



## **Application Note**

### **Asterisk BE with SIP Trunking - Configuration Guide**

23 January 2009

# Table of Contents

<b>1</b>	<b>ASTERISK BUSINESS EDITION AND INGATE.....</b>	<b>1</b>
1.1	SIP TRUNKING SUPPORT.....	2
<b>2</b>	<b>INGATE STARTUP TOOL.....</b>	<b>3</b>
<b>3</b>	<b>CONNECTING THE INGATE FIREWALL/SIPARATOR.....</b>	<b>4</b>
<b>4</b>	<b>USING THE STARTUP TOOL .....</b>	<b>6</b>
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	ITSP .....	27
4.6	UPLOAD CONFIGURATION.....	30
<b>5</b>	<b>ADDITIONAL MANUAL CONFIGURATION .....</b>	<b>32</b>
5.1	USER DATABASE.....	32
5.1.1	Local User Account .....	32
5.1.2	Asterisk INVITE Authentication Account.....	33
5.2	DIAL PLAN .....	34
<b>6</b>	<b>ASTERISK BUSINESS EDITION SETUP .....</b>	<b>36</b>
6.1	VOIP TRUNKS .....	36
6.2	OUTGOING CALLING RULES.....	37
6.3	INCOMING CALLING RULES .....	38
6.4	DIAL PLAN.....	39
6.5	SIP SETTINGS.....	39
6.6	OUTBOUND PROXY SETTINGS WHEN USING SIPARATOR.....	41
<b>7</b>	<b>TROUBLESHOOTING .....</b>	<b>42</b>
7.1	INGATE – ASTERISK BE REGISTRATION .....	42
7.2	INGATE – ASTERISK BE INCOMING CALLING.....	43
7.3	STARTUP TOOL .....	44
7.3.1	Status Bar .....	44
7.3.2	Configure Unit for the First Time.....	44
7.3.3	Change or Update Configuration .....	45
7.3.4	Network Topology.....	46
7.3.5	IP-PBX.....	47
7.3.6	ITSP.....	47
7.3.7	Apply Configuration .....	48
7.4	DNS BENEFITS AND ISSUES .....	49

Tested versions: Ingate Firewall and SIParator version 4.6.4  
Startup Tool version 2.4.2  
Asterisk Business Edition version 2.1.1

## Revision History:

Revision	Date	Author	Comments
	2009-01-23	Scott Beer	Minor Edits

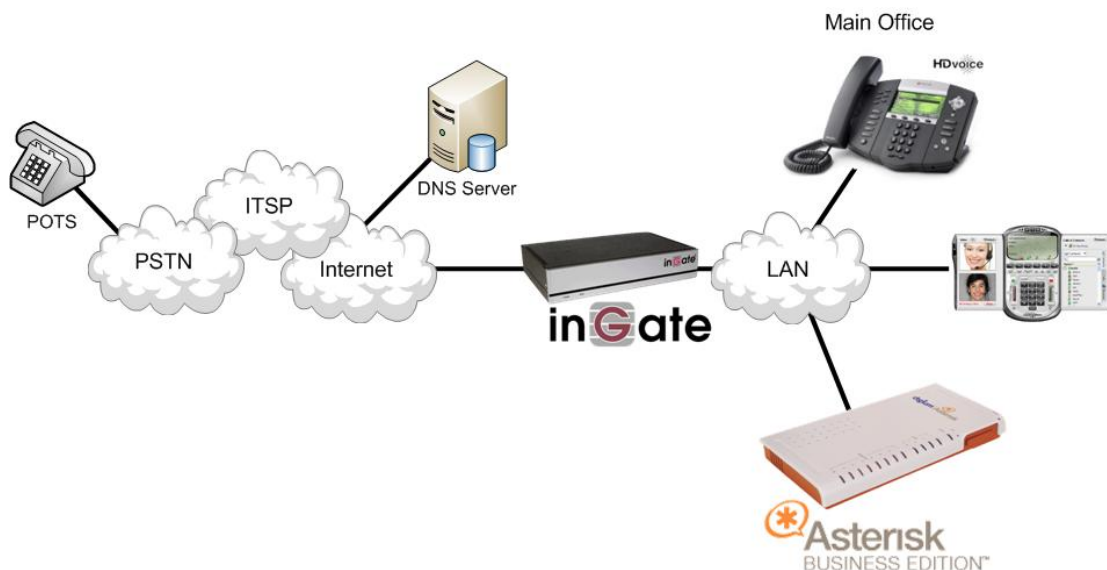
# 1 Asterisk Business Edition and Ingate

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 Internet Telephony Service Providers (ITSP) or SIP Trunking Service Providers. These Service Providers offer PSTN access using SIP Trunking as a method of connectivity to the PSTN. The Asterisk BE will terminate these trunks and deliver them to users and applications on the Asterisk server.

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 SIP Trunking connectivity to the Asterisk Business Edition IP-PBX solution. 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 any ITSP in a secure and reliable manner.



## 1.1 SIP Trunking 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 attacks.

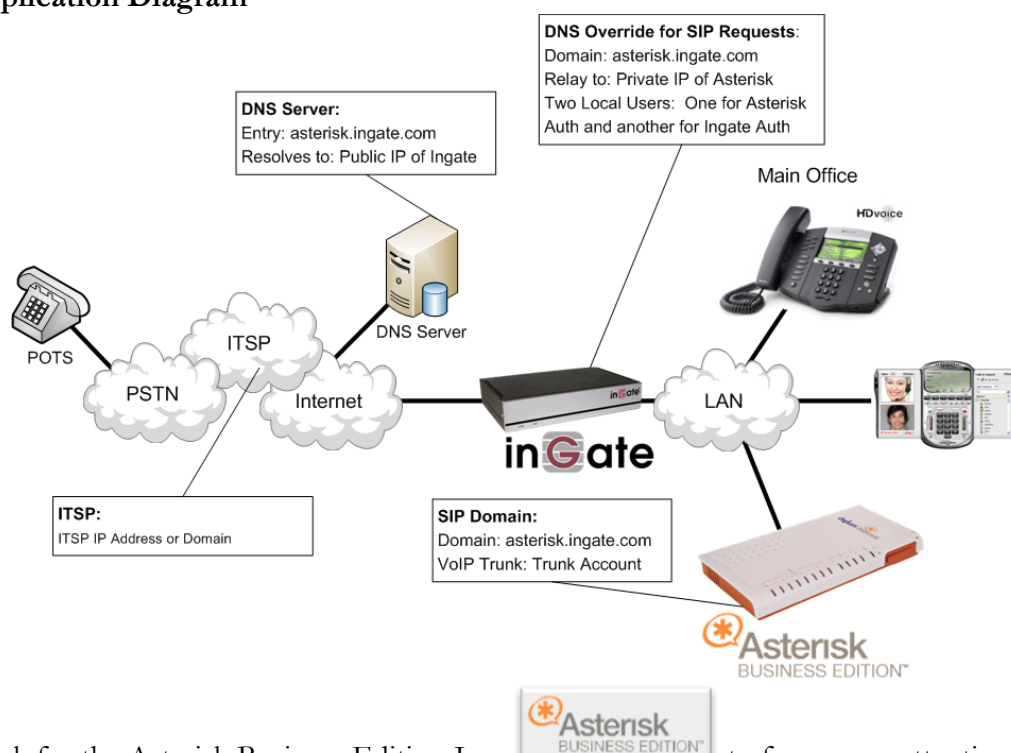
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.


The Internet Telephony Service Provider can be of any vendor, located anywhere across the Internet or any remote private 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) There are some User/Trunk Accounts to be setup on between the Asterisk and Ingate for INVITE Authentication requirements.
- 3) The Ingate must have the SIP Trunking Module to provide Routing Rules, basic Security Policies, Client/Server Registrar, B2BUA capabilities, SIP Protocol 'Normalization' and more.

### Application Diagram



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

## 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.

**Note:** For this solution the Startup Tool does not adequately program everything necessary for proper integration with the Asterisk BE. There are several manual steps required for completion.

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, SIP trunking service provider of their choice, 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 ITSPs.

Download Free of Charge: The Startup Tool is free of charge for all Ingate Firewalls and SIParators. Get the latest version of the Startup Tool at [http://www.ingate.com/Startup\\_Tool.php](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](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 IP-PBX to an ITSP. Additional programming and administration of this Ingate unit should be done through the Web Administration.

### 3 Connecting the Ingate Firewall/SIParator

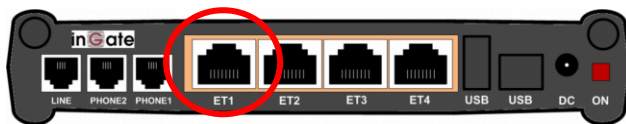
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

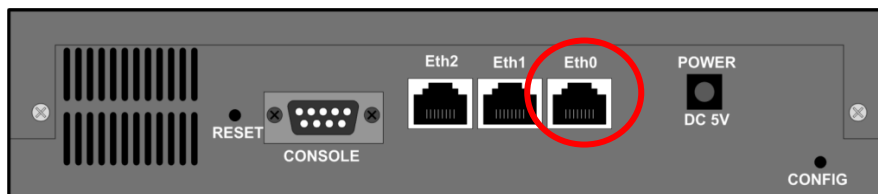
#### Configuration Steps:

- 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”.

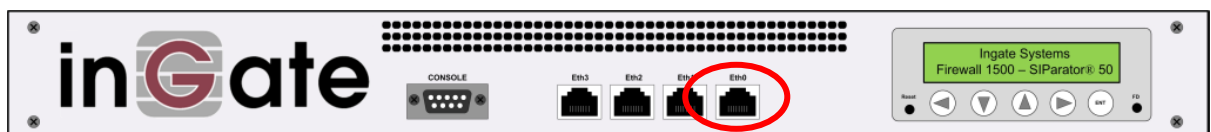
#### Ingate SIParator SBE (Back)



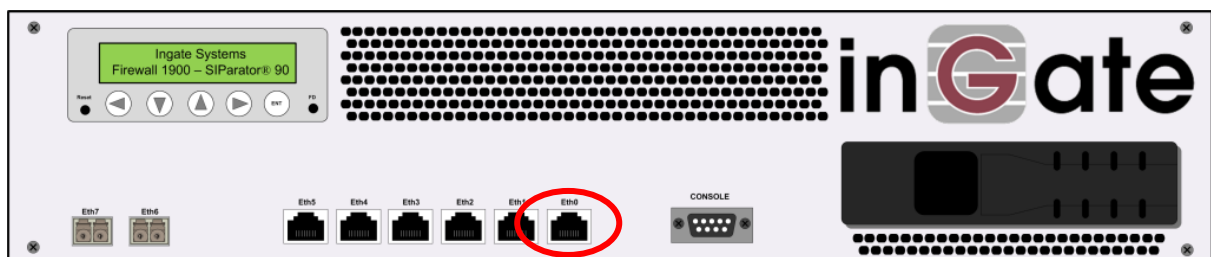
#### Ingate 1190 Firewall and SIParator 19 (Back)



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

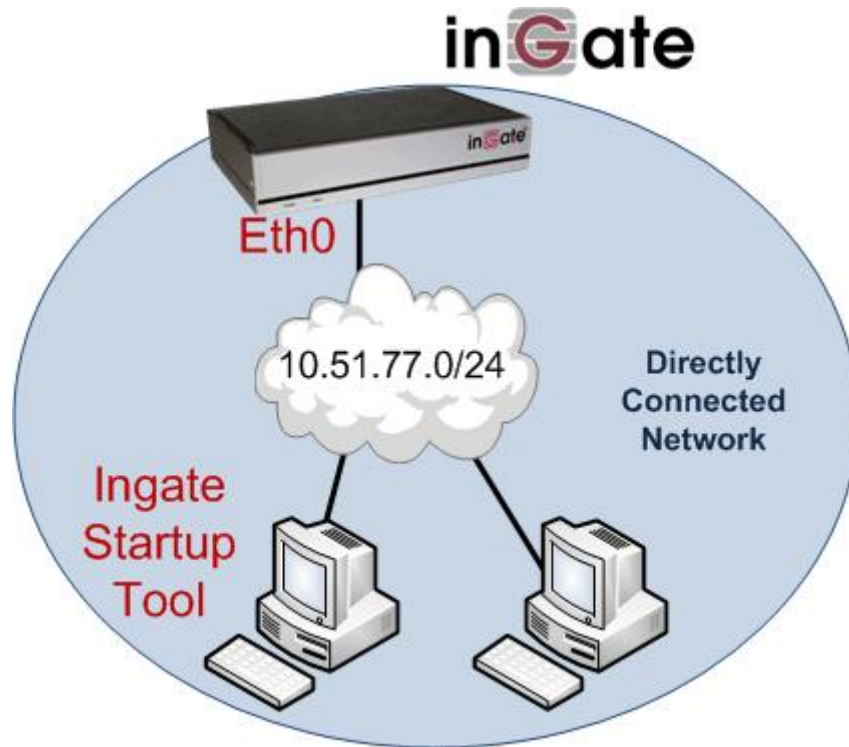


#### Ingate 1900 Firewall and SIParator 90



- 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

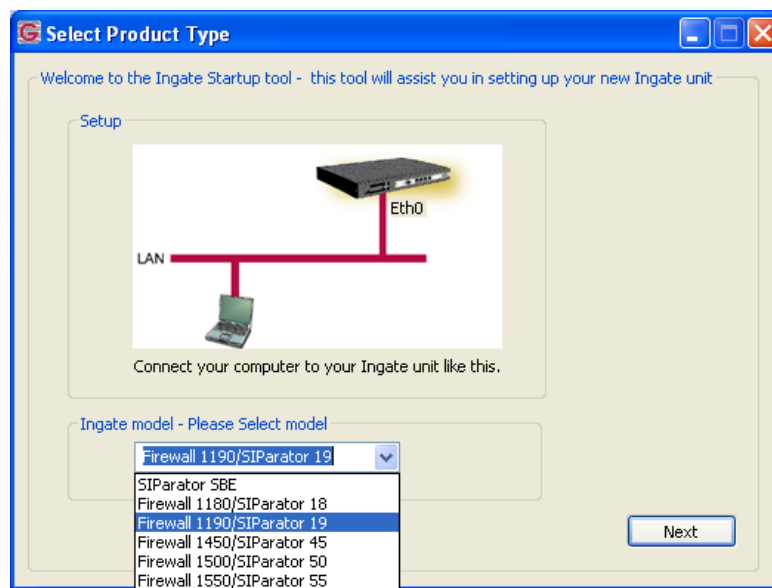
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.



- 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  
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
- ☒ Enable SIP module
- ☐ Configure Remote SIP Connectivity
- ☒ Configure SIP trunking
- ☐ Backup the created configuration
- ☐ Create a config without connecting to a unit
- ☐ This tool remembers passwords

Assign IP address and password, establish contact

Inside (Interface Eth0)

IP Address: 10 . 51 . 77 . 100

MAC Address: 00-d0-c9-a2-44-55

Select a password

Password: .....

Confirm Password: .....

Contact

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 SIP Trunking” if you want the tool to configure SIP Trunking between the Asterisk Business Edition server and ITSP.

- b. Select “Register this unit with Ingate” if you want the tool to connect with [www.ingate.com](http://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](http://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: ••••••

Contact

- 8) Proceed to Section 4.3: Network Topology.

## 4.2 Change or Update Configuration

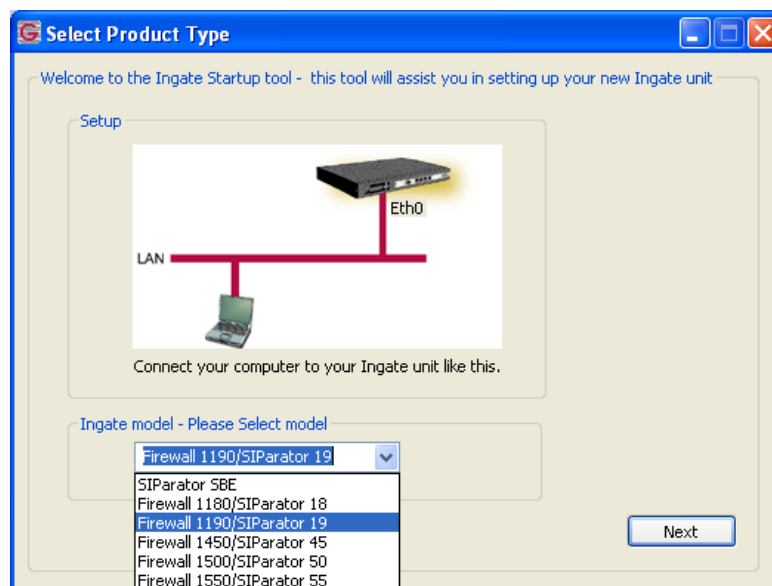
When selecting the “Change or update configuration of the unit” setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – “Configure the unit for the first time” or via the Console port.

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.



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

Ingate Startup Tool - Helps configure your Ingate unit

Ingate Startup Tool Version  
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
- ☒ 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: .....

Contact

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”,

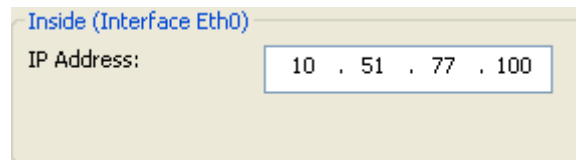
First select what you would like to do:

- ☐ 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 SIP Trunking” if you want the tool to configure SIP Trunking between the Asterisk Business Edition server and ITSP.

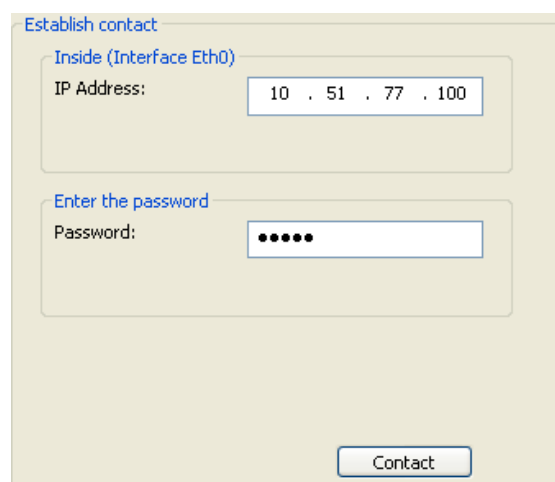
- b. Select “Register this unit with Ingate” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) to register the unit. If selected, consult the Startup Tool – Getting Started Guide.
  - c. Select “Upgrade this unit” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) 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 of the Ingate Unit.



- 6) In the “Enter a Password”, enter the Password of the Ingate unit.



- 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.



- 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.

The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'Standalone SIParator'. The 'Inside (Interface Eth0)' section shows IP address '10 . 51 . 77 . 100' and Netmask '255 . 255 . 255 . 0'. The 'Outside (Interface Eth1)' section has checkboxes for 'Use DHCP to obtain IP' (unchecked) and 'Allow https access to web interface from Internet' (unchecked), with IP address '172 . 51 . 77 . 100', Netmask '255 . 255 . 255 . 0', and Gateway '172 . 51 . 77 . 1'. A network diagram shows the 'Ingate SIParator' connected to a 'LAN' with an 'IP-PBX' and an 'Existing firewall' connected to the 'Internet'. The 'DNS server' section has Primary '4 . 2 . 2 . 2' and Secondary '0 . 0 . 0 . 0'. The 'Status' section shows 'Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0' and a list of features: VoIP Survival, VPN, QoS, Enhanced Security, 10 SIP Traversal Licenses, 10 SIP User Registration Licenses, and Software Version: 4.6.2. A 'Help' button is at the bottom right.

### Configuration Steps:

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

A close-up of the 'Product Type' dropdown menu, showing 'Standalone SIParator' selected.

**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.

### 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.

The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'Firewall'. The 'Inside (Interface Eth0)' section shows an IP address of 10.51.77.1 and a Netmask of 255.255.255.0. The 'Outside (Interface Eth1)' section has the 'Use DHCP to obtain IP' checkbox selected, with a Gateway of 12.23.34.1. A diagram on the right shows the 'Ingate Firewall' connected to the 'Internet' and a 'LAN' with an 'IP-PBX'. The 'DNS server' section has a Primary of 4.2.2.1 and a Secondary of 4.2.2.2. The 'Status' section shows the tool version (2.4.0) and connection details (Ingate Firewall 1190, IG-092-719-5012-4). A list of features includes Remote SIP Connectivity, VPN, QoS, Enhanced Security, 15 SIP Traversal Licenses, and 20 SIP User Registration Licenses. The software version is 4.6.2.

#### Configuration Steps:

- 1) In Product Type, select “Firewall”.

A close-up of the 'Product Type' dropdown menu, showing 'Firewall' selected.

- 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.

A close-up of the 'Inside (Interface Eth0)' configuration fields. The 'IP address' field contains '10 . 51 . 77 . 1' and the 'Netmask' field contains '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 DHCP.

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,
- 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

- 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 OK Cancel

Expire in (days): (Required) 365

Country Code (C): US

Organisation (O): Company Name

State/province(ST): NY

Organizational Unit(OU): Department

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.

The screenshot shows the 'Ingate Startup Tool' window with the 'IP-PBX' tab selected. The 'Product Type' is set to 'Standalone SIParator'. The 'Inside (Interface Eth0)' section shows IP address '10 . 51 . 77 . 100' and Netmask '255 . 255 . 255 . 0'. The 'Outside (Interface Eth1)' section has 'Use DHCP to obtain IP' checked, with IP Address '12 . 23 . 34 . 45', Netmask '255 . 255 . 255 . 248', and Gateway '12 . 23 . 34 . 41'. A diagram shows the Ingate SIParator connected to a LAN with an IP-PBX and to the Internet via an existing firewall. DNS server settings are Primary: '4 . 2 . 2 . 1' and Secondary: '4 . 2 . 2 . 2'. The status bar indicates 'Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0' and lists features like VoIP Survival, VPN, QoS, Enhanced Security, and 10 SIP Traversal Licenses.

#### Configuration Steps:

- 1) In Product Type, select “Standalone SIParator”.

The close-up shows the 'Product Type:' label followed by a dropdown menu currently displaying '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.

The close-up shows the 'Inside (Interface Eth0)' section with the IP address field set to '10 . 51 . 77 . 100' and the Netmask field set to '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 DHCP.

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): Your Name

Expire in (days): 365

Country Code (C): US

Organisation (O): Company Name

State/province(ST): NY

Organizational Unit(OU): Department

Email address: admin@email.com

Locality/town(L): Your City

OK Cancel

- 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.

The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'DMZ SIParator'. The 'DMZ (Interface Eth0)' section shows an IP address of 10.51.77.100 and a Netmask of 255.255.255.0. The 'LAN IP address range' section shows a Low IP of 192.168.1.1 and a High IP of 192.168.1.255. The 'Gateway' is 10.51.77.1 and the 'Firewall extern IP' is 12.23.34.45. A network diagram on the right shows the Internet connected to a Firewall, which is connected to the Ingate SIParator and the LAN. The LAN is connected to an IP-PBX. The 'DNS server' section shows a Primary of 4.2.2.2 and a Secondary of 4.2.2.1. The 'Status' section shows the Ingate Startup Tool Version 2.4.0, connected to Ingate SIParator 19, IG-092-702-2122-0. The status list includes VoIP Survival, VPN, QoS, Enhanced Security, 10 SIP Traversal Licenses, 10 SIP User Registration Licenses, and Software Version: 4.6.2.

#### Configuration Steps:

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

The close-up shows the 'Product Type' dropdown menu with 'DMZ SIParator' selected.

- 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.

The close-up shows the 'DMZ (Interface Eth0)' section with the IP address field set to 192.168.100.100 and the Netmask field set to 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 Firewall's 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:

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

The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'DMZ-LAN SIParator'. The 'Inside (Interface Eth0)' section shows IP address '10 . 51 . 77 . 100' and Netmask '255 . 255 . 255 . 0'. The 'DMZ (Interface Eth1)' section has 'Use DHCP to obtain IP' unchecked, with IP address '192 . 168 . 100 . 100' and Netmask '255 . 255 . 255 . 0'. The 'Gateway' is '192 . 186 . 100 . 1' and 'Firewall extern IP' is '98 . 87 . 76 . 65'. A checkbox 'Allow https access to web interface from Internet' is checked. The 'DNS server' section shows 'Primary: 4 . 2 . 2 . 1' and 'Secondary: (Optional) 4 . 2 . 2 . 2'. The 'Status' section shows 'Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0' and a list of features: VoIP Survival, VPN, QoS, Enhanced Security, 10 SIP Traversal Licenses, 10 SIP User Registration Licenses, and Software Version: 4.6.2. A network diagram on the right shows the Internet, Existing firewall, Ingate SIParator, DMZ, LAN, and IP-PBX.

#### Configuration Steps:

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

The screenshot shows the 'Product Type' dropdown menu with 'DMZ-LAN SIParator' selected.

- 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.

The screenshot shows the 'Inside (Interface Eth0)' configuration fields with 'IP address: 10 . 51 . 77 . 100' and '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 DHCP.

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 Firewall's 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

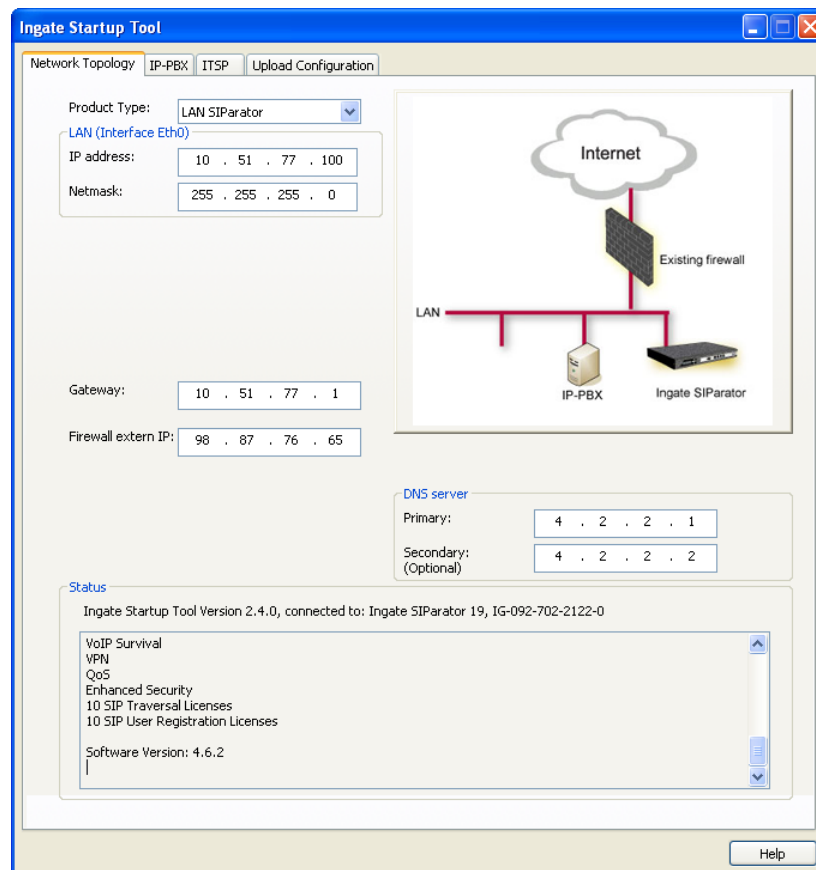
- 7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

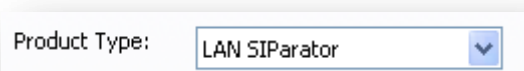
### 4.3.5 Product Type: LAN SIParator

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.

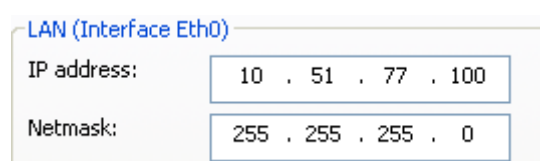


#### Configuration Steps:

- 1) In Product Type, select “LAN SIParator”.



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



- 3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewall's 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:

- Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- 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.

The screenshot shows the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The 'Product Type' is set to 'LAN SIParator'. The 'LAN (Interface ET1)' section shows the IP address '10 . 51 . 77 . 200' and Netmask '255 . 255 . 255 . 0'. The 'Gateway' is '10 . 51 . 77 . 1'. The 'Firewall extern IP' is '98 . 87 . 76 . 65' and the 'Port range' is '58024 - 60999'. There is a checkbox for 'Allow DHCP Server, (setup in web GUI)'. The 'DNS server' section has 'Primary' as '4 . 2 . 2 . 1' and 'Secondary (Optional)' as '4 . 2 . 2 . 2'. The 'Status' section shows the tool version and connection status. A network diagram on the right shows the Internet connected to an Existing firewall, which is connected to the LAN. The LAN contains an IP-PBX and the Ingate SIParator.

#### Configuration Steps:

- 1) In Product Type, select “LAN SIParator”.

The close-up shows the 'Product Type' dropdown menu with 'LAN SIParator' selected.

- 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.

The close-up shows the 'LAN (Interface Eth0)' section with the IP address '10 . 51 . 77 . 100' and Netmask '255 . 255 . 255 . 0'.

- 3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewall's IP Address on the DMZ network.

Gateway:	<input type="text" value="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:	<input type="text" value="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:	<input type="text" value="58024"/>	-	<input type="text" value="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:	<input type="text" value="4 . 2 . 2 . 1"/>
Secondary: (Optional)	<input type="text" value="4 . 2 . 2 . 2"/>

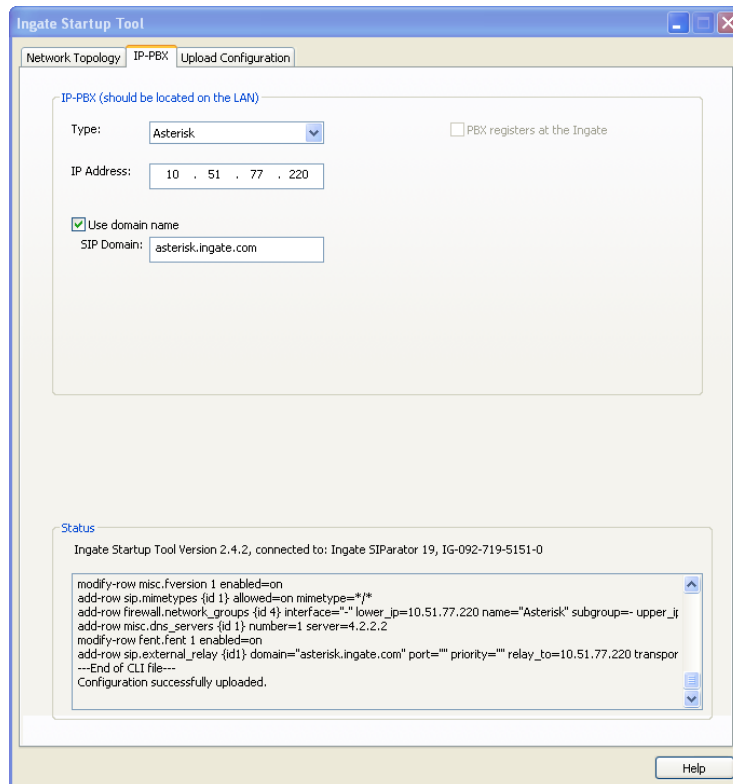
- 7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- Port Forward the WAN/Internet interface SIP Signaling port of 5060 with a UDP/TCP Forward to the Ingate SIParator
- 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 SIP Trunking. 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 with the Asterisk BE server.



The screenshot shows the 'Ingate Startup Tool' window with the 'IP-PBX' tab selected. The configuration fields are as follows:

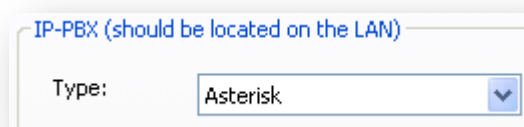
- IP-PBX (should be located on the LAN):**
  - Type:** Asterisk (selected from a dropdown menu)
  - IP Address:** 10 . 51 . 77 . 220
  - Use domain name:** ☒ (checked)
  - SIP Domain:** asterisk.ingate.com
  - PBX registers at the Ingate:** ☐ (unchecked)
- Status:**
  - Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-719-5151-0
  - CLI output: modify-row misc.fversion 1 enabled=on; add-row sip.minetypes {id 1} allowed=on minetype=\*/\*; add-row firewall.network\_groups {id 4} interface="" lower\_ip=10.51.77.220 name="Asterisk" subgroup=- upper\_ip=10.51.77.220; 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 {id 1} domain="asterisk.ingate.com" port="" priority="" relay\_to=10.51.77.220 transport=UDP; ---End of CLI file---
  - Configuration successfully uploaded.

A 'Help' button is located at the bottom right of the window.

### Configuration Steps:



- 1) In the IP-PBX Type drop down list, select "Asterisk". Ingate has confirmed interoperability the Asterisk BE, the unique requirements of the testing are contained in the Startup Tool.



This image is a close-up of the 'Type' dropdown menu in the IP-PBX configuration section. The dropdown is open, showing 'Asterisk' as the selected option.



- 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 an 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

<input checked="" type="checkbox"/> Use domain name
SIP Domain: asterisk.ingate.com

## 4.5 ITSP

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

The screenshot shows the 'Ingate Startup Tool' window with the 'ITSP\_1' tab selected. The 'Name' dropdown is set to 'Generic ITSP'. The 'Provider address' section includes an 'IP Address' field with '0 . 0 . 0 . 0' and an unchecked 'Use domain name' checkbox. The 'Advanced' section has three sub-sections: 'Prefix to match and remove from inbound calls' with an empty 'Prefix' field, 'Prefix to add to outbound calls' with an empty 'Prefix' field, and 'Forward 3xx messages' with a checked 'Enable' checkbox. The 'Account information' section has an unchecked 'Use account' checkbox, an 'Authentication name' field with '(same as DID if blank)' and an unchecked 'Increment authentication name for ranges' checkbox, a 'Domain' field, and a 'Password' field. There is also an unchecked 'Use user account on incoming call' checkbox. The 'PBX local numbers (advanced)' section has a 'Local number(start of range, use same as DID if local numbers are not used):' field, a 'Password (only used if PBX registers at the Ingate):' field, and an unchecked 'PBX registers at the Ingate' checkbox. The 'Status' section at the bottom shows 'Ingate Startup Tool Version 2.4.0, connected to: Ingate SIPParator 19, IG-092-702-2122-0' and a list of features: 'VoIP Survival', 'VPN', 'QoS', 'Enhanced Security', '10 SIP Traversal Licenses', and '10 SIP User Registration Licenses'. The 'Software Version' is '4.6.2'. A 'Help' button is in the bottom right corner.

### Configuration Steps:

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

This close-up shows the 'Name:' label and a dropdown menu. The dropdown menu is open, showing 'Generic ITSP' as the selected option. The dropdown arrow is pointing downwards.

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

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

Provider address

IP Address:

☐ Use domain name

Provider address

Domain:

☒ Use domain name

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

Account information:

☒ Use account

Authentication name:  
(same as DID if blank)

☐ Increment authentication name for ranges

Domain:

Password:

☒ Use user account on incoming call

- i. Enter a DID (Username) in which the Ingate will register with the Service Provider. The Startup Tool also has the ability to program a sequential range of DIDs.

DID (start of range)  
(user name):

DID range size:

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

Account information:

☒ Use account

Authentication name:  
(same as DID if blank)

☐ Increment authentication name for ranges

Domain:

Password:

☒ Use user account on incoming call

- 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.

Advanced

Prefix to match and remove from inbound calls

Prefix:

Prefix to add to outbound calls

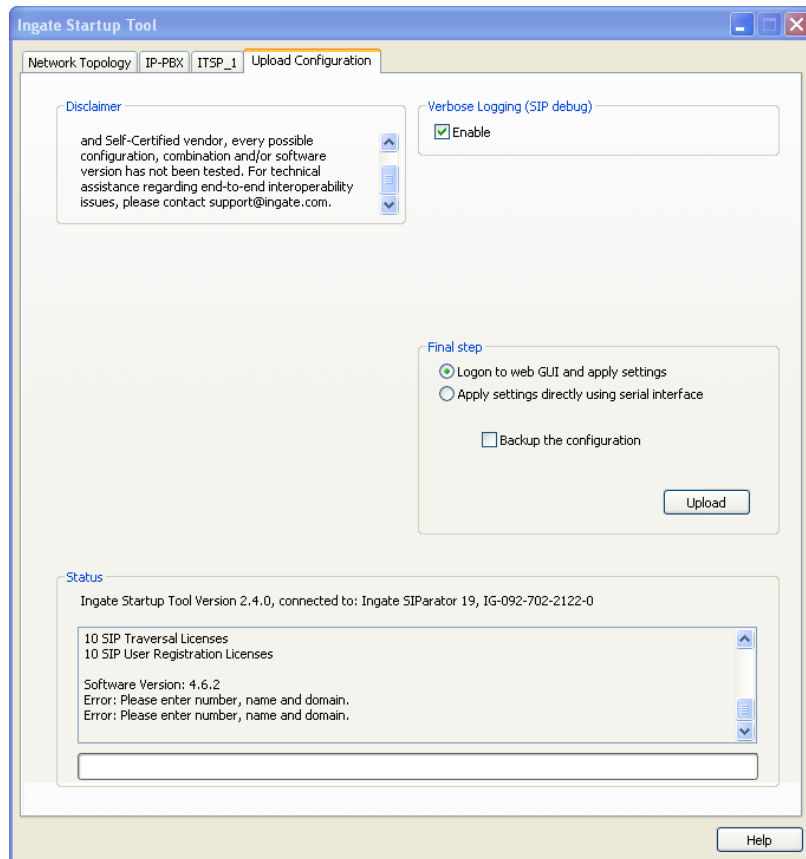
Prefix:

Forward 3xx messages

☒ Enable

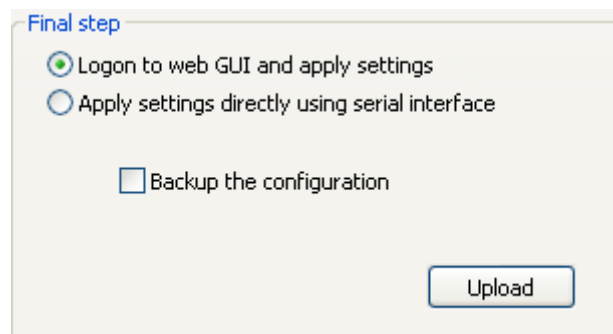
## 4.6 Upload Configuration

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.

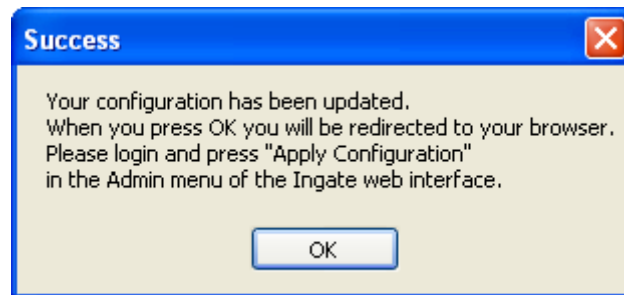


### Configuration Steps:

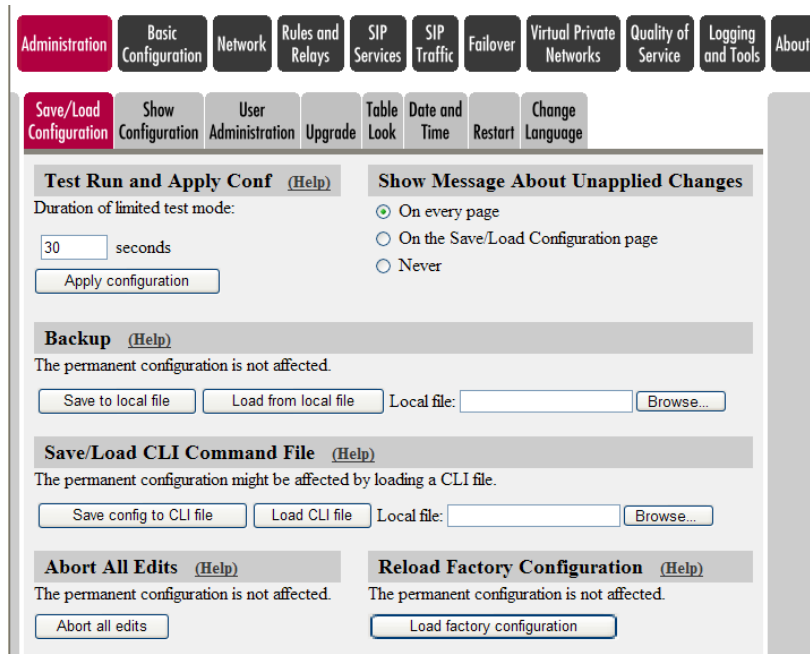
- 1) Press the “Upload” button. If you would like the Startup Tool to create a Backup file also select “Backup the configuration”. Upon pressing the “Upload” button the Startup Tool will push a database into the Ingate unit.



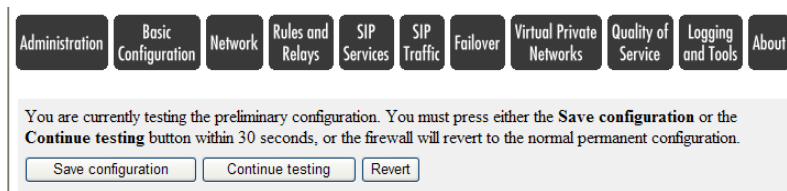
- 2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



- 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.



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



## 5 Additional Manual Configuration

### 5.1 User Database

The screenshot shows the Asterisk BE configuration interface. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for SIP Methods, Filtering, User Database (highlighted), Authentication and Accounting, Dial Plan, Routing, Time Classes, and SIP Status. The main content area is divided into two sections: 'Local SIP Domains' and 'Local SIP User Database'. The 'Local SIP Domains' section has a table with columns 'Domain' and 'Delete'. It contains one row with the domain '10.51.77.100' and a delete checkbox. Below the table is a button 'Add new rows' and a text '1 rows.'. The 'Local SIP User Database' section has a table with columns: Username, Domain, Authentication Name, Password, Account Type, Register From, and Delete. It contains two rows. The first row has Username '16139630933', Domain 'asterisk.ingate.co', Authentication Name 'asterisk', Password 'Change Password', Account Type 'XF', Register From 'LAN', and a delete checkbox. The second row has Username 'asterisk', Domain '10.51.77.100', Authentication Name 'asterisk', Password 'Change Password', Account Type 'User', Register From 'LAN', and a delete checkbox.

#### 5.1.1 Local User Account



The Asterisk BE will attempt to register a User Account with the Ingate. A “User” Account type will need to be created.

#### Configuration Steps:

- 1) Go to SIP Traffic, User Database.
- 2) Under Local SIP Domains, press “Add new rows”
- 3) Under Domain, enter the LAN IP Address (eth0) of the Ingate.

The screenshot shows the 'Local SIP Domains' configuration window. It has a title bar 'Local SIP Domains (Help)'. Inside, there is a table with columns 'Domain' and 'Delete'. The 'Domain' column contains the text '10.51.77.100' and the 'Delete' column contains a checkbox.

**Note:** The following steps must correspond with the programming in the Asterisk BE configuration, found in Trunks, then VOIP Trunks. See Section 6.1.

The screenshot shows the 'Edit SIP trunk asterisk' configuration window. It has a title bar 'Edit SIP trunk asterisk'. Inside, there are several fields: 'Provider Name' (Ingate Direct), 'Hostname' (10.51.77.100), 'Username' (asterisk), 'Password' (123456), 'Codecs' (First: u-law, Second: a-law, Third: G.729, Fourth: None, Fifth: None), and 'CallerID' (16139630933). There is a checkbox 'Enable Remote MWI' which is unchecked. At the bottom, there are 'Cancel' and 'Add' buttons.

- 4) Under Local SIP User Database, press “Add new rows”

**Local SIP User Database** [\(Help\)](#)

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
asterisk	10.51.77.100	asterisk	<a href="#">Change Password</a>	User	LAN	<input type="checkbox"/>



- 5) Enter the follow attribute that correspond with the Asterisk BE - VOIP Trunks
  - a. **Username** – Enter the Username from the Asterisk BE
  - b. **Domain** – LAN IP Address of the Ingate
  - c. **Authentication Name** – Enter the Username from the Asterisk BE
  - d. **Password** – Enter the Password from the Asterisk BE
  - e. **Account Type** – Select “User”
  - f. **Register From** – Select “LAN” or “Asterisk” (when using the Startup Tool)

### 5.1.2 Asterisk INVITE Authentication Account



When the Ingate sends a call to the Asterisk BE, the Asterisk BE requires the INVITE to be authenticated. An Account is required to provide the Asterisk BE the Authentication details.

#### Configuration Steps:

**Note:** The following steps must correspond with the programming in the Asterisk BE configuration, found in Trunks, then VOIP Trunks. See Section 6.1.

- 1) Go to SIP Traffic, User Database.
- 2) Under Local SIP User Database, press “Add new rows”

**Local SIP User Database** [\(Help\)](#)

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
16139630933	asterisk.ingate.co	asterisk	<a href="#">Change Password</a>	XF	LAN	<input type="checkbox"/>



- 3) Enter the follow attribute that correspond with the Asterisk BE - VOIP Trunks
  - a. **Username** – Enter the DID from the Service Provider
  - b. **Domain** – Enter the Asterisk SIP Domain FQDN
  - c. **Authentication Name** – Enter the Username from the Asterisk BE
  - d. **Password** – Enter the Password from the Asterisk BE
  - e. **Account Type** – Select “XF”
  - f. **Register From** – Select “LAN” or “Asterisk” (when using the Startup Tool)

## 5.2 Dial Plan



The Startup Tool creates a generic Dial Plan to accept incoming calls and direct the calls to the Asterisk Server, and to take calls from the Asterisk Server and direct the calls to the ITSP.

The purpose of this section is to make a minor modification to the Forward To section to add the User Account to satisfy the Asterisk BE INVITE Authentication requirements.

Administration
Basic Configuration
Network
SIP Services
SIP Traffic
Failover
Virtual Private Networks
Quality of Service
Logging and Tools
About

SIP Methods
Filtering
User Database
Authentication and Accounting
Dial Plan
Routing
Time Classes
SIP Status

### Matching From Header [\(Help\)](#)

Name	Use This ...		... Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
Asterisk	*	*		UDP	Asterisk	<input type="checkbox"/>
Bandwidth.com	*	*		UDP	ITSP_IP	<input type="checkbox"/>
LAN	*	*		UDP	LAN	<input type="checkbox"/>
WAN	*	*		Any	WAN	<input type="checkbox"/>

Add new rows 1 rows.

### Matching Request-URI [\(Help\)](#)

Name	Use This ...					... Or This	Delete
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Inbound			-			sip:\+1(.*)@12.12	<input type="checkbox"/>
Outbound			-			sip:(.*)@10.51.77	<input type="checkbox"/>

Add new rows 1 rows.

### Forward To [\(Help\)](#)

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
+ Asterisk	1	16139630933@asterisk.ingate.com			-		<input type="checkbox"/>
+ Bandwidth.com	1	-			-	sip:+\$1@216.82.2	<input type="checkbox"/>
	2	-			-	sip:+\$1@216.82.2	<input type="checkbox"/>

Add new rows 1 groups with 1 rows per group.

### Dial Plan [\(Help\)](#)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM
					Forward	ENUM	
1	Asterisk	Outbound	Forward	Bandwidth.com			-
2	Bandwidth.com	Inbound	Forward	Asterisk			-
3	WAN	-	Reject	-			-



### Configuration Steps:

- 1) The Startup Tool has configured the Ingate Dial Plan
- 2) Go to the Forward To section, under the row labeled “Asterisk”
  - a. Remove the Regular Expression
  - b. Under Use This Account column, select the User Account created in section 5.1.2.

Forward To <a href="#">(Help)</a>							
Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
<a href="#">+ Asterisk</a>	1	16139630933@asterisk.ingate.com ▼			- ▼		<input type="checkbox"/>
<a href="#">+ Bandwidth.com</a>	1	- ▼			- ▼	sip:+\$1@216.82.1	<input type="checkbox"/>
	2	- ▼			- ▼	sip:+\$1@216.82.1	<input type="checkbox"/>

**Note:** Be sure to APPLY and SAVE all settings in the Administration page.

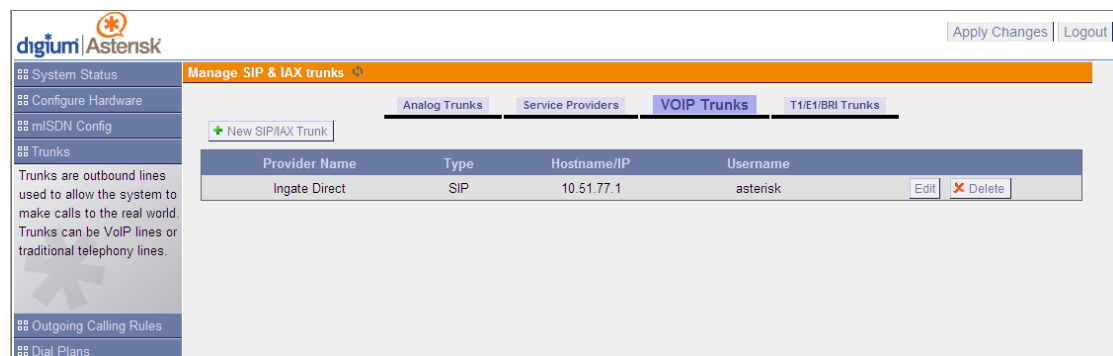
## 6 Asterisk Business Edition Setup



The Asterisk setup involves setting up the VOIP Trunks, Dial Plans, Outgoing Calling Rules, associating the SIP Domain, and adding an Outbound Proxy when using an Ingate SIParator.

### 6.1 VOIP Trunks

Trunks are outbound lines used to allow the system to make calls to the real world.



#### Configuration Steps:

- 1) Select “New SIP/IAX Trunk” and the Asterisk BE will launch another screen.
- 2) In the Create New SIP/IAX Trunk, select the following:
  - a. **Type:** Select “SIP”
  - b. **Provider Name:** Enter a unique label
  - c. **Hostname:** Enter the LAN IP Address (eth0) of the Ingate
  - d. **Password:** Enter a Password for Authentication on the Ingate

## 6.2 Outgoing Calling Rules

Calling Rules define dialing permissions and routing rules. An outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g. "local" 7-digit dials through a PRI but "long distance" 10-digit dials through a low-cost SIP trunk). Asterisk BE contains several default Calling Rules.

**Manage Calling Rules**

[+ New Calling Rule](#) [Restore Default Calling Rules](#)

**Outgoing Calling Rules**

An outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g. "local" 7-digit dials through a PRI but "long distance" 10-digit dials through a low-cost SIP trunk). You can optionally set a failover trunk to use when the primary trunk fails. Note that this panel manages only individual outgoing call rules. See the Dial Plans section to associate multiple outgoing calling rules to be used for User outbound dialing.

Calling Rule	Pattern	Trunk	Failover Trunk	Edit	Delete
Longdistance	_91XXXXXXX!	Ingate Direct	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>
IAXTEL	_91700XXXX!	None Assigned	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>
Local	_9613XXXX!	Ingate Direct	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>
Local	_9XXXX!	Ingate Direct	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>
International	_9011XXXX!	Ingate Direct	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>
911	_911!	None Assigned	None Selected	<a href="#">Edit</a>	<a href="#">Delete</a>

### Configuration Steps:

- 1) Select "Edit" on the corresponding Calling Rule and the Asterisk BE will launch another screen. Must be done for each Calling Rule.
- 2) In the "Send this call through trunk" section, select the following:
  - a. **Use Trunk:** Select "Provider Name" entered in the VOIP Trunk setup
  - b. **Strip:** (Optional) Enter the number of digits the strip from the front
  - c. **Prepend these digits:** (Optional) Enter the number of digits before dial

**Edit Calling Rule**

Calling Rule Name: Longdistance

Pattern: 91XXXXXXXX!

☐ Send to Local Destination

Destination: [Dropdown]

**Send this call through trunk:**

Use Trunk: Ingate Direct

Strip: 1 digits from front

and Prepend these digits: before dialing

☐ Use FailOver Trunk

fail over Trunk: Ingate Direct

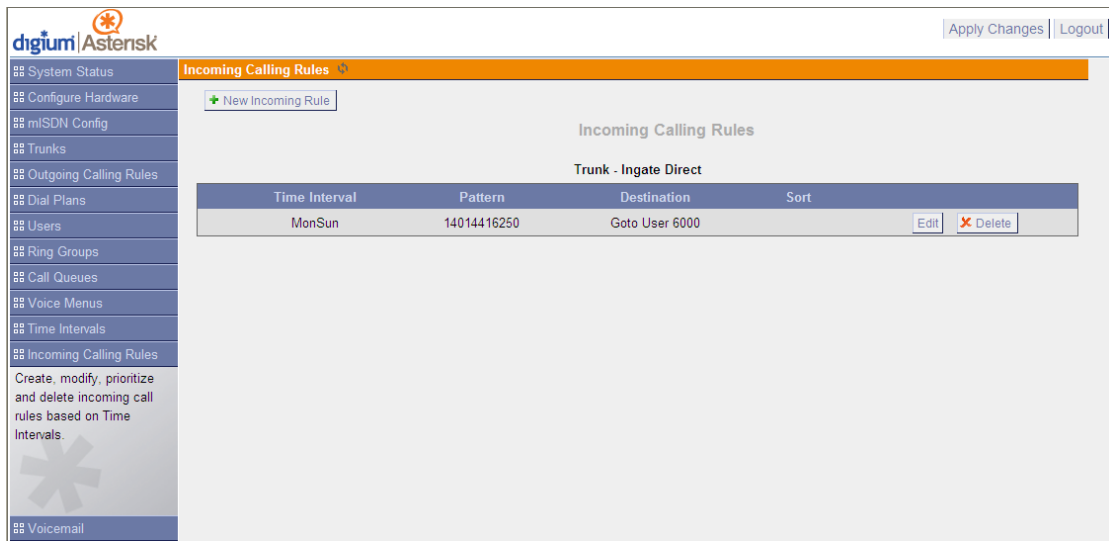
Strip: digits from front

and Prepend these digits: before dialing

[Cancel](#) [Save](#)

## 6.3 Incoming Calling Rules

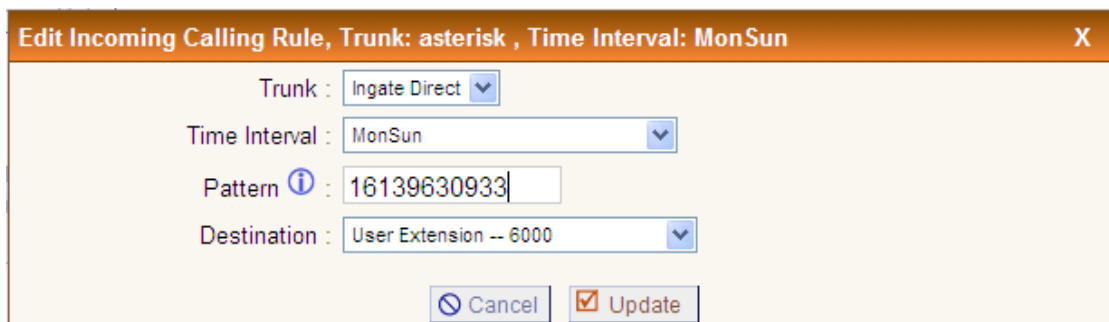
Create, modify, prioritize and delete incoming call rules based on Time Intervals.



The screenshot shows the Asterisk web interface. On the left is a sidebar menu with options: System Status, Configure Hardware, miSDN Config, Trunks, Outgoing Calling Rules, Dial Plans, Users, Ring Groups, Call Queues, Voice Menus, Time Intervals, Incoming Calling Rules (selected), and Voicemail. The main content area is titled "Incoming Calling Rules" and includes a "+ New Incoming Rule" button. Below this is a table titled "Trunk - Ingate Direct" with columns: Time Interval, Pattern, Destination, and Sort. The table contains one row: MonSun, 14014416250, Goto User 6000. To the right of this row are "Edit" and "Delete" buttons. At the top right of the interface are "Apply Changes" and "Logout" links.

### Configuration Steps:

- 1) Select "New Incoming Rule" and the Asterisk BE will launch another screen.
- 2) In the "New Incoming Rule" section, select the following:
  - a. **Trunk:** Select "Provider Name" entered in the VOIP Trunk setup
  - b. **Time Interval:** Enter the Time Interval
  - c. **Pattern:** Enter the DID number dialed into the Asterisk BE
  - d. **Destination:** Select from the List of User Extensions and Applications.



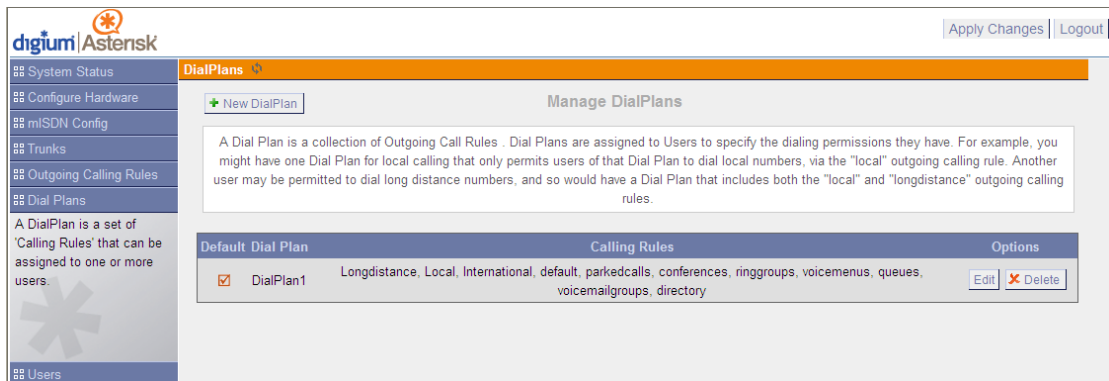
The screenshot shows the "Edit Incoming Calling Rule" form. The title bar reads "Edit Incoming Calling Rule, Trunk: asterisk , Time Interval: MonSun" with a close button (X). The form contains the following fields:

- Trunk :** A dropdown menu showing "Ingate Direct".
- Time Interval :** A dropdown menu showing "MonSun".
- Pattern ⓘ :** A text input field containing "16139630933".
- Destination :** A dropdown menu showing "User Extension -- 6000".

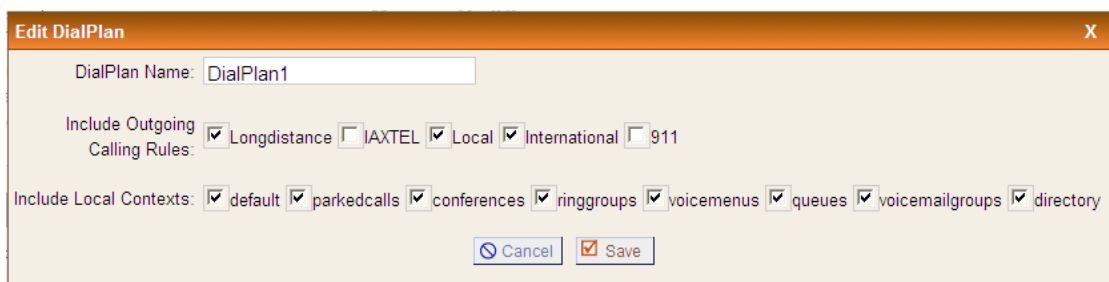
At the bottom of the form are two buttons: "Cancel" and "Update" (which has a checked checkbox next to it).

## 6.4 Dial Plan

A Dial Plan is a set of 'Calling Rules' that can be assigned to one or more users. A Dial Plan is a collection of Outgoing Call Rules. Dial Plans are assigned to Users to specify the dialing permissions they have. The Asterisk BE comes with a Default Dial Plan.



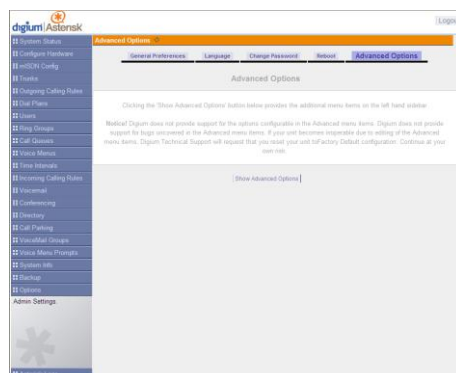
Ensure the Calling Rules are selected in the Dial Plan.



## 6.5 SIP Settings

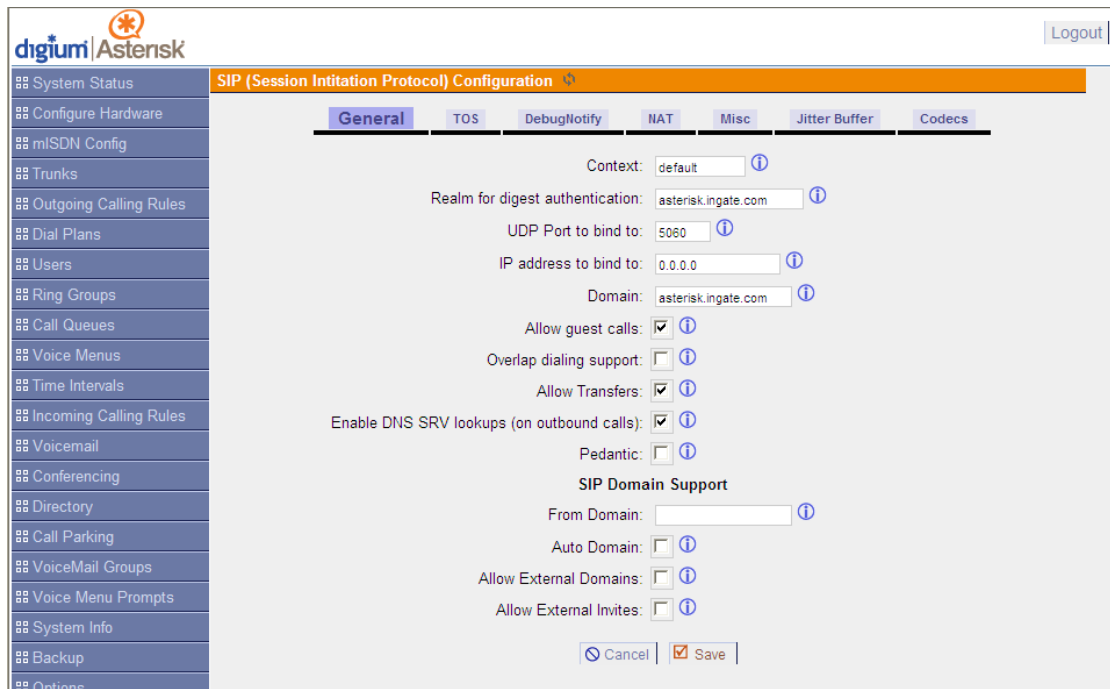
Clicking the 'Show Advanced Options' button below provides the advanced menu items on the left hand sidebar

**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.



## 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

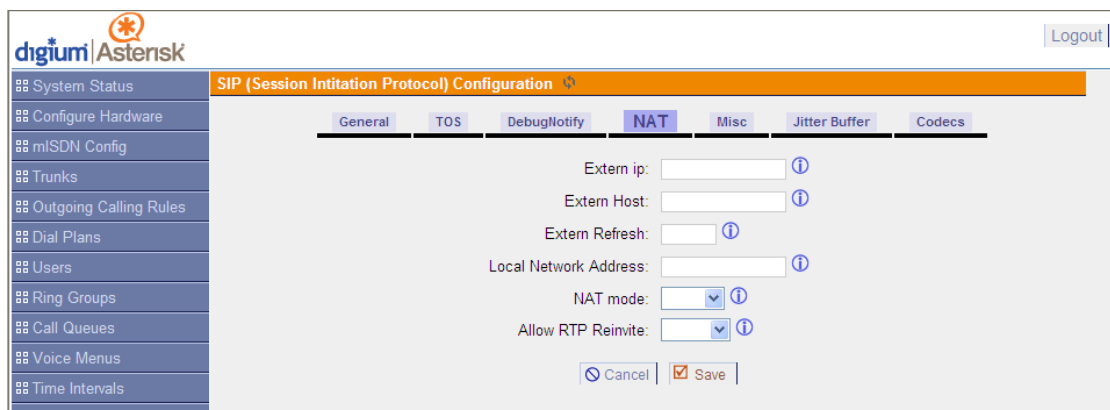


The screenshot shows the Asterisk SIP Configuration interface. The left sidebar contains a menu with options like System Status, Configure Hardware, mISDN Config, Trunks, Outgoing Calling Rules, Dial Plans, Users, Ring Groups, Call Queues, Voice Menus, Time Intervals, Incoming Calling Rules, Voicemail, Conferencing, Directory, Call Parking, VoiceMail Groups, Voice Menu Prompts, System Info, Backup, and Options. The main content area is titled 'SIP (Session Initiation Protocol) Configuration' and has several tabs: General, TOS, Debug/Notify, NAT, Misc, Jitter Buffer, and Codecs. The 'General' tab is selected. It contains the following fields and options:

- 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: ☐

At the bottom of the form are 'Cancel' and 'Save' buttons.

**Note:** The NAT area is left Blank



The screenshot shows the Asterisk SIP Configuration interface with the 'NAT' tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'SIP (Session Initiation Protocol) Configuration' and has tabs: General, TOS, Debug/Notify, NAT, Misc, Jitter Buffer, and Codecs. The 'NAT' tab is selected. It contains the following fields and options:

- Extern ip:
- Extern Host:
- Extern Refresh:
- Local Network Address:
- NAT mode:
- Allow RTP Reinvite:

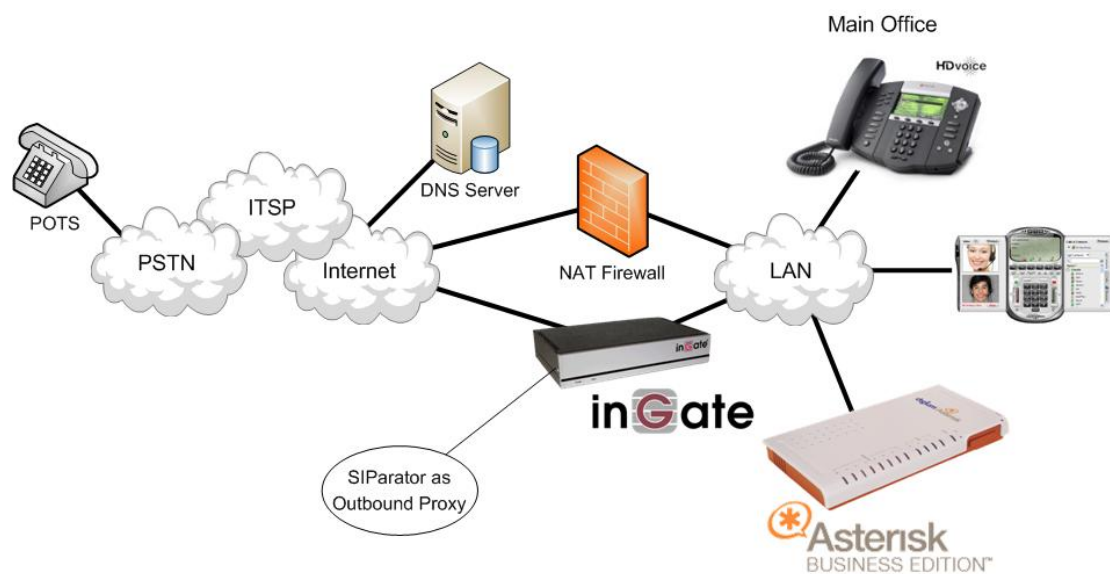
At the bottom of the form are 'Cancel' and 'Save' buttons.

## 6.6 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.

**Note:** This variable is not needed with the Ingate Firewall Product.



## 7 Troubleshooting

### 7.1 Ingate – Asterisk BE Registration

The Asterisk BE – VOIP Trunk will register with the Ingate. Here is how the Username and Passwords all match up. In addition, the Asterisk BE will challenge any incoming INVITE, so the Authentication Username and Password needs to be added to an additional account.

The screenshot displays the Asterisk Manager GUI configuration for a SIP trunk. The top navigation bar includes tabs for Administration, Basic Configuration, Network, SIP Services, SIP Traffic (selected), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, the 'User Database' tab is active, showing the 'Local SIP User Database' section.

The 'Local SIP Domains' section contains a table with one entry:

Domain	Delete
10.51.77.100	<input type="checkbox"/>

Below this is a button 'Add new rows' and a text field '1 rows'.

The 'Local SIP User Database' section contains a table with two entries:

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
16139630933	asterisk.ingate.co	asterisk	Change Password	XF	LAN	<input type="checkbox"/>
asterisk	10.51.77.100	asterisk	Change Password	User	LAN	<input type="checkbox"/>

The 'Edit SIP trunk asterisk' dialog box is open, showing the following fields:

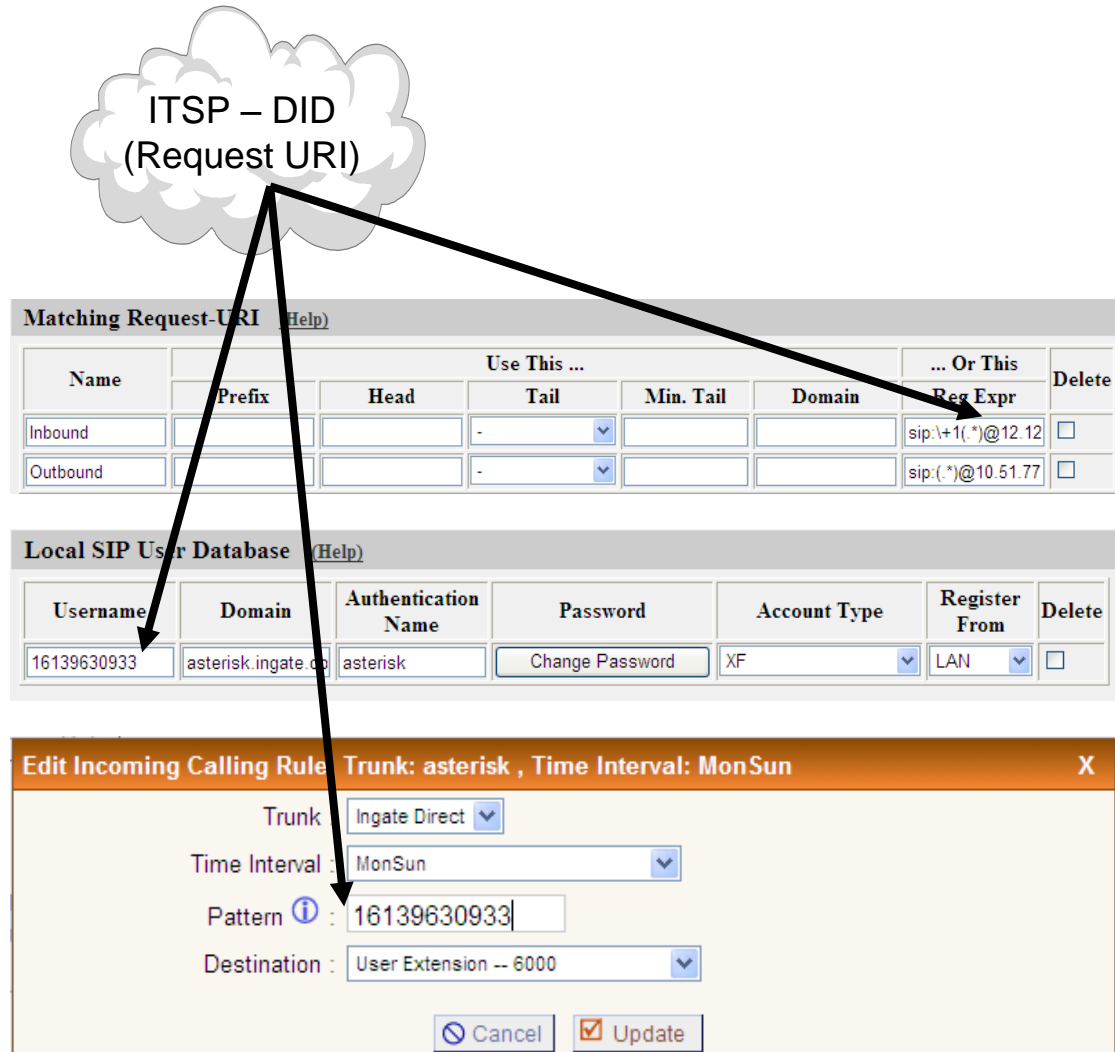
- Provider Name: Ingate Direct
- Hostname: 10.51.77.100
- Username: asterisk
- Password: 123456
- Codecs: First: u-law, Second: a-law, Third: G.729, Fourth: None, Fifth: None
- CallerID: 16139630933
- Enable Remote MWI: ☐

Arrows indicate the mapping of values between the database and the trunk configuration:

- A red arrow points from the 'Domain' field '10.51.77.100' in the 'Local SIP Domains' table to the 'Hostname' field in the 'Edit SIP trunk asterisk' dialog.
- A red arrow points from the 'Username' field 'asterisk' in the 'Local SIP User Database' table to the 'Username' field in the 'Edit SIP trunk asterisk' dialog.
- A red arrow points from the 'Authentication Name' field 'asterisk' in the 'Local SIP User Database' table to the 'Username' field in the 'Edit SIP trunk asterisk' dialog.
- A blue arrow points from the 'Password' field 'Change Password' in the 'Local SIP User Database' table to the 'Password' field in the 'Edit SIP trunk asterisk' dialog.

## 7.2 Ingate – Asterisk BE Incoming Calling

This call starts at the Service Provider, they will deliver a DID, contained in the Request URI header of a SIP INVITE. Typically the ITSP 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@Domain\_of\_Asterisk”.



## 7.3 Startup Tool

### 7.3.1 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.



### 7.3.2 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 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.

Possible Problems	Possible Resolution
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
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...	<ol style="list-style-type: none"> <li>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”</li> <li>2) Factory Default the Database, then try again.</li> </ol>

### 7.3.3 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.

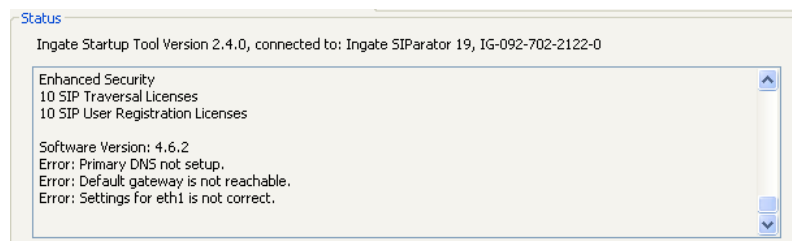


## Possible Problems and Resolutions

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...	<ol style="list-style-type: none"> <li>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.</li> <li>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".</li> </ol>

### 7.3.4 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.

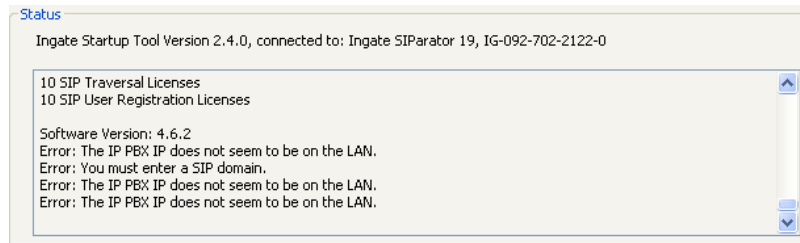


## Possible Problems and Resolutions

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

### 7.3.5 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 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.

### 7.3.6 ITSP

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

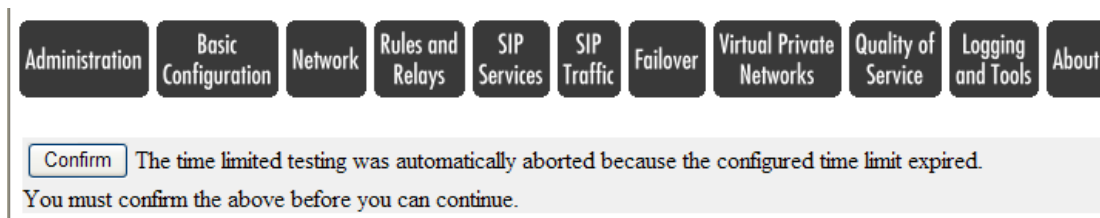


#### Possible Problems and Resolutions

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

### 7.3.7 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 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.

## **7.4 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](http://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.