

Application Note

Avaya QE - Configuration Guide

17 July 2008

Avaya QE - Configuration Guide

Table of Contents

1	AVAYA QUICK EDITION AND INGATE PRODUCTS	1
2	CONNECTING THE INGATE FIREWALL/SIPARATOR	2
3	USING THE STARTUP TOOL	4
	 3.1 CONFIGURE THE UNIT FOR THE FIRST TIME	
4	3.6 UPLOAD CONFIGURATION AVAYA OUICK EDITION SETUP	
	4.1 Device Management	
5	TROUBLESHOOTING	
	 5.1 AVAYA QE IDENTITY REGISTRATION INFORMATION 5.2 REGISTRATION STATUS 5.3 INCOMING ROUTING 	

Tested versions:

Ingate Firewall and SIParator version 4.6.2 Startup Tool version 2.4.0

Revision History:

Revision	Date	Author	Comments
	2008-07-17	Scott Beer	1 st draft

1 Avaya Quick Edition and Ingate Products

The Ingate Startup Tool is an installation tool for Ingate Firewall® and Ingate SIParator® products using the Ingate SIP Trunking module or the Remote SIP Connectivity module, which facilitates the setup of complete SIP Trunking solutions or remote user solutions.

The Startup Tool is designed to simplify the initial "out of the box" commissioning and programming of the Network Topology, SIP Trunk deployments and Remote User deployments. The tool will automatically configure a user's Ingate Firewall or SIParator to work with the Avaya QE as the IP-PBX and a SIP Trunking service provider of your choice, and sets up all the routing needed to enable remote users to access and use the Avaya QE solution. Thanks to detailed interoperability testing, Ingate has been able to create this tool with pre-configured set ups for the Avaya QE and various ITSPs.

Download Free of Charge: The Startup Tool is free of charge for all Ingate Firewalls and SIParators. Get the latest version of the Startup Tool at http://www.ingate.com/startuptool.php

Avaya Quick Edition is a simple yet sophisticated phone system for small businesses or small branch offices of enterprises. It delivers big business communications capabilities - including a host of call handling and mobility features, voicemail, and auto attendants - to help small offices work more efficiently and serve customers better. With Quick Edition, all the intelligence is built into the phones, simplifying set-up and ongoing management.

Look for the Avaya ONE-X Quick Edition Icon

to focus your attention to specific Avaya QE setup instructions. These instructions are specific to the Ingate & Avaya QE deployment.



2 Connecting the Ingate Firewall/SIParator

From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

The following will describe a process to connect the Ingate unit to the network then have the Ingate Startup Tool assign an IP Address and Password to the Unit.

Configuration Steps:

- 1) Connect Power to the Unit.
- 2) Connect an Ethernet cable to "Eth0". This Ethernet cable should connect to a LAN network. Below are some illustrations of where "Eth0" are located on each of the Ingate Model types. On SIParator SBE connect to "ET1".

Ingate SIParator SBE (Back)



Ingate 1190 Firewall and SIParator 19 (Back)



Ingate 1500/1550/1650 Firewall and SIParator 50/55/65



Ingate 1900 Firewall and SIParator 90



3) The PC/Server with the Startup Tool should be located on the same LAN segment/subnet. Preferably the Ingate unit and the Startup Tool are on the same LAN Subnet to which you are going to assign an IP Address to the Ingate Unit. Note: When configuring the unit for the first time, avoid having the Startup Tool on a PC/Server on a different Subnet, or across a Router, or NAT device, Tagged VLAN, or VPN Tunnel.



4) Proceed to Section 4: Using the Startup Tool for instructions on using the Startup Tool.

3 Using the Startup Tool

There are three main reasons for using the Ingate Startup Tool. First, the "Out of the Box" configuring the Ingate Unit for the first time. Second, is to change or update an existing configuration. Third, is to register the unit, install a License Key, and upgrade the unit to the latest software.

3.1 Configure the Unit for the First Time

From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

In the Startup Tool, when selecting "Configure the unit for the first time", the Startup Tool will find the Ingate Unit on the network and assign an IP Address and Password to the Ingate unit. This procedure only needs to be done ONCE. When completed, the Ingate unit will have an IP Address and Password assigned.

Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: "Change or Update Configuration".

Configuration Steps:

- 1) Launch the Startup Tool
- 2) Select the Model type of the Ingate Unit, and then click Next.



3) In the "Select first what you would like to do", select "Configure the unit for the first time".

ingate Startup Tool Version	Help	
You are running the latest version of this tool.	Help	
irst select what you would like to do: • Configure the unit for the first time • Change or update configuration of the unit • Check SIP configuration and logs • Register this unit with Ingate • Upgrade this unit • Enable SIP module • Configure Remote SIP Connectivity • Configure SIP trunking • Backup the created configuration • Create a config without connecting to a unit • This tool remembers passwords	Assign IP address and password, establish contact Inside (Interface Eth0) IP Address: 10 . 51 . 77 . 100 MAC Address: 00-d0-c9-a2-44-55 Select a password Password: Confirm Password: ••••••	
Ingate Startup Tool Version 2.4.0 Startup tool version available on the Ingate web: 2. You are running the latest version of the Startup to More information is available here: http://www.inga	Contact .4.0 vol. ate. com/startuptool.php	

4) Other Options in the "Select first what you would like to do",

First select what you would like to do:
 Configure the unit for the first time
Change or update configuration of the unit
Check SIP configuration and logs
Register this unit with Ingate
Upgrade this unit
Enable SIP module
Configure Remote SIP Connectivity
Configure SIP trunking
Backup the created configuration
Create a config without connecting to a unit
This tool remembers passwords

- a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
- b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

- c. Select "Register this unit with Ingate" if you want the tool to connect with <u>www.ingate.com</u> to register the unit. If selected, see Section 4.3: Licenses and Upgrades.
- d. Select "Upgrade this unit" if you want the tool to connect with <u>www.ingate.com</u> to download the latest software release and upgrade the unit. If selected, see Section 4.3: Licenses and Upgrades.
- e. Select "Backup the created configuration" if you want the tool to apply the settings to an Ingate unit and save the config file.
- f. Select "Creating a config without connecting to a unit" if you want the tool to just create a config file.
- g. Select "The tool remembers passwords" if you want the tool to remember the passwords for the Ingate unit.
- 5) In the "Inside (Interface Eth0)",
 - a. Enter the IP Address to be assigned to the Ingate Unit.
 - b. Enter the MAC Address of the Ingate Unit, this MAC Address will be used to find the unit on the network.

-Inside (Interface Eth0) -	
IP Address:	10 . 51 . 77 . 100
MAC Address:	00-D0-C9-A2-44-55

6) In the "Select a Password", enter the Password to be assigned to the Ingate unit.

Select a password	
Password:	••••
Confirm Password:	••••

7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool find the Ingate unit on the network, assign the IP Address and Password.

IP Address:	10 . 51 . 77 . 100
MAC Address:	00-D0-C9-A2-44-55
Select a password	
Password:	•••••
Confirm Password:	

8) Proceed to Section 4.4: Network Topology.

3.2 Change or Update Configuration

The "Change or update configuration of the unit" setting in the Startup Tool, the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

In the Startup Tool, when selecting "Change or update configuration of the unit", the Startup Tool will connect directly with the Ingate Unit on the network with the provided IP Address and Password. When completed, the Startup Tool will completely overwrite the existing configuration in the Ingate unit with the new settings.

Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: "Configure the Unit for the First Time".

Configuration Steps:

- 1) Launch the Startup Tool
- 2) Select the Model type of the Ingate Unit, and then click Next.



3) In the "Select first what you would like to do", select "Change or update configuration of the unit".

ngate Startup Tool Version You are running the latest version of this tool.	Help	Help
irst select what you would like to do: Configure the unit for the first time Change or update configuration of the unit Check SIP configuration and logs Register this unit with Ingate Upgrade this unit Configure Remote SIP Connectivity Configure SIP trunking Backup the created configuration Create a config without connecting to a unit This tool remembers passwords	Establish contact Inside (Interface Eth0) IP Address: Enter the password Password:	10 . 51 . 77 . 100
Ingate Startup Tool Version 2.4.0 Startup tool version available on the Ingate web: 2. You are running the latest version of the Startup too More information is available here: http://www.ingai	4.0 ol. te.com/startuptool.php	

4) Other Options in the "Select first what you would like to do",

First colect what you would like to do.
First select what you would like to do:
Configure the unit for the first time
 Change or update configuration of the unit
\bigcirc Check SIP configuration and logs
Register this unit with Ingate
Upgrade this unit
Enable SIP module
Configure Remote SIP Connectivity
🔽 Configure SIP trunking
Backup the created configuration
Create a config without connecting to a unit
This tool remembers passwords

- a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
- b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

- c. Select "Register this unit with Ingate" if you want the tool to connect with <u>www.ingate.com</u> to register the unit. If selected, see Section 4.3: Licenses and Upgrades.
- d. Select "Upgrade this unit" if you want the tool to connect with <u>www.ingate.com</u> to download the latest software release and upgrade the unit. If selected, see Section 4.3: Licenses and Upgrades.
- e. Select "Backup the created configuration" if you want the tool to apply the settings to an Ingate unit and save the config file.
- f. Select "Creating a config without connecting to a unit" if you want the tool to just create a config file.
- g. Select "The tool remembers passwords" if you want the tool to remember the passwords for the Ingate unit.
- 5) In the "Inside (Interface Eth0)",
 - a. Enter the IP Address of the Ingate Unit.

-Inside (Interface Eth0)-		
IP Address:	10 . 51 . 77 . 100	
	·	

6) In the "Select a Password", enter the Password of the Ingate unit.

Enter the password	
Password:	•••••

7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.

Establish contact Inside (Interface Eth0) – IP Address:	10 . 51 . 77 . 100
Enter the password Password:	•••••
	Contact

8) Proceed to Section 4.4: Network Topology.

3.3 Network Topology

The Network Topology is where the IP Addresses, Netmask, Default Gateways, Public IP Address of NAT'ed Firewall, and DNS Servers are assigned to the Ingate unit. The configuration of the Network Topology is dependent on the deployment (Product) type. When selected, each type has a unique set of programming and deployment requirements, be sure to pick the Product Type that matches the network setup requirements.

nses and Upgrades	Network Topology	IP-PBX ITSP	_1 Upload Configuration		
Product Type:	Standalone SIPara	itor 💌			
Inside (Interface	Eth0)			Internet	
IP address:	10 . 51 . 7	7 . 100		N	
Netmask:	255 . 255 . 25	55.0			
Outside (Interfa	te Eth1)			E	xisting firewall
Use DHCP to	obtain IP		Ingate SIPa	rator	
IP Address:	172 . 51 . 7	77 . 100	LAN	_	
Netmask:	255 . 255 . 2	55 . 0	6	<u>'</u> '	
Allow https a	ccess to web interface	e from Internet	IP-	PBX	
Gateway:	172 51 7	77 1			
			DNS server Primary:	4 . 2 . 2 . 2	
			DNS server Primary: Secondary: (Optional)	4 . 2 . 2 . 2	
⊂ Status			DNS server Primary: Secondary: (Optional)	4 . 2 . 2 . 2	
Status Ingate Startup	o Tool Version 2.4.0, (connected to: I	DNS server Primary: Secondary: (Optional) ngate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP User R	o Tool Version 2.4.0, d urity sal Licenses egistration Licenses	connected to: 1	DNS server Primary: Secondary: (Optional) Ingate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R Software Vers	o Tool Version 2.4.0, o urity sal Licenses egistration Licenses ion: 4.6.2	connected to: I	DN5 server Primary: Secondary: (Optional) ngate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R Software Vers	o Tool Version 2.4.0, (urity sal Licenses egistration Licenses iion: 4.6.2	connected to: I	DN5 server Primary: Secondary: (Optional) ngate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	

Configuration Steps:

1) In the Product Type drop down list, select the deployment type of the Ingate Firewall or SIParator.

Product Type:	Standalone SIParator	~

Hint: Match the picture to the network deployment.

2) When selecting the Product Type, the rest of the page will change based on the type selected. Go to the Sections below to configure the options based on your choice.

3.3.1 Product Type: Firewall

When deploying an Ingate Firewall, there is only one way the Firewall can be installed. The Firewall must be the Default Gateway for the LAN; it is the primary edge device for all data and voice traffic out of the LAN to the Internet.

Product Type:	Network Topology IP-PBX ITSP	Upload Configuration
Product Type: Inside (Interface El		
IP address:	10 51 77 1	Internet
Netmask:	255 . 255 . 255 . 0	
Outside (Interface	Eth1)	
Use DHCP to ob	tain IP	Ingate Firewall
IP Aduress:	12 . 23 . 34 . 45	
Netmask:	255 . 255 . 255 . 0	LAN
Allow https acce	ess to web interface from Internet	
Gateway:	12 . 23 . 34 . 1	1
		∠DNS server
		Primary: 4 . 2 . 2 . 1
		Secondary: 4 . 2 . 2 . 2
Status Ingate Startup T	ool Version 2.4.0, connected to: Ing	gate Firewall 1190, IG-092-719-5012-4
Remote SIP Con VPN QoS Enhanced Secur 15 SIP Traversa 20 SIP User Rec	nectivity ity I Licenses Istration Licenses	<u>~</u>
Software Version	n: 4.6.2	~

Configuration Steps:

1) In Product Type, select "Firewall".

2) Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.

-Inside (Interface E	th0)
IP address:	10 . 51 . 77 . 1
Netmask:	255 . 255 . 255 . 0

- 3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
 - a. A Static IP Address and Netmask can be entered
 - b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically using DCHP.

Outside (Interface	Eth1)	
Use DHCP to ob	tain IP	
IP Address:	12 . 23 . 34 . 45	
Netmask:	255 . 255 . 255 . 248	
Allow https acce	ess to web interface from Interne	et

- 4) **Optional:** To configure Secure Web (https) from the Internet to the Ingate Unit for remote administration,
 - a. Select "Allow https access to web interface from Internet"

Outside (Interfac	e Eth1)
Use DHCP to a	obtain IP
IP Address:	12 . 23 . 34 . 45
Netmask:	255 . 255 . 255 . 248
Allow https ac	cess to web interface from Internet

b. Create a Private Certificate for https access, enter the corresponding information required to generate a certificate.

G Create certificate for h	ittps access	
Common Name (CNV)		
(Required)	Your Name	ОК
Expire in (days): (Required)	365	Cancel
Country Code (C):	US	
Organisation (O):	Company Name	
State/province(ST):	NY	
Organizational Unit(OU):	Deptartment	
Email address:	admin@email.com	
Locality/town(L):	Your City	

5) Enter the Default Gateway for the Ingate Firewall. The Default Gateway for the Ingate Firewall will always be an IP Address of the Gateway within the network of the outside interface (Eth1).

Gateway:	12	•	23	•	34	•	41
_		_					

6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

-DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

3.3.2 Product Type: Standalone

When deploying an Ingate SIParator in a Standalone configuration, the SIParator resides on a LAN network and on the WAN/Internet network. The Default Gateway for SIParator resides on the WAN/Internet network. The existing Firewall is in parallel and independent of the SIParator. Firewall is the primary edge device for all data traffic out of the LAN to the Internet. The SIParator is the primary edge device for all voice traffic out of the LAN to the Internet.

'k Topology IP-F	BX ITSP	Upload Co	onfiguration									
Product Type:	Standalor	ne SIParator	*				_	_	_			
Inside (Interface	Eth0)	10 517 di decor				1	Inte	rne	a 1	5		
IP address:	10 .	51 . 77	. 100									
Netmask:	255 . 3	255 . 255	. 0			L						
Outside (Interfac	e Eth1)				-	- 101	-				Exis	ting firewa
Use DHCP to a	btain IP			Ingat	e SIParato					-		
IP Address:	12 .	23 . 34	. 45	LAN -	-	-	-		-	-	۰.	
Netmask:	255 . :	255 . 255	. 248									
Allow https ac	cess to web	interface fr	om Internet		IP-PB)	, K						
Gateway:	12	23 34	41									
				DNS server Primary:		4.	2		2		1	
				DNS server Primary: Secondary: (Optional)		4.	2	•	2	•	1]
Status Ingate Startup	Tool Versio	n 2.4.0, con	nected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, I	G-092-70	4 . 4 . 2-212	2 2 2-0	•	2	•	1 2]
Status Ingate Startup VOIP Survival VPN OoS	Tool Version	n 2.4.0, coni	nected to: Inc	DNS server Primary: Secondary: (Optional) Hate SIParator 19, I	G-092-70	4 . 4 . 2-212	2 2 2-0	•	2	•	1]
Status Ingate Startup VoIP Survival VPN QoS Enhanced Seco 10 SIP Travers 10 SIP User Re	Tool Version urity ral Licenses gistration Li	n 2.4.0, con	nected to: Ing	DNS server Primary: Secondary: (Optional) late SIParator 19, 1	G-092-70	4 . 4 . 2-212	2 2	•	2	•	1 2]
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re Software Versi I	Tool Version urity ral Licenses egistration Li ion: 4.6.2	n 2.4.0, coni icenses	nected to: Ing	DNS server Primary: Secondary: (Optional) late SIParator 19, 1	G-092-70	4 . 4 . 2-212	2 2-0	•	2	•	1	
Status Ingate Startup VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re Software Versi	Tool Version urity sal Licenses gistration Li ion: 4.6.2	n 2.4.0, coni	nected to: Inç	DNS server Primary: Secondary: (Optional) late SIParator 19, 1	G-092-70	4 . 4 . 2-212	2 2	•	2	•	1 2	

Configuration Steps:

1) In Product Type, select "Standalone SIParator".

Product Type:	Standalone SIParator	*

2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.

-Inside (Interface E	th0)
IP address:	10 . 51 . 77 . 100
Netmask:	255 . 255 . 255 . 0

- 3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
 - a. A Static IP Address and Netmask can be entered
 - b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically using DCHP.

Outside (Interface	ith1) ——		
Use DHCP to ob	ain IP		
IP Address:	12 . 2	23 . 34 .	45
Netmask:	255 . 2	55 . 255 .	248
Allow https acce	ss to web i	nterface from	n Internet

- 4) **Optional:** To configure Secure Web (https) from the Internet to the Ingate Unit for remote administration,
 - c. Select "Allow https access to web interface from Internet"

-Outside (Interface	Eth1)	
Use DHCP to ob	tain IP	
IP Address:	12 . 23 . 34 .	45
Netmask:	255 . 255 . 255 . 2	248
Allow https acce	ss to web interface from :	Internet

d. Create a Private Certificate for https access, enter the corresponding information required to generate a certificate.

G Create certificate for h	ittps access	X
Common Name (CN): (Required)	Your Name	ОК
Expire in (days): (Required)	365	Cancel
Country Code (C):	US	
Organisation (O):	Company Name	
State/province(ST):	NY	
Organizational Unit(OU):	Deptartment	
Email address:	admin@email.com	
Locality/town(L):	Your City	

5) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

Gateway:	12	. 23	. 34	. 41]
_	_	_	_	_	

6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

3.3.3 Product Type: DMZ SIParator

When deploying an Ingate SIParator in a DMZ configuration, the Ingate resides on a DMZ network connected to an existing Firewall. This existing Firewall must be the Default Gateway for the DMZ network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN and DMZ to the Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, both from the Internet to the SIParator and from the DMZ to the LAN.

ises and Upgrades	Network Topology	IP-PBX	ITSP_1	Upload Configuration			
Product Type:	DMZ SIParator		*		\int		
IP address:	10 . 51 . 7	7.100			Interne	et)
Netmask:	255 , 255 , 25	55,0					
LAN IP address ra	inge				DMZ	Existi	ng firewall
Low IP:	192 . 168 .	1.1		Ingate SIPara	ator		
High IP:	192 . 168 .	1.255			-		
Gateway:	10 . 51 . 7	7.1		IP-PBX			
Firewall extern IP	12 . 23 . 3	84 . 45					
				DNS server			
				Primary:	4.2.	2.2	
				Secondary: (Optional)	4.2.	2.1	
Status Ingate Startup	Tool Version 2.4.0, (onnected	to: Inga	te SIParator 19, IG-092	-702-2122-0		
VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re	urity al Licenses gistration Licenses						~
Software Vers	on: 4.6.2						~

Configuration Steps:

1) In Product Type, select "DMZ SIParator".

Product Type:	DMZ SIParator	~
---------------	---------------	---

2) Define the IP Address and Netmask of the DMZ (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.

-DMZ (Interface Eth	10)
IP address:	192 . 168 . 100 . 100
Netmask:	255 . 255 . 255 . 0

3) Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.

∼LAN IP address ran	ige							
Low IP:	10	•	10	•	10	•	1	
High IP:	10	•	10	•	10	•	255	

4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

5) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.

Firewall extern IP:	98	•	87	•	76	•	65]
	_		_		_		_	

6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.



7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- a. Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- b. Port Forward the a range of RTP Media ports of 58024 to 60999 with a UDP Forward to the Ingate SIParator
- c. If necessary; provide a Rule that allows the SIP Signaling on port 5060 using UDP/TCP transport on the DMZ network to the LAN network
- d. If necessary; provide a Rule that allows a range of RTP Media ports of 58024 to 60999 using UDP transport on the DMZ network to the LAN network.

3.3.4 Product Type: DMZ-LAN SIParator

When deploying an Ingate SIParator in a DMZ-LAN configuration, the Ingate resides on a DMZ network connected to an existing Firewall and also on the LAN network. This existing Firewall must be the Default Gateway for the DMZ network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN and DMZ to the Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

e Startup Tool					
work Topology IP-	PBX ITSP	Upload Configuration			
Product Type:	DMZ-LAN	SIParator 😽		\sim	
IP address:	10 .	51 . 77 . 100		Internet	
Netmask:	255 . :	255 . 255 . 0			
DMZ (Interface E	th1) obtain IP	168 . 100 . 100	Ingate SIParato	DMZ Existing	firewall
Netmask:	255 .	255 . 255 . 0	LAN		
Allow https ad	cess to web	interface from Internet		1 • •	
Gateway:	192 .	186 . 100 . 1	IP-PB	x	
Firewall extern IF	98 .	87 . 76 . 65			
			DNS server		
			Primary:	4 . 2 . 2 . 1	
			Secondary: (Optional)	4 . 2 . 2 . 2	
Status Ingate Startup	Tool Versio	n 2.4.0. connected to: Ina	ate SIParator 19, IG-09	2-702-2122-0	
VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R	urity sal Licenses egistration L	censes			^
Software Vers	ion: 4.6.2				-
					Help

Configuration Steps:

1) In Product Type, select "DMZ SIParator".

Product Type:	DMZ-LAN SIParator	*

 Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.

–Inside (Interface E	:h0)
IP address:	10 . 51 . 77 . 100
Netmask:	255 . 255 . 255 . 0

- 3) Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.
 - a. A Static IP Address and Netmask can be entered
 - b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically using DCHP.

- DMZ (Interface Eth1)						
IP Address:	192 . 168 . 100 . 100					
Netmask:	255 . 255 . 255 . 0					
Allow https access to web interface from Internet						

4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

Gateway:	192	. 186	. 100	1
	_	_	_	 _

5) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.



6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

DNS server								
Primary:	4	•	2	•	2	•	1	
Secondary: (Optional)	4	•	2	•	2	•	2	

7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- a. Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- b. Port Forward the a range of RTP Media ports of 58024 to 60999 with a UDP Forward to the Ingate SIParator

3.3.5 Product Type: LAN SIParator

When deploying an Ingate SIParator in a LAN configuration, the Ingate resides on a LAN network with all of the other network devices. The existing Firewall must be the Default Gateway for the LAN network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN to the WAN/Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

ate Startup Tool		
twork Topology IP-F	PBX ITSP Upload Configu	ation
Product Type: LAN (Interface Et	LAN SIParator	
IP address:	10 . 51 . 77 . 100	Internet
Netmask:	255 . 255 . 255 . 0	Existing firewall
Gateway:	10 . 51 . 77 . 1	IP-PBX Ingate SIParator
Firewall extern IP	98 . 87 . 76 . 65	
		DN5 server
		Primary: 4 . 2 . 2 . 1
		Secondary: (Optional) 4 . 2 . 2 . 2
Status Ingate Startup	Tool Version 2.4.0, connected	to: Ingate SIParator 19, IG-092-702-2122-0
VoIP Survival VPN QoS Enhanced Secu 10 SIP Travers 10 SIP User Re	urity al Licenses Igistration Licenses	
Software Versi	on: 4.6.2	

Configuration Steps:

1) In Product Type, select "LAN SIParator".

Product Type:	LAN SIParator	*
	LAN DIFARACO	

2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.

-LAN (Interface Eth	0)
IP address:	10 . 51 . 77 . 100
Netmask:	255 . 255 . 255 . 0

3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

Gateway:	10	. 51	. 77	•	1]
_	-	-	-		-	

4) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.



5) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4		2		2	•	2

6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- a. Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- b. Port Forward the a range of RTP Media ports of 58024 to 60999 with a UDP Forward to the Ingate SIParator

3.3.6 Product Type: LAN SIParator - "SBE SIParator Only"

This section is specific to the Ingate SBE SIParator when deploying in a LAN SIParator configuration, the Ingate SBE resides on a LAN network with all of the other network devices. The existing Firewall must be the Default Gateway for the LAN network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN to the WAN/Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

Ingate Startup Tool	
Network Topology IP-PBX ITSP Upload Configuration	
Product Type: LAN SIParator LAN (Interface ET1) IP address: 10 . 51 . 77 . 200	Internet
Netmask: 255 . 255 . 255 . 0	Existing firewall
Gateway: 10 . 51 . 77 . 1	IP-PBX Ingate SIParator
Firewall extern IP: 98 87 76 65 Port range: 58024 - 60999	CDNS server
Allow DHCP Server, (setup in web GUI)	Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional)
Status Ingate Startup Tool Version 2.4.0, connected to: In	igate SIParator SBE,
Ingate Startup Tool Version 2.4.0 Startup tool version available on the Ingate web: 2. You are running the latest version of the Startup to More information is available here: http://www.inga	.4.0 Iol. ste.com/startuptool.php
	×
	Help

Configuration Steps:

1) In Product Type, select "LAN SIParator".

2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.

-LAN (Interface Eth	0)
IP address:	10 . 51 . 77 . 100
Netmask:	255 . 255 . 255 . 0

3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

Gateway:	10	. 51	. 77	•	1]
_	-	-	-	-	-	-

4) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.

Firewall extern IP:	98	. 87	. 76	. 65	
_					-

5) Enter a Port Range of media ports you need to configure the firewall to forward to the LAN SIParator

Port range:	58024	-	60999	
			_	

6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

-DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- a. Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- b. Port Forward the a range of RTP Media ports of 58024 to 60999 with a UDP Forward to the Ingate SIParator

3.4 IP-PBX Setup for Avaya QE

The IP-PBX section is where the IP Addresses and Domain location are provided to the Ingate unit. The configuration of the IP-PBX will allow for the Ingate unit to know the location of the IP-PBX as to direct SIP traffic for the use with SIP Trunking and Remote Phones. The IP Address of the IP-PBX must be on the same network subnet at the IP Address of the inside interface of the Ingate unit. Ingate has confirmed interoperability several of the leading IP-PBX vendors.

Ingate Startup Tool		
Network Topology IP	PBX ITSP_1 Upload Configuration	
⊂ IP-PBX (should b	e located on the LAN)	
Type:	Avaya QE PBX registers at the	ne Ingate
IP Address:	10 . 51 . 77 . 20	
Use domair SIP Domain:		
Status Ingate Startu	p Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-719-5151-0	
Ingate Startu Startup tool v You are runni More informa 10.51.77.100 Wait for the v The web serv New passwor IG-092-719-5	up Tool Version 2.4.0 version available on the Ingate web: 2.4.0 ing the latest version of the Startup tool. tion is available here: http://www.ingate.com/startuptool.php) has been assigned to etho. web server of the Ingate unit to restart, takes 30 - 120s depending on model. ver has restarted. d set. 1151-0	
		Help

Configuration Steps:



1) In the IP-PBX Type drop down list, select the Avaya QE. Ingate has confirmed interoperability with the Avaya QE solution. The unique requirements of the Avaya QE testing are contained in the Startup Tool.

Type:	Avaya QE	~

2) Enter the IP Address of any Avaya QE phone. The IP Address should be on the same LAN subnet as the Ingate unit.

IP Address:	10 . 51 . 77 . 20
_	

3) When Avaya QE is selected as the IP-PBX type, then the option "PBX registers at the Ingate" is automatically selected. When is option is enabled, the Ingate Registrar is enabled, later on the ITSP configuration, Avaya QE Identities are assigned on the Registrar and associated to the incoming call characteristics. So the Avaya QE registers to the Ingate and the Ingate sends the incoming call to these registered users/identities.



3.5 ITSP for Avaya QE

The ITSP section is where all of the attributes of the SIP Trunking Service Provider are programmed. Details like the IP Addresses or Domain, DIDs, Authentication Account information, Prefixes, and PBX local number. The configuration of the ITSP will allow for the Ingate unit to know the location of the ITSP as to direct SIP traffic for the use with SIP Trunking. Ingate has confirmed interoperability many of the leading ITSP vendors.

ork Topology IP-PBX ITSP_1 Upload Configuration	
Name: Generic ITSP	DID (start of range) (user name): DID range size:
Provider address IP Address: 0 , 0 , 0 , 0 Use domain name	Account information: Use account Authentication name: (same as DID if blank)
Advanced Prefix to match and remove from inbound calls Prefix:	Domain: Password:
Prefix to add to outbound calls Prefix:	Use user account on incoming call PBX local numbers (advanced) Local number(start of range, use same as DID if local numbers are not used): Password (only used if PBX registers at the Ingate): PBX registers at the Ingate
Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIPe	rator 19, IG-092-702-2122-0
VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses Software Version: 4.6.2	
	▼

Configuration Steps:

1) In the ITSP drop down list, select the appropriate ITSP vendor. Ingate has confirmed interoperability several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool. If the vendor choice is not seen, select "Generic ITSP".

Name:	Generic ITSP	*
-------	--------------	---

When you select a specific ITSP vendor, the Startup Tool will have the individual connection requirements predefined for that ITSP, the only additional entries may be the specific site requirements.

- 2) Service Providers come in one of two flavors, either they have a trusted IP deployment or they require a Registration account.
 - a. In the case where the Service Provider uses a Trusted IP deployment, all which is required is to enter the IP Address or Domain of the Service Providers SIP Server or SBC. Enter the IP Address here, or select "Use domain name" and enter the FQDN of the Service Provider.

Provider address								1	
IP Address:	0	·	0	·	0	•	0		
Use domain name									
- Provider address									
								1	
Domain:									
🔽 Use domain nan	ne								

b. In the case where the Service Provider requires the Ingate to register with the Service Providers SIP Server or SBC, select "Use Account". When "Use Account" is selected, the Registration Account information from the Service Provider is required. Information such as Username/DID, Service Providers Domain, Authentication Username, and Authentication Password.

Account information:	
🔽 Use account	
Authentication name: (same as DID if black)	
Increment authentica	tion name for ranges
	_
Domain:	
Deserved	
Password:	
🔽 Use user account	on incoming call

i. Registrations often require the use of an Authentication Username and Password. Also enter the Domain or IP Address of the Service Provider.

Account information:	
Use account	
Authentication name:	
(same as DID if Diank)	ies
	,03
Domain:	
Password:	
🔽 Use user account on incoming call	



c. Enter a DID (Username) from the Service Provider. These DIDs will be directed from the Ingate to the registration Identities from the Avaya QE. The Startup Tool also has the ability to program a sequential range of DIDs.

DID (start of range) (user name):	6135559876
DID range size:	3



d. The Avaya QE requires the use of Ingate's Registrar, where the Avaya QE registers Local Identities on the Ingate. The Ingate will direct calls to these registered Identities. Here enter the start of the range of Identity being registered to the Ingate from the Avaya QE.



3) The Ingate has the ability to add/remove digits and characters from the Request URI Header. A typical scenario is the addition/removal of ENUM character "+". Many IP-PBX and ITSPs either need to add or remove this character prior to sending or receiving SIP requests. Here you can enter values to Match and remove from the Request URI.

Prefix:	
Prefix to add to Prefix:	outbound calls
Forward 3xx me	ssages

3.6 Upload Configuration

At this point the Startup Tool has all the information required to push a database into the Ingate unit. The Startup Tool can also create a backup file for later use.

ettings erial interface on Upload

Configuration Steps:

 Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.

ſ	Final step
	 Logon to web GUI and apply settings
	O Apply settings directly using serial interface
	Backup the configuration
	Upload

2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.

Success	×
Your configuration has been updated. When you press OK you will be redirected to your bro Please login and press "Apply Configuration" in the Admin menu of the Ingate web interface. OK	wser.

3) Although the Startup Tool has pushed a database into the Ingate unit, the changes have not been applied to the unit. Press "Apply Configuration" to apply the changes to the Ingate unit.



4) A new page will appear after the previous step requesting to save the configuration. Press "Save Configuration" to complete the saving process.



4 Avaya Quick Edition Setup

Quick Edition

4.1 Device Management

By default the Avaya QE will add devices into the Device Management section as each phone or gateway is connected to the LAN. These are the Extensions of the Avaya QE. Users can call these extensions from their Avaya phones.

System options	Device M	lanag	ement			
Device	Device Manage	ement >De	vices			
Management	Devices	<u>Softwa</u>	nre Upgrade Bac	kup & Resto	re	
Corporate Directory						
» Applications	Name	Ext.	IP Address	Туре	Version	Status
Dialina	Kerry	201	10.51.77.59	Phone	7.4.2514	Active
Configuration	Scott	200	10.51.77.58	Phone	7.4.2514	Active
Service Provider	Unknown	202	10.51.77.60	Gateway	7.4.2514	Active
SIP Proxy						
Security						
Localization						
Notworking						

4.2 Service Provider

Here is where we add the Ingate Firewall/SIParator information into the Avaya QE.

	Quick Edition	Logout Change Admin Password Help
System Options	Service Providers	
» Device	Service Provider	
Management	Configurations (1)	
» Corporate Directory		Add Configuration
» Applications	Do	main
Dialing » Configuration	<u>10.51.77.1</u>	
» Service Provider	_	
» SIP Proxy		
» Security	_	
» Localization		
» Networking	_	

Configuration Steps:

1. In the Service Provider page, press "Add Configuration".

Add Configuration

- 2. Enter the following to configure the Ingate on the Avaya QE:
 - a. Domain Name: IP Address of the Ingate (or FQDN)
 - b. Proxy Host: IP Address of the Ingate (or FQDN)
 - c. **Proxy Port:** 5060
 - d. Registrar Host: IP Address of the Ingate (or FQDN)
 - e. Registrar Port: 5060
 - f. Outbound Proxy Host: "Blank"
 - g. Outbound Proxy Port: "Blank"
 - h. **Realm:** IP Address of the Ingate (or FQDN)
 - i. Register Expiry Time: 300 (default)
 - j. Keep-Alive Time: 300 (default)
 - k. International Notation (+): Either Disabled or Enabled

		Logout Char	nge Admin Password He
System Options	Configuration(10.51.77.1)		
Device Management	Service Provider > Configuration	_	_
Corporate Directory			Delete Configuration
Applications	View Configuration Details		
Dialing Configuration	Domain Name:	10.51.77.1	<u>Change Details</u>
Service Provider	Proxy Host:	10.51.77.1	
SIP Proxy	Registrar Host:	10.51.77.1	
Security	Registrar Port:	5060	
Localization	Outbound Proxy Host:		
Networking	Outbound Proxy Port:		
	Realm:	10.51.77.1	
	Register Expiry Time:	300	
	Keep-Alive Time:	300	
	International Notation (+):	Disabled	

3. Once the Ingate has been added as a Service Provider, Click on "Identities", then "Add Identity".

Add Identity

	<™ Quio	k Edition	Logout Change Admir	Password H
System Options	Identit	ies(10.51.77.1)		
Device	Service Pro	vider >Identities		
Management	Configur	ation Identities		
Corporate Directory				Add Identit
Applications	Identit	y Incoming Extension	Outgoing Extension	Register
Dipling	<u>11200</u>	200	GLOBAL	Yes
Configuration	11201	201	GLOBAL	Yes
Service Provider	11500	GLOBAL	GLOBAL	Yes
SIP Proxy				
> Security				
Localization				
Networking				

- 4. This "Identity" will register to the Ingate and the Avaya QE will associate the identity with an Extension in Device Management. Complete the following:
 - a. **Identity:** Enter an Identity that matches the Identity entered in Section 3.5 Configuration Step 2d.
 - b. Authorized User: Enter the Identity number, same as above.
 - c. **Password:** Enter a Password
 - d. **Incoming Extension:** Select an Extension from the drop down list, or the Auto Attendant Extension.
 - e. Outgoing Extension: Select "Global"
 - f. Register: Select "Yes"
 - g. **AA Enabled:** Enable only for Auto Attendant Use, otherwise disable.
 - h. AA Extension: Select the Auto Attendant Extension number.

System Options	Identity(10.51.77.1)		
Device Management	Service Provider >Identities >Identity Configuration Identities		
Corporate Directory			Delete Identity
 Applications 	View Identity Details		
Dialing Configuration	Identity:	11200	<u>Change Details</u>
Service Provider	Authorized User:	11200	
SID Provid	Password:	*****	
SIP Proxy	Incoming Extension:	200	
> Security	Outgoing Extension:	GLOBAL	
Localization	Register:	Yes	
Networking	AA Enabled:	Disabled	
	AA Extension:	500	

5. Avaya QE Dial Configuration needs no adjustment. Simply, to use the Service Provider, the "8" prefix needs to be dialed from the Avaya phone.

System Options	Dial Plan Settings	
» Device Management	Dialing Configuration >Dial Plan Settings	erator
© Corporate Directory	View Dial Plan Settings	
» Applications		Edit Dial Plan Reset Dial Plan
Dialing [»] Configuration	Extension Range: Auto Attendant Extension Range:	200 - 599 500 - 599
» Service Provider	Emergency Code:	911
» SIP Proxy	Operator Code:	0
» Security	PSTN Code: SIP Code:	9 8
» Localization	International Direct Dialing Prefix:	011
» Networking	National Direct Dialing Prefix	1
	Country Code:	1
	Area Codes:	613

5 Troubleshooting

5.1 Avaya QE Identity Registration Information



Here is how the Avaya QE "Identities" register to Ingate's Registrar. The Avaya QE Identities provider Username, Authentication Username, Password and Realm to the Ingate Registrar.

ervice Provider >0	Configuration							
onfigurati	ion <u>Identitie</u>	<u>.s</u>			Service Provider >Iden	ities >Identity		
			Delete C	onfiguration	Configuration Ic	lentities		
/iew Configurat	ion Details							Delete Identity
			<u>Cha</u>	ange Details	View Identity Detail	5		
Domain Name:		10.51.77.1						Change Details
Proxy Host:		10.51.77.1			Identity:		11200	
Proxy Port:		5060			Authorized User:		11200	
egistrar Host:		10.51.77.1			Password:		*****	
egistrar Port:		5060			Incoming Extension:		200	
utbound Proxy	Host:				Outgoing Extension:		GLOBAL	
utbound Proxy	Port:				Register:		Yes	
ealm:		sip.office-on-	-the.net		AA Enabled:		Disabled	
egister Expiry	ime:	300			AA Extension:		500	
eep-Alive Time		300		/ /				
histration Config P nods Filtering D	ic ration Network I Iser abase and Account	Rules and SIP Relays Services (r on ing Dial tan Routing	alP Failover Virtuel riva N .works SIP Status	e Qualit of Logging Succe and Tools	lbout	Administration Conf	Basic iguration Network R	ules and SIP Relays Services Traff
ocal SIP De Domain	nams <u>(Help)</u> Delete					Methods Filtering	Database and Accountin	n 19 Dial Plan Routing St
10.51.77.1						SIP Authent	ication	
sip.office-on-the.r						⊙ On ⊖ Off		
Add new rows	rows.					SIP Realm		
.ocal SIP Us	er Database 🕧	Help)				sip.office-on-the.	n	
Username	Domain	Authentication Name	Password	Account Type	Register From			
1200	10.51.77.1	11200	Change Password	User 💌	LAN			
201	10.51.77.1	11201	Change Password	User 💌	LAN			
1500	10.51.77.1	11500	Change Password	User 🗸	LAN			

5.2 Registration Status

The successful registration of the Avaya QE Identities can be seen in SIP Traffic -> SIP Status.

ministration Basic Configuration	Networ	k Rules Rela	and Sei	SIP rvices Tr	SIP affic Failove	r Virtual Private Qua Networks Se	
SIP User Iethods Filtering Database	Authen and Acc	tication ounting	Dial Plan	Routing	SIP Status		
Active Sessions (0 so Chere are no active sess Monitored SIP Serv	ession ions. rers	15)					
Monitored SIP Server	Port	Transp	ort Mo	nitored	SIP Server	Status	
ingate.com	5060	UDP	Mor	Monitored SIP server is online			
10.51.77.60	5060	UDP	Mor	Monitored SIP server is online			
Registered Users (11	l usei	rs)					
Use			Regist	ered From	Survival Aliases		
11200@10.51.77.1			10.51.7	7.58	-		
11201@10.51.77.1				10.51.7	7.59	-	
11500@10.51.77.1				10.51.7	7.58	-	

5.3 Incoming Routing

Depending on whether the ITSP requirement was for the Ingate to provide Registration or whether the ITSP was a just an IP, depends on whether the Startup Tool creates a Static Registration or a User Routing. For ITSPs that just use IP addresses a Static Route will be created, and if the ITSP requires Registrations, User Routing will be created.

The DID from the ITSP (INVITE Request URI header) will have to match the "Request to User" and then be forwarded to the Registration accounts in the Ingate to route to the Avaya QE.

ministro	^{ition} Con	Basic Ifiguratio	n Network SI Serv	P SIP ices Traffi	Failov	er Vir	tual Pri Networl
SIP ethods	Filtering	User Databas	Authentication and Accounting	Dial Plan	Routing	Time Classes	SIP Statu:
Stati	c Regis	tratio	ns <u>(Help)</u> Also F	Corward T			
Requests To User							
Requ	iests To	User	User	sip/sips	Trans	port D	elete
Req1 + 61	1 ests To 35559876	User 5@172	User 11200@10.51.77	sip/sips	Transp -	port D	elete
Req1 + 61 + 61	1 ests To 35559876 35559877	User 6@172 7@172	User 11200@10.51.77 11201@10.51.77	sip/sips . sip 🗸	Transj -	port D	elete