ingate

Application Note

Asterisk BE with Remote Phones - Configuration Guide

15 January 2009

Table of Contents

1 ASTERISK BUSINESS EDITION AND INGATE 1

1.1 REMOTE SIP PHONE SUPPORT 2

2 INGATE STARTUP TOOL 3

3 CONNECTING THE INGATE FIREWALL/SIPARATOR 4

4 USING THE STARTUP TOOL 6

4.1 CONFIGURE THE UNIT FOR THE FIRST TIME 6
4.2 CHANGE OR UPDATE CONFIGURATION 9
4.3 NETWORK TOPOLOGY 12
4.3.1 Product Type: Firewall 13
4.3.2 Product Type: Standalone 15
4.3.3 Product Type: DMZ SIParator 17
4.3.4 Product Type: DMZ-LAN SIParator 19
4.3.5 Product Type: LAN SIParator 21
4.3.6 Product Type: LAN SIParator – "SBE SIParator Only" 23
4.4 IP-PBX 25
4.5 UPLOAD CONFIGURATION 27

5 ASTERISK BUSINESS EDITION SETUP 29

5.1 USER EXTENSION ON PBX SETUP 29
5.2 SIP SETTINGS 30
5.3 OUTBOUND PROXY SETTINGS WHEN USING SIPARATOR 31

6 TROUBLESHOOTING 32

6.1 SIP PHONE REGISTRATION INFORMATION 32
6.2 STARTUP TOOL 33
6.2.1 Status Bar 33
6.2.2 Startup Tool - Configure Unit for the First Time 33
6.2.3 Change or Update Configuration 34
6.2.4 Network Topology 35
6.2.5 IP-PBX 36
6.3 INGATE WEB GUI - APPLY CONFIGURATION 36
6.4 DNS BENEFITS AND ISSUES 37

Tested versions:	Ingate Firewall and SIParator version 4.6.4 Startup Tool version 2.4.0 Asterisk Business Edition version 2.1.1

Revision History:

Revision	Date	Author	Comments
	2009-01-15	Scott Beer	Minor Edits

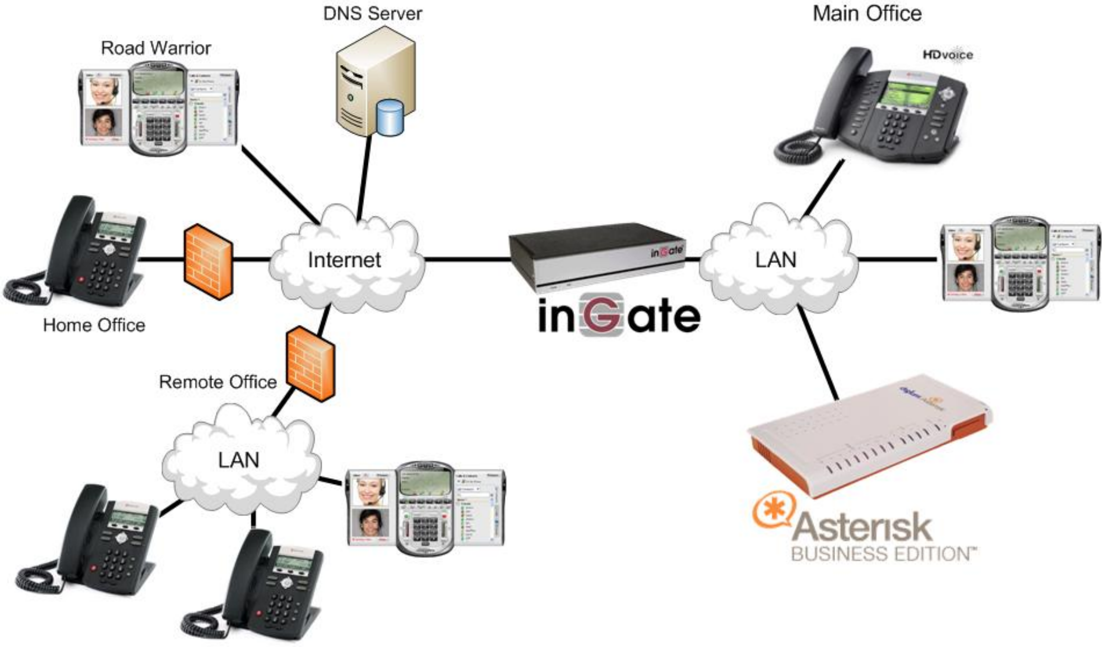
1 Asterisk Business Edition and Ingate

Digium offers Asterisk Business Edition, a professional-grade version of the Asterisk open source PBX, for the Linux operating system. Tailored for small and medium sized business applications, Asterisk Business Edition provides tested reliability of critical functions and features. It solves a wide range of challenges, from common PBX and key system replacements to highly-specialized applications. Asterisk Business Edition supports from 10 to 240 simultaneous calls per system.

The Asterisk Business Edition solution allows for the connectivity and use of a wide variety of SIP Phones, both desk phones and soft-phones. These SIP Phones can be from a number of different vendors, such as Polycom, Snom, Counterpath and more. These SIP Phones can be located both on the Enterprise LAN or abroad over the Internet, and in Remote/Home Offices.

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.

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 remote SIP Phones connectivity to the Asterisk Business Edition IP-PBX solution. The Ingate products offer the use of the Remote SIP Connectivity Module, where there are features such as Far End NAT Traversal and a STUN Server. These features allow the Ingate to overcome NAT issues on the far end of the call.



1.1 Remote SIP Phone Support

In this application, the Asterisk Business Edition solution is the IP-PBX and SIP Domain Server. It 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 protected by the Ingate from any malicious attacks.

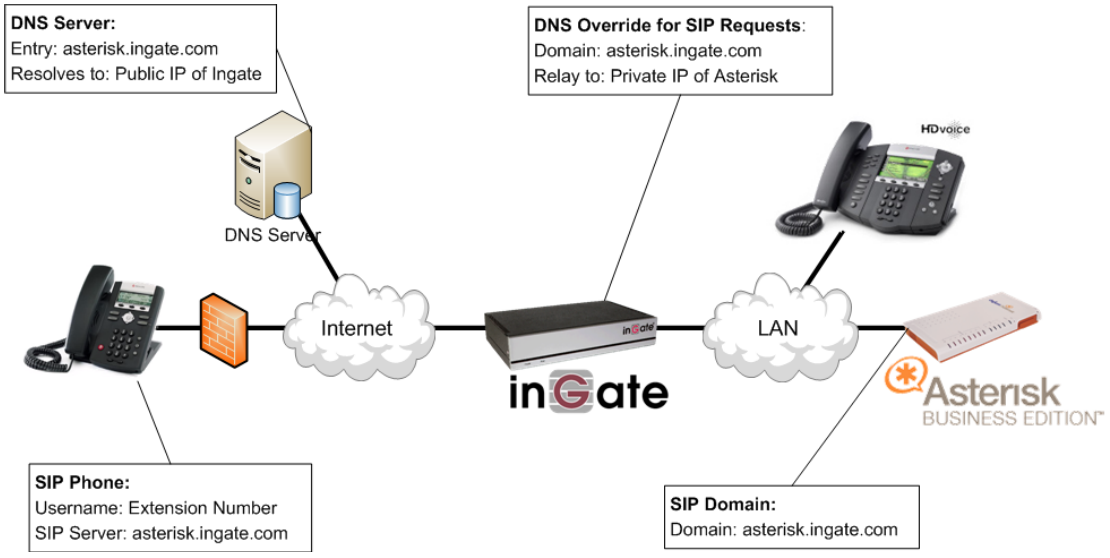
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

The SIP Phones can be of any vendor type, located anywhere across the Internet or any remote networks.

Requirements:

1) The use of a Fully Qualified Domain Name (FQDN) to resolve the SIP Domain of the Asterisk BE server. Meaning the Asterisk BE must respond to this SIP Domain, the SIP Phones must have this FQDN as the SIP Server address, all devices need to be able to do a DNS Lookup to resolve the FQDN to an IP address.
2) The Ingate must have the Remote SIP Connectivity Module to solve Far End NAT Traversal issues with remote phones.

Application Diagram


DNS Server:
Entry: asterisk.ingate.com
Resolves to: Public IP of Ingate
DNS Override for SIP Requests:
Domain: asterisk.ingate.com
Relay to: Private IP of Asterisk
HDvoice
DNS Server
Internet
ingate
inGate
LAN
Asterisk
BUSINESS EDITION
SIP Phone:
Username: Extension Number
SIP Server: asterisk.ingate.com
SIP Domain:
Domain: asterisk.ingate.com

Look for the Asterisk Business Edition Icon Asterisk BUSINESS EDITION to focus your attention to specific Asterisk BE setup instructions. These instructions are specific to the Ingate & Asterisk deployment with Remote SIP Phone.

2 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 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 Asterisk BE solution IP-PBX, this will setup all the routing needed to enable remote users to access and use the enterprise Asterisk BE IP-PBX. Thanks to detailed interoperability testing, Ingate has been able to create this tool with pre-configured setups for the Asterisk BE IP-PBX solutions with use with remote phones.

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 or ITSP in the lists, 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 Asterisk BE IP-PBX to any Remote SIP Phone. Additional programming and administration of this Ingate unit should be done through the Web Administration.

3 Connecting the Ingate Firewall/SIParator

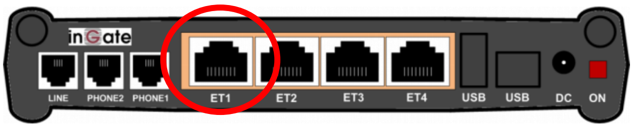
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

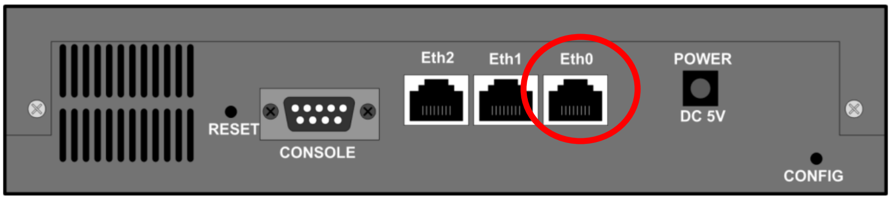
Configuration Steps:

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".

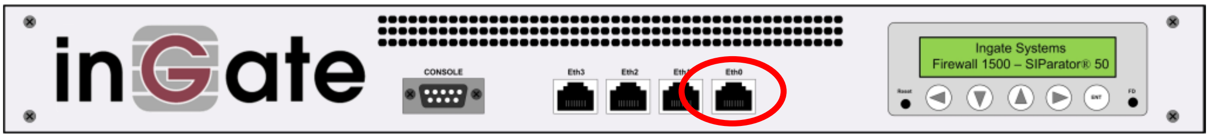
Ingate SIParator SBE (Back)



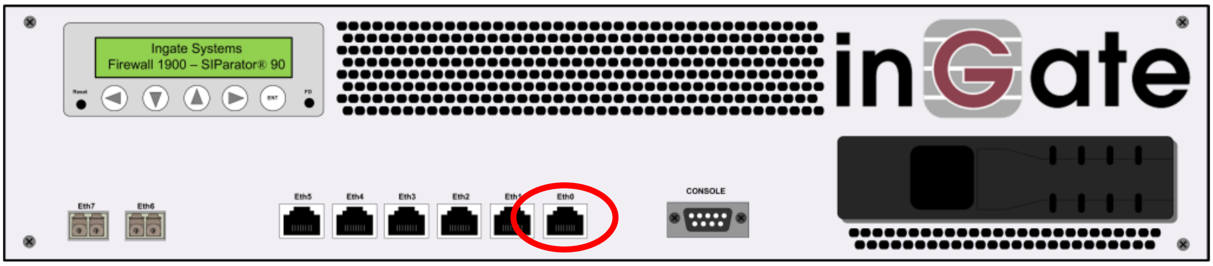
Ingate 1190 Firewall and SIParator 19 (Back)



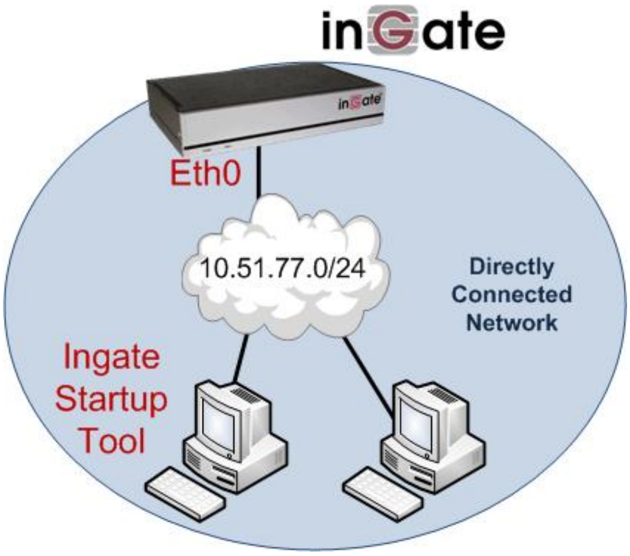
Ingate 1500/1550/1650 Firewall and SIParator 50/55/65



Ingate 1900 Firewall and SIParator 90



3) The PC/Server with the Startup Tool should be located on the same LAN segment/subnet. 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 4: Using the Startup Tool for instructions on using the Startup Tool.

4 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.

4.1 Configure the Unit for the First Time

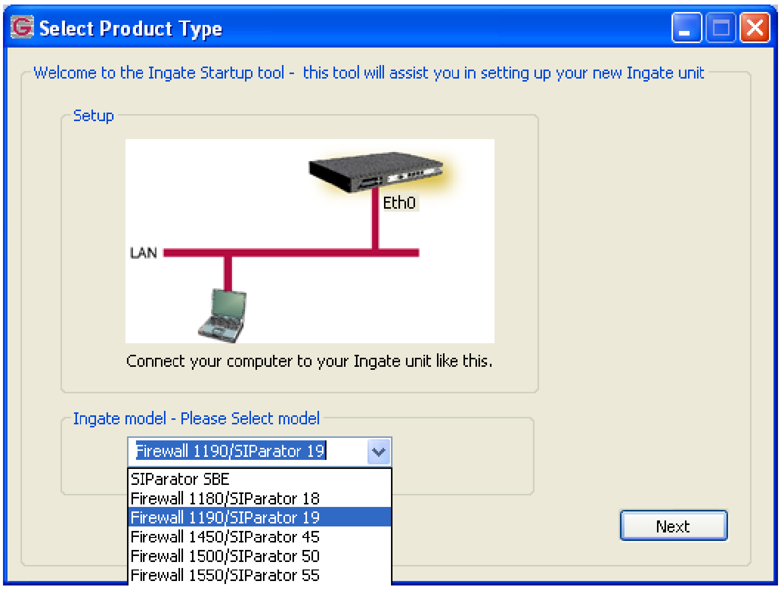
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.



Select Product Type

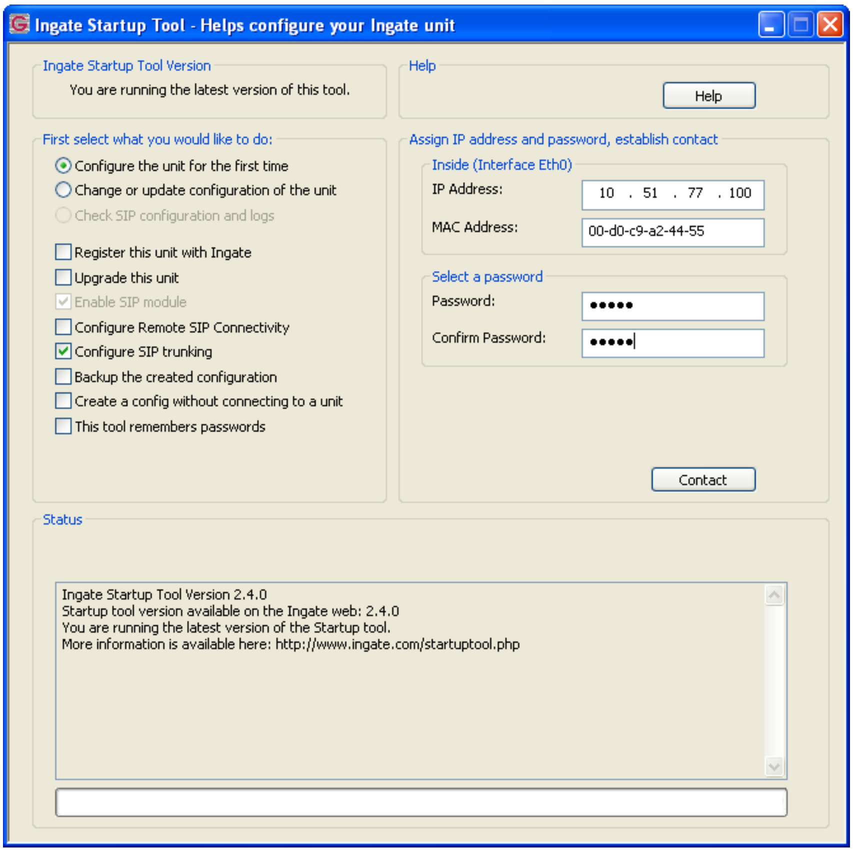
Welcome to the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit

Connect your computer to your Ingate unit like this.

Ingate model - Please Select model: Firewall 1190/SIParator 19

Setup
Eth0
LAN
SIParator SBE
Firewall 1180/SIParator 18
Firewall 1190/SIParator 19
Firewall 1450/SIParator 45
Firewall 1500/SIParator 50
Firewall 1550/SIParator 55
Next

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


Ingate Startup Tool - Helps configure your Ingate unit
Ingate Startup Tool Version
Help
Help
First select what you would like to do:
Assign IP address and password, establish contact
Inside (Interface Eth0)
Select a password
Contact
Status

You are running the latest version of this tool.

● Configure the unit for the first time
○ Change or update configuration of the unit
○ Check SIP configuration and logs

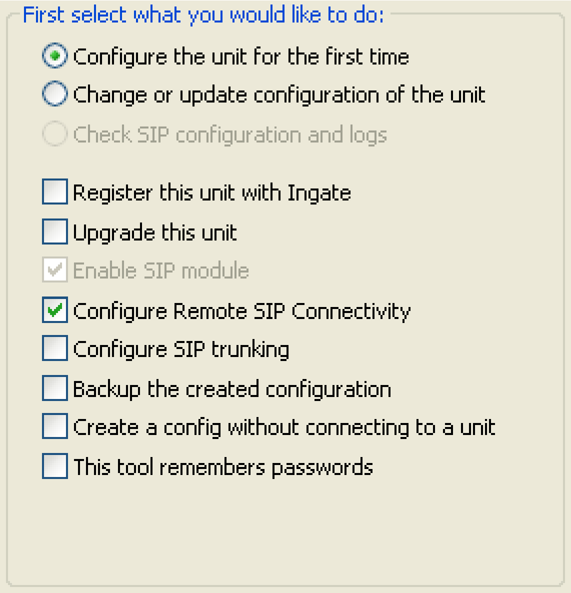
□ Register this unit with Ingate
□ Upgrade this unit
☑ Enable SIP module
□ Configure Remote SIP Connectivity
☑ Configure SIP trunking
□ Backup the created configuration
□ Create a config without connecting to a unit
□ This tool remembers passwords

IP Address: 10 . 51 . 77 . 100
MAC Address: 00-d0-c9-a2-44-55

Password: •••••
Confirm Password: •••••

```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

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



First select what you would like to do:

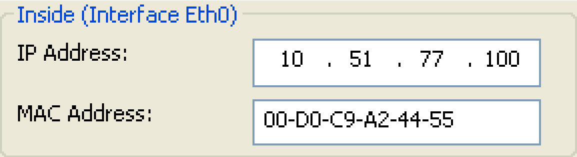
● Configure the unit for the first time
○ Change or update configuration of the unit
○ Check SIP configuration and logs

□ 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 Remote SIP Connectivity" if you want the tool to configure Remote Phone access to the Asterisk Business Edition server.

b. Select “Register this unit with Ingate” if you want the tool to connect with www.ingate.com to register the unit. If selected, consult the Startup Tool – Getting Started Guide.
c. Select “Upgrade this unit” if you want the tool to connect with www.ingate.com to download the latest software release and upgrade the unit. If selected, consult the Startup Tool – Getting Started Guide.
d. Select “Backup the created configuration” if you want the tool to apply the settings to an Ingate unit and save the config file.
e. Select “Creating a config without connecting to a unit” if you want the tool to just create a config file.
f. 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. The MAC Address can be found on a sticker attached to the unit.

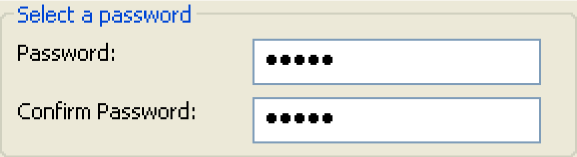


Inside (Interface Eth0)

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.

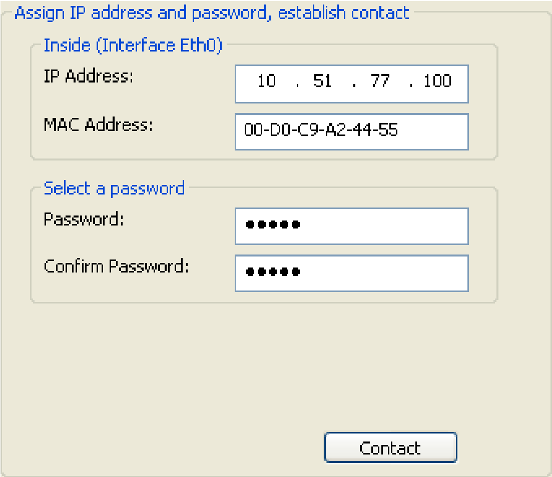


Select a password

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.



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: ●●●●●

8) Proceed to Section 4.3: Network Topology.

4.2 Change or Update Configuration

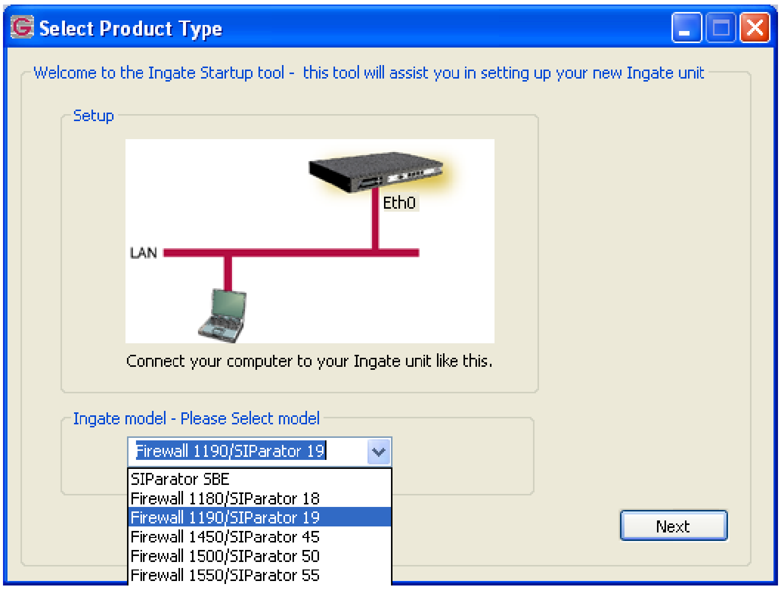
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

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 4.1: "Configure the Unit for the First Time".

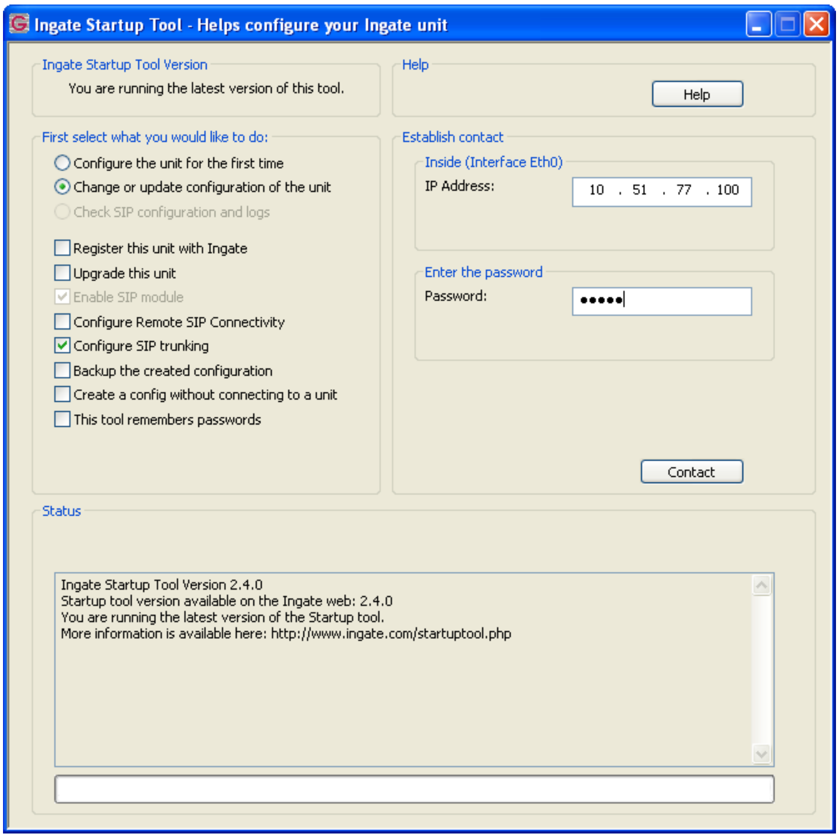
Configuration Steps:

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


Select Product Type
Welcome to the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit
Setup
Eth0
LAN
Ingate model - Please Select model
Firewall 1190/SIParator 19
SIParator SBE
Firewall 1180/SIParator 18
Firewall 1190/SIParator 19
Firewall 1450/SIParator 45
Firewall 1500/SIParator 50
Firewall 1550/SIParator 55
Next

Connect your computer to your Ingate unit like this.

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



Ingate Startup Tool Version
You are running the latest version of this tool.

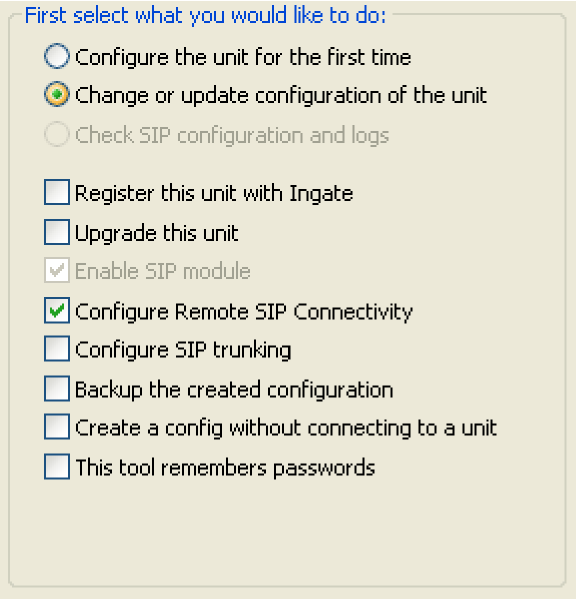
First select what you would like to do:
○ Configure the unit for the first time
● Change or update configuration of the unit
○ Check SIP configuration and logs
□ Register this unit with Ingate
□ Upgrade this unit
☑ Enable SIP module
□ Configure Remote SIP Connectivity
☑ Configure SIP trunking
□ Backup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

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

Status

```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

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

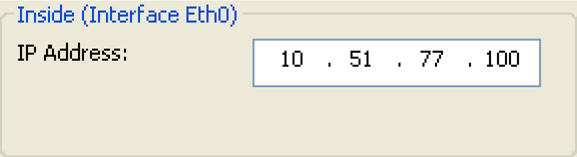


First select what you would like to do:
○ Configure the unit for the first time
● Change or update configuration of the unit
○ Check SIP configuration and logs
□ Register this unit with Ingate
□ Upgrade this unit
☑ Enable SIP module
☑ Configure Remote SIP Connectivity
□ Configure SIP trunking
□ Backup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

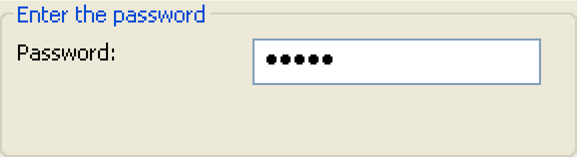
a. Select “Configure Remote SIP Connectivity” if you want the tool to configure Remote Phone access to the Asterisk Business Edition server.

b. Select "Register this unit with Ingate" if you want the tool to connect with www.ingate.com to register the unit. If selected, consult Startup Tool – Getting Started Guide.
c. Select "Upgrade this unit" if you want the tool to connect with www.ingate.com to download the latest software release and upgrade the unit. If selected, consult Startup Tool – Getting Started Guide.
d. Select "Backup the created configuration" if you want the tool to apply the settings to an Ingate unit and save the config file.
e. Select "Creating a config without connecting to a unit" if you want the tool to just create a config file.
f. Select "The tool remembers passwords" if you want the tool to remember the passwords for the Ingate unit.

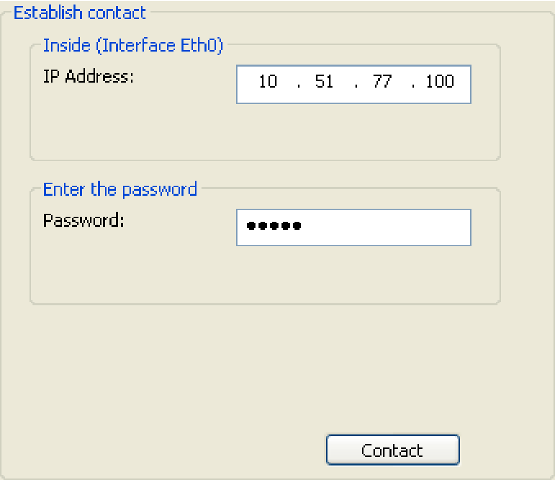
5) In the "Inside (Interface Eth0)",
   a. Enter the IP Address of the Ingate Unit.


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

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


Enter the password
Password: ●●●●●

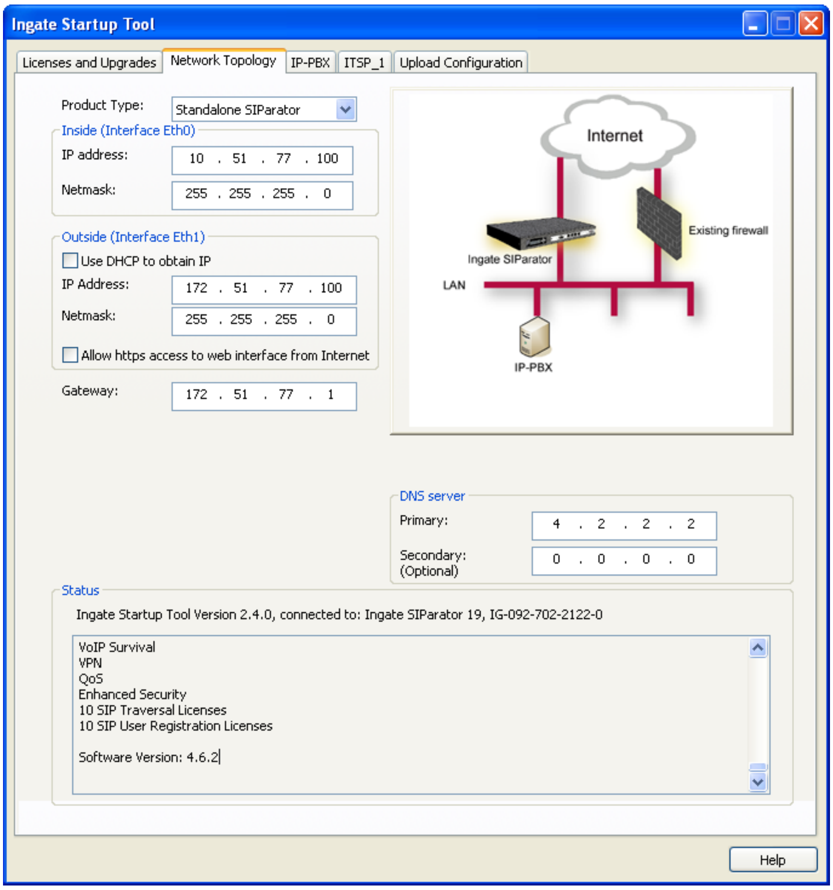
7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.


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

8) Proceed to Section 4.3: Network Topology.

4.3 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.



Product Type: Standalone SIParator

Inside (Interface Eth0)

IP address: 10 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

Outside (Interface Eth1)

□ Use DHCP to obtain IP

IP Address: 172 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

□ Allow https access to web interface from Internet

Gateway: 172 . 51 . 77 . 1

DNS server

Primary: 4 . 2 . 2 . 2

Secondary: (Optional) 0 . 0 . 0 . 0

Status

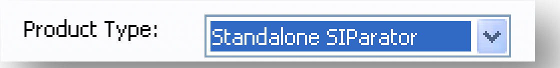
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

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



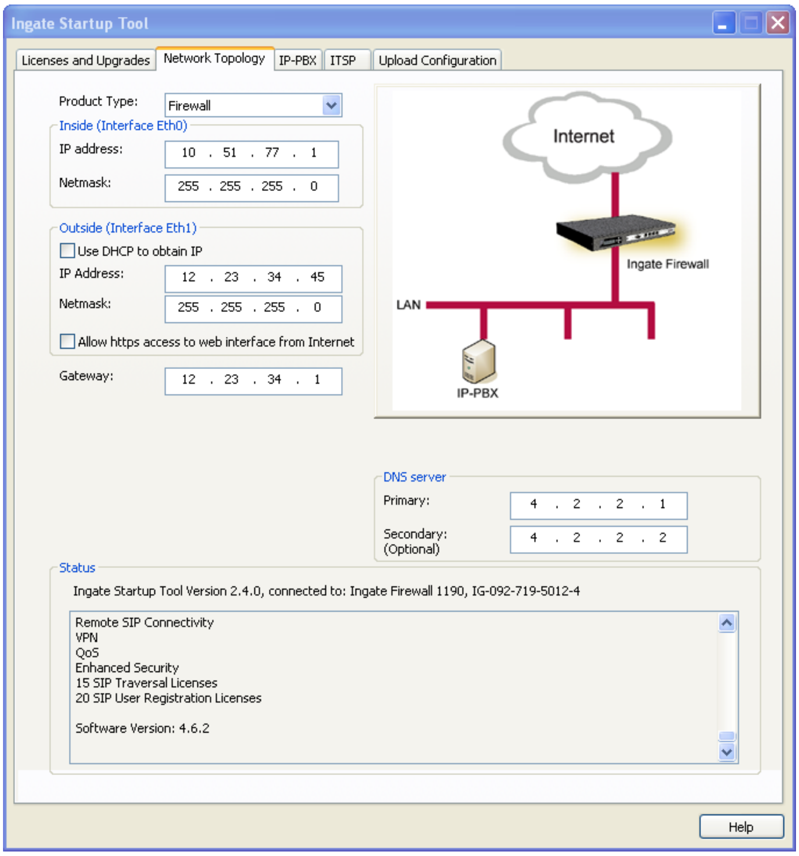
Product Type: Standalone SIParator

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. Select; Firewall, DMZ SIParator, DMZ-LAN SIParator, LAN SIParator, and Standalone SIParator.

4.3.1 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: Firewall

Inside (Interface Eth0)

IP address: 10 . 51 . 77 . 1

Netmask: 255 . 255 . 255 . 0

Outside (Interface Eth1)

□ Use DHCP to obtain IP

IP Address: 12 . 23 . 34 . 45

Netmask: 255 . 255 . 255 . 0

□ Allow https access to web interface from Internet

Gateway: 12 . 23 . 34 . 1

DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

Status

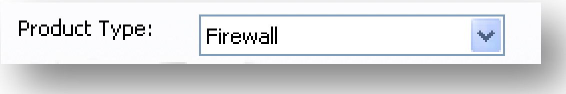
Ingate Startup Tool Version 2.4.0, connected to: Ingate Firewall 1190, IG-092-719-5012-4

Remote SIP Connectivity
VPN
QoS
Enhanced Security
15 SIP Traversal Licenses
20 SIP User Registration Licenses

Software Version: 4.6.2

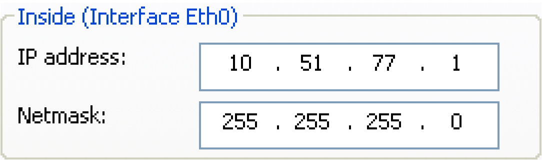
Configuration Steps:

1) In Product Type, select "Firewall".



Product Type: 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.

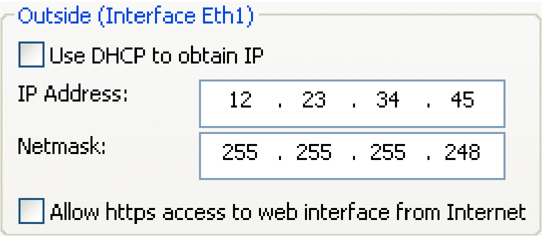


Inside (Interface Eth0)

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)

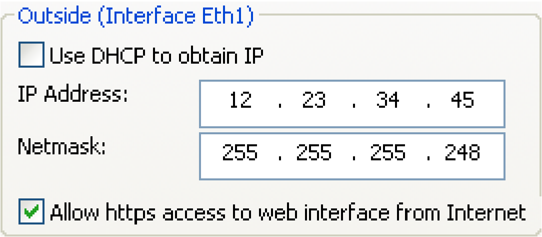
□ Use DHCP to obtain IP

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,
   a. Select "Allow https access to web interface from Internet"



Outside (Interface Eth1)

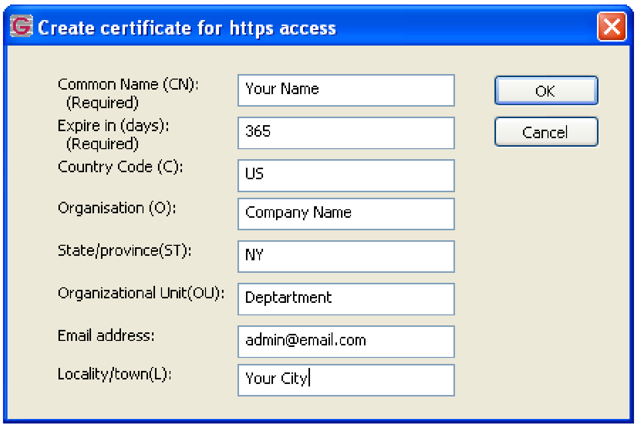
□ Use DHCP to obtain IP

IP Address: 12 . 23 . 34 . 45

Netmask: 255 . 255 . 255 . 248

☑ Allow https access to web interface from Internet

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



Create certificate for https access

Common Name (CN): (Required): Your Name

Expire in (days): (Required): 365

Country Code (C): US

Organisation (O): Company Name

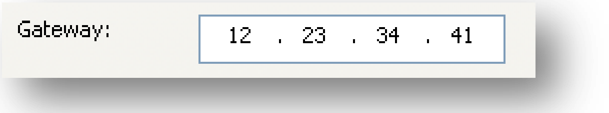
State/province(ST): NY

Organizational Unit(OU): Deptartment

Email address: admin@email.com

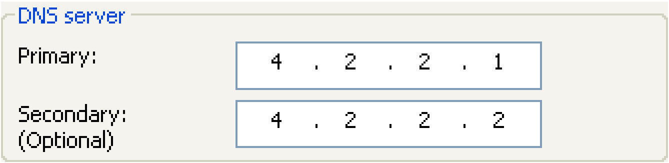
Locality/town(L): Your City

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.



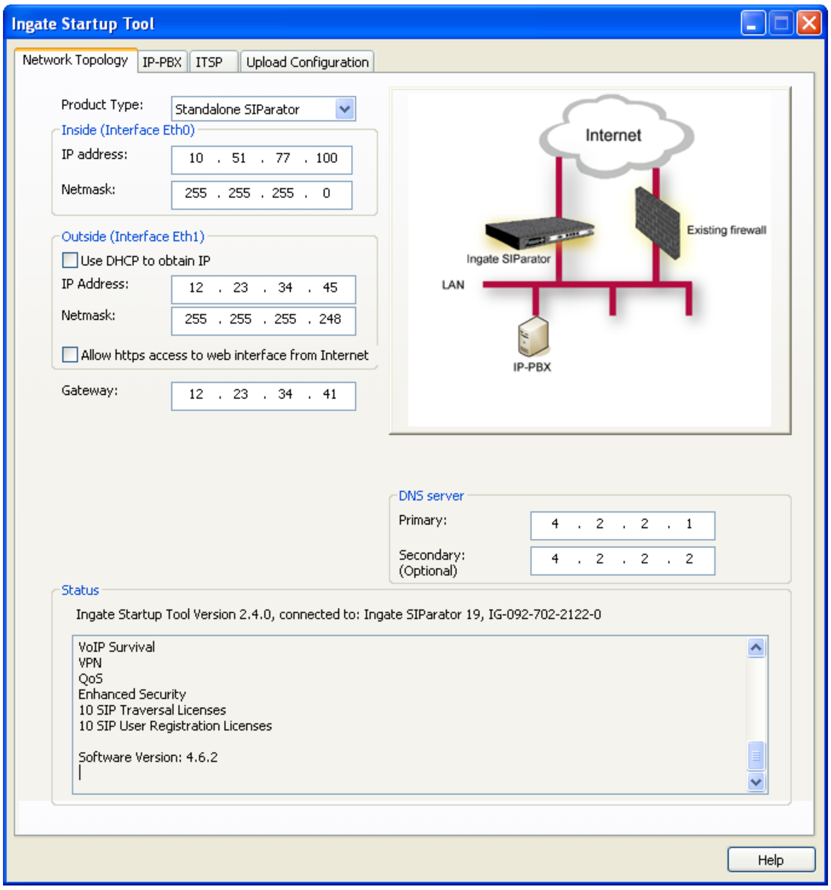
DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

4.3.2 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.



Product Type: Standalone SIParator

Inside (Interface Eth0)

IP address: 10 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

Outside (Interface Eth1)

□ Use DHCP to obtain IP

IP Address: 12 . 23 . 34 . 45

Netmask: 255 . 255 . 255 . 248

□ Allow https access to web interface from Internet

Gateway: 12 . 23 . 34 . 41

DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

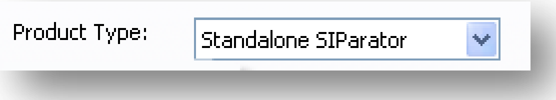
Status

Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

```
VoIP Survival
VPN
QoS
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2
```

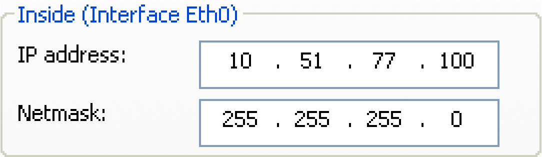
Configuration Steps:

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 Eth0)

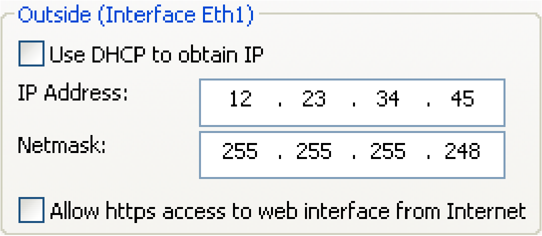
IP address: 10 . 51 . 77 . 100

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 obtain IP

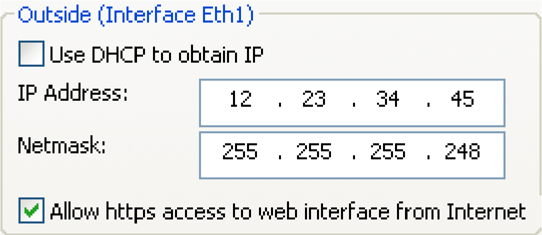
IP Address: 12 . 23 . 34 . 45

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)

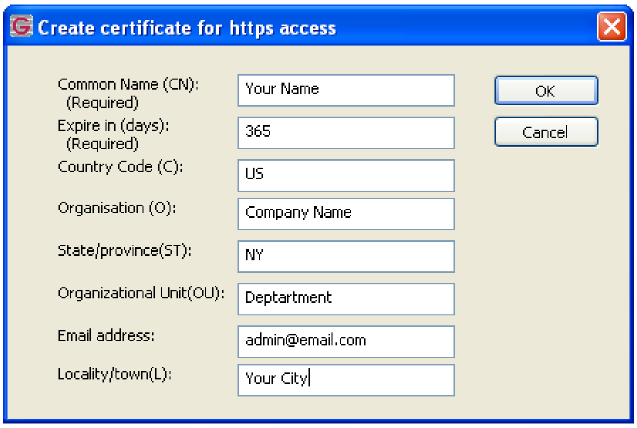
□ Use DHCP to obtain IP

IP Address: 12 . 23 . 34 . 45

Netmask: 255 . 255 . 255 . 248

☑ Allow https access to web interface from Internet

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



Create certificate for https access

Common Name (CN): (Required): Your Name

Expire in (days): (Required): 365

Country Code (C): US

Organisation (O): Company Name

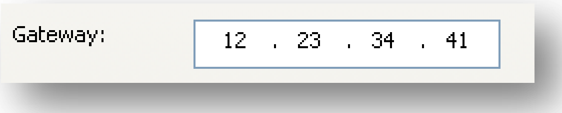
State/province(ST): NY

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.

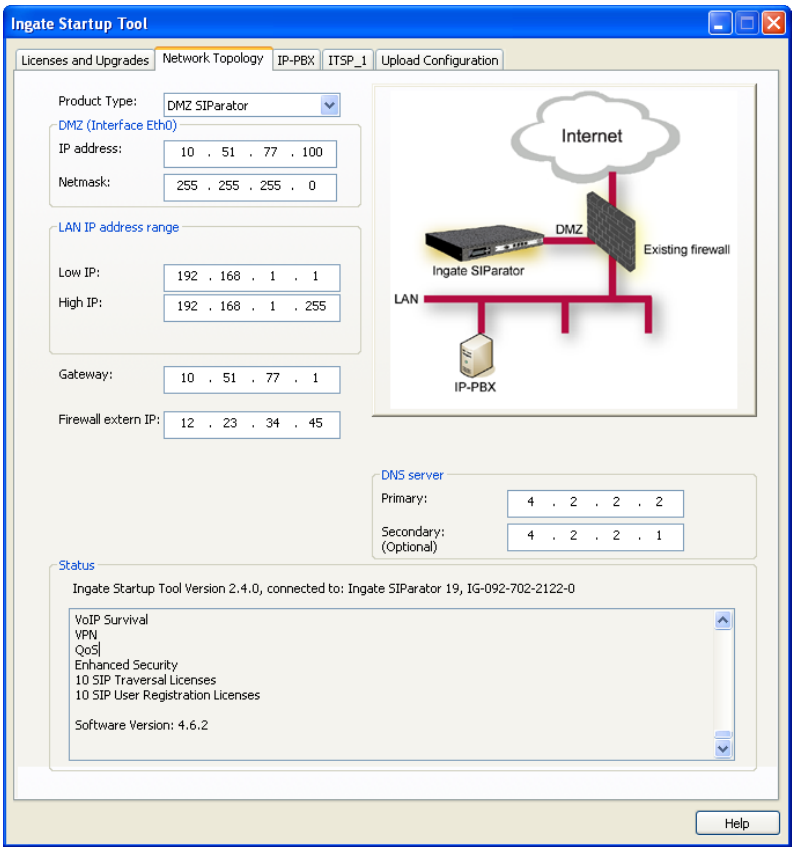


Gateway: 12 . 23 . 34 . 41

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.

4.3.3 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.



Product Type: DMZ SIParator

DMZ (Interface Eth0)
IP address: 10 . 51 . 77 . 100
Netmask: 255 . 255 . 255 . 0

LAN IP address range
Low IP: 192 . 168 . 1 . 1
High IP: 192 . 168 . 1 . 255

Gateway: 10 . 51 . 77 . 1
Firewall extern IP: 12 . 23 . 34 . 45

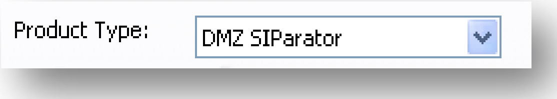
DNS server
Primary: 4 . 2 . 2 . 2
Secondary: (Optional) 4 . 2 . 2 . 1

Status
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 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
```

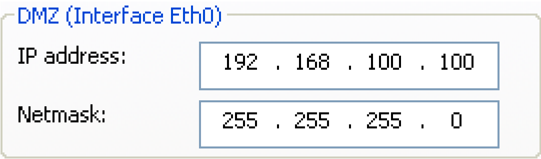
Configuration Steps:

1) In Product Type, select “DMZ SIParator”.



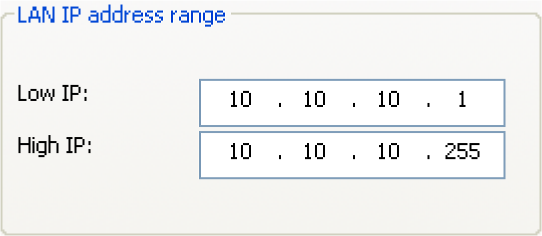
Product Type: DMZ SIParator

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 Eth0)
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.

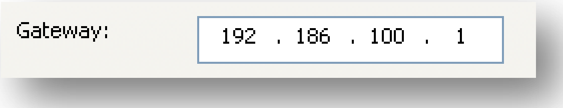


LAN IP address range

Low IP: 10 . 10 . 10 . 1

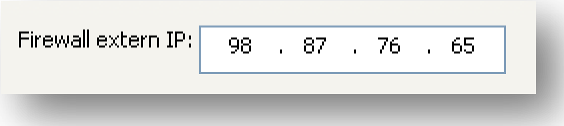
High IP: 10 . 10 . 10 . 255

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.



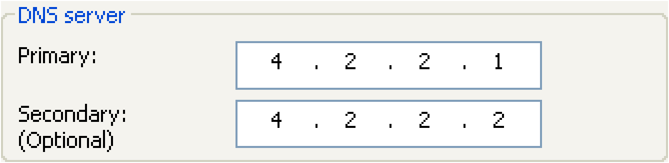
Gateway: 192 . 186 . 100 . 1

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.



DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

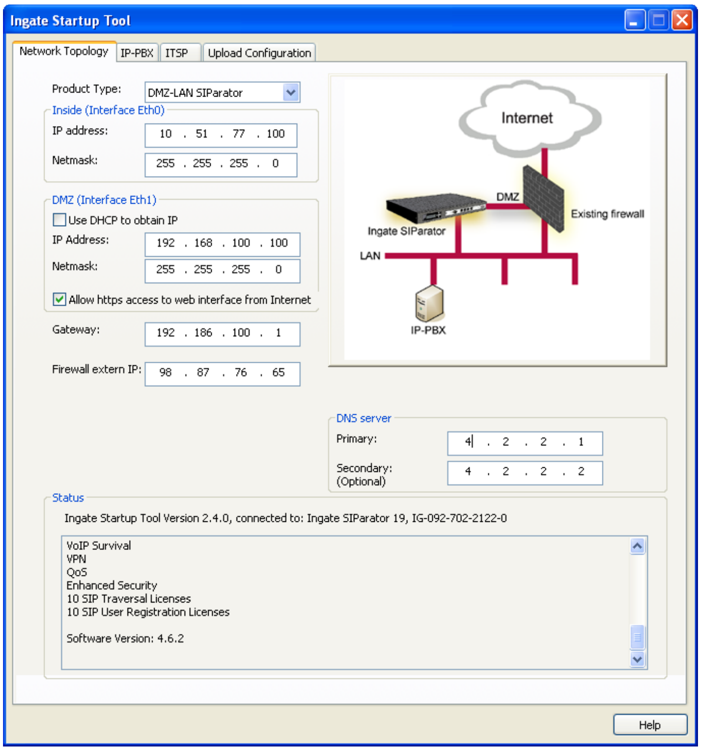
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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
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.

4.3.4 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.



Ingate Startup Tool

Network Topology | IP-PBX | ITSP | Upload Configuration

Product Type: DMZ-LAN SIParator

Inside (Interface Eth0)

IP address: 10 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

DMZ (Interface Eth1)

☐ Use DHCP to obtain IP

IP Address: 192 . 168 . 100 . 100

Netmask: 255 . 255 . 255 . 0

☑ Allow https access to web interface from Internet

Gateway: 192 . 186 . 100 . 1

Firewall extern IP: 98 . 87 . 76 . 65

DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

Status

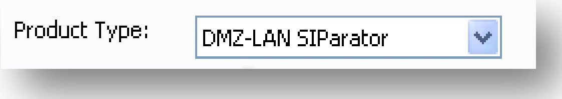
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

VoIP Survival
VPN
QoS
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2

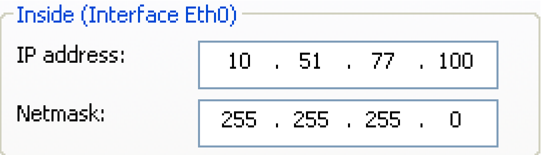
Configuration Steps:

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.



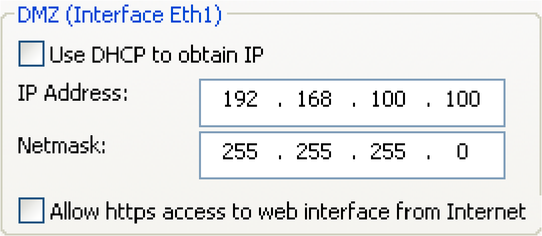
Inside (Interface Eth0)

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)

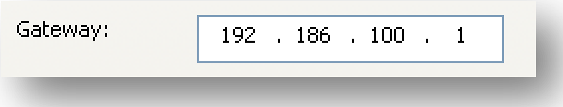
☐ Use DHCP to obtain IP

IP Address: 192 . 168 . 100 . 100

Netmask: 255 . 255 . 255 . 0

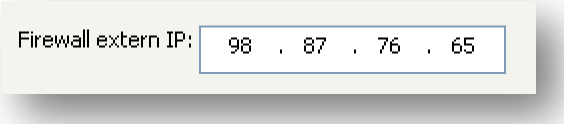
☐ Allow https access to web interface from Internet

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.



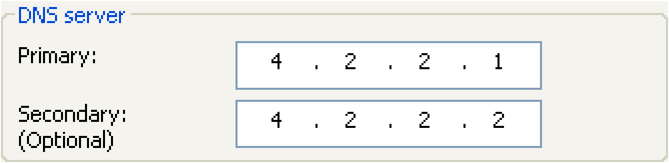
Gateway: 192 . 186 . 100 . 1

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.



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.



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.

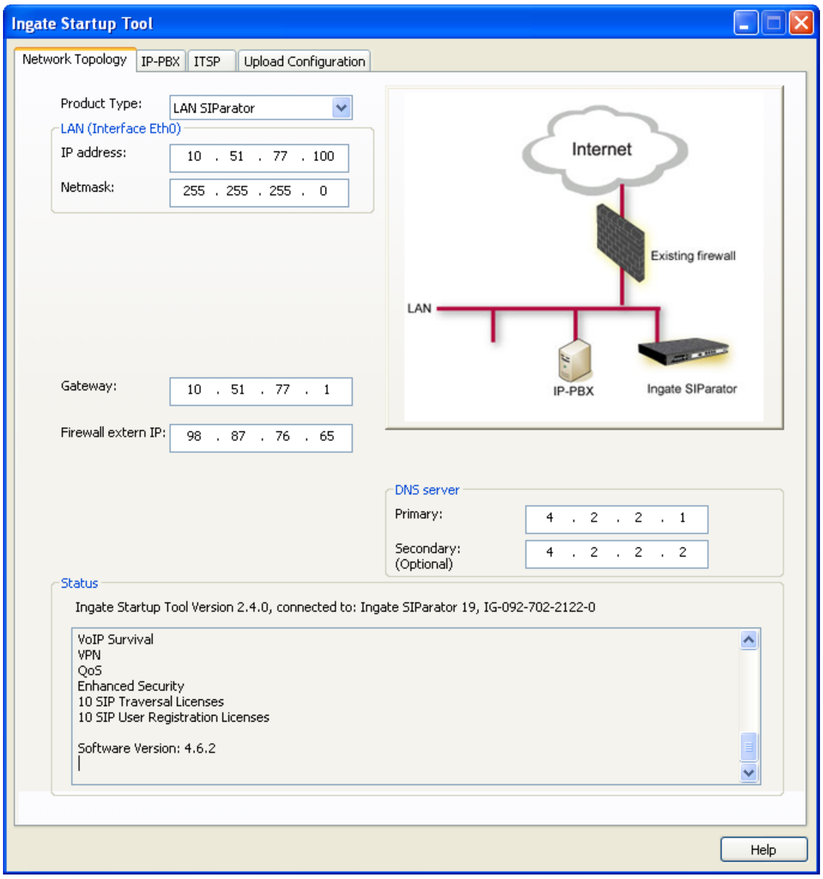
On the existing Firewall:

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

4.3.5 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.



Product Type: LAN SIParator

LAN (Interface Eth0)

IP address: 10 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

Gateway: 10 . 51 . 77 . 1

Firewall extern IP: 98 . 87 . 76 . 65

DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

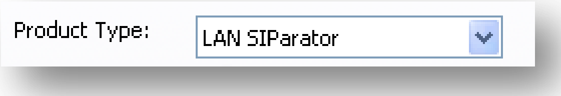
Status

Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

```
VoIP Survival
VPN
QoS
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2
```

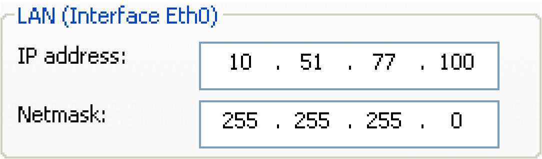
Configuration Steps:

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.

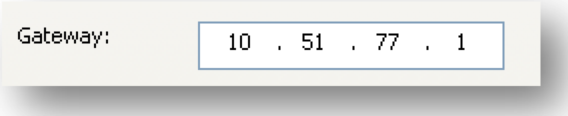


LAN (Interface Eth0)

IP address: 10 . 51 . 77 . 100

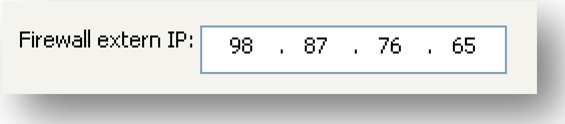
Netmask: 255 . 255 . 255 . 0

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.



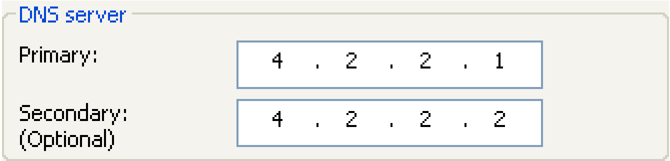
Gateway: 10 . 51 . 77 . 1

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 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

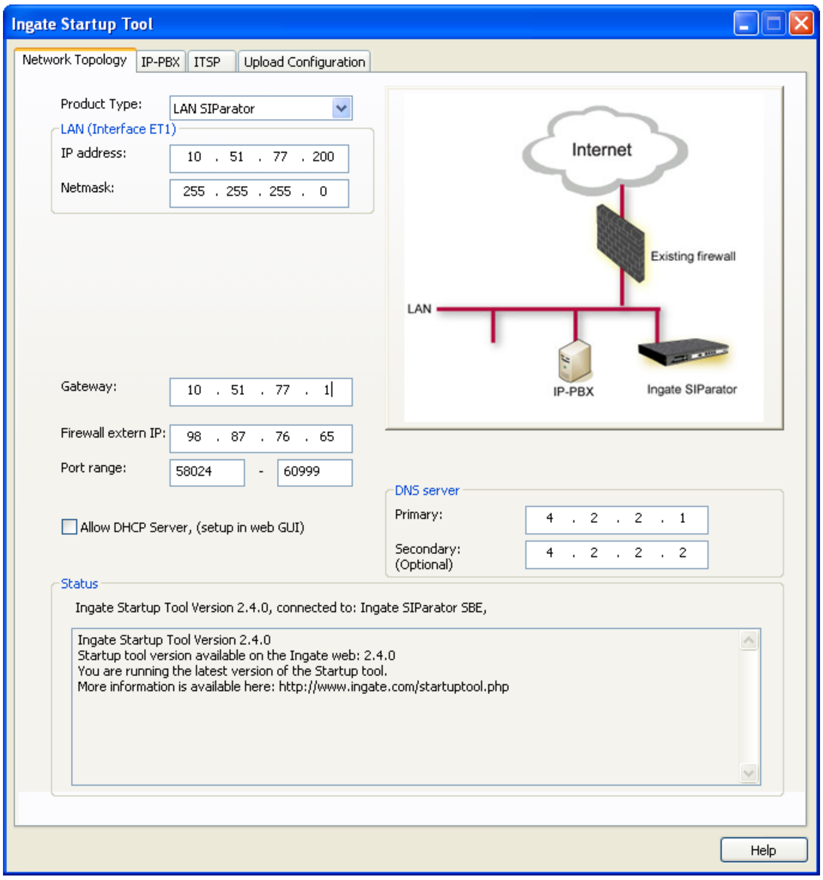
6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

4.3.6 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.



Product Type: LAN SIParator

LAN (Interface ET1)

IP address: 10 . 51 . 77 . 200

Netmask: 255 . 255 . 255 . 0

Gateway: 10 . 51 . 77 . 1

Firewall extern IP: 98 . 87 . 76 . 65

Port range: 58024 - 60999

□ Allow DHCP Server, (setup in web GUI)

DNS server

Primary: 4 . 2 . 2 . 1

Secondary: (Optional) 4 . 2 . 2 . 2

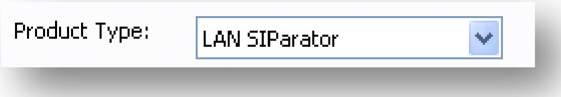
Status

Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator SBE,

```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

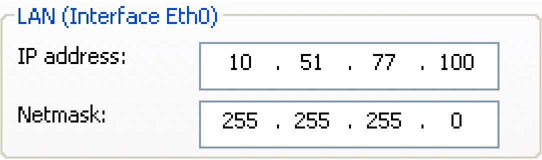
Configuration Steps:

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.

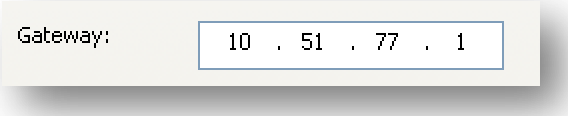


LAN (Interface Eth0)

IP address: 10 . 51 . 77 . 100

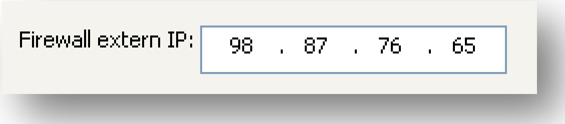
Netmask: 255 . 255 . 255 . 0

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.



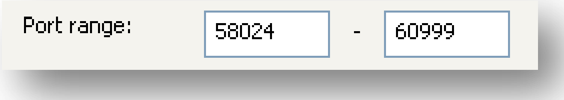
Gateway: 10 . 51 . 77 . 1

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.



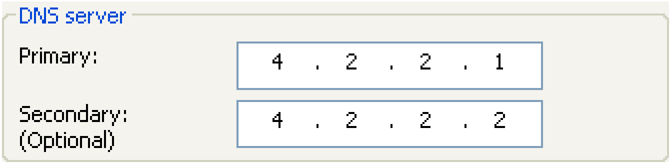
Firewall extern IP: 98 . 87 . 76 . 65

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

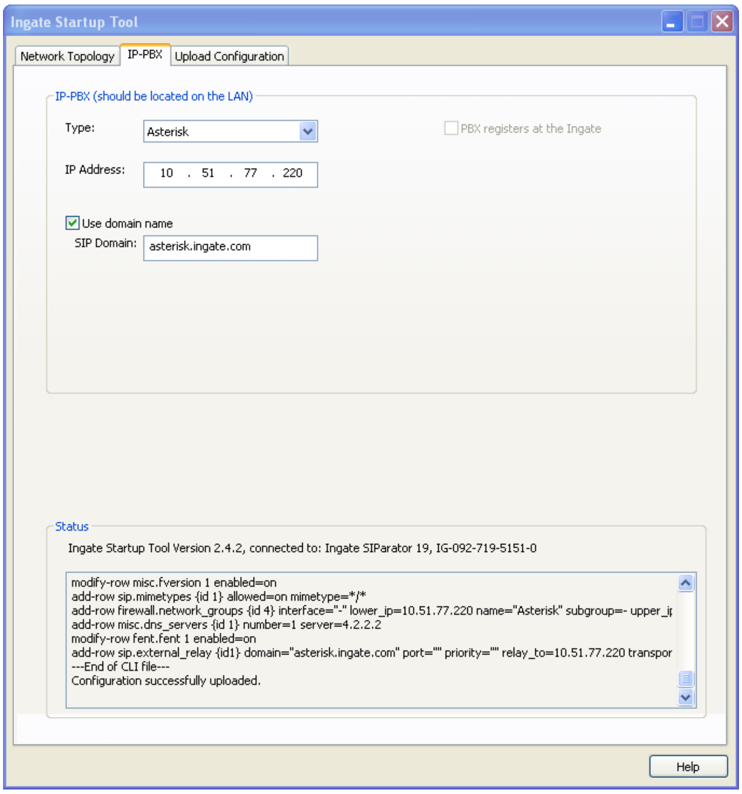
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

4.4 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 Asterisk BE server as to direct SIP traffic for the use with the Remote Phones. The IP Address of the Asterisk BE server must be on the same network subnet at the IP Address of the inside interface of the Ingate unit. Ingate has confirmed interoperability with the Asterisk BE.



Type: Asterisk

□ PBX registers at the Ingate

IP Address: 10 . 51 . 77 . 220

☑ Use domain name

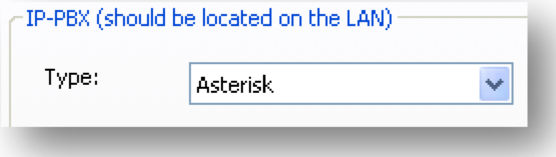
SIP Domain: asterisk.ingate.com

Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-719-5151-0

```
modify-row misc.fversion 1 enabled=on
add-row sip.mimetypes {id 1} allowed=on mimetype=*/*
add-row firewall.network_groups {id 4} interface="-" lower_ip=10.51.77.220 name="Asterisk" subgroup=- upper_ip
add-row misc.dns_servers {id 1} number=1 server=4.2.2.2
modify-row fent.fent 1 enabled=on
add-row sip.external_relay {id1} domain="asterisk.ingate.com" port="" priority="" relay_to=10.51.77.220 transpor
---End of CLI file---
Configuration successfully uploaded.
```

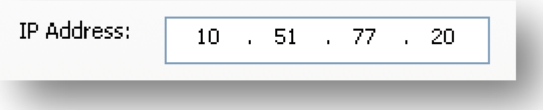
Configuration Steps:

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”.



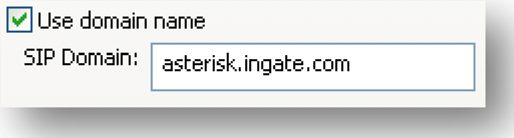
Type: Asterisk

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



IP Address: 10 . 51 . 77 . 20

3) This solution requires the use of a FQDN for the SIP Domain of the Asterisk BE. This domain name is used to route SIP Requests to the Asterisk BE associated with that domain. Select "Use domain name" and enter the FQDN

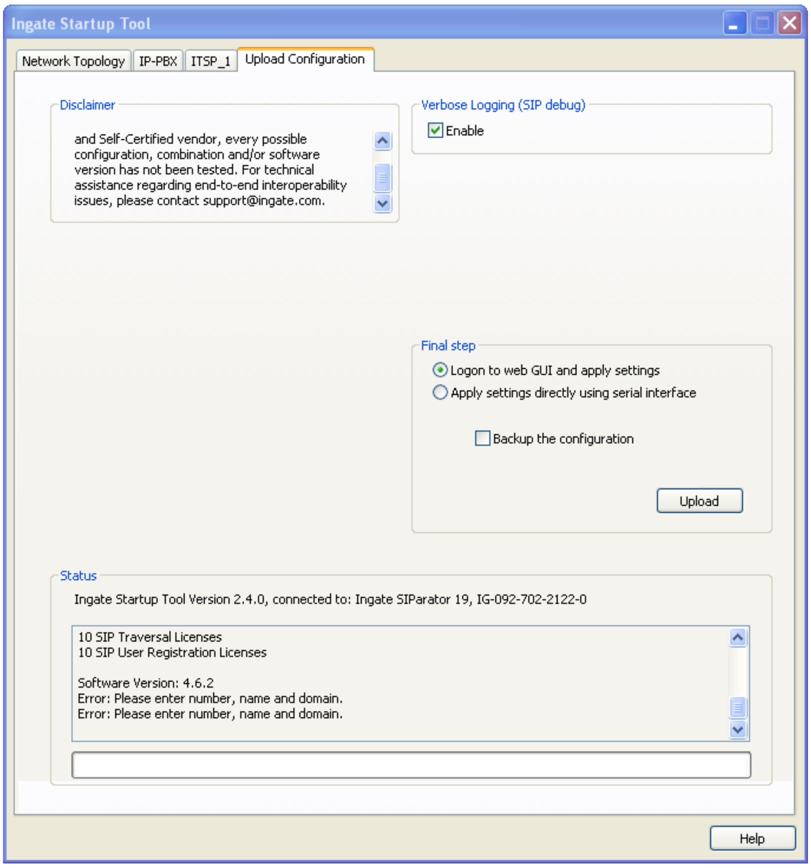


☑ Use domain name

SIP Domain: asterisk.ingate.com

4.5 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.



and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical assistance regarding end-to-end interoperability issues, please contact support@ingate.com.

☑ Enable

● Logon to web GUI and apply settings
○ Apply settings directly using serial interface

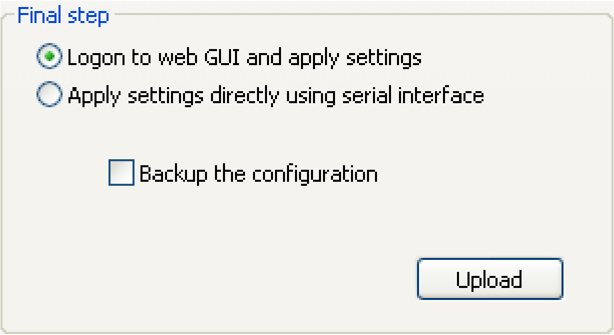
□ Backup the configuration

Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

```
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2
Error: Please enter number, name and domain.
Error: Please enter number, name and domain.
```

Configuration Steps:

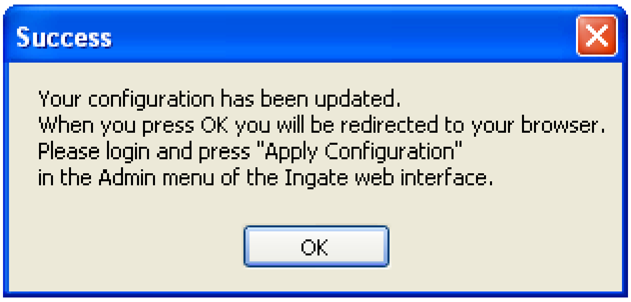
1) Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



● Logon to web GUI and apply settings
○ Apply settings directly using serial interface

□ Backup the configuration

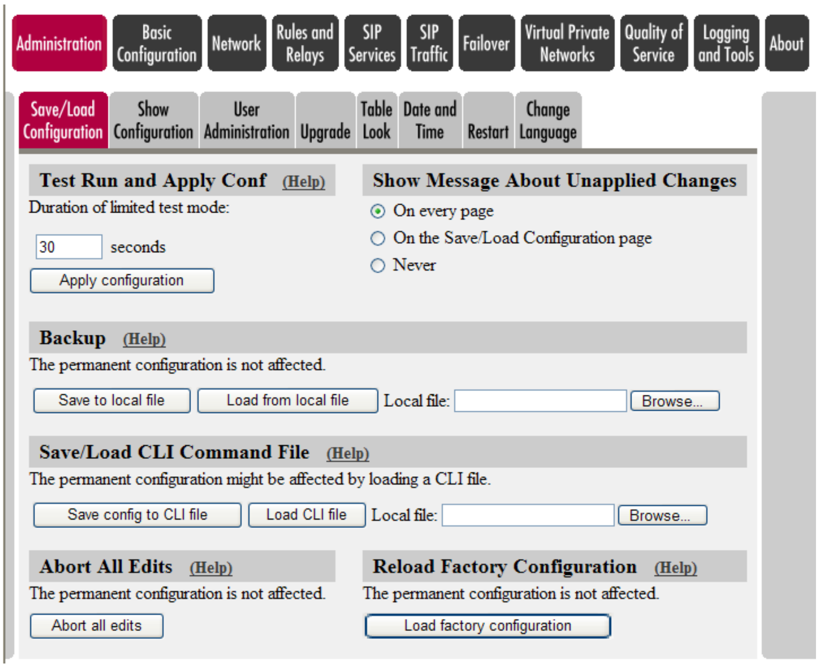
2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



Success

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

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.



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Show Message About Unapplied Changes

● On every page
○ On the Save/Load Configuration page
○ Never

Backup (Help)

The permanent configuration is not affected.

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

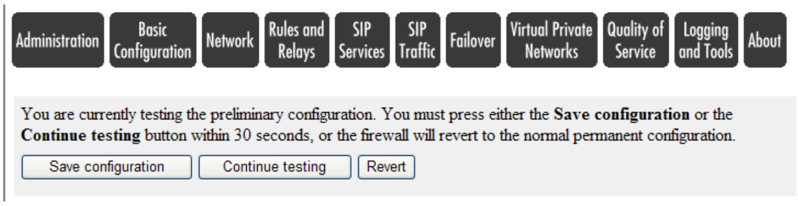
Abort All Edits (Help)

The permanent configuration is not affected.

Reload Factory Configuration (Help)

The permanent configuration is not affected.

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



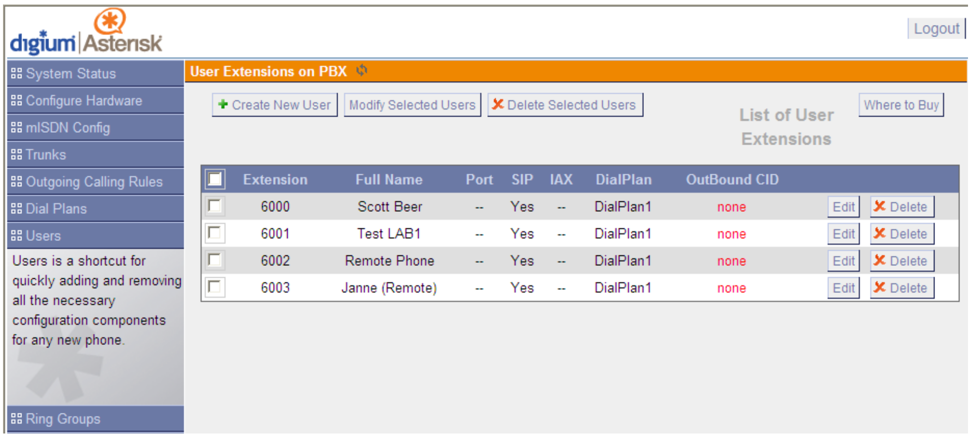
You are currently testing the preliminary configuration. You must press either the **Save configuration** or the **Continue testing** button within 30 seconds, or the firewall will revert to the normal permanent configuration.

5 Asterisk Business Edition Setup

The Asterisk setup involves setting up the User Extensions, associating the SIP Domain, and adding an Outbound Proxy when using an Ingate SIParator.

5.1 User Extension on PBX Setup

Users is a shortcut for quickly adding and removing all the necessary configuration components for any new phone.

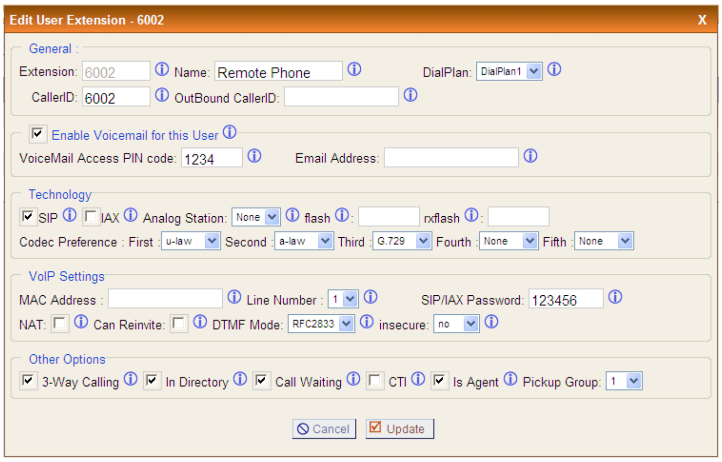


Users is a shortcut for quickly adding and removing all the necessary configuration components for any new phone.

☐	Extension	Full Name	Port	SIP	IAX	DialPlan	OutBound CID		
☐	6000	Scott Beer	--	Yes	--	DialPlan1	none	Edit	Delete
☐	6001	Test LAB1	--	Yes	--	DialPlan1	none	Edit	Delete
☐	6002	Remote Phone	--	Yes	--	DialPlan1	none	Edit	Delete
☐	6003	Janne (Remote)	--	Yes	--	DialPlan1	none	Edit	Delete

Configuration Steps:

1) Select "Create New User" and the Asterisk BE will select the next available extension number and launch another screen.
2) In VoIP Settings section,
   a. De-select NAT
   b. Enter a Password for Authentication on the SIP Phone
3) The rest of the settings are phone or PBX specific features.



Edit User Extension - 6002

General :
Extension: 6002 Name: Remote Phone DialPlan: DialPlan1
CallerID: 6002 OutBound CallerID:

☑ Enable Voicemail for this User
VoiceMail Access PIN code: 1234 Email Address:

Technology
☑ SIP ☐ IAX Analog Station: None flash: rxflash:
Codec Preference : First : u-law Second : a-law Third : G.729 Fourth : None Fifth : None

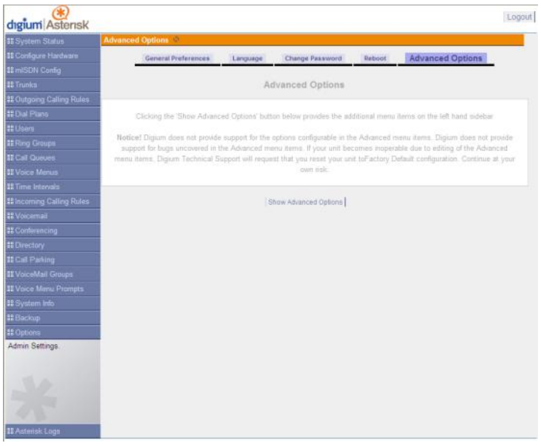
VoIP Settings
MAC Address : Line Number : 1 SIP/IAX Password: 123456
NAT: ☐ Can Reinvite: ☐ DTMF Mode: RFC2833 insecure: no

Other Options
☑ 3-Way Calling ☑ In Directory ☑ Call Waiting ☐ CTI ☑ Is Agent Pickup Group: 1

5.2 SIP Settings

Clicking the 'Show Advanced Options' button below provides the advanced menu items on the left hand sidebar

Note: Digium does not provide support for the options configurable in the Advanced menu items. Digium does not provide support for bugs uncovered in the Advanced menu items. If your unit becomes inoperable due to editing of the Advanced menu items, Digium Technical Support will request that you reset your unit to Factory Default configuration. Continue at your own risk.



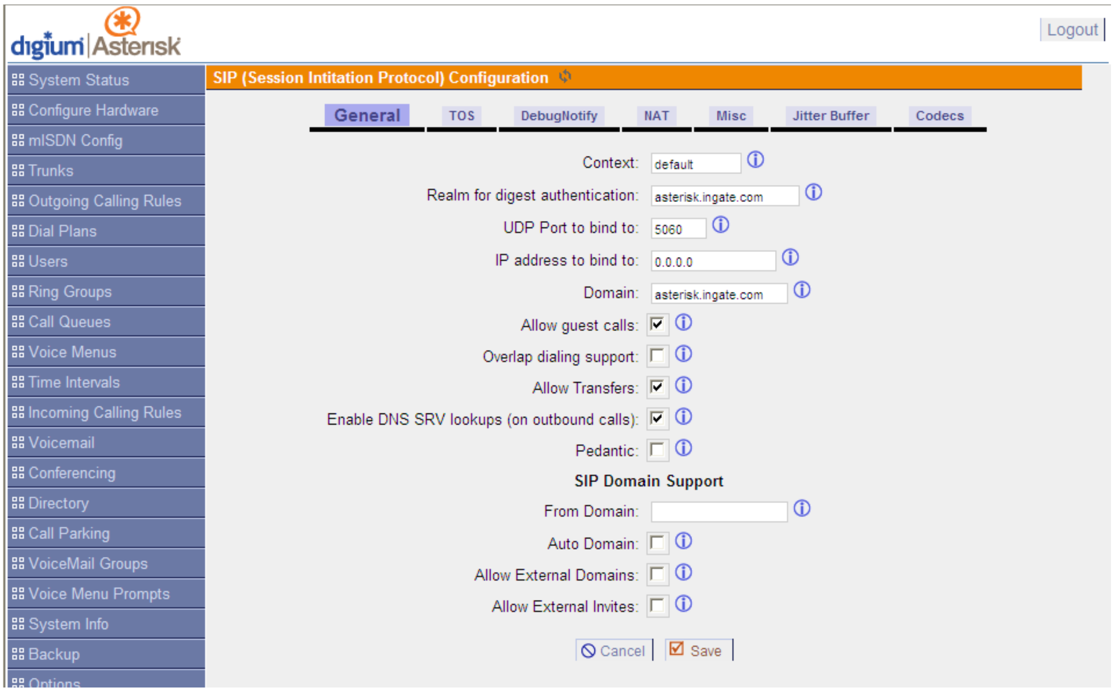
Advanced Options

Clicking the 'Show Advanced Options' button below provides the additional menu items on the left hand sidebar

Notice! Digium does not provide support for the options configurable in the Advanced menu items. Digium does not provide support for bugs uncovered in the Advanced menu items. If your unit becomes inoperable due to editing of the Advanced menu items, Digium Technical Support will request that you reset your unit toFactory Default configuration. Continue at your own risk.

Configuration Steps:

1) In the General configuration area
   a. In the Domain field, enter the FQDN for the SIP Domain
   b. In the Realm for digest authentication field, enter the FQDN of the SIP Domain



Context: default

Realm for digest authentication: asterisk.ingate.com

UDP Port to bind to: 5060

IP address to bind to: 0.0.0.0

Domain: asterisk.ingate.com

Allow guest calls: ☑

Overlap dialing support: □

Allow Transfers: ☑

Enable DNS SRV lookups (on outbound calls): ☑

Pedantic: □

SIP Domain Support

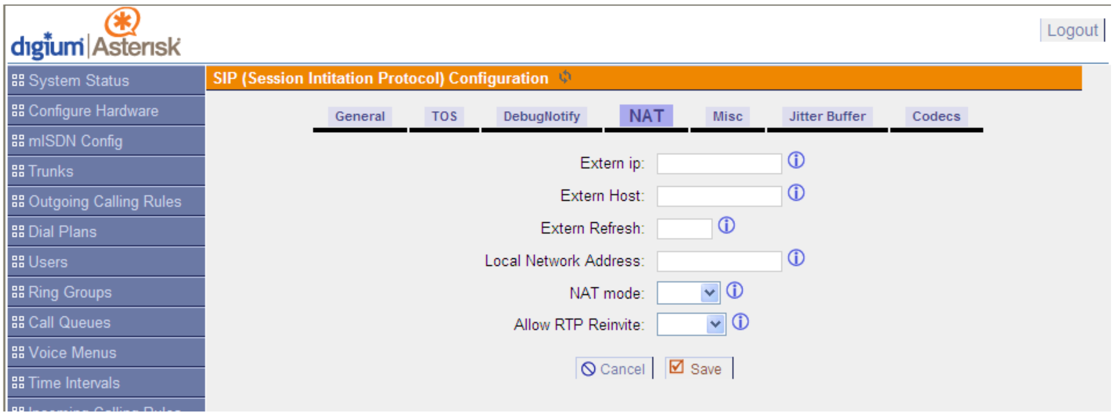
From Domain:

Auto Domain: □

Allow External Domains: □

Allow External Invites: □

Note: The NAT area is left Blank



SIP (Session Intitation Protocol) Configuration

Extern ip:

Extern Host:

Extern Refresh:

Local Network Address:

NAT mode:

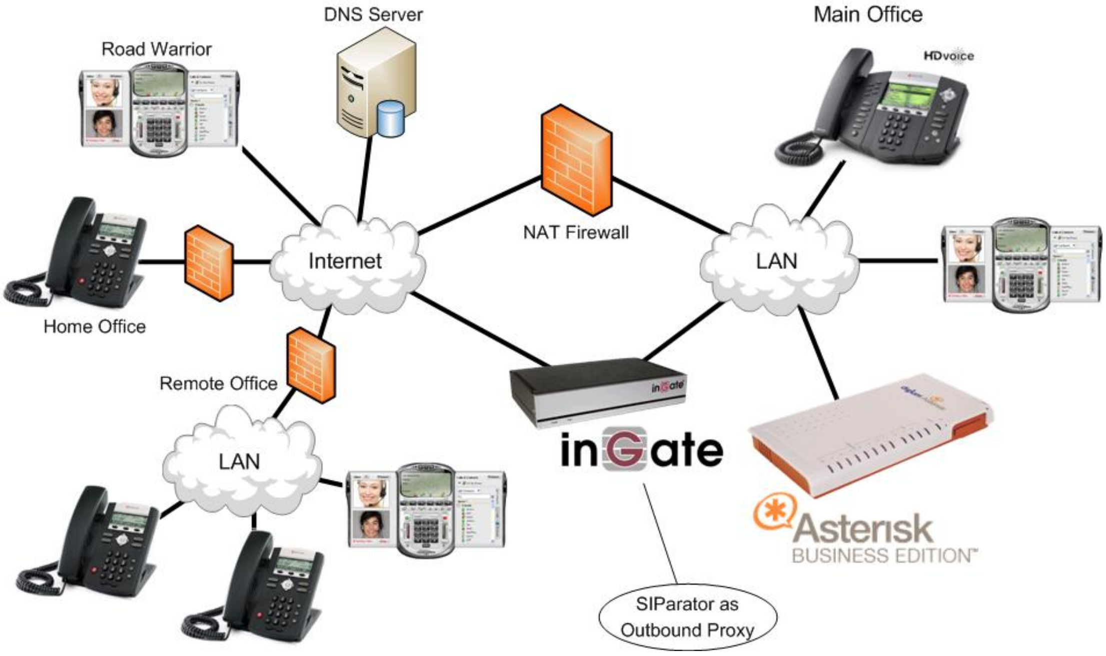
Allow RTP Reinvite:

5.3 Outbound Proxy Settings when using SIParator

Typically the Ingate SIParator is not Default Gateway of the network, so an Outbound Proxy must be configured in the Asterisk BE. Unfortunately, this feature isn't configurable through the GUI. However, you can set it up manually using the "outboundproxy" variable in /etc/asterisk/sip.conf. Use of this variable is fully documented inline within sip.conf.

The "outboundproxy" variable in /etc/asterisk/sip.conf is the Private IP Address of the Ingate SIParator.

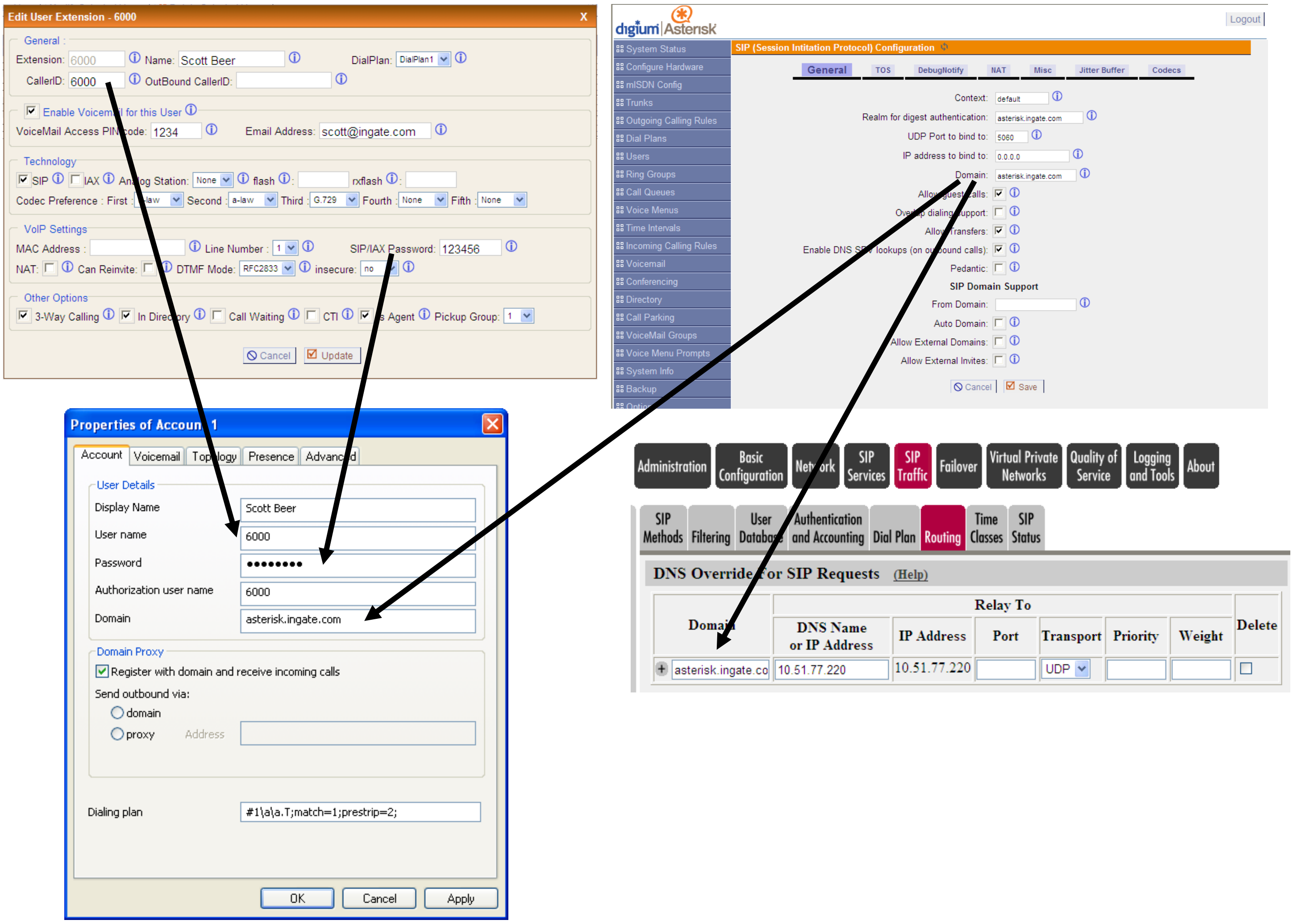
This variable is not needed with the Ingate Firewall Product.



6 Troubleshooting

6.1 SIP Phone Registration Information

Now there are too many SIP Phone vendors to list here, so only an example of the CounterPath X-Lite will be shown.



Edit User Extension - 6000

General :
Extension: 6000 Name: Scott Beer DialPlan: DialPlan1
CallerID: 6000 OutBound CallerID:

☑ Enable Voicemail for this User
VoiceMail Access PIN code: 1234 Email Address: scott@ingate.com

Technology
☑ SIP ☐ IAX Analog Station: None flash: rxflash:
Codec Preference : First : u-law Second : a-law Third : G.729 Fourth : None Fifth : None

VoIP Settings
MAC Address : Line Number : 1 SIP/IAX Password: 123456
NAT: ☐ Can Reinvite: ☐ DTMF Mode: RFC2833 insecure: no

Other Options
☑ 3-Way Calling ☑ In Directory ☐ Call Waiting ☐ CTI ☑ Is Agent Pickup Group: 1

SIP (Session Intitation Protocol) Configuration

Context: default
Realm for digest authentication: asterisk.ingate.com
UDP Port to bind to: 5060
IP address to bind to: 0.0.0.0
Domain: asterisk.ingate.com
Allow guest calls: ☑
Overlap dialing support: ☐
Allow Transfers: ☑
Enable DNS SRV lookups (on outbound calls): ☑
Pedantic: ☐

SIP Domain Support
From Domain:
Auto Domain: ☐
Allow External Domains: ☐
Allow External Invites: ☐

Properties of Account 1

User Details
Display Name: Scott Beer
User name: 6000
Password: ••••••••
Authorization user name: 6000
Domain: asterisk.ingate.com

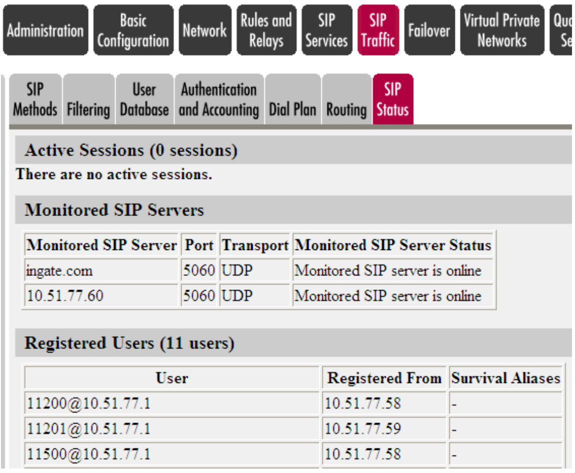
Domain Proxy
☑ Register with domain and receive incoming calls
Send outbound via:
○ domain
○ proxy Address

Dialing plan: #1\a\a.T;match=1;prestrip=2;

DNS Override For SIP Requests (Help)

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
asterisk.ingate.co	10.51.77.220	10.51.77.220		UDP			☐

Note: The successful registration of the SIP Phones can be seen in SIP Traffic -> SIP Status.



Active Sessions (0 sessions)

There are no active sessions.

Monitored SIP Servers

Monitored SIP Server	Port	Transport	Monitored SIP Server Status
ingate.com	5060	UDP	Monitored SIP server is online
10.51.77.60	5060	UDP	Monitored SIP server is online

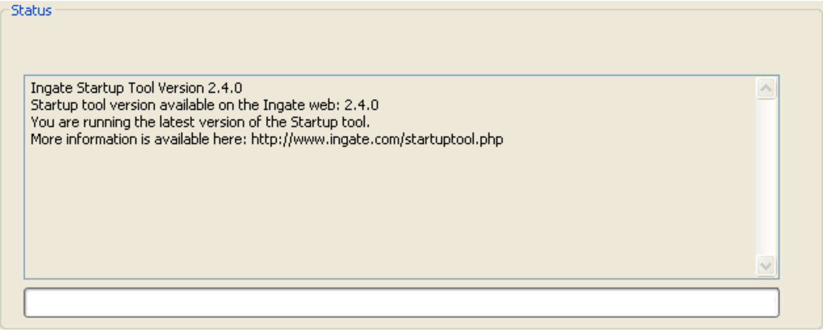
Registered Users (11 users)

User	Registered From	Survival Aliases
11200@10.51.77.1	10.51.77.58	-
11201@10.51.77.1	10.51.77.59	-
11500@10.51.77.1	10.51.77.58	-

6.2 Startup Tool

6.2.1 Status Bar

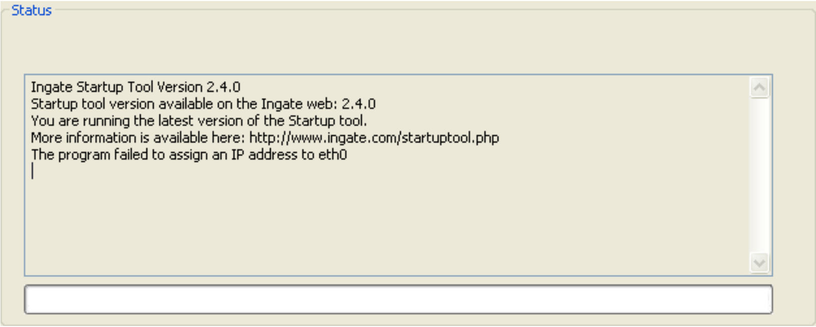
Located on every page of the Startup Tool is the Status Bar. This is a display and recording of all of the activity of the Startup Tool, displaying Ingate unit information, software versions, Startup Tool events, errors and connection information. Please refer to the Status Bar to acquire the current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



```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

6.2.2 Startup Tool - 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"**.



```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
The program failed to assign an IP address to eth0
```

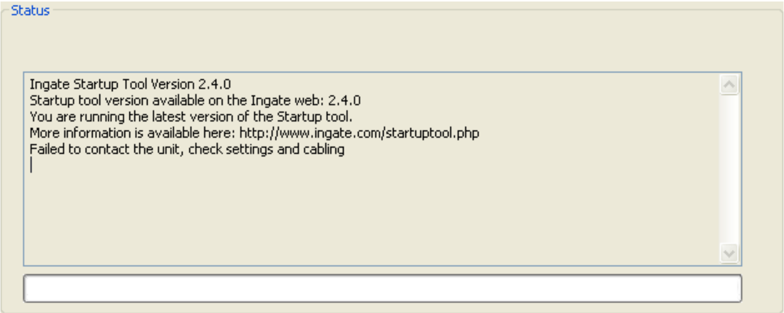
Possible Problems and Resolutions

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.	Eth0 must always be used with the Startup Tool.
Incorrect MAC Address	Check the MAC address on the Unit itself. MAC Address of Eth0.
An IP Address and/or Password have already been assigned to the Ingate Unit	It is possible that an IP Address or Password have been already been assigned to the unit via the Startup Tool or Console

Possible Problems	Possible Resolution
Ingate Unit on a different Subnet or Network	The Startup Tool uses an application 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.



```
Ingate Startup Tool Version 2.4.0
Startup tool version available on the Ingate web: 2.4.0
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
Failed to contact the unit, check settings and cabling
```

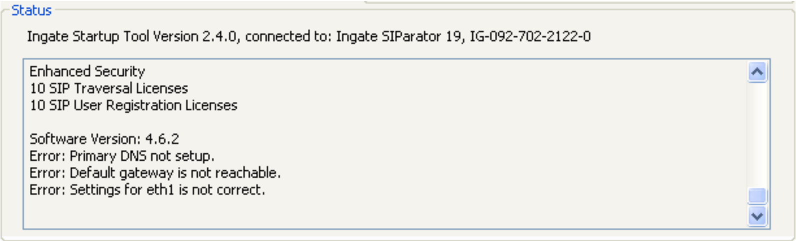
Possible Problems and Resolutions

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.

Possible Problems	Possible Resolution
Despite your best efforts…	1) 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. 2) 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.



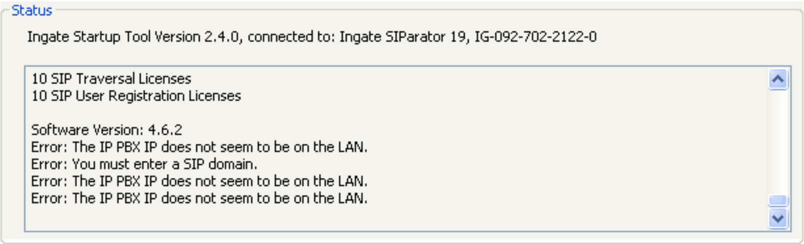
```
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2
Error: Primary DNS not setup.
Error: Default gateway is not reachable.
Error: Settings for eth1 is not correct.
```

Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: Default gateway is not reachable.	The Default Gateway is always the way 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 correct.	IP Address of Netmask is in an Invalid format.
Error: Please provide a correct netmask for eth0/1	Netmask is in an Invalid format.
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.



Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0

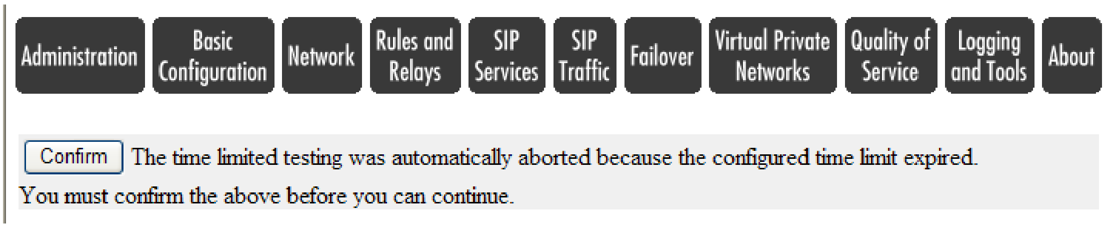
```
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.2
Error: The IP PBX IP does not seem to be on the LAN.
Error: You must enter a SIP domain.
Error: The IP PBX IP does not seem to be on the LAN.
Error: The IP PBX IP does not seem to be on the LAN.
```

Possible Problems and Resolutions

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

6.3 Ingate Web GUI - 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.



The time limited testing was automatically aborted because the configured time limit expired.

You must confirm the above before you can continue.

Possible Problems and Resolutions

Possible Problems	Possible Resolution
Eth0 Interface IP Address has changed	Increase the duration of the test mode, press “Apply Configuration” and start a new browser to the new IP address, then press “Save Configuration”
Access Control does not allow administration from the IP address of the PC.	Verify the IP address of the PC with the Startup Tool. Go to “Basic 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.

6.4 DNS Benefits and Issues

As this solution is reliant on the resolution of a FQDN for the SIP Domain, the SIP Phones, the Ingate, and the Asterisk BE all need to be able to resolve the FQDN.

DNS Standard Lookup
Ensure that SIP Phones, PCs and servers all have a DNS Server to which they can query a host name. There are some enterprises that have a internal DNS Server to manage internal host names.

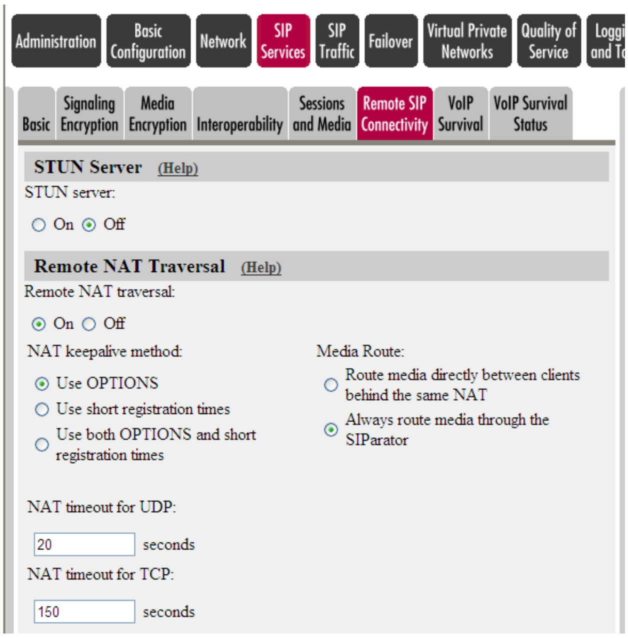
PING tests using a domain is a good test to see if a network can resolve FQDNs.

DYN DNS
Dynamic DNS is a tool that can be use to provide smaller enterprises the ability to use a FQDN in a Dynamic Public IP environment. Visit dyndns.org to get your free Domain name with Dynamic updating of the Enterprise IP address.

DNS SRV Records
DNS Service Records offer the ability to do Load Balancing and Residency to any SIP Phone deployment. It offers the ability to use one FQDN and break the FQDN into multiple services, one for Web and another for SIP communications.

6.5 Remote SIP Connectivity Module

The Startup Tool will enable the Remote SIP Connectivity Module when selected. There are some additional options which help when running into some Far End NAT Traversal issues.



STUN Server (Help)

STUN server:

○ On ● Off

Remote NAT Traversal (Help)

Remote NAT traversal:

● On ○ Off

NAT keepalive method:

● Use OPTIONS
○ Use short registration times
○ Use both OPTIONS and short registration times

Media Route:

○ Route media directly between clients behind the same NAT
● Always route media through the SIParator

NAT timeout for UDP:

20 seconds

NAT timeout for TCP:

150 seconds

The SIParator can properly rewrite all the Remote SIP Phones SIP signaling. For this to work, the NAT box in front of the SIP client must keep the NAT hole open. In the SIParator there are two methods for doing this; using OPTIONS packets or using short registration times.

If the clients can respond to OPTIONS messages, you can use this method for keeping the NAT hole open. When this is used, the SIParator will send OPTIONS messages to the client with a frequency determined by the NAT timeout.

If the clients cannot respond to OPTIONS messages, you can instead use short registration times. This requires that the server accepts a registration time of the same length as the NAT timeout.

The NAT timeouts are used by the SIParator to determine how often OPTIONS or registrations should be sent.

In calls where the Remote NAT Traversal is used, the media (voice, video etc.) is usually routed through the SIParator. For two SIP clients behind the same remote NAT device, you can make the SIParator route media directly between the clients instead.