



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Ingate SIParator with Avaya Quick Edition 3.3 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the Ingate SIParator with Avaya Quick Edition.

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 network. The compliance testing focused on telephony scenarios between Avaya Quick Edition IP Telephones at an enterprise site connected via the SIParator to a SIP service provider for external access. The SIParator protects the enterprise site from external SIP-based attacks.

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 Ingate SIParator with Avaya Quick Edition.

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 network. The compliance testing focused on telephony scenarios between Avaya Quick Edition IP Telephones at an enterprise site connected via the SIParator to a SIP service provider for external access. The SIParator protects the enterprise site from external SIP-based attacks.

The focus of the compliance testing was with the Ingate SIParator and not the service provider infrastructure.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows Avaya Quick Edition IP Telephones at an enterprise site connected to a SIP service provider across an untrusted network. The enterprise site has a data firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. Also connected to the edge of the enterprise site is a SIParator SBC. The public side of the SIParator is connected to the untrusted network and the private side is connected to the trusted corporate LAN. The SIParator could also reside in the demilitarized zone (DMZ) of the enterprise but this configuration was not tested.

All SIP traffic between the Avaya Quick Edition IP Telephones and the SIP service provider flows through the SIParator. In this manner, the SIParator can protect the enterprise site's infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. All non-SIP traffic bypasses the SIParator and flows directly between the untrusted network and the private LAN of the enterprise if permitted by the data firewall.

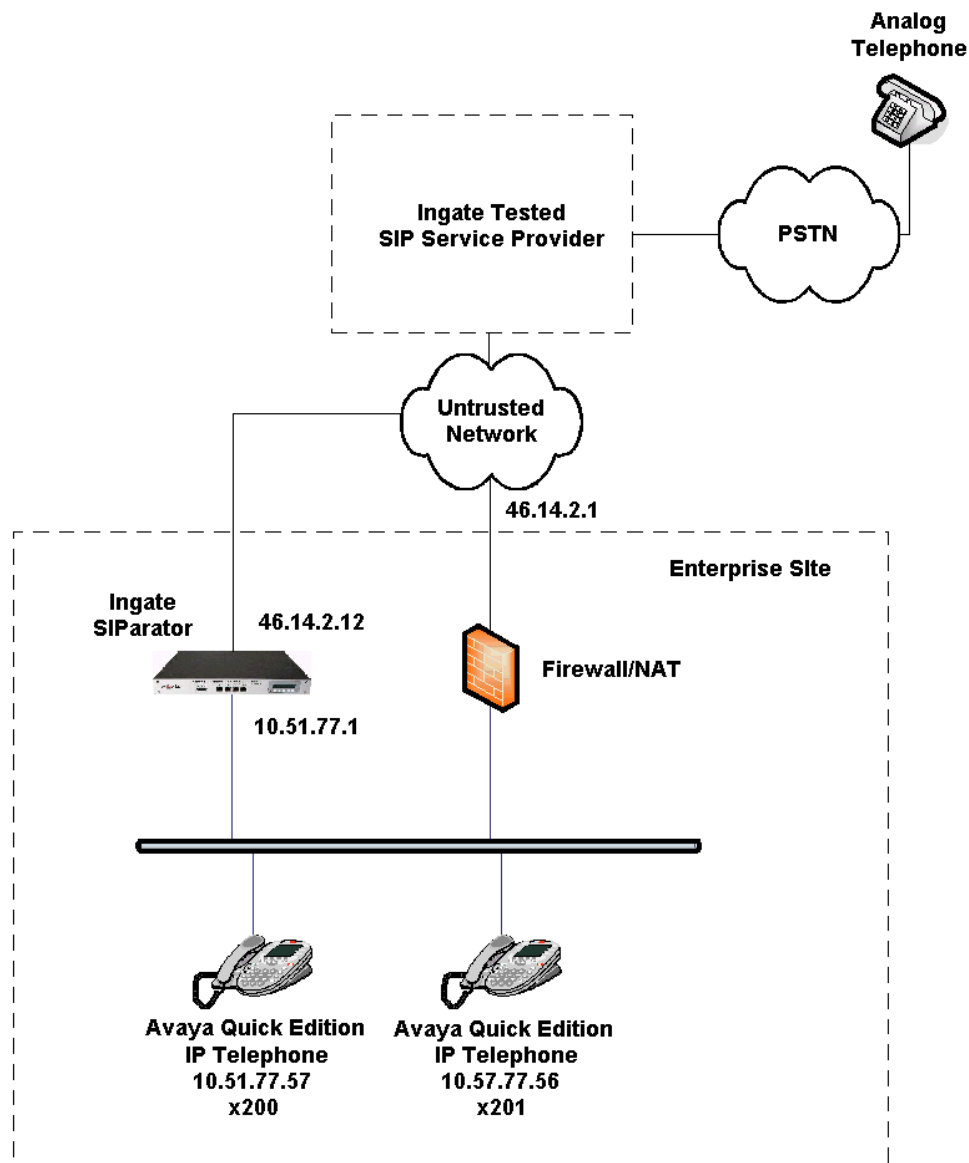


Figure 1: Test Configuration

2. Equipment and Software Validated

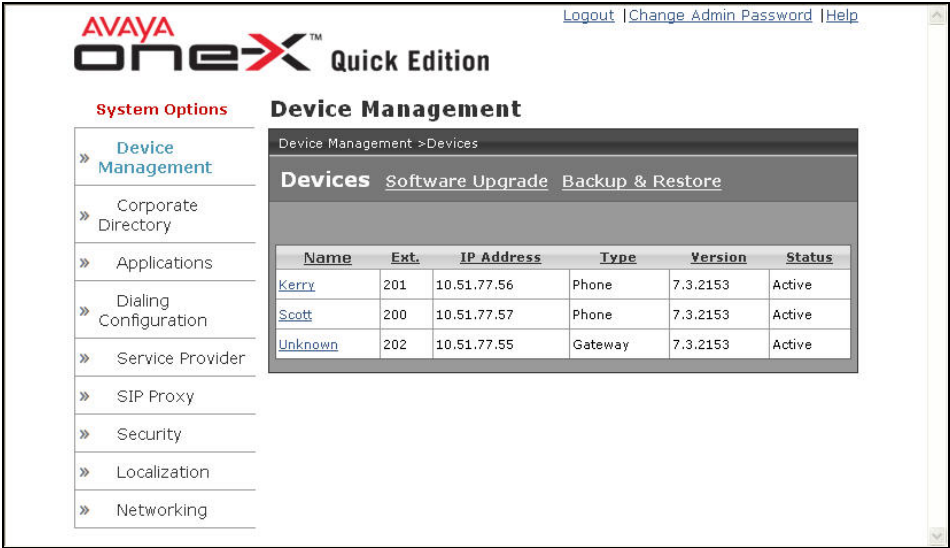
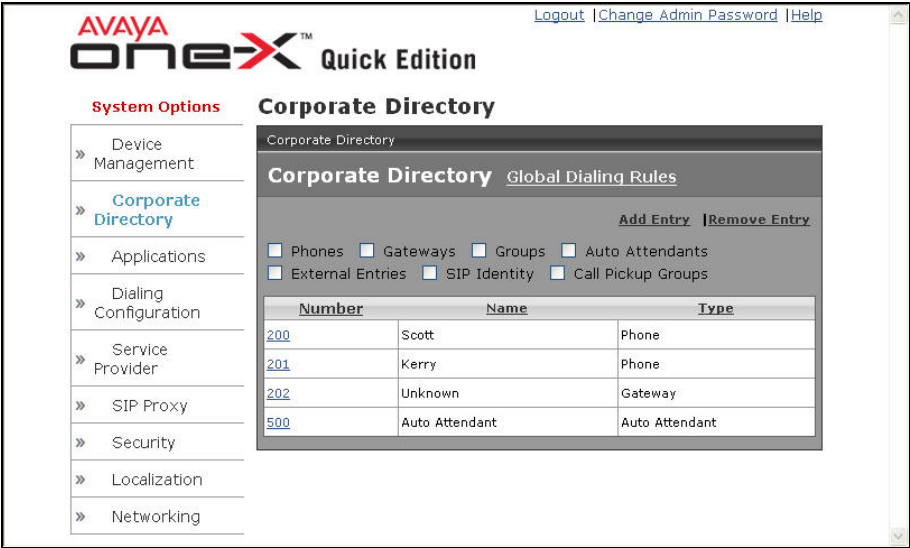
The following equipment and software/firmware were used for the sample configuration:

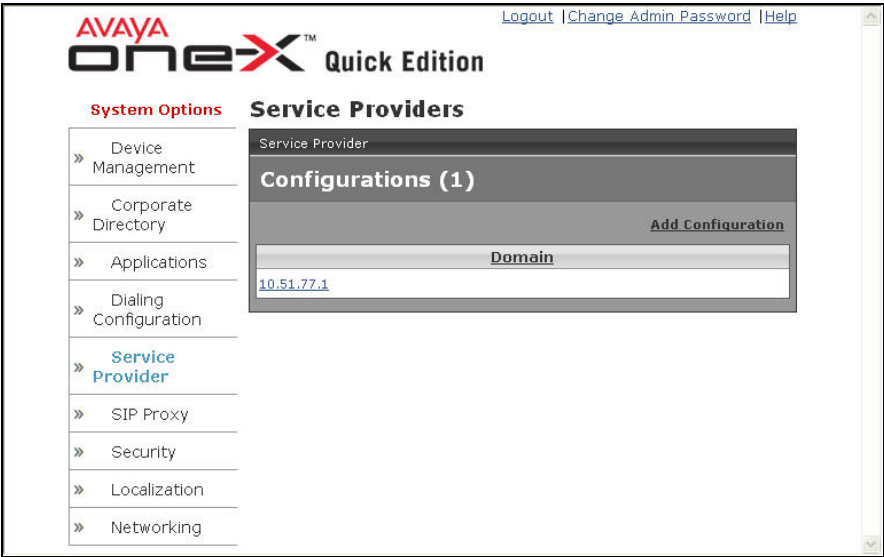
Equipment	Software/Firmware
Avaya Quick Edition IP Telephones	Avaya Quick Edition 3.3
Analog Telephone	-
Ingate SIParator QoS Module (optional)	4.6.2

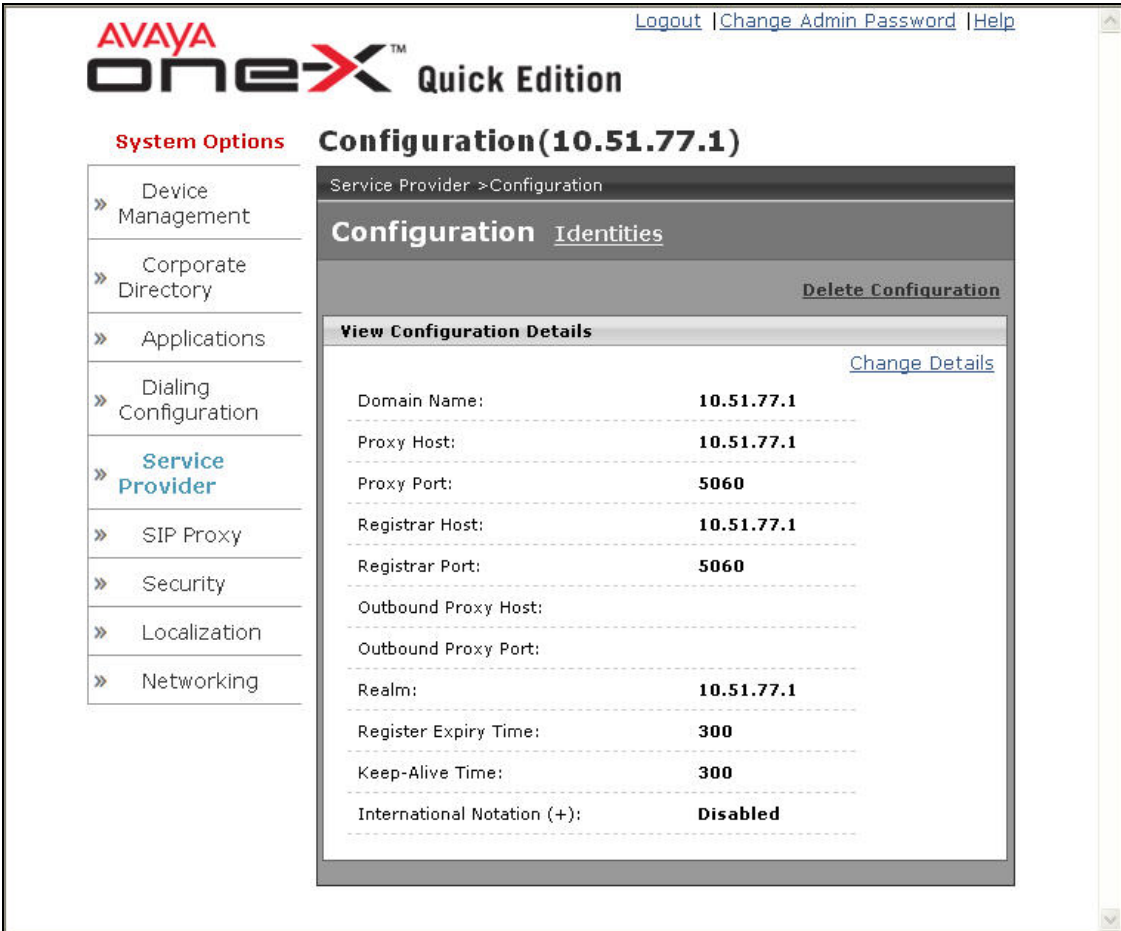
3. Configure Avaya Quick Edition

This section describes the Avaya Quick Edition configuration at the enterprise site to connect to a SIP service provider using the SIParator. It assumes the basic Avaya Quick Edition installation procedures have been performed as described in [1] and [2]. For the purposes of the compliance test, Avaya Quick Edition was configured via the web administration interface. Some of the configuration described below could also be performed from the Avaya Quick Edition IP Telephone interface, refer to [1] for more information on this approach.

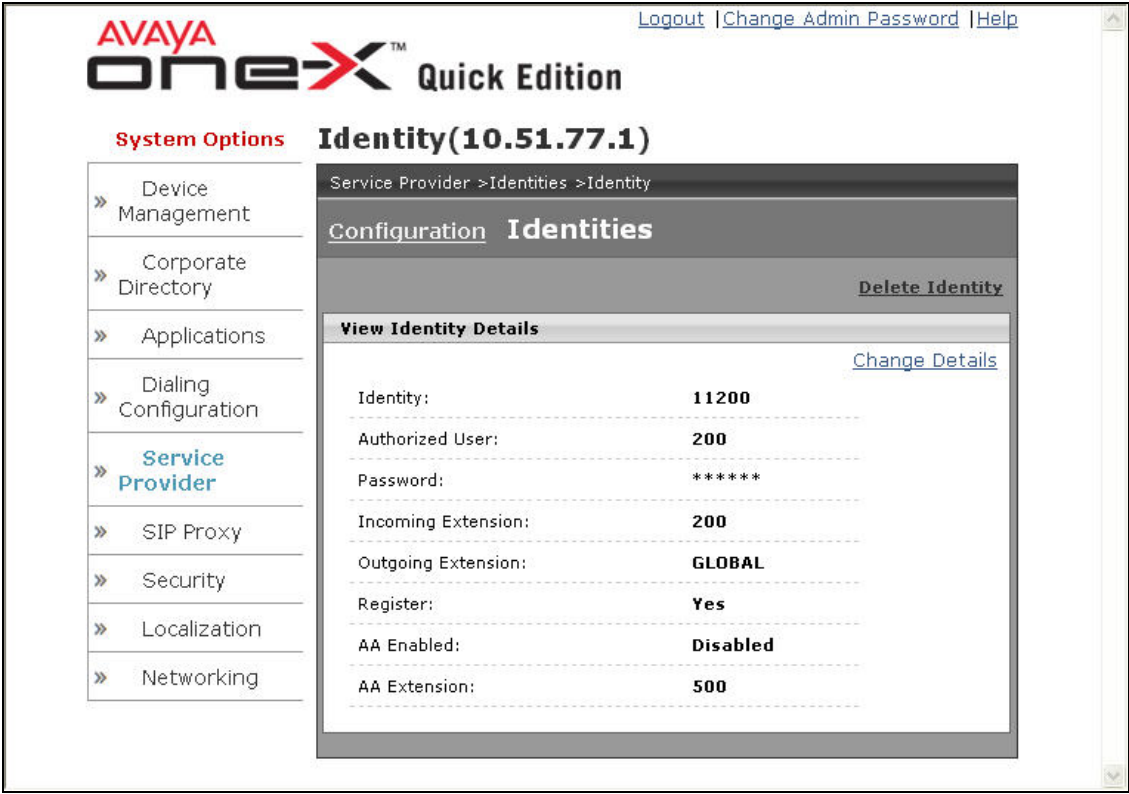
Step	Description
1.	<p>Connect to Avaya Quick Edition</p> <p>The Avaya Quick Edition web administration interface is accessed using a web browser. Enter the IP address of any Avaya Quick Edition IP Telephone in the network in the Address field of the browser. On the login page, click System Options and then enter the administration password when prompted.</p>

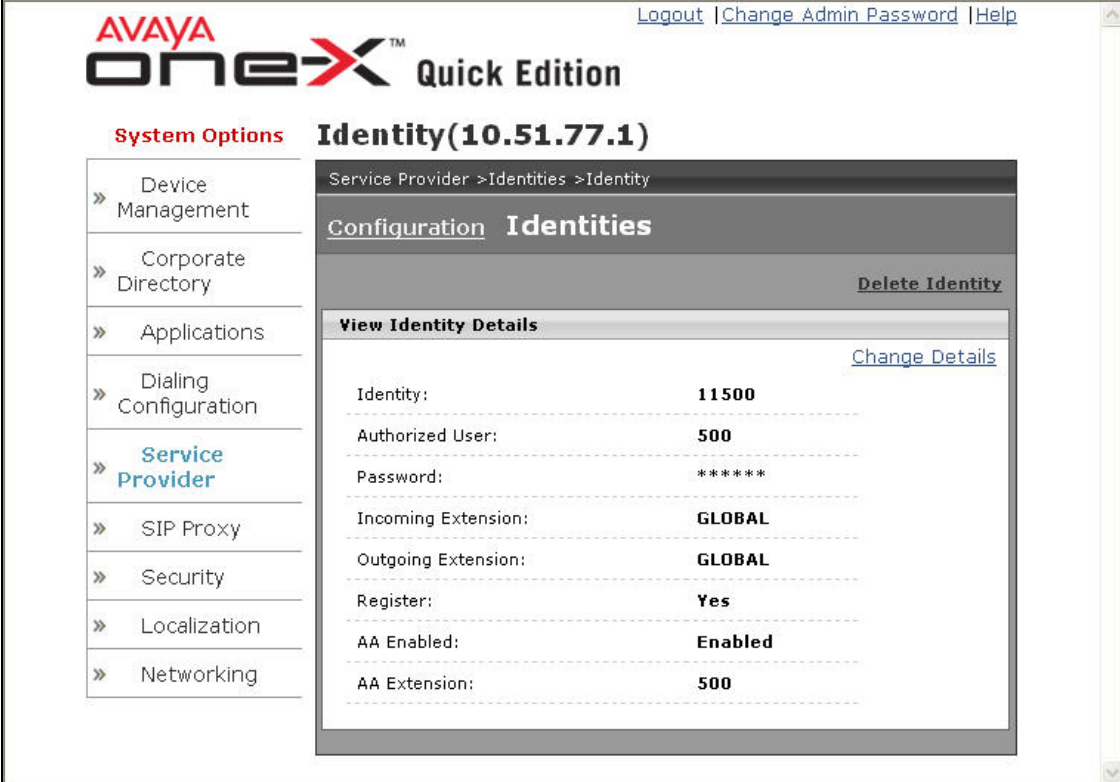
Step	Description
2.	<div><div><div>Device Management</div><div>After login, the Device Management page will appear as shown below. This page shows all the devices in the Avaya Quick Edition network. The gateway shown in the list of devices was not used for the compliance test and is not shown in Figure 1.</div></div><div></div></div>
3.	<div><div><div>Extensions</div><div>As part of the Avaya Quick Edition installation procedures, each Avaya Quick Edition IP Telephone and the Auto Attendant are automatically assigned an extension. To view these extensions, click Corporate Directory in the menu tree on the left side of the window.</div></div><div></div></div>

Step	Description
4.	<p>Service Provider</p> <p>To configure a service provider for the Avaya Quick Edition, click the Service Provider link followed by Add Configuration. The example below shows a configuration with domain name 10.51.77.1 that was created previously and used for the compliance test. To view the details of the configuration, click on the domain name in the table below.</p> 

Step	Description																								
5.	<p>Service Provider - Continued</p> <p>The service provider configuration contains all the operational parameters needed by Avaya Quick Edition to interoperate with the service provider. In the case of the compliance test, the SIParator acts as the service provider for the Avaya Quick Edition. Thus, the Domain Name, Proxy Host, Registrar Host and Realm are all set to the private side IP address of the SIParator. All other parameters can be left at their default values.</p>  <p>The screenshot shows the Avaya One-X Quick Edition web interface. The top navigation bar includes links for Logout, Change Admin Password, and Help. The main header displays the Avaya One-X Quick Edition logo. On the left, a 'System Options' menu lists various configuration areas, with 'Service Provider' highlighted in blue. The main content area is titled 'Configuration (10.51.77.1)' and contains a sub-section for 'Service Provider > Configuration'. This section has tabs for 'Configuration' and 'Identities', with 'Configuration' selected. A 'Delete Configuration' link is visible. Below this, a 'View Configuration Details' section shows a list of configuration parameters and their values:</p> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Domain Name:</td> <td>10.51.77.1</td> </tr> <tr> <td>Proxy Host:</td> <td>10.51.77.1</td> </tr> <tr> <td>Proxy Port:</td> <td>5060</td> </tr> <tr> <td>Registrar Host:</td> <td>10.51.77.1</td> </tr> <tr> <td>Registrar Port:</td> <td>5060</td> </tr> <tr> <td>Outbound Proxy Host:</td> <td></td> </tr> <tr> <td>Outbound Proxy Port:</td> <td></td> </tr> <tr> <td>Realm:</td> <td>10.51.77.1</td> </tr> <tr> <td>Register Expiry Time:</td> <td>300</td> </tr> <tr> <td>Keep-Alive Time:</td> <td>300</td> </tr> <tr> <td>International Notation (+):</td> <td>Disabled</td> </tr> </tbody> </table>	Parameter	Value	Domain Name:	10.51.77.1	Proxy Host:	10.51.77.1	Proxy Port:	5060	Registrar Host:	10.51.77.1	Registrar Port:	5060	Outbound Proxy Host:		Outbound Proxy Port:		Realm:	10.51.77.1	Register Expiry Time:	300	Keep-Alive Time:	300	International Notation (+):	Disabled
Parameter	Value																								
Domain Name:	10.51.77.1																								
Proxy Host:	10.51.77.1																								
Proxy Port:	5060																								
Registrar Host:	10.51.77.1																								
Registrar Port:	5060																								
Outbound Proxy Host:																									
Outbound Proxy Port:																									
Realm:	10.51.77.1																								
Register Expiry Time:	300																								
Keep-Alive Time:	300																								
International Notation (+):	Disabled																								

Step	Description																
6.	<p>Service Provider Identities</p> <p>Service Provider identities represent the users that Avaya Quick Edition will register with the service provider (in this case the SIParator). Navigate to Service Provider → Identities to view the existing identities. To create a new identity, click Add Identity.</p> <p>The example below shows the three identities created for the compliance test that will register to the SIParator. One for each of the two Avaya Quick Edition IP Telephones and one for the automated attendant. To view the details of an identity, click on the identity in the table below.</p> <div><div><div>AVAYA oneX™ Quick Edition</div><div><div>System Options</div><div><div>» Device Management</div><div>» Corporate Directory</div><div>» Applications</div><div>» Dialing Configuration</div><div>» Service Provider</div><div>» SIP Proxy</div><div>» Security</div><div>» Localization</div><div>» Networking</div></div></div><div><div>Identities(10.51.77.1)</div><div><div>Service Provider >Identities</div><div><div>Configuration</div><div>Identities</div><div>Add Identity</div><table><thead><tr><th>Identity</th><th>Incoming Extension</th><th>Outgoing Extension</th><th>Register</th></tr></thead><tbody><tr><td>11200</td><td>200</td><td>GLOBAL</td><td>Yes</td></tr><tr><td>11201</td><td>201</td><td>GLOBAL</td><td>Yes</td></tr><tr><td>11500</td><td>GLOBAL</td><td>GLOBAL</td><td>Yes</td></tr></tbody></table></div></div></div></div></div>	Identity	Incoming Extension	Outgoing Extension	Register	11200	200	GLOBAL	Yes	11201	201	GLOBAL	Yes	11500	GLOBAL	GLOBAL	Yes
Identity	Incoming Extension	Outgoing Extension	Register														
11200	200	GLOBAL	Yes														
11201	201	GLOBAL	Yes														
11500	GLOBAL	GLOBAL	Yes														

Step	Description																		
7.	<p>Service Provider Identities - Continued</p> <p>The example below shows the identity details for extension 200. The Identity field must match a value in the range specified in Section 4, Step 7, Advanced: DID – Mapping to Local user section. The Authorized User is set to the user extension. Enter a password in the Password field. For simplicity in configuring the SIParator with the Start-up Tool, enter the same password for each identity (Section 4, Step 7). In the Incoming Extension field, select an extension that will map to this identity. Set the AA Extension to the extension of the automated attendant. Leave the default values in the remaining fields. Repeat this step for each of the Avaya Quick Edition IP Telephone extensions.</p>  <p>The screenshot displays the Avaya One-X Quick Edition web interface. On the left, a sidebar lists 'System Options' including Device Management, Corporate Directory, Applications, Dialing Configuration, Service Provider (highlighted), SIP Proxy, Security, Localization, and Networking. The main content area is titled 'Identity(10.51.77.1)' and contains a 'Configuration Identities' section. Within this section, there is a 'View Identity Details' table with the following data:</p> <table border="1"> <thead> <tr> <th colspan="2">View Identity Details</th> </tr> </thead> <tbody> <tr> <td>Identity:</td> <td>11200</td> </tr> <tr> <td>Authorized User:</td> <td>200</td> </tr> <tr> <td>Password:</td> <td>*****</td> </tr> <tr> <td>Incoming Extension:</td> <td>200</td> </tr> <tr> <td>Outgoing Extension:</td> <td>GLOBAL</td> </tr> <tr> <td>Register:</td> <td>Yes</td> </tr> <tr> <td>AA Enabled:</td> <td>Disabled</td> </tr> <tr> <td>AA Extension:</td> <td>500</td> </tr> </tbody> </table>	View Identity Details		Identity:	11200	Authorized User:	200	Password:	*****	Incoming Extension:	200	Outgoing Extension:	GLOBAL	Register:	Yes	AA Enabled:	Disabled	AA Extension:	500
View Identity Details																			
Identity:	11200																		
Authorized User:	200																		
Password:	*****																		
Incoming Extension:	200																		
Outgoing Extension:	GLOBAL																		
Register:	Yes																		
AA Enabled:	Disabled																		
AA Extension:	500																		

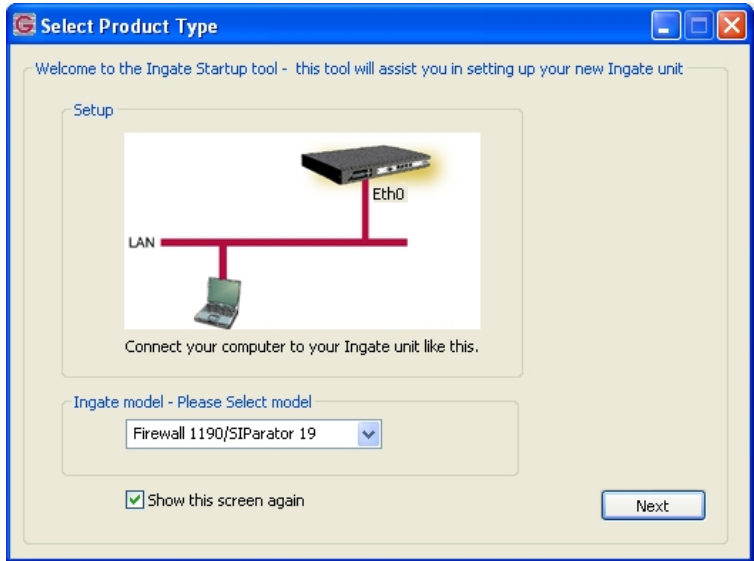
Step	Description																		
8.	<p>Service Provider Identities - Continued</p> <p>The following identity for the automated attendant was created in the same manner as the identities for the telephone extensions with the exception that the AA Enabled field was set to <i>Enabled</i>.</p>  <p>The screenshot displays the Avaya One-X Quick Edition web interface. On the left, a sidebar lists 'System Options' including Device Management, Corporate Directory, Applications, Dialing Configuration, Service Provider (highlighted), SIP Proxy, Security, Localization, and Networking. The main content area shows the 'Configuration' and 'Identities' tabs, with 'Identities' selected. A 'View Identity Details' section displays the following information:</p> <table border="1"> <thead> <tr> <th colspan="2">View Identity Details</th> </tr> </thead> <tbody> <tr> <td>Identity:</td> <td>11500</td> </tr> <tr> <td>Authorized User:</td> <td>500</td> </tr> <tr> <td>Password:</td> <td>*****</td> </tr> <tr> <td>Incoming Extension:</td> <td>GLOBAL</td> </tr> <tr> <td>Outgoing Extension:</td> <td>GLOBAL</td> </tr> <tr> <td>Register:</td> <td>Yes</td> </tr> <tr> <td>AA Enabled:</td> <td>Enabled</td> </tr> <tr> <td>AA Extension:</td> <td>500</td> </tr> </tbody> </table>	View Identity Details		Identity:	11500	Authorized User:	500	Password:	*****	Incoming Extension:	GLOBAL	Outgoing Extension:	GLOBAL	Register:	Yes	AA Enabled:	Enabled	AA Extension:	500
View Identity Details																			
Identity:	11500																		
Authorized User:	500																		
Password:	*****																		
Incoming Extension:	GLOBAL																		
Outgoing Extension:	GLOBAL																		
Register:	Yes																		
AA Enabled:	Enabled																		
AA Extension:	500																		

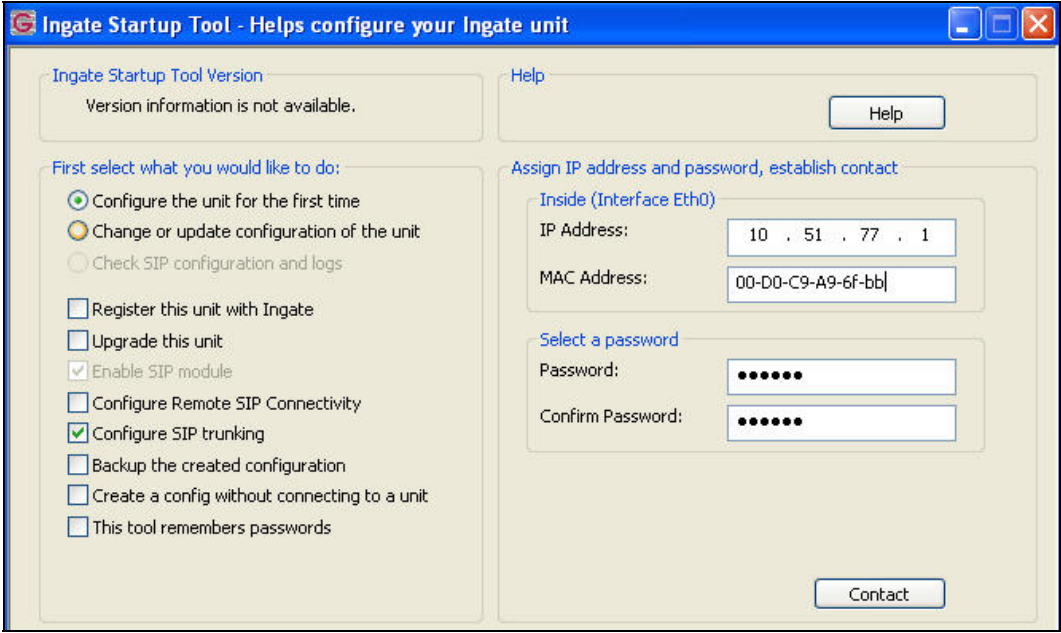
4. Configure the Ingate SIParator

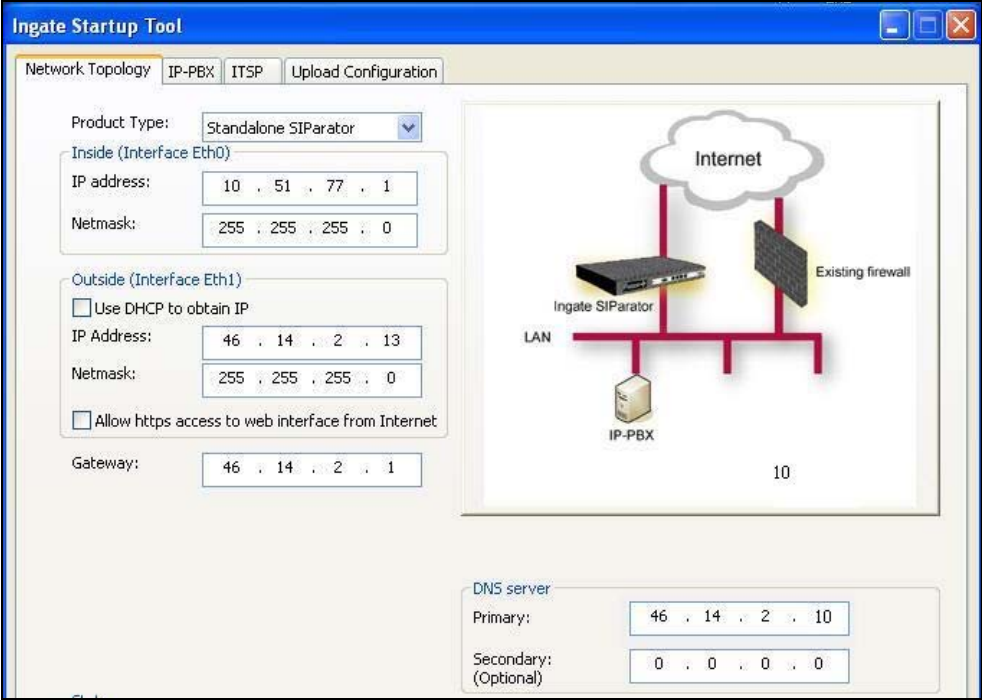
This section describes the configuration of the Ingate SIParator. To support the setting of the Differentiated Services Code Point (DSCP) bits for quality of service, the QoS module must be installed and requires additional licensing.

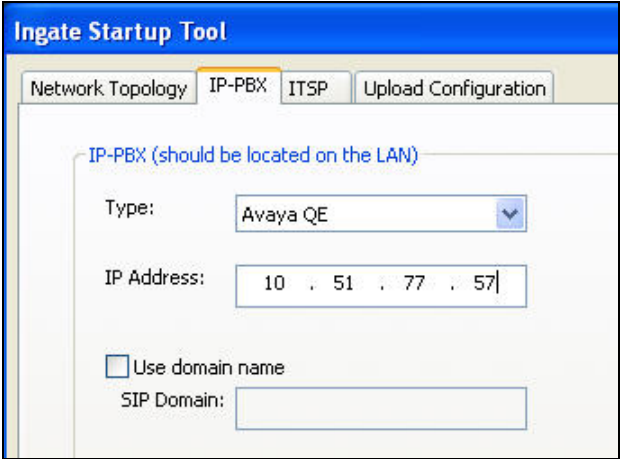
The SIParator is configured initially with the Ingate Startup Tool. Based on the provided input, the Startup Tool will create an initial configuration that can be uploaded to the SIParator. Much of the detailed SIP configuration is not visible from the Startup Tool but is driven by the type of IP-PBX and Service Provider chosen in the Startup Tool. The results of the configuration can 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.

For more details on configuring the SIParator with Avaya Quick Edition in different network configurations or with different service provider options, refer to [5].

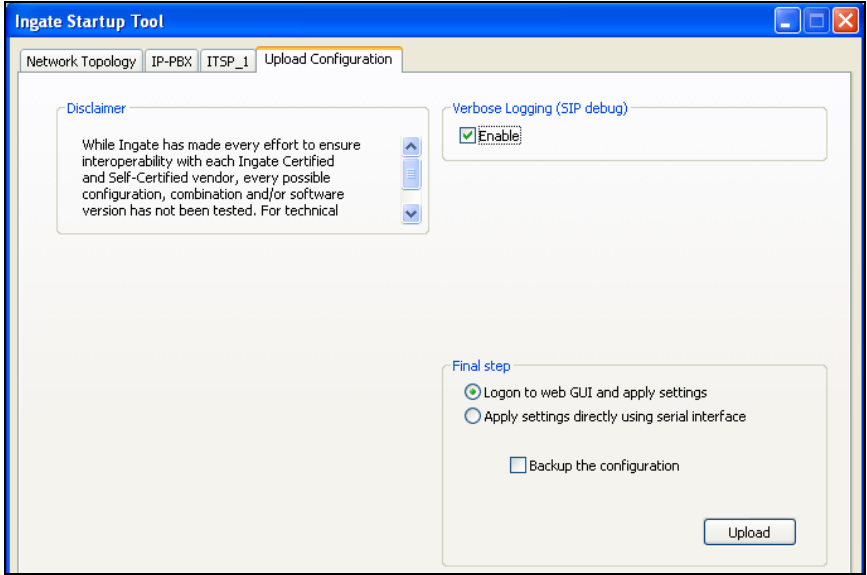
Step	Description
1.	Launch Startup Tool The Ingate Startup Tool is a Windows application which is launched from the Windows Start Menu by navigating to Start→All Programs→Shortcut to StartupTool.exe .
2.	Select Product Type The initial Ingate Startup Tool screen is shown below. Verify the PC is running 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 Ingate model drop-down menu. Click the Next button. 

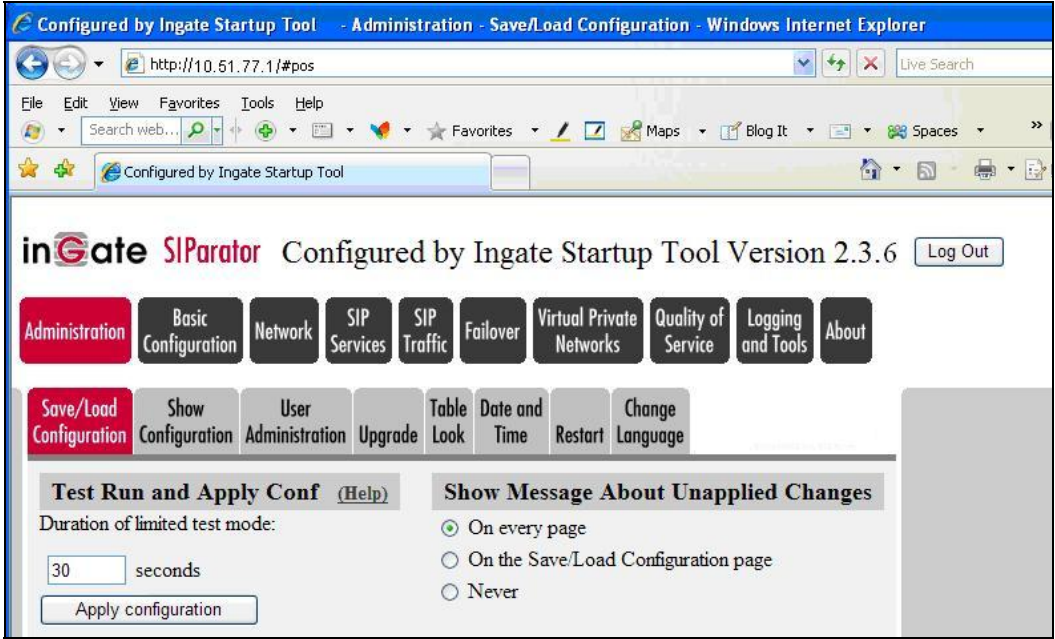
Step	Description
3.	<p>Select Configuration Options and Assign Private IP</p> <p>Select options for Configure the unit for the first time and Configure SIP trunking. Enter the inside IP address, MAC address and a password. Click the Contact button to establish a connection to the SIParator. For future updates, click the option - Change or update configuration of the unit.</p> 

Step	Description
4.	<p>Network Topology</p> <p>After connecting to the SIParator, the following page appears. Select the Network Topology tab. Select <i>Standalone SIParator</i> from the Product Type drop-down menu. Enter an IP address and subnet mask for both the inside and outside interfaces as shown in Figure 1. The Gateway field is set to the IP address of the default gateway on the public side of the SIParator. The primary DNS server can be set to an external WAN address (as provided by an Internet Service Provider (ISP)) or an internal LAN address of a corporate DNS server. The example below shows the DNS server set to an external WAN address.</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 10.51.77.1 and a netmask of 255.255.255.0. The 'Outside (Interface Eth1)' section has an IP address of 46.14.2.13, a netmask of 255.255.255.0, and a gateway of 46.14.2.1. The 'DNS server' section has a primary address of 46.14.2.10 and a secondary (optional) address of 0.0.0.0. A network diagram on the right shows the SIParator connected to the Internet, LAN, and IP-PBX.</p>

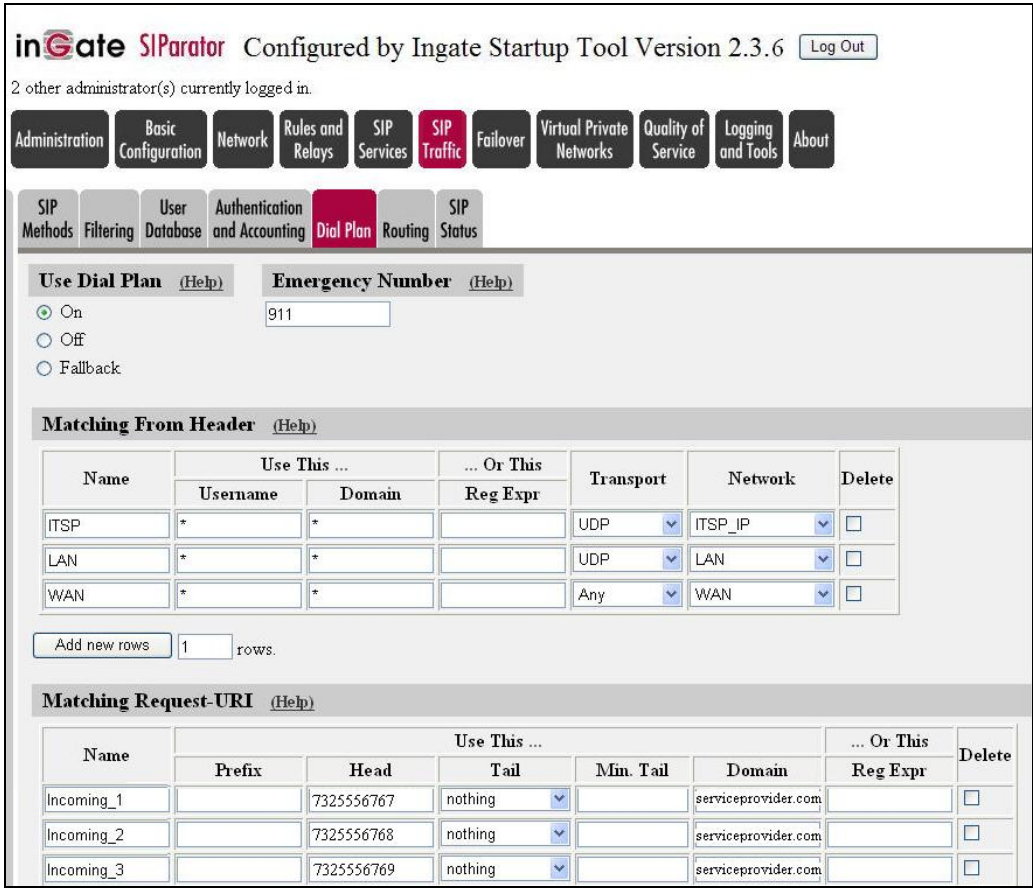
Step	Description
5.	<p>IP-PBX Settings</p> <p>Select the IP-PBX tab. Select <i>Avaya QE</i> from the Type drop-down menu. This will instruct the Startup Tool to configure the SIP parameters on the internal interface to be compatible with Avaya Quick Edition. Enter the IP address of any Avaya Quick Edition IP Telephone in the network in the IP Address field.</p> 

Step	Description
6.	<p>Service Provider Settings</p> <p>Select the ITSP_1 tab. This tab contains the configuration necessary for the SIParator to interoperate with the SIP service provider providing PSTN access. Select the specific SIP service provider being used from the Name drop-down menu. Ingate has confirmed interoperability with many leading SIP service providers. For the purposes of these Application Notes, the actual name of the SIP service provider used is not shown. Instead, the example below shows Generic ITSP in the Name field.</p> <p>Enter the first number of the DID range assigned to the enterprise site by the service provider in the DID/User name field.</p> <p>If the service provider requires the SIParator to register, then check the Use Account box and fill in the Account information as supplied by the service provider. In the case of the compliance test, the service provider required registration so a Domain and Password were entered as shown below. Alternatively, if the service provider does not require registration, then leave the Use Account box unchecked and enter the service provider SIP proxy IP address and optionally the domain name under the Provider Address section.</p> <p>Configuration of the ITSP_1 tab continues in the next step.</p>

Step	Description
7.	<p>Service Provider Settings – Continued</p> <p>Lastly, under the Advanced: DID – Mapping to Local user section (shown in Step 6), enter the number of DID numbers to be mapped to sequential local users in the DID range size field. Enter the first SIP identity from the range of identities shown in Section 3, Step 6 in the Local phone numbers field. Enter the password for this identity in the Password field. The same password will be used for each local number and must match the password used for each Avaya QE SIP identity in Section 3, Step 7. The SIParator will use this information to map each DID number to a SIP user beginning at the top of the DID range and assigning numbers to SIP users in succession. Since the default automated attendant extension (x500) is not sequential with the other users, it must be added manually after the Startup Tool configuration is completed. See Step 10.</p>
8.	<p>Upload Configuration</p> <p>Select the Upload Configuration tab to upload the configuration to the SIParator. Click the Upload button to begin the upload.</p> 

Step	Description
9.	<p>Apply Configuration</p> <p>After uploading the configuration, the Startup Tool opens a web browser to the Administration→Save/Load Configuration page of the SIParator. Click the Apply configuration 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																								
10.	<p>SIP User – Automated Attendant</p> <p>All users with sequential extensions were created automatically by the Start-up Tool in Step 7. Since the automated attendant did not have a sequential extension it must be created manually. To create the user for the automated attendant, navigate to SIP Traffic → User Database on the SIParator web interface.</p> <p>In the example below, the first two entries for Username 11200 and 11201 were created by the Start-up Tool. The third entry was created manually by clicking the Add new rows button and entering a Username of 11500 and Authentication Name as 500. All other values are the same as the other users.</p> <div><div><div><div><div>inGate SIParator</div><div>Configured by Ingate Startup Tool Version</div></div><div>1 other administrator(s) currently logged in.</div><div><div>Administration</div><div>Basic Configuration</div><div>Network</div><div>Rules and Relays</div><div>SIP Services</div><div>SIP Traffic</div><div>Failover</div><div>Virtual Private Networks</div><div>Quality of Service</div></div><div><div>SIP Methods</div><div>Filtering</div><div>User Database</div><div>Authentication and Accounting</div><div>Dial Plan</div><div>Routing</div><div>SIP Status</div></div><div><div>Local SIP Domains</div><div>(Help)</div></div><div><div>Domain</div><div>10.51.77.1</div><div>Add new rows</div><div>1</div><div>rows.</div></div><div><div>Local SIP User Database</div><div>(Help)</div></div><div><table><thead><tr><th>Username</th><th>Domain</th><th>Authentication Name</th><th>Password</th><th>Account Type</th><th>Register From</th></tr></thead><tbody><tr><td>11200</td><td>10.51.77.1</td><td>200</td><td></td><td>User</td><td>LAN</td></tr><tr><td>11201</td><td>10.51.77.1</td><td>201</td><td></td><td>User</td><td>LAN</td></tr><tr><td>11500</td><td>10.51.77.1</td><td>500</td><td></td><td>User</td><td>LAN</td></tr></tbody></table></div></div></div></div>	Username	Domain	Authentication Name	Password	Account Type	Register From	11200	10.51.77.1	200		User	LAN	11201	10.51.77.1	201		User	LAN	11500	10.51.77.1	500		User	LAN
Username	Domain	Authentication Name	Password	Account Type	Register From																				
11200	10.51.77.1	200		User	LAN																				
11201	10.51.77.1	201		User	LAN																				
11500	10.51.77.1	500		User	LAN																				

Step	Description
11.	<p>SIP Dial Plan</p> <p>The mapping of DID numbers to local users is also done automatically by the Start-up Tool for sequential extensions, but must be done manually for non-sequential extensions like the automated attendant. To map a DID number to the automated attendant, navigate to SIP Traffic → SIP Dial Plan.</p> <p>The mapping is comprised of several parts. First, an entry must be created in the Matching Request-URI table. The first two entries were created by the Start-up Tool. The third was created manually by clicking the Add new rows button below the table (not shown). The third entry defines a name Incoming_3 that corresponds to a Request-URI containing 7325556769@serviceprovider.com. The number 7325556769 was the next available DID number assigned to the enterprise by the service provider.</p> 

Step

Description

12.

SIP Dial Plan - Continued

The next part needed in creating the DID mapping is an entry in the **Forward To** table. On the **SIP Traffic → Dial Plan** page shown in **Step 11**, scroll down to the **Forward To** table. The first two entries in the table were created by the Start-up Tool. The third was created manually by clicking the **Add new rows** button below the table (not shown). The third entry defines a name *Avaya_AutoAtt* that corresponds to a SIP contact of sip:11500@10.51.77.1.

Forward To (Help)

Name	Subno.	Use This Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
+ Avaya_4610	1	-			-	sip:11201@10.51	<input type="checkbox"/>
+ Avaya_4621	1	-			-	sip:11200@10.51	<input type="checkbox"/>
+ Avaya_AutoAtt	1	-			-	sip:11500@10.51	<input type="checkbox"/>

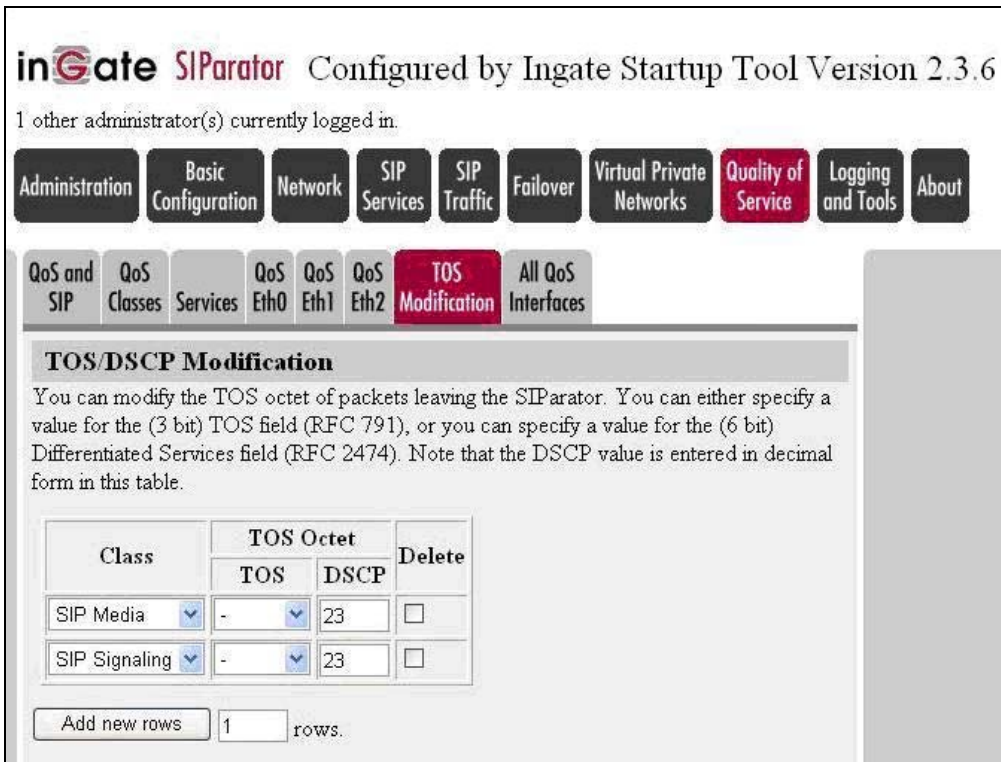
13.

SIP Dial Plan - Continued

Lastly, to complete the mapping an entry is required in the Dial Plan. On the **SIP Traffic → Dial Plan** page shown in **Step 11**, scroll down to the **Dial Plan** section. The first two entries in the table were created by the Start-up Tool. The third was created manually by clicking the **Add new rows** button below the table (not shown). The third entry defines a route that forwards call from the **WAN** with a **Request-URI** that matches *Incoming_3* to the **Forward To** destination known as *Avaya_AutoAtt*.

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM R.
					Forward	ENUM	
1	WAN	Incoming_1	Forward	Avaya_4610			-
2	WAN	Incoming_2	Forward	Avaya_4621			-
3	WAN	Incoming_3	Forward	Avaya_AutoAtt			-

Step	Description
14.	<p>Quality of Service</p> <p>In order to set the Type of Service (TOS) or DSCP bits, the optional QoS module must first be installed. To set the values for these bits, navigate to Quality of Service→TOS modification. In the case of the compliance test, both the SIP media and SIP signaling packets were marked with a DSCP value of 23 (decimal).</p> 
15.	<p>Apply Configuration</p> <p>Repeat Step 9 to apply the manual configuration changes made in Steps 10 – 14.</p>

5. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of the Ingate SIParator with Avaya Quick Edition. This section covers the general test approach and the test results.

5.1. General Test Approach

The general test approach was to make calls between Avaya Quick Edition and the PSTN routed through the SIParator and the SIP service provider using various codec settings and exercising common telephony features.

5.2. Test Results

The SIParator passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Successful registrations of the Avaya Quick Edition IP Telephones with the SIParator.
- Calls between the Avaya Quick Edition and the PSTN.
- G.711MU and G.729AB codec support.
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- Telephony features including Hold, Transfer, Call Forwarding, Conference and Automated Attendant.
- Proper system recovery after a SIParator restart and loss of IP connection.

6. Verification Steps

The following steps may be used to verify the configuration:

- Verify that calls can be placed between the Avaya Quick Edition and the PSTN.

7. Support

For technical support on the SIParator, contact Ingate via the support link at www.ingate.com.

8. Conclusion

The Ingate SIParator passed compliance testing. These Application Notes describe the procedures required to configure the Ingate SIParator to interoperate with Avaya Quick Edition to connect to a SIP service provider as shown in **Figure 1**.

9. Additional References

- [1] *Avaya Quick Edition IP Telephone Safety and Installation Instructions*, Doc # 16-601408, Issue 5, January 2008.
- [2] *Avaya Quick Edition Release 3.3 System Administration Guide*, Doc # 16-601412, Issue 4, April 2008.
- [3] *Ingate SIParator Getting Started Guide*.
- [4] *Ingate SIParator Reference Guide*.
- [5] *Ingate Application Note Avaya QE – Configuration Guide*, July 17, 2008.

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 link at <http://www.ingate.com>.

©2008 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.