

Application Note

AT&T IP Flex Reach - Configuration Guide

21 May 2009

Revision History:

Revision	Date	Author	Comments
	2009-05-21	Scott Beer	First Draft

Table of Contents

1	AT&T IP FLEX REACH AND INGATE	3
	 1.1 INGATE SIPARATOR WITH AT&T IP FLEXIBLE REACH 1.2 SIP TRUNKING 	3
2	INCATE SIDADATOR VERSION	5
2		
3	INGATE STARTUP TOOL	0
4	CONNECTING THE INGATE FIREWALL/SIPARATOR	7
5	USING THE STARTUP TOOL	9
	5.1 CONFIGURE THE UNIT FOR THE FIRST TIME	9
	5.2 CHANGE OR UPDATE CONFIGURATION	12
	5.3 NETWORK TOPOLOGY	15
	5.3.1 Product Type: Firewall	
	5.3.2 Product Type: Standalone	18
	5.3.5 Froduct Type: DMZ-IAN SIParator	20
	5.3.5 Product Type: LAN SIParator	
	5.4 IP-PBX	
	5.5 ITSP	28
	5.6 UPLOAD CONFIGURATION	
6	TROUBLESHOOTING	32
	6.1 AT&T IP FLEX TO INGATE TO IP-PBX CALL FLOW	
	6.2 STARTUP TOOL	
	6.2.1 Status Bar	
	6.2.2 Configure Unit for the First Time	
	6.2.3 Change or Update Configuration	
	6.2.4 Network Topology	
	0.2.5 IP-PBA	30 36
	6.2.7 Apply Configuration	
	6.3 INGATE TROUBLESHOOTING TOOLS	
	6.3.1 Display Logs	
	6.3.2 Packet Capture	
	6.3.3 Check Network	
7	APPENDIX – NORTEL CS1000 CONFIGURATION	41
	7.1 NORTEL CS1000 AND INGATE SIPARATOR (SBC) WITH AT&T IP FLEXIBLE REACH	41
	7.1.1 Ingate SIParator Configuration	41
	7.2 CONFIGURING THE SIPARATOR TO FAILOVER TO A SECONDARY IPBE	
	7.3 EXAMPLE INGATE CONFIGURATION WITH NORTEL	
	7.3.1 Networks - Networks & Computers	
	7.3.2 SIP Services - Interoperativity 7.3.3 SIP Traffic – Dial Plan	43 44
	7.4 CENTRALIZED VOICEMAIL IN AN IP FLEXIBLE REACH ENVIRONMENT	
	7.4.1 Detailed Sample Network Diagram	
	7.4.2 Nortel CS1000 Configuration	46
	7.4.3 Ingate SIParator Configuration	47
8	APPENDIX – SPECIAL NOTES	49
	Tested versions: Ingate Firewall and SIParator version 4.7.1	

l versions: Ingate Firewall and SIParator version 4.7. Startup Tool version 2.5.1 Nortel CS1000

1 AT&T IP Flex Reach and Ingate

This document provides a configuration guide to assist AT&T administrators and various IP-PBX vendors in connecting an Ingate Systems SIParator® to the AT&T IP Flexible Reach SIP Trunking service.

1.1 Ingate SIParator with AT&T IP Flexible Reach

AT&T IP Flexible Reach is a SIP "Trunking" service that delivers integrated access for Key System (analog phones), TDM PBX and IP PBX environments. This managed voice over IP communication solution supports inbound and outbound calling on your data network giving you local, U.S. long distance and international reach for your U.S. sites. With AT&T you gain the efficiency and economic benefits of network convergence for your organization.

Ingate offers SIParators and Firewalls, an Enterprise level SIP Session Border Controller (E-SBC) and SIP Security device. A powerful tool that offers enterprises a controlled and secured migration to VoIP (Voice over IP) and other live communications, based on Session Initiation Protocol (SIP). With the SIParator and Firewall, even the largest of businesses, with branch offices around the world and remote workers, can easily harness the productivity and cost-saving benefits of VoIP and other IP-based communications while maintaining current investments in security technology.

Various IP-PBXs provide call control, various business orientated features and supports desktop devices and applications for enterprises. The IP-PBX is an integral element of a business portfolio of products that: facilitate business wide communication and collaboration, enhance workforce mobility and extend enterprise connectivity, improve client service and contact management, provide tools to manage communication overload.

In this application, above and beyond the E-SBC capabilities that the Ingate products provide, the SIParator and Firewall are providing a number of additional features to enable SIP Trunking connectivity to various IP-PBX solutions using the AT&T IP Flex Reach SIP Trunking service. The Ingate products offer the use of the SIP Trunking Module, where there are features such as Routing Rules, basic Security Policies, Client/Server Registrar, B2BUA capabilities, SIP Protocol 'Normalization' and more. These features allow the Ingate to connect with AT&T IP Flex Reach in a secure and reliable manner.

1.2 SIP Trunking

In this application, the IP-PBX is the call control server processing the phone features and PBX functionality required for an enterprise. It resides on the private LAN segment of enterprise, away from the Internet and serviced by the Ingate as a Session Border Controller.

The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

The AT&T IP Flexible Reach is located across the AT&T Global MPLS Network.

Application Diagram



at&t

Look for the AT&T Icon

to focus your attention to specific AT&T IP Flexible Reach setup instructions. These instructions are specific to the Ingate & AT&T IP Flexible Reach deployment with SIP Trunking.

2 Ingate SIParator Version

The Ingate SIParator[®] has software version 4.7.1. You can check the version of the SIParator[®] by viewing the About page.

The SIP Trunking Module is required for AT&T IP Flexible Reach connectivity, and the Remote SIP Connectivity Module is optional for Far End NAT Traversal functionality.



Licensing and Modules

SIP Trunking Module	Provides Advanced Routing and SIP	
_	Normalization features specific to the SIP trunking	
	application	
Remote SIP Connectivity Module	Provide Far End NAT Traversal solutions and	
	STUN Server	
SIP Traversal Licenses	Provides number of concurrent calls limit, each	
	HW variant has different limits.	

3 Ingate Startup Tool

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.

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 IP-PBX of their choice and AT&T IP Flexible Reach SIP Trunking service, and sets up all the routing needed to enable remote users to access and use the enterprise IP-PBX. Thanks to detailed interoperability testing, Ingate has been able to create this tool with pre-configured set ups for several of the leading IP-PBX vendors and AT&T.

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/Startup_Tool.php

For more detailed programming instructions consult the Startup Tool – Getting Started Guide, available here:

http://www.ingate.com/appnotes/Ingate_Startup_Tool_Getting_Started_Guide.pdf

Make sure that you always have the latest version of the configuration tool as Ingate continuously adds new vendors once interoperability testing is complete. If you don't find your IP-PBX vendor, please contact Ingate for further information.

The Startup Tool will install and run on any Windows 2000, Windows XP, Windows Vista, and Wine on Linux operating systems.

Keep in mind, this Ingate Startup Tool is a commissioning tool, not an alternate administration tool. This tool is meant to get an "out of the box" Ingate started with a pre-configured setup, enough to make your first call from IP-PBX to AT&T. Additional programming and administration of this Ingate unit should be done through the Web Administration.

4 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.

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. It is required that 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. Keep the network Simple.



4) Proceed to Section 5: Using the Startup Tool for instructions on using the Startup Tool.

5 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.

5.1 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	
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 V 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 pass Inside (Interface Eth0) IP Address: MAC Address: Select a password Password: Confirm Password:	word, establish contact 10 51 77 100 00-d0-c9-a2-44-55]
Status 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 ol. ate.com/startuptool.php	Contact	

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. *Optional:* All other selections, if selected, consult the Startup Tool Getting Started Guide available at www.ingate.com.
- 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. The MAC Address can be found on a sticker attached to the unit.

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 5.3: Network Topology.

5.2 Change or Update Configuration

When selecting 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 5.1: "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".

igate Startup Tool Version	Help	
You are running the latest version of this tool.		Help
rst select what you would like to do: O Configure the unit for the first time ① Change or update configuration of the unit	Establish contact Inside (Interface Eth0 IP Address:)
Check SIP configuration and logs Register this unit with Ingate Ungrade this unit	Enter the password	
Fnable SIP module Configure Remote SIP Connectivity Configure SIP trunking	Password:	•••••
Backup the created configuration Create a config without connecting to a unit This tool remembers passwords		
atus		Contact
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 ol. te.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
O 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. *Optional:* All other selections, if selected, consult the Startup Tool Getting Started Guide available at www.ingate.com.
- 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 "Enter 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 5.3: Network Topology.

5.3 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.

es and Upgrades	Network Topology	IP-PBX ITSP_1	Upload Configuration		
Product Type:	Standalone SIPara	itor 🗸		\bigcirc	
Inside (Interface	Eth0)			Internet	
IP address:	10 . 51 . 7	7 . 100		The second	
Netmask:	255 . 255 . 25	55.0			
Outside (Interfac	e Eth1)				xisting firewall
Use DHCP to	obtain IP		Ingate SIPa	rator	
IP Address:	172 . 51 . 3	77 . 100	LAN	<u> </u>	
Netmask:	255 . 255 . 2	55 . 0	6		
Allow https ac	cess to web interfac	e from Internet	IP-	PBX	
Gateway:	172 51	77 1			
			ONS server		
			DNS server Primary:	4 . 2 . 2 . 2	
			DNS server Primary: Secondary: (Optional)	4 . 2 . 2 . 2	
Status	7- 10-01-040		DNS server Primary: Secondary: (Optional)		
Status Ingate Startup) Tool Version 2.4.0,	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	
Status Ingate Startup VeIP Survival VPN) Tool Version 2.4.0, (connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0	
Status Ingate Startup VorN QoS) Tool Version 2.4.0, r	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver) Tool Version 2.4.0, r urity sal Licenses	connected to: Ing	DNS server Primary: Secondary: (Optional) ate 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	o Tool Version 2.4.0, , urity sal Licenses egistration Licenses	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R Software Vers	u Tool Version 2.4.0, urity egistration Licenses egistration Licenses	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R Software Vers	u Tool Version 2.4.0, urity sal Licenses egistration Licenses iion: 4.6.2	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0 - - - - - -	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R. Software Vers	urity sal Licenses egistration Licenses ion: 4.6.2	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0	
Status Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP User R Software Vers	o Tool Version 2.4.0, urity egistration Licenses ion: 4.6.2	connected to: Ing	DNS server Primary: Secondary: (Optional) ate SIParator 19, IG-092	4 . 2 . 2 . 2 0 . 0 . 0 . 0 -702-2122-0	

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.

5.3.1 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.

ate Startup Tool	
enses and Upgrades Network Topology IP-PBX ITSP	Upload Configuration
Product Type: Firewall Inside (Interface Eth0) IP address: 10 , 51 , 77 , 1	Internet
Netmask: 255 . 255 . 255 . 0	
Outside (Interface Eth1) Use DHCP to obtain IP IP Address: 12 . 23 . 34 . 45 Netmask: 255 . 255 . 255 . 0	I AN
Ollow bttps access to web interface from Interpet	
	IP-PBX DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2
Status	
Ingate Startup Tool Version 2.4.0, connected to: Ir Remote SIP Connectivity VPN QoS Enhanced Security 15 SIP Traversal Licenses 20 SIP User Registration Licenses Software Version: 4.6.2	Igate Firewaii 1190, IG-092-719-5012-4
	Help

Configuration Steps:

1) In Product Type, select "Firewall".

Product Type:	Firewall	*
	1 II CAACIII	

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

5.3.2 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-	PBX ITSP Upload Configuration	
Product Type:	Standalone SIParator 🗸 🗸	\frown
Inside (Interface	Eth0)	Internet
IP address:	10 . 51 . 77 . 100	
Netmask:	255 . 255 . 255 . 0	
Outside (Interfa	ce Eth1)	Existing fireway
Use DHCP to	obtain IP	Ingate SIParator
IP Address:	12 . 23 . 34 . 45	LAN
Netmask:	255 . 255 . 255 . 248	
Allow https a	ccess to web interface from Internet	IP-PBX
Gateway:	12 23 24 41	
		DNS server
		DNS server Primary: 4 , 2 , 2 , 1
		DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2
Status		DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2
Status Ingate Startuj	o Tool Version 2.4.0, connected to: Ir	DNS server Primary: 4 , 2 , 2 , 1 Secondary: 4 , 2 , 2 , 2 (Optional) 4 , 2 , 2 , 2
Status Ingate Startuj VoIP Survival	o Tool Version 2.4.0, connected to: Ir	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VoIP Survival VPN Qo5	o Tool Version 2.4.0, connected to: Ir	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VoIP Survival VPN QoS Enhanced Sec 10 SIP Taccord	o Tool Version 2.4.0, connected to: Ir unity	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R	o Tool Version 2.4.0, connected to: Ir unity sal Licenses egistration Licenses	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VoIP Survival VPN QoS Enhanced Sec 10 SIP User R Software Ver	o Tool Version 2.4.0, connected to: Ir urity sal Licenses egistration Licenses ion: 4.6.2	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VoIP Survival VPN QoS Enhanced Sec 10 SIP User R Software Ver:	o Tool Version 2.4.0, connected to: Ir urity sal Licenses egistration Licenses sion: 4.6.2	DNS server Primary: 4 2 2 1 Secondary: 4 2 2 2 Ingate SIParator 19, IG-092-702-2122-0 Image: Comparison of the second and the s
Status Ingate Startuj VPN QoS Enhanced Sec 10 SIP User R Software Ver:	o Tool Version 2.4.0, connected to: Ir urity sal Licenses egistration Licenses sion: 4.6.2	DNS server Primary: 4 2 2 1 Secondary: 4 2 2 2 Ingate SIParator 19, IG-092-702-2122-0 Image: Comparison of the second and the s
Status Ingate Startuj VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R Software Ver:	o Tool Version 2.4.0, connected to: Ir unity sal Licenses egistration Licenses ion: 4.6.2	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 2
Status Ingate Startuj VPN QoS Enhanced Sec 10 SIP Traver 10 SIP Traver 10 SIP User R Software Ver:	o Tool Version 2.4.0, connected to: Ir unity sal Licenses egistration Licenses iion: 4.6.2	DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 (Optional) 4 . 2 . 2 . 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	Eth1)	-		
Use DHCP to ob	tain IP			
IP Address:	12 . 23 . 34 . 45			
Netmask:	255 . 255 . 255 . 248			
Allow https access to web interface from 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	itain IP				
IP Address:	12	. 23	. 34	. 45	
Netmask:	255	. 255	. 255	. 248	ĺ
Allow https acce	ess to v	veb inte	rface fr	om Intern	net

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) Expire in (days):	Your Name	OK
(Required) Country Code (C): Organisation (O):	US	Cancor
State/province(ST):	NY	
Organizational Unit(OU): Email address:	Deptartment 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	. 4:	L
_	_	_	_	_	

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.

5.3.3 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. The Ingate needs to know what the Public IP Address of the 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.

gate Startup Tool				
Licenses and Upgrades	Network Topology	IP-PBX ITSP_1	Upload Configuration	
Product Type: DMZ (Interface El IP address:	DMZ SIParator h0) 10 . 51 . 7	7 . 100	Interr	net
LAN IP address ra	255 , 255 , 25	5.0	DMZ	Existing firewall
Low IP: High IP:	192 . 168 192 . 168	1 . 1 1 . 255	Ingate SIParator	「
Gateway: Firewall extern IP	10 . 51 . 7	7 . 1	IP-PBX	
Shire			DNS server Primary: 4 4 4 4 4 4	2 . 2 2 . 1
Ingate Startup	Tool Version 2.4.0, c	connected to: Inga	te SIParator 19, IG-092-702-2122-0	
VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re Software Versi	urity al Licenses igistration Licenses on: 4.6.2			<u> </u>
				Help

Configuration Steps:

• In Product Type, select "DMZ SIParator".

Product Type:	DMZ SIParator	*

• 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	0)
IP address:	192 . 168 . 100 . 100
Netmask:	255 . 255 . 255 . 0

• 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.

Low IP:	10 . 10 . 10 . 1
High IP:	10 . 10 . 10 . 255

• 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
_	

• 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	
					-			

• 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

• 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.

5.3.4 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. The Ingate needs to know what the Public IP Address of the 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, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

Startup Tool				Jl
rk Topology IP-P	BX ITSP Upload Configuration			
Product Type:	DMZ-LAN SIParator		\sim	
IP address:	10 . 51 . 77 . 100		Internet	
Netmask:	255 . 255 . 255 . 0			
DMZ (Interface Et	h1)		DMZ Existing frewa	all
Use DHCP to o	btain IP	Ingate SIParator		
IP Address:	192 . 168 . 100 . 100	LAN		
Netmask:	255 . 255 . 255 . 0			
Allow https acc	ess to web interface from Internet	1-1		
Gateway:	192 . 186 . 100 . 1	IP-PBX		
Firewall extern IP:	98 . 87 . 76 . 65			_
		DN5 server		
		Primary:	4 . 2 . 2 . 1	
		Secondary: (Ontional)	4.2.2.2	
Status		(()))		
Ingate Startup	Tool Version 2.4.0, connected to: In	gate SIParator 19, IG-092-70	02-2122-0	
VoIP Survival				
VPN				
Enhanced Secu	rity			
10 SIP Travers 10 SIP User Re	ai Licenses gistration Licenses			
Software Versi	-			
Soleware versi	an none			
				븬
				He

Configuration Steps:

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

Product Type:	DMZ-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.

-Inside (Interface E	th0)
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 Eth	1) tain IP
IP Address:	192 . 168 . 100 . 100
Netmask:	255 . 255 . 255 . 0
Allow https acce	ess 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.

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

5.3.5 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.

te Startup Tool		
work Topology IP-	PBX ITSP Upload Configuration	<u>ا</u>
Product Type:	LAN SIParator	\sim
IP address:	10 . 51 . 77 . 100	Internet
Netmask:	255 . 255 . 255 . 0	Existing firewall
Gateway:	10 . 51 . 77 . 1	LAN IP-PBX Ingate SIParator
Firewall extern IF	98 . 87 . 76 . 65	
		DNS server Primary: 4 2 2 1
		Secondary: (Optional)
Status Ingate Startup	Tool Version 2.4.0, connected to: :	Ingate SIParator 19, IG-092-702-2122-0
VoIP Survival VPN Qo5 Enhanced Sect 10 SIP Travers 10 SIP User Re	urity al Licenses gistration Licenses	-
Software Vers	on: 4.6.2	
		Help

Configuration Steps:

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

Product Type:	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.



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

5.4 IP-PBX

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.

igate Startup Tool	
Vetwork Topology IP-PBX ITSP Upload Configuration	
←IP-PBX (should be located on the LAN)	
Type: Generic PBX	
IP Address: 10 . 51 . 77 . 20	
Use domain name	
SIP Domain:	
Status	
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0	
VoIP Survival VPN	<u>^</u>
Qo5 Enhanced Security	
10 SIP Traversal Licenses 10 SIP User Registration Licenses	
Software Version: 4.6.2	
	Help

Configuration Steps:

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

Type:	Generic PBX	~

2) Enter the IP Address of the IP-PBX. The IP Address should be on the same LAN subnet as the Ingate unit.

IP Address:	10 . 51 . 77 . 20
_	

3) *Optional:* For some IP-PBX solutions they require a SIP Domain. This domain name is used to route SIP Requests to the IP-PBX associated with that domain. Select "Use domain name" and enter the FQDN

📃 Use domain	name	
SIP Domain:		н

4) Optional: Only for when Generic PBX is selected, will this option become available. When is option is enabled, the Ingate Registrar is enabled, later on the ITSP configuration, Identities or Users are assigned on the Registrar and associated to the incoming call characteristics. So the PBX registers to the Ingate and the Ingate sends the incoming call to these registered users/identities.

PBX registers at the Ingate	

5.5 ITSP

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

	Ingate Startup Tool	
	Network Topology IP-PBX ITSP_1 Upload Configuration	
🗿 at&t	Name: Generic ITSP	DID (start of range) (user name): DID range size:
	Provider address IP Address: U . 0 . 0 . 0 Use domain name Advanced Prefix: Prefix: Prefix: Prefix: Forward 3cx messages VEnable	Account Information: Use account Authentication name: (ame as Did Fibink) Domain: Password: Use user account on incoming call PBX local numbers (advanced) Local numbers (advanced) Local numbers are not used): Password (if PBX Password only used if PBX Password only used if PBX Password confu used): Password (if PBX Password (if PBX Password confu used): Password (if PBX
	Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIPa VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses Software Version: 4.6.2	wator 19, IG-092-702-2122-0

Configuration Steps:

1) In the ITSP drop down list, select AT&T. Ingate has confirmed interoperability with AT&T IP Flexible Reach. The unique requirements of the testing are contained in the Startup Tool.

Name:	AT&T	*

2) AT&T IP Flexible Reach uses a Trusted IP deployment, all that is required is to enter the IP Address or Domain of the AT&T IP Flexible Reach IP Border Element's IP. Enter the IP Address here.

Provider address —						
IP Address:	0	0	0	0		
🔲 Use domain nam	ne					

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 to add to outbound calls	Prefix:	
1.1.001031	Prefix to add to Prefix:	outbound calls

5.6 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.

e Startup 1001	•
ork Topology IP-PBX ITSP_1 Upload Configuration	
Disclaimer and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical	- Verbose Logging (SIP debug) I Enable
assistance regarding end-to-end interoperability issues, please contact support@ingate.com.	
	 Final step Logon to web GUI and apply settings Apply settings directly using serial interface
	Backup the configuration
- Status	SIDwater 10. IC-002-702-2122-0
10 SIP Traversal Licenses	51Paratur 19, 13-092-702-2122-0
Software Version: 4.6.2 Error: Please enter number, name and domain. Error: Please enter number, name and domain.	

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.



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.



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.

Administration	Basic Configuration	Network	Rules and Relays	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
Save/Load Configuration	Show Configuration	User Administratio	on Upgrade	Table Look	Date and Time	Restart	Change Language			
Test Ru	n and App	ly Conf	(Help)	Sh	ow Mes	ssage A	About Unap	plied Ch	anges	
Duration of	limited test m	ode:) ۞	On every	page				
30	seconds			00	On the Sa	ave/Load	d Configuration	page		
Apply o	configuration			01	Never					
Backup	(Help)									
The permar	ient configura	tion is not a	ffected.							
Save to	local file	Load fro	m local file		ocal file:			Browse		
Save/Lo	ad CLI Co	ommand	File (He	<u>lp)</u>						
The permar	nent configura	tion might b	e affected i	by load	ing a CL	I file.				
Save	config to CLI fil	e Lo	oad CLI file	Loc	al file:			Browse		
Abort A	ll Edits (Help)		Re	load Fa	ictory	Configurati	on <u>(Help</u>	0	
The perman	nent configura	tion is not a	ffected.	The p	ermaner	it configu	uration is not af	fected.		
Abort all	edits				Load fac	tory con	figuration			

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



6 Troubleshooting

This section should provide some tips for troubleshooting problems, including troubleshooting commands and contact numbers within Vendor X's Company for trouble escalation.

6.1 AT&T IP Flex to Ingate to IP-PBX Call Flow

For an Incoming call the call starts at the AT&T IP Flex IP Border Element's IP, they will deliver a DID, contained in the Request URI header of a SIP INVITE. Typically AT&T IP Flex IP Border Element will send an INVITE to the SIP URI address of "DID@IP_Address_of_Ingate". The Ingate then processes this through the Dial Plan and forwards the INVITE to the SIP URI address "DID@IP_Address_IP-PBX".

For an outgoing call the call starts at the IP-PBX, they will deliver a DID, contained in the Request URI header of a SIP INVITE. Typically IP-PBX will send an INVITE to the SIP URI address of "DID@IP_Address_of_Ingate". The Ingate then processes this through the Dial Plan and forwards the INVITE to the SIP URI address "DID@IP_Address_AT&T".



6.2 Startup Tool

6.2.1 Status Bar

Located on every page of the Startup Tool is the Status Bar. This is a display and recording of all of the activity of the Startup Tool, displaying Ingate unit information, software versions, Startup Tool events, errors and connection information. Please refer to the Status Bar to acquire the current status and activity of the Startup Tool.

~

6.2.2 Configure Unit for the First Time

Right "Out of the Box", sometimes connecting and assigning an IP Address and Password to the Ingate Unit can be a challenge. Typically, the Startup Tool cannot program the Ingate Unit. The Status Bar will display **"The program failed to assign an IP address to eth0"**.



Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power
	(Trust me, I've been there)
Ethernet cable is not connected to	Eth0 must always be used with the
Eth0.	Startup Tool.
Incorrect MAC Address	Check the MAC address on the Unit
	itself. MAC Address of Eth0.
An IP Address and/or Password have	It is possible that an IP Address or
already been assigned to the Ingate	Password have been already been
Unit	assigned to the unit via the Startup
	Tool or Console

Possible Problems	Possible Resolution
Ingate Unit on a different Subnet or	The Startup Tool uses an application
Network	called "Magic PING" to assign the IP
	Address to the Unit. It is heavily
	reliant on ARP, if the PC with the
	Startup Tool is located across
	Routers, Gateways and VPN Tunnels,
	it is possible that MAC addresses
	cannot be found. It is the intension
	of the Startup Tool when configuring
	the unit for the first time to keep the
	network simple. See Section 3.
Despite your best efforts	1) Use the Console Port, please refer to
	the Reference Guide, section
	"Installation with a serial cable", and
	step through the "Basic
	Configuration". Then you can use the
	Startup Tool, this time select "Change
	or Update the Configuration"
	2) Factory Default the Database, then try
	again.

6.2.3 Change or Update Configuration

If the Ingate already has an IP Address and Password assigned to it, then you should be able use a Web Browser to reach the Ingate Web GUI. If you are able to use your Web Browser to access the Ingate Unit, then the Startup should be able to contact the Ingate unit as well. The Startup Tool will respond with **"Failed to contact the unit, check settings and cabling"** when it is unable to access the Ingate unit.

ruoning the latest version of the Starty tool. formation is available here: http://www.ingate.com/startuptool.php o contact the unit. check estions and cabling

Possible Problems and Resolutions

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power
Incorrect IP Address	Check the IP Address using a Web
	Browser.
Incorrect Password	Check the Password.
Despite your best efforts	 Since this process uses the Web (http) to access the Ingate Unit, it should seem that any web browser should also have access to the Ingate Unit. If the Web Browser works, then the Startup Tool should work. If the Browser also does not have access, it might be possible the PC's IP Address does not have connection privileges in "Access Control" within the Ingate. Try from a PC that have access to the Ingate Unit, or add the PC's IP Address into "Access Control".

6.2.4 Network Topology

There are several possible error possibilities here, mainly with the definition of the network. Things like IP Addresses, Gateways, NetMasks and so on.



Possible Problems	Possible Resolution
Error: Default gateway is not	The Default Gateway is always the way
reachable.	to the Internet, in the Standalone or
	Firewall it will be the Public Default
	Gateway, on the others it will be a
	Gateway address on the local network.
Error: Settings for eth0/1 is not	IP Address of Netmask is in an Invalid
correct.	format.
Error: Please provide a correct	Netmask is in an Invalid format.
netmask for $eth0/1$	
Error: Primary DNS not setup.	Enter a DNS Server IP address

6.2.5 IP-PBX

The errors here are fairly simple to resolve. The IP address of the IP-PBX must be on the same LAN segment/subnet as the Eth0 IP Address/Mask.



Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: The IP PBX IP does not	The IP Address of the IP-PBX must be
seem to be on the LAN.	on the same subnet as the inside
	interface of the Ingate Eth0.
Error: You must enter a SIP	Enter a Domain, or de-select "Use
domain.	Domain"
Error: As you intend to use RSC	Enter a Domain or IP Address used for
you must enter a SIP domain.	Remote SIP Connectivity. Note: must
Alternatively you may configure a	be a Domain when used with SIP
static IP address on eth1 under	Trunking module.
Network Topology	_

6.2.6 ITSP

The errors here are fairly simple to resolve. The IP address, Domain, and DID of the ITSP must be entered.



Possible Problems	Possible Resolution
Error: Please enter a domain name	Enter a Domain, or de-select "Use
for your provider	Domain"
Error: Please enter number, name	Enter a DID and Domain, or de-select
and domain.	"Use Account"

6.2.7 Apply Configuration

At this point the Startup Tool has pushed a database to the Ingate Unit, you have Pressed "Apply Configuration" in Step 3) of Section 4.7 Upload Configuration, but the "Save Configuration" is never presented. Instead after a period of time the following webpage is presented. This page is an indication that there was a change in the database significant enough that the PC could no longer web to the Ingate unit.



Possible Problems	Possible Resolution
Eth0 Interface IP Address has	Increase the duration of the test mode,
changed	press "Apply Configuration" and start a
	new browser to the new IP address, then
	press "Save Configuration"
Access Control does not allow	Verify the IP address of the PC with the
administration from the IP address	Startup Tool. Go to "Basic
of the PC.	Configuration", then "Access Control".
	Under "Configuration Computers",
	ensure the IP Address or Network
	address of the PC is allowed to HTTP to
	the Ingate unit.

6.3.1 Display Logs

Administration Basic Configuration Network SIP SIP Failover Virtual Private Quality Services Traffic	r of Logging and Tools About	
Display Log Capture Network Configuration Classes Sending		
Search the Log (Heln)	Support Report (Help)	
	Include configuration database:	
Display log 2000 fows page (timeout seconds)	O Yes O No	
Periodica arch 180 seconds until next search		
	Make sure the Log class for SIP debug messages is set to Local if you have a SIP-related problem.	
Press "Display Log"	Export support report	
to see internal logs		Always create a
Packet selection of the selection are three	Time Limits	"Support Report"
packets as selected choice.	Show log from: (clear)	for Ingate Support
	MM-DD) (HH:MM:SS)	for ingate support
Packet Type Selection		
All packets	Show log until: (clear)	
IP Address Selection (Help)	date (YYYY- time	
A: D this address	MM-DD) (HH:MM:SS)	
B: not this address	✓ Show newest at top	
$\bigcirc A \text{ src } \bigcirc A \text{ dst } \odot A \text{ any}$ $\bigcirc A \text{ to } B \bigcirc B \text{ to } A \bigcirc B \text{ etween } A \& B$ in this combination		
	Show This	Show newest
Protocol/Port Selection	Select: <u>All</u> , <u>None</u> , <u>SIP</u> .	log on top
 All IP protocols 	Configuration server logins	
	Administration and configuration	
	Manual reconfigurations and	
0 CDF	reboots	
OICMP	Time changes	
O ESP	DHCP/PPPoE client	
	RADIUS errors	
○ Protocol number:(Help) □ not	SNMP problems	
	Hardware errors	
SIP Packet Selection (Help)	Mail errors	
Call ID:	Negotiated IPsec tunnels	
Call-ID.	IPsec key negotiations	
SIP Methods:	IPsec key negotiation debug	
IP addresses:	messages	
From Header:	IPsec user authentication	
Filter of SIP	PPTP negotiations	
specific fields	SIP errors	
	✓ SIP signaling	
	✓ SIP packets	Filter on SIP
	✓ SIP license messages	traffic only
	✓ SIP media messages	traffic Only
	✓ SIP debug messages	
Export the Log (Help)		
Export log IAB-separated file 20 MB max	Clear form	

6.3.2 Packet Capture

Administration Basic Network SIP SIP Failover Virtual Private Quality of Lo Services Traffic Failover Networks Service and	pgging d Tools
Display Packet Check Logging Log Log Log Capture Network Configuration Classes Sending	_[
Capture status: Inactive	
Captured data size: 7 kB Captured when: 2009-04-28 12:52:21	
Ingate SIParator has a built-in packet capture function which produces pcap trace files.	
You can select to capture traffic on one specific interface or on all interfaces.	
For contacts with the Ingate Support Team, a packet capture is not what is usually expected (sometimes it is even not useful). For these purposes, please always send a <u>Support Report</u> .	1
Network Interface Selection	
All interfaces	
You can also select the type of IP pace cook multiple captures	
port. from multiple interfaces	
IP Address Selection (Help) into one PCAP	
A: not this address	
B: not this address	
\land A src \land A dst \diamond A any \land A to B \land B to A \land Between A&B	
Protocol/Port Selection	
All IP protocols	
O TCP	
O UDP Filter on Port,	
OICMP Other criteria	
	Download PCAP File
O Protocol number:(Help)	
Start capture Download captured data	
Stop capture Delete captured data	
Start Capture, reproduce the problem, then Stop Capture	

6.3.3 Check Network



7 Appendix – Nortel CS1000 Configuration

7.1 Nortel CS1000 and Ingate SIParator (SBC) with AT&T IP Flexible Reach

The Nortel CS1000 IP PBX was also tested with an on-site Ingate SIParator used as a session border controller (SBC). In this architecture, the CS1000 directs SIP signaling to the Ingate SIParator (SBC), which communicates with the AT&T IP Border Elements. The media should also traverse through the Ingate SIParator (SBC).

The Ingate SIParator is currently supported by AT&T and Nortel on IP Flexible Reach and can be deployed at a customer site.



Nortel CS1000 Configuration

Please refer to AT&T VOIP Nortel CS 1000 (Release 5.00W / 5.50J) SIP Configuration Guide (NN10000-104 Issue 2.4) Section 4 for configuration of the CS1000 for IP Flexible Reach, with one change: In Section 4.3.3, enter the on-site Ingate SIParator's (SBC) IP address (instead of the IP Border Element's IP) for the Primary Proxy or Redirect (TLAN) IP address, ensure the Port used is 5060, and the Transport Protocol used is UDP.

7.1.1 Ingate SIParator Configuration

Section 4.0 of this document describes the setup requirements for the Ingate SIParator and Firewall products. The Ingate Startup Tool can be used to accurately provide the necessary programming within the Ingate products to deliver the AT&T IP Flex SIP Trunk to the Nortel CS1000.

7.2 Configuring the SIParator to Failover to a Secondary IPBE

AT&T will provide the customer with multiple IPBE addresses for failover conditions. The SIParator can be configured to send calls to a secondary IPBE, if the primary IPBE is unavailable.

Go to SIP Traffic \Box Dial Plan, under the "Forward To" section, add a subgroup for the "AT&T" group; under "Reg Expr", enter the expression sip:1@x.x.x.x as the one above it, replacing x.x.x.x with the IP address of the secondary IPBE.

Forward To	<u>Help)</u>							
k	C.L.	Use This	Or	This		Or This	Delete	
Name Subno.		Account	Replacement URI	eplacement URI Port Transport		Reg Expr	Delete	
€ AT&T	1	- 💙			· •	sip:\$1@135.25;		
	2	• •			• 💌	sip:\$1@135.25.		
							1 m m	

In this example, the "Reg Expr" for the primary IPBE is sip:\$1@135.25.29.74, and for the secondary IPBE, sip:\$1@135.25.29.135. This will allow the SIParator to send calls to the primary IPBE at 135.25.29.74, and if there is no response from the primary, the SIParator will send the call to the secondary IPBE at 135.25.29.135.

7.3 Example Ingate Configuration with Nortel

7.3.1 Networks - Networks & Computers

Here is an example of a SIParator in a LAN SIParator configuration when used with the Nortel CS1000. Networks and Computers section is like a Route List, used to identify various Networks and associate them to specific interfaces. In the case of a LAN SIParator, there is only one interface so referencing it is not necessary. Stand-alone and DMZ-LAN will have references to the WAN Interface, DMZ Interface and the LAN Interface for each of the networks connected.

Administration	Basic Configuration	Network	SIP Service	SIP Traffic	Failover	Virtual Private Networks	Quality of Logg Service and T	ing ools About		
Networks and Computers	Default Gateways Int	All erfaces VLA	AN EthO) Eth1 Eth	Interfa 12 Status	ce s PPPoE Topo	blogy			
Network	s and Con	puters								
				I	Lower Li	mit	Up (for	per Limit IP ranges)		Delete
Nai	me	Subgrou	р	DNS N or IP Ad	Name Idress	IP Address	DNS Name or IP Addres	e IP Address	Interface/VLAN	Row
+ Central	Site -		~ 1	72.16.6.0		172.16.6.0	172.16.6.255	172.16.6.255	· •	
+ Generic	- PBX		v 1	72.16.5.61	1	172.16.5.61			- •	
+ ITSP_IF	· -		~ 1	35.25.29.0)	135.25.29.0	135.25.29.255	135.25.29.255	- •	
+ LAN	-		~ 1	72.16.5.0		172.16.5.0	172.16.5.255	172.16.5.255	· •	
+ WAN	- 1		~ 0	.0.0.0		0.0.0.0	255.255.255.255	255.255.255.255	- •	
+ localhos	st -		v 1	27.0.0.1		127.0.0.1			- 🗸	

7.3.2 SIP Services - Interoperability

The Interoperability page is where common deviations from the SIP Standard are programmed.

- 1. Remove the Nortel CS1000 IP Address from the VIA Headers.
- 2. Ensure the recommended settings of Signaling Order of Re-INVITE.



7.3.3 SIP Traffic – Dial Plan

The Dial Plan is how the Ingate defines the traffic routing policies. Incoming and Outgoing, by defining three attributes;

- 1. Matching FROM Header to perform Source based matching
- 2. Matching Request URI to perform SIP routing matching
 - a. Inbound expression has the Ingate's IP
 - b. Outbound has AT&T IPBE's IP
- 3. Forward To defines the target destination
 - a. The AT&T expression has IPBE's IP
 - b. The Nortel PBX's expression has CS1000's IP

Finally the three attributes are put together in the Dial Plan to form a routing policy.

inistration Co	Basic onfiguration	vork SIP Services	SIP Traffic Failove	Virtual Private Networks	Quality Servio	of Loggi ce and To	ng ols Ab	out			
SIP thods Filtering	Local Auth g Registrar and	entication SII Accounting Accou	P <mark>Dial</mark> Ints <mark>Plan</mark> Routi	ing Classes Statu	5						
Use Dial F	Plan <u>(Help)</u>	Emerger	icy Number	r <u>(Help)</u>							
) On		911									
) Off) Fallback											
Matching	From Head	u (Help)									
wratening	From mead	ti <u>(itelp)</u>		0.71	_						
Name	Useri	Use Ihis Jame I	Domain	Or This Reg Expr	Tra	Transport		etwork	Delete Row		
AT&T	*	*		reg zapi	UDP	*	ITSP	IP 🗸			
Generic PB	<pre> / *</pre>	*			UDP	~	Gene	ric PBX 🗸			
LAN	*	*			UDP	~	LAN	v			
WAN	*	*			Any	~	WAN	~			
localhost	*	*			Any	~	localh	iost 🗸			
Name Inbound Outbound	Pre	fix	Head	Use This Tail - ×		(in. Tail		Domain	 F sip:(. Or This Reg Expr .*)@172.16.5 .*)@135.25.2	- D
Add new ro Forward 1	ws 1 1 Γο <u>(Help)</u>	ows.		Or	This			Or Th	nis		1
Nam	e Sub	no. Accou	nt Replace	ment Domain	Port	Trans	port	Reg Exp	pr 1	Delete Row	
+ AT&T	1	- 🗸				-	•	sip:\$1@135	.25.29		
+ Generic F	PBX 1	- 🗸				-	•	sip:\$1@172	.16.5.		
Add new ro Dial Plan	ws 1 g	roups with 1	rows per	group.							
No	From Hooder	Request-				Former	Te		Add	Prefix	
140.	From Heade	URI		Action		rorward	110	Forward		ENUN	I
1	Generic PBX	Outbound	Forward		*	AT&T	*				
2	AT&T	Inbound	Forward		*	Generic P	BX 🗸				
3	localhost	/ - ·	Allow		*	-	*				
4	WAN		Reject		*	-	*				

7.4 Centralized Voicemail in an IP Flexible Reach Environment

It is common for Nortel customers with large IP PBX solutions to use the centralized voicemail architecture. In this architecture, the larger IP PBX servers at the main locations host the voicemail capabilities, and the "remote" or "non-voicemail" sites communicate to main location IP PBX servers to access voicemail.

NOTE Currently, this configuration applies to Nortel CS1000 environments. Additionally, IP Flexible Reach is deployed at each CS1000 location.

NOTE The Nortel CS1000 Centralized Voicemail application has one caveat when the Ingate SIParator is deployed in a LAN SIParator Mode

For centralized voicemail, an Ingate SIParator session border controller (SBC) is required at the remote site B. See below figure:



Figure: Centralized Voicemail, Standard Call Flow with Ingate SIParator

Inbound calls are sent to the Ingate SIParator (SBC) before reaching the CS1000. When an incoming call to the non-voicemail site B is forwarded to voicemail at site A, the bidirectional RTP media traverses the Ingate SIParator (SBC). This is a standard and supported IP Flexible Reach call flow.

7.4.1 Detailed Sample Network Diagram

Refer to the following network diagram as an example (please keep in mind that not all physical/logical connections are defined in this diagram):



Figure: Sample Centralized Voicemail Network Diagram

The following are required for centralized voicemail in an IP Flexible Reach environment:

- Each location will have IP Flexible Reach
- Each location has at least TWO Signaling Servers: one for interfacing with IP Flexible Reach, another for private MCDN networking. The Network Routing Server (NRS) is required for private MCDN networking call control Nortel recommends deploying the NRS at the main/central location(s).
- Ingate SIParator (SBC) at each branch (non-voicemail) site, an Ingate SIParator at the main site is optional but not required

7.4.2 Nortel CS1000 Configuration

Please refer to AT&T VOIP Nortel CS 1000 (Release 5.00W / 5.50J) SIP Configuration Guide (NN10000-104 Issue 2.4) Section 4 for configuration of the CS1000 for IP Flexible Reach and the Centralized Voicemail application.

7.4.3 Ingate SIParator Configuration

Section 5.0 of this document describes the setup requirements for the Ingate SIParator and Firewall products with the Nortel CS1000 for AT&T IP Flexible Reach application.

The Nortel CS1000 Centralized Voicemail application has one caveat when the Ingate SIParator is deployed in a LAN SIParator Mode. There is one additional programming setup required for correct operation, Network – Topology section. The purpose of this Topology section is where you list all networks, as defined on the "Networks and Computers" dialogue that are known by your firewall and not reached via the default gateway of the firewall. All networks that can reach each other without going through the firewall should be grouped together.

7.4.3.1 Networks and Computers

Here is an example of a SIParator in a LAN SIParator configuration when used with the Nortel CS1000. Networks and Computers section is like a Route List, used to identify various Networks and associate them to specific interfaces. In the case of a LAN SIParator, there is only one interface so referencing it is not necessary. There is an addition of the "Central Site" Network addresses to be later used to define the "Topology".

Admini	istration C	Basic Configurat	ion Netwo	ork _{Se}	SIP rvices	SII Traf	p fic Fo	ailover	Virtual Priv Network	vate cs	Quality of Service and To	ing pols	About			
Netwo Com	orks and I nputers G	Default iateways	All Interfaces	VLAN	Eth0	Eth1	Eth2	Interface Status	e PPPoE	Topol	ogy					
Ne	Networks and Computers															
						Lower Limit					Upper Limit (for IP ranges)					Delete
	Name		Subgroup			DNS Name or IP Address			IP Addr	ess	DNS Name or IP Addres	s	Interface/VLAN IP Address			Row
+	CentralSit	te		•	17	2.16.	5.0		172.16.6	5.0	172.16.6.255		172.16.6.255	-	~	
+	Generic F	PBX	-	•	17	2.16.	5.61		172.16.5	5.61				-	~	
÷	ITSP_IP		-	•	13	5.25.2	29.0		135.25.2	29.0	135.25.29.255		135.25.29.255	-	~	
÷	LAN		-	•	17	2.16.	5.0		172.16.5	5.0	172.16.5.255		172.16.5.255	-	~	
+	WAN		-	•	0.0	0.0.0			0.0.0.0		255.255.255.255		255.255.255.255	-	~	
÷	localhost		-	•	12	7.0.0	1		127.0.0.	1				-	~	

7.4.3.2 Topology

The result of putting two IP addresses in the same Surrounding is that the SIParator will not NAT any traffic between them. If two devices are in different Surroundings, the SIParator will rewrite the SIP signaling to make all SIP media be sent to itself instead of directly between the end devices. By default, the SIParator will not allow media between endpoints if the unit negotiating the media stream is not in the same Surrounding as the endpoint that will receive media. This can happen when you have an IP-PBX on one network and the clients on a different network. To enable the endpoints to receive media, you can allow additional negotiators for a Surrounding. In the case of the IP-PBX and the clients above, you would allow the IP-PBX network as an Additional Negotiator for the client Surrounding.

Ad	ministration	Bas Configu	ic ration Netw	ork S	SIP ervices	SII Traf	P fic F	ailover	'irtual Pr Networ	ivate ks	Quality of Service	Log and	ging Tools	About
N	letworks and Computers	Default Gateway	All s Interfaces	VLAN	Eth0	Eth 1	Eth2	Interface Status	PPPoE	Topolo	gy			
I	Surroun f your SIPa	dings rator typ	(<u>Help)</u> be is not set	to DN	AZ, th	e sett	ings i	n this sec	tion wil	l have 1	no effect			
L	Netwo	rk .	Additional	Negot	iators	s De	lete I	Row						
Ш	LAN	*	CentralSite	*										
L	CentralSit	e 💙	LAN	*										

7.4.3.3 Interoperability

Remove the Nortel CS1000 IP Address from the VIA Headers. And ensure the recommended settings of Signaling Order of Re-INVITE.

Administration Basic Configurati	on Network Se	SIP SIP SIP Traffic	Failover V	'irtual Privat Networks	e Quality of Service	f Logging About About					
SignalingMediaBasicEncryptionEncryption	ion Interoperabili	Sessions ty and Media	Remote SIP Connectivity	VoIP Survival							
Remove Via He	Remove Via Headers (Help) Signaling Order of Re-INVITEs (Help)										
SIP Ser	ver				Recon	ommended setting: Send re-INVITEs all the way directly					
DNS Name or IP Address	IP Address	Delete Row	ſ		⊙ S	Send re-INVITEs all the way directly Send response before re-INVITEs are forwarded					
135.25.29.74	135.25.29.74										

8 Appendix – Special Notes

Emergency 911/E911 Services Limitations

While AT&T IP Flexible Reach services support E911/911 calling capabilities in certain circumstances, there are significant limitations on how these capabilities are delivered. Please review the AT&T IP Flexible Reach Service Guide in detail to understand these limitations and restrictions.

NAT'ing From Header

The Ingate does not NAT the From Header, although there is no technical impact, it was an observation. This is scheduled to be resolved in next release of the Ingate software.