b>Configure Routing</b></p> <p>Navigate to <b>SIP Traffic</b>→<b>Routing</b> to add entries for DNS override for SIP requests. Add one entry for the outside interface and one entry for the inside interface as shown below. The configured parameters are:</p> <ul style="list-style-type: none"> <li>• <b>Domain:</b> domain names for the main enterprise site (<i>avaya.com</i>) and the 2<sup>nd</sup> site(<i>devconnect.com</i>)</li> <li>• <b>DNS Name or IP Address:</b> IP addresses for the Avaya component connected to the SIParator on the outside (<i>10.64.20.31</i>) and on the inside (Session Manager IP address – <i>10.64.21.31</i>)</li> <li>• Transport: select <i>TCP</i></li> </ul>  <p>The screenshot shows the configuration interface for SIP Traffic. The 'Routing' tab is selected. Below the navigation tabs, the 'DNS Override For SIP Requests' section is visible, containing a table with the following data:</p> <table border="1"> <thead> <tr> <th rowspan="2">Domain</th> <th colspan="7">Relay To</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>DNS Name or IP Address</th> <th>IP Address</th> <th>Port</th> <th>Transport</th> <th>Priority</th> <th>Weight</th> <th>Auth</th> </tr> </thead> <tbody> <tr> <td>+ avaya.com</td> <td>10.64.21.31</td> <td>10.64.21.31</td> <td>5060</td> <td>TCP</td> <td></td> <td></td> <td>No</td> <td><input type="checkbox"/></td> </tr> <tr> <td>+ devconnect.com</td> <td>10.64.20.31</td> <td>10.64.20.31</td> <td>5060</td> <td>TCP</td> <td></td> <td></td> <td>No</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Domain	Relay To							Delete Row	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	+ avaya.com	10.64.21.31	10.64.21.31	5060	TCP			No	<input type="checkbox"/>	+ devconnect.com	10.64.20.31	10.64.20.31	5060	TCP			No	<input type="checkbox"/>
Domain	Relay To							Delete Row																											
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth																												
+ avaya.com	10.64.21.31	10.64.21.31	5060	TCP			No	<input type="checkbox"/>																											
+ devconnect.com	10.64.20.31	10.64.20.31	5060	TCP			No	<input type="checkbox"/>																											

Step	Description																																																													
10.	<p data-bbox="315 233 751 268"><b>Configure Eth0 Inside Interface</b></p> <p data-bbox="315 268 1419 411">The Eth0 inside interface is shown below for reference and completeness. In order to support endpoints on networks within the enterprise other than the subnet to which the SIParator is directly connected, a static route must be configured on the internal interface (not shown).</p> <div data-bbox="315 457 1430 1822"> <p data-bbox="326 464 1393 533">Administration Basic Configuration <b>Network</b> Rules and Relays SIP Services SIP Traffic SIP Trunks Failover Virtual Private Networks Quality of Service Logging and Tools About</p> <p data-bbox="326 558 1117 625">Networks and Computers Default Gateways All Interfaces NAT VLAN <b>Eth0</b> Eth1 Eth2 Eth3 Interface Status PPPoE Topology</p> <p data-bbox="354 646 959 678"><b>General</b> <b>Speed and Duplex</b></p> <p data-bbox="342 680 683 793">Physical device: eth0 This interface is: <input checked="" type="radio"/> Active <input type="radio"/> Inactive Interface name: <input type="text" value="inside"/></p> <p data-bbox="732 680 959 842"><input checked="" type="radio"/> Automatic negotiation <input type="radio"/> 100 Mbit/s, full duplex <input type="radio"/> 100 Mbit/s, half duplex <input type="radio"/> 10 Mbit/s, full duplex <input type="radio"/> 10 Mbit/s, half duplex</p> <p data-bbox="347 873 751 905"><b>Directly Connected Networks</b> <a href="#">(Help)</a></p> <table border="1" data-bbox="354 919 1430 1020"> <thead> <tr> <th>Name</th> <th>Address Type</th> <th>DNS Name or IP Address</th> <th>IP Address</th> <th>Netmask / Bits</th> <th>Network Address</th> <th>Broadcast Address</th> <th>VLAN Id</th> </tr> </thead> <tbody> <tr> <td>inside</td> <td>Static</td> <td>10.64.21.99</td> <td>10.64.21.99</td> <td>255.255.255.0</td> <td>10.64.21.0</td> <td>10.64.21.255</td> <td></td> </tr> </tbody> </table> <p data-bbox="347 1052 613 1073">Add new rows <input type="text" value="1"/> rows.</p> <p data-bbox="347 1115 483 1146"><b>Alias</b> <a href="#">(Help)</a></p> <p data-bbox="337 1150 813 1171">Below are the ranges from which you can select aliases.</p> <p data-bbox="342 1192 574 1224"><input type="text" value="10.64.21.1-10.64.21.254"/></p> <table border="1" data-bbox="354 1241 938 1341"> <thead> <tr> <th>Name</th> <th>DNS Name or IP Address</th> <th>IP Address</th> <th>Delete Row</th> </tr> </thead> <tbody> <tr> <td>Remote_Phones</td> <td>10.64.21.97</td> <td>10.64.21.97</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="347 1373 613 1394">Add new rows <input type="text" value="1"/> rows.</p> <p data-bbox="347 1436 553 1467"><b>Proxy ARP</b> <a href="#">(Help)</a></p> <table border="1" data-bbox="354 1482 1393 1583"> <thead> <tr> <th rowspan="2">Get Network From</th> <th colspan="3">Proxy ARPed Network</th> <th rowspan="2">VLAN Id</th> <th rowspan="2">VLAN Name</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>DNS Name or Network Address</th> <th>Network Address</th> <th>Netmask / Bits</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p data-bbox="347 1604 613 1625">Add new rows <input type="text" value="1"/> rows.</p> <p data-bbox="347 1667 589 1698"><b>Static Routing</b> <a href="#">(Help)</a></p> <table border="1" data-bbox="354 1713 1320 1814"> <thead> <tr> <th colspan="3">Routed Network</th> <th colspan="3">Router</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>DNS Name or Network Address</th> <th>Network Address</th> <th>Netmask / Bits</th> <th>Dynamic</th> <th>DNS Name or IP Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </div>	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	inside	Static	10.64.21.99	10.64.21.99	255.255.255.0	10.64.21.0	10.64.21.255		Name	DNS Name or IP Address	IP Address	Delete Row	Remote_Phones	10.64.21.97	10.64.21.97	<input type="checkbox"/>	Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row	DNS Name or Network Address	Network Address	Netmask / Bits								Routed Network			Router			Delete Row	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address							
Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id																																																							
inside	Static	10.64.21.99	10.64.21.99	255.255.255.0	10.64.21.0	10.64.21.255																																																								
Name	DNS Name or IP Address	IP Address	Delete Row																																																											
Remote_Phones	10.64.21.97	10.64.21.97	<input type="checkbox"/>																																																											
Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row																																																								
	DNS Name or Network Address	Network Address	Netmask / Bits																																																											
Routed Network			Router			Delete Row																																																								
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address																																																									

Step	Description
11.	<p data-bbox="315 233 773 264"><b>Configure Eth1 Outside Interface</b></p> <p data-bbox="315 268 1271 300">The Eth1 outside interface is shown below for reference and completeness.</p> <div data-bbox="315 348 1438 1709">  </div>

Step	Description																																							
12.	<p data-bbox="316 231 1429 336"><b>Configure Networks and Computers</b> The <b>Network</b>→<b>Networks and Computers</b> configuration is shown below for reference and completeness.</p> <div data-bbox="316 388 1429 829">  <table border="1" data-bbox="341 577 1421 829"> <thead> <tr> <th rowspan="2">Name</th> <th rowspan="2">Subgroup</th> <th colspan="2">Lower Limit</th> <th colspan="2">Upper Limit (for IP ranges)</th> <th rowspan="2">Interface/VLAN</th> </tr> <tr> <th>DNS Name or IP Address</th> <th>IP Address</th> <th>DNS Name or IP Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>Avaya Aura SM</td> <td>-</td> <td>10.64.21.31</td> <td>10.64.21.31</td> <td></td> <td></td> <td>-</td> </tr> <tr> <td>ITSP_IP</td> <td>-</td> <td>10.64.20.31</td> <td>10.64.20.31</td> <td></td> <td></td> <td>-</td> </tr> <tr> <td>LAN</td> <td>-</td> <td>10.64.21.0</td> <td>10.64.21.0</td> <td>10.64.21.255</td> <td>10.64.21.255</td> <td>inside (eth0 untagged)</td> </tr> <tr> <td>WAN</td> <td>-</td> <td>0.0.0.0</td> <td>0.0.0.0</td> <td>255.255.255.255</td> <td>255.255.255.255</td> <td>outside (eth1 untagged)</td> </tr> </tbody> </table> </div>	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Avaya Aura SM	-	10.64.21.31	10.64.21.31			-	ITSP_IP	-	10.64.20.31	10.64.20.31			-	LAN	-	10.64.21.0	10.64.21.0	10.64.21.255	10.64.21.255	inside (eth0 untagged)	WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)
Name	Subgroup			Lower Limit		Upper Limit (for IP ranges)			Interface/VLAN																															
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address																																			
Avaya Aura SM	-	10.64.21.31	10.64.21.31			-																																		
ITSP_IP	-	10.64.20.31	10.64.20.31			-																																		
LAN	-	10.64.21.0	10.64.21.0	10.64.21.255	10.64.21.255	inside (eth0 untagged)																																		
WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)																																		

Step	Description																																																																																																																																																													
14.	<p data-bbox="315 235 587 268"><b>Configure Dial Plan</b></p> <p data-bbox="315 268 1295 340">The <b>SIP Traffic</b> → <b>Dial Plan</b> configuration is shown below for reference and completeness.</p> <div data-bbox="315 386 1425 1604"> <p data-bbox="321 390 974 428"> <span>Administration</span> <span>Basic Configuration</span> <span>Network</span> <span>Rules and Relays</span> <span>SIP Services</span> <span><b>SIP Traffic</b></span> <span>SIP Trunks</span> <span>Failover</span> <span>Virtual Private Networks</span> <span>Quality of Service</span> <span>Logging and Tools</span> <span>About</span> </p> <p data-bbox="321 445 867 483"> <span>SIP Methods</span> <span>Filtering</span> <span>Local Registrar</span> <span>Authentication and Accounting</span> <span>SIP Accounts</span> <span><b>Dial Plan</b></span> <span>Routing</span> <span>Status</span> <span>IDS/IPS</span> <span>IDS/IPS Status</span> <span>SIP Test</span> <span>SIP Test Status</span> </p> <p data-bbox="337 499 698 525"> <b>Use Dial Plan</b> (Help) <b>Emergency Number</b> (Help)         </p> <p data-bbox="337 525 600 583"> <input checked="" type="radio"/> On 911  <input type="radio"/> Off  <input type="radio"/> Fallback         </p> <p data-bbox="337 604 552 630"><b>Matching From Header</b> (Help)</p> <table border="1" data-bbox="344 634 1042 772"> <thead> <tr> <th rowspan="2">Name</th> <th colspan="2">Use This ...</th> <th>... Or This</th> <th rowspan="2">Transport</th> <th rowspan="2">Network</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>Username</th> <th>Domain</th> <th>Reg Expr</th> </tr> </thead> <tbody> <tr> <td>Avaya Aura SM</td> <td>*</td> <td>*</td> <td></td> <td>TCP</td> <td>Avaya Aura SM</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Generic ITSP</td> <td>*</td> <td>*</td> <td></td> <td>TCP</td> <td>ITSP_IP</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN</td> <td>*</td> <td>*</td> <td></td> <td>TCP</td> <td>LAN</td> <td><input type="checkbox"/></td> </tr> <tr> <td>WAN</td> <td>*</td> <td>*</td> <td></td> <td>Any</td> <td>WAN</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="337 785 503 810">Add new rows 1 rows.</p> <p data-bbox="337 827 552 852"><b>Matching Request-URI</b> (Help)</p> <table border="1" data-bbox="344 856 1140 949"> <thead> <tr> <th rowspan="2">Name</th> <th colspan="4">Use This ...</th> <th>... Or This</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>Prefix</th> <th>Head</th> <th>Tail</th> <th>Min. Tail</th> <th>Domain</th> </tr> </thead> <tbody> <tr> <td>Inbound</td> <td></td> <td></td> <td>-</td> <td></td> <td>Reg Expr sip.(.*)@devconnect.com</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Outbound</td> <td></td> <td></td> <td>-</td> <td></td> <td>Reg Expr sip.(.*)@avaya.com</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="337 961 503 987">Add new rows 1 rows.</p> <p data-bbox="337 1003 470 1029"><b>Forward To</b> (Help)</p> <table border="1" data-bbox="344 1033 1127 1125"> <thead> <tr> <th rowspan="2">Name</th> <th rowspan="2">Subno.</th> <th colspan="2">Use This ...</th> <th colspan="2">... Or This</th> <th>... Or This</th> <th>... Or This</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>Account</th> <th>Replacement Domain</th> <th>Port</th> <th>Transport</th> <th>Reg Expr</th> <th>Trunk</th> </tr> </thead> <tbody> <tr> <td>Avaya Aura SM</td> <td>1</td> <td>-</td> <td></td> <td></td> <td>-</td> <td>Reg Expr sip.\$1@avaya.com;transp</td> <td>-</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Generic ITSP</td> <td>1</td> <td>-</td> <td></td> <td></td> <td>-</td> <td>Reg Expr sip.\$1@devconnect.com;t</td> <td>-</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="337 1138 665 1163">Add new rows 1 groups with 1 rows per group.</p> <p data-bbox="337 1180 454 1205"><b>Dial Plan</b> (Help)</p> <table border="1" data-bbox="344 1209 1409 1323"> <thead> <tr> <th rowspan="2">No.</th> <th rowspan="2">From Header</th> <th rowspan="2">Request-URI</th> <th rowspan="2">Action</th> <th rowspan="2">Forward To</th> <th colspan="2">Add Prefix</th> <th rowspan="2">ENUM Root</th> <th rowspan="2">Time Class</th> <th rowspan="2">Comment</th> <th rowspan="2">Delete Row</th> </tr> <tr> <th>Forward</th> <th>ENUM</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Avaya Aura SM</td> <td>Outbound</td> <td>Forward</td> <td>Generic ITSP</td> <td></td> <td></td> <td>-</td> <td>-</td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>2</td> <td>Generic ITSP</td> <td>Inbound</td> <td>Forward</td> <td>Avaya Aura SM</td> <td></td> <td></td> <td>-</td> <td>-</td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>3</td> <td>WAN</td> <td>-</td> <td>Reject</td> <td>-</td> <td></td> <td></td> <td>-</td> <td>-</td> <td></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="337 1335 503 1360">Add new rows 1 rows.</p> <p data-bbox="337 1377 535 1402"><b>Methods in Dial Plan</b> (Help)</p> <p data-bbox="337 1402 893 1428">The ACK, PRACK, CANCEL, BYE, UPDATE and INFO methods cannot be handled by the Dial Plan.</p> <table border="1" data-bbox="344 1432 519 1600"> <thead> <tr> <th>Method</th> <th>Delete Row</th> </tr> </thead> <tbody> <tr> <td>INVITE</td> <td><input type="checkbox"/></td> </tr> <tr> <td>OPTIONS</td> <td><input type="checkbox"/></td> </tr> <tr> <td>SUBSCRIBE</td> <td><input type="checkbox"/></td> </tr> <tr> <td>MESSAGE</td> <td><input type="checkbox"/></td> </tr> <tr> <td>REFER</td> <td><input type="checkbox"/></td> </tr> <tr> <td>NOTIFY</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p data-bbox="539 1432 753 1457"><b>REGISTER in Dial Plan</b> (Help)</p> <p data-bbox="539 1457 948 1491"> <input checked="" type="radio"/> Keep To headers for REGISTER requests passed through the Dial Plan  <input type="radio"/> Rewrite To headers for REGISTER requests passed through the Dial Plan         </p> </div>	Name	Use This ...		... Or This	Transport	Network	Delete Row	Username	Domain	Reg Expr	Avaya Aura SM	*	*		TCP	Avaya Aura SM	<input type="checkbox"/>	Generic ITSP	*	*		TCP	ITSP_IP	<input type="checkbox"/>	LAN	*	*		TCP	LAN	<input type="checkbox"/>	WAN	*	*		Any	WAN	<input type="checkbox"/>	Name	Use This ...				... Or This	Delete Row	Prefix	Head	Tail	Min. Tail	Domain	Inbound			-		Reg Expr sip.(.*)@devconnect.com	<input type="checkbox"/>	Outbound			-		Reg Expr sip.(.*)@avaya.com	<input type="checkbox"/>	Name	Subno.	Use This ...		... Or This		... Or This	... Or This	Delete Row	Account	Replacement Domain	Port	Transport	Reg Expr	Trunk	Avaya Aura SM	1	-			-	Reg Expr sip.\$1@avaya.com;transp	-	<input type="checkbox"/>	Generic ITSP	1	-			-	Reg Expr sip.\$1@devconnect.com;t	-	<input type="checkbox"/>	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row	Forward	ENUM	1	Avaya Aura SM	Outbound	Forward	Generic ITSP			-	-		<input type="checkbox"/>	2	Generic ITSP	Inbound	Forward	Avaya Aura SM			-	-		<input type="checkbox"/>	3	WAN	-	Reject	-			-	-		<input type="checkbox"/>	Method	Delete Row	INVITE	<input type="checkbox"/>	OPTIONS	<input type="checkbox"/>	SUBSCRIBE	<input type="checkbox"/>	MESSAGE	<input type="checkbox"/>	REFER	<input type="checkbox"/>	NOTIFY	<input type="checkbox"/>
Name	Use This ...		... Or This	Transport	Network				Delete Row																																																																																																																																																					
	Username	Domain	Reg Expr																																																																																																																																																											
Avaya Aura SM	*	*		TCP	Avaya Aura SM	<input type="checkbox"/>																																																																																																																																																								
Generic ITSP	*	*		TCP	ITSP_IP	<input type="checkbox"/>																																																																																																																																																								
LAN	*	*		TCP	LAN	<input type="checkbox"/>																																																																																																																																																								
WAN	*	*		Any	WAN	<input type="checkbox"/>																																																																																																																																																								
Name	Use This ...				... Or This	Delete Row																																																																																																																																																								
	Prefix	Head	Tail	Min. Tail	Domain																																																																																																																																																									
Inbound			-		Reg Expr sip.(.*)@devconnect.com	<input type="checkbox"/>																																																																																																																																																								
Outbound			-		Reg Expr sip.(.*)@avaya.com	<input type="checkbox"/>																																																																																																																																																								
Name	Subno.	Use This ...		... Or This		... Or This	... Or This	Delete Row																																																																																																																																																						
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk																																																																																																																																																							
Avaya Aura SM	1	-			-	Reg Expr sip.\$1@avaya.com;transp	-	<input type="checkbox"/>																																																																																																																																																						
Generic ITSP	1	-			-	Reg Expr sip.\$1@devconnect.com;t	-	<input type="checkbox"/>																																																																																																																																																						
No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row																																																																																																																																																				
					Forward	ENUM																																																																																																																																																								
1	Avaya Aura SM	Outbound	Forward	Generic ITSP			-	-		<input type="checkbox"/>																																																																																																																																																				
2	Generic ITSP	Inbound	Forward	Avaya Aura SM			-	-		<input type="checkbox"/>																																																																																																																																																				
3	WAN	-	Reject	-			-	-		<input type="checkbox"/>																																																																																																																																																				
Method	Delete Row																																																																																																																																																													
INVITE	<input type="checkbox"/>																																																																																																																																																													
OPTIONS	<input type="checkbox"/>																																																																																																																																																													
SUBSCRIBE	<input type="checkbox"/>																																																																																																																																																													
MESSAGE	<input type="checkbox"/>																																																																																																																																																													
REFER	<input type="checkbox"/>																																																																																																																																																													
NOTIFY	<input type="checkbox"/>																																																																																																																																																													

## 8. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager**→**System Status**→**SIP Entity Monitoring**, and click on the appropriate SIP Entities to verify that the Entity Links to the SIParator and Communication Manager are up.
- From the Communication Manager SAT, use the **status signaling-group x** command to verify that the SIP signaling group is in-service (where **x** is the signaling group number associated with the trunk between Communication Manager and Session Manager).
- From the Communication Manager SAT, use the **status trunk-group y** command to verify that the SIP trunk group is in-service (where **y** is the trunk group number for the trunk between Communication Manager and Session Manager).
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

## 9. Conclusion

The Ingate SIParator passed compliance testing. These Application Notes describe the procedures required to configure the Ingate SIParator to interoperate with Session Manager and Communication Manager to support the network shown in **Figure 1** where Session Manger connects the SIParator to Communication Manager using SIP trunking interface.

## 10. Additional References

- [1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Doc # 555-245-205, August 2010.
- [2] *Administering Avaya Aura® Communication Manager*, Doc # 03-300509, August 2010.
- [3] *Administering Avaya Aura® Session Manager*, Doc # 03-603324, December 2010.
- [4] *Installing and Configuring Avaya Aura® Session Manager*, Doc # 03-603472, January 2011.
- [5] *Ingate SIParator Getting Started Guide*
- [6] *Ingate SIParator Reference Guide*.

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

Product documentation for the SIParator can be obtained from Ingate. Contact Ingate using the “Contact us” link at <http://www.ingate.com>.

---

**©2012 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).