



Application Note

Mitel 3300 ICP with SIP Trunking - Configuration Guide

19 February 2009

Table of Contents

1	MITEL 3300 ICP AND INGATE	1
1.1	SIP TRUNKING	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	<i>Product Type: Firewall.....</i>	<i>13</i>
4.3.2	<i>Product Type: Standalone</i>	<i>15</i>
4.3.3	<i>Product Type: DMZ SIParator</i>	<i>17</i>
4.3.4	<i>Product Type: DMZ-LAN SIParator</i>	<i>19</i>
4.3.5	<i>Product Type: LAN SIParator</i>	<i>21</i>
4.3.6	<i>Product Type: LAN SIParator – “SBE SIParator Only”</i>	<i>23</i>
4.4	IP-PBX.....	25
4.5	ITSP	27
4.6	UPLOAD CONFIGURATION.....	30
5	MITEL 3300 ICP SETUP.....	32
5.1	SYSTEM IP CONFIGURATION	33
5.2	NETWORK ELEMENT ASSIGNMENT	34
5.2.1	<i>Outbound Proxy with SIParator</i>	<i>35</i>
5.3	SIP PEER PROFILE.....	36
5.4	SIP PEER PROFILE ASSIGNMENT BY INCOMING DID.....	37
5.5	ARS SETUP.....	38
6	TROUBLESHOOTING	40
6.1	STATUS BAR	40
6.2	CONFIGURE UNIT FOR THE FIRST TIME	41
6.3	CHANGE OR UPDATE CONFIGURATION	42
6.4	NETWORK TOPOLOGY.....	43
6.5	IP-PBX.....	44
6.6	ITSP	44
6.7	APPLY CONFIGURATION	45

Tested versions: Ingate Firewall and SIParator version 4.6.4
Startup Tool version 2.4.2
Mitel 3300 ICP version 7.0.21.4 & 9.0.1.17

Revision History:

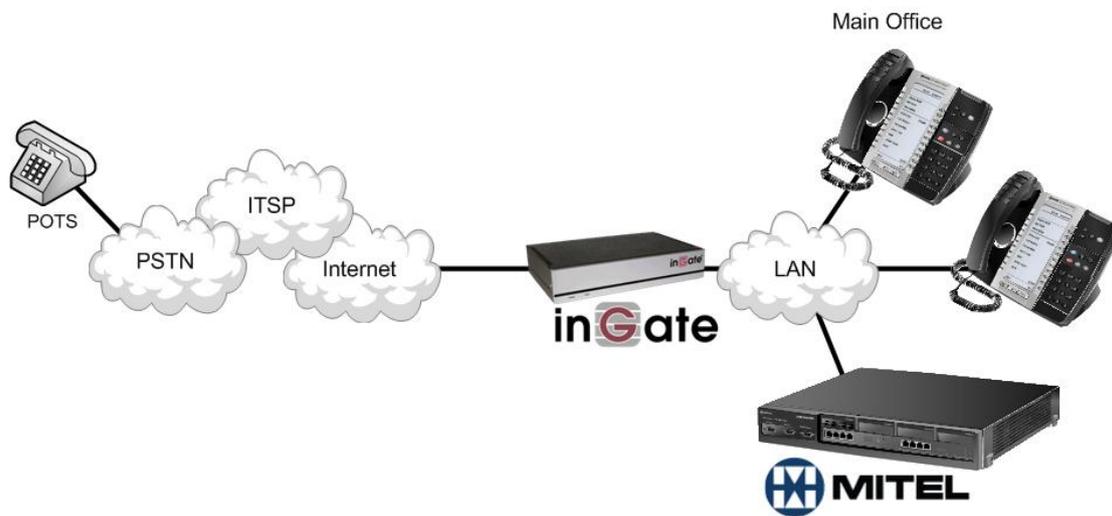
Revision	Date	Author	Comments
	2009-02-19	Scott Beer	Minor Edits

1 Mitel 3300 ICP and Ingate

The Mitel 3300 IP Communications Platform is a highly scalable IP-PBX that provides robust call control, extensive features and supports a wide range of innovative desktop devices and applications for medium-to-large enterprises. 3300 ICP is an integral element of the Mitel Networked Business portfolio of products that: facilitate business wide communication and collaboration, enhance workforce mobility and extend enterprise connectivity, improve client service and contact management, provide tools to manage communication overload, and reduce total cost of ownership.

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 Mitel 3300 ICP 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

In this application, the Mitel 3300 ICP 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.

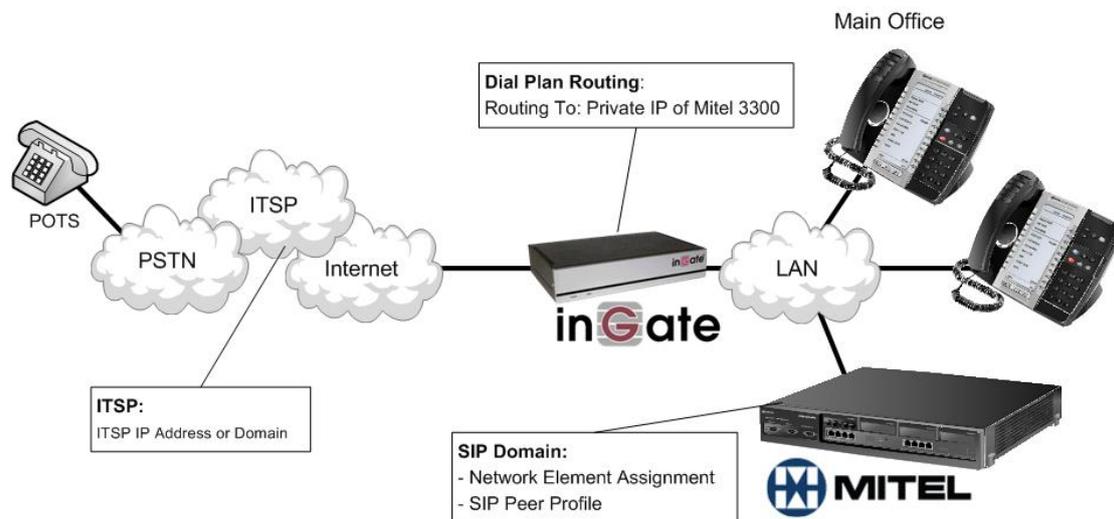
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

The Internet Telephony Service Provider can be of any vendor, located anywhere across the Internet or any foreign un-trusted private networks.

Requirements:

- 1) 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 Mitel Icon to focus your attention to specific Mitel 3300 ICP setup instructions. These instructions are specific to the Ingate & Mitel 3300 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.

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

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 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

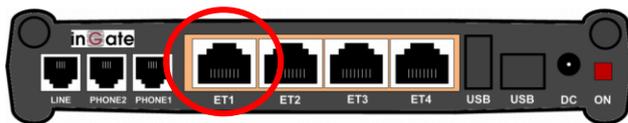
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

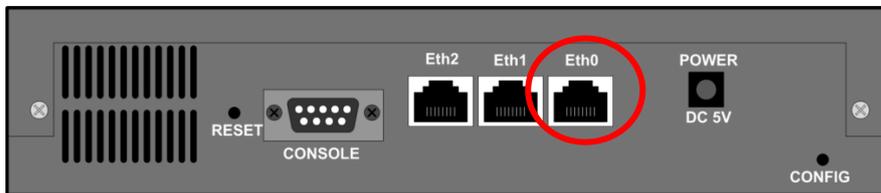
Configuration Steps:

- 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”.

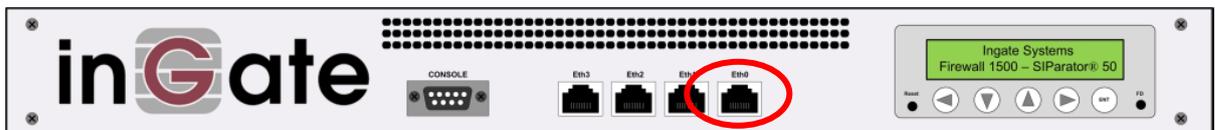
Ingate SIParator SBE (Back)



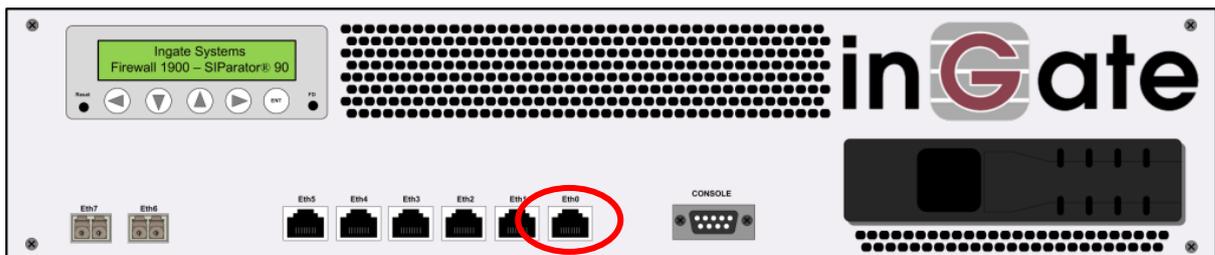
Ingate 1190 Firewall and SIParator 19 (Back)



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

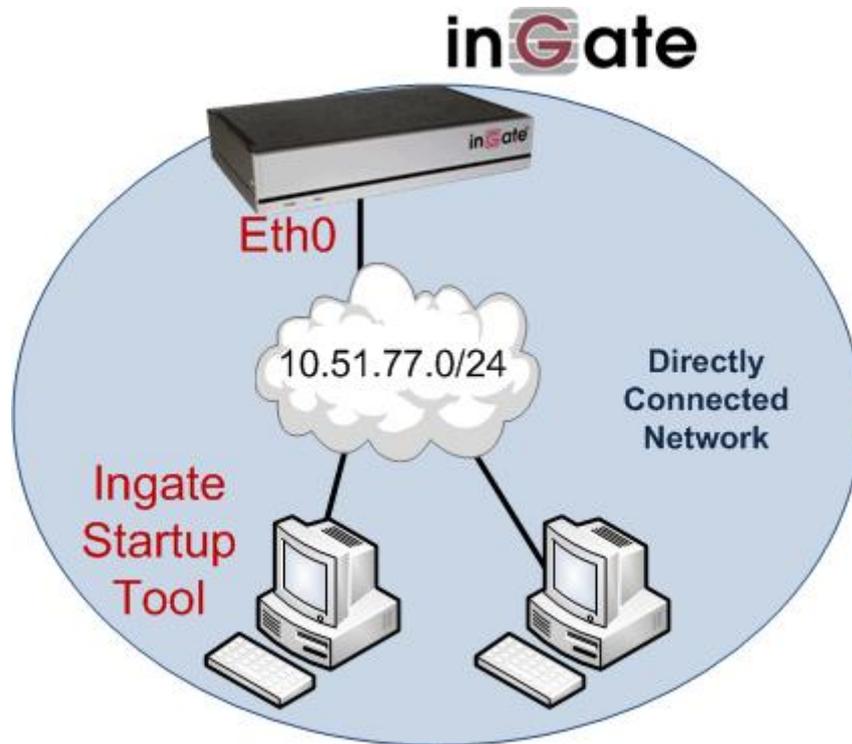


Ingate 1900 Firewall and SIParator 90



- 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

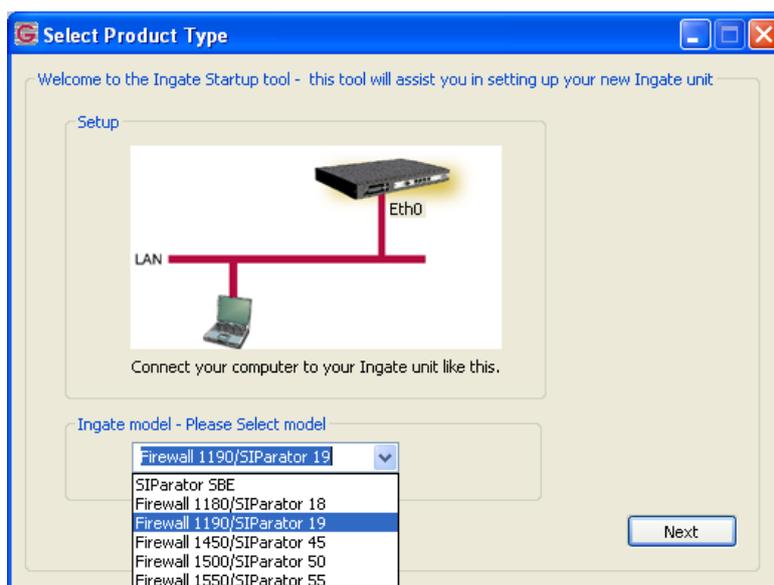
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

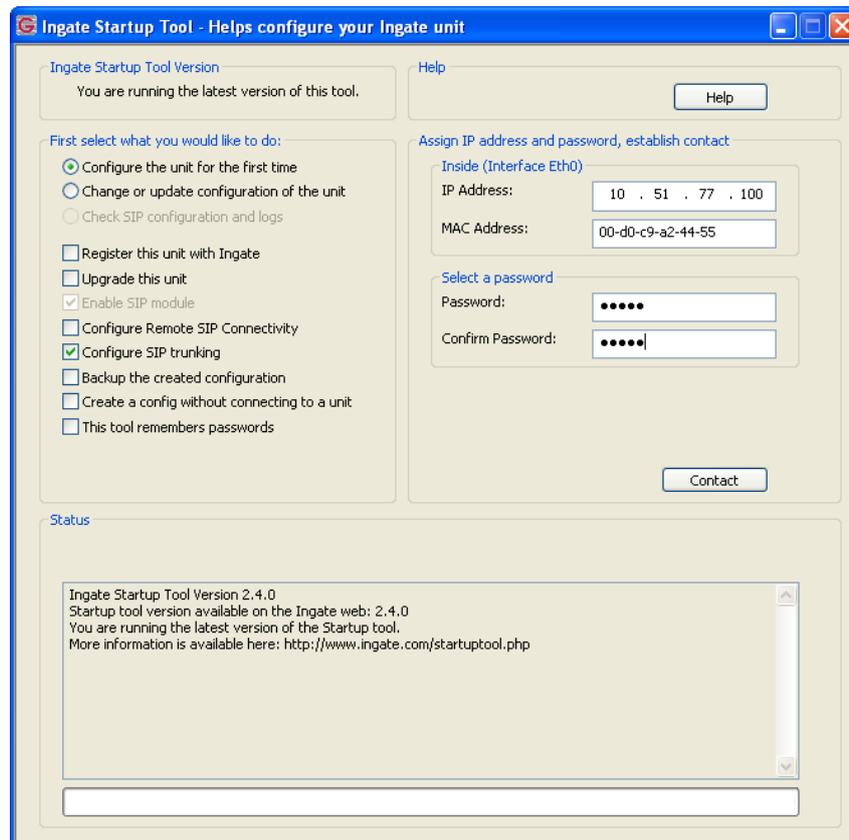
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: “Change or Update Configuration”.

Configuration Steps:

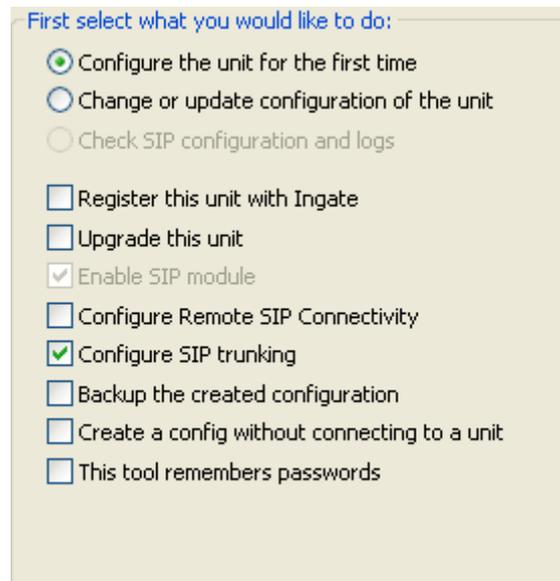
- 1) Launch the Startup Tool
- 2) Select the Model type of the Ingate Unit, and then click Next.



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



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



- a. Select “Configure SIP Trunking” if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.

- 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:

MAC Address:

- 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:

MAC Address:

Select a password

Password:

Confirm Password:

- 8) Proceed to Section 4.3: Network Topology.

4.2 Change or Update Configuration

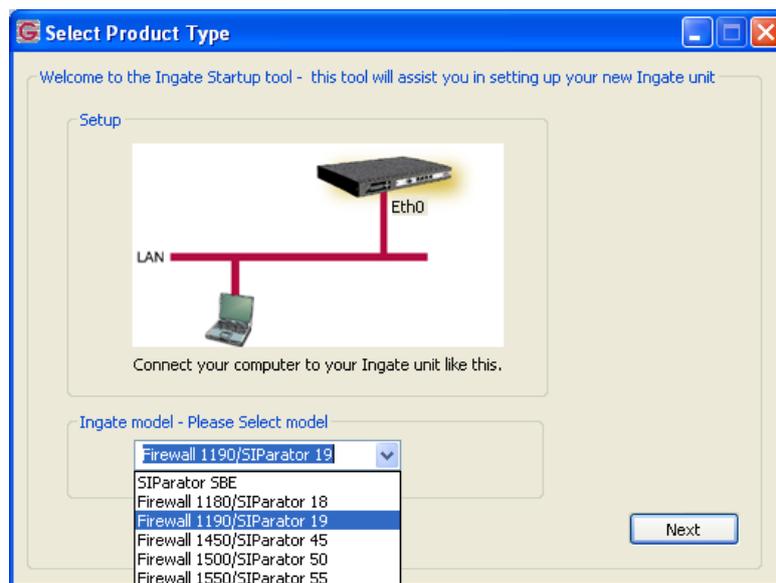
When selecting the “Change or update configuration of the unit” setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – “Configure the unit for the first time” or via the Console port.

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.

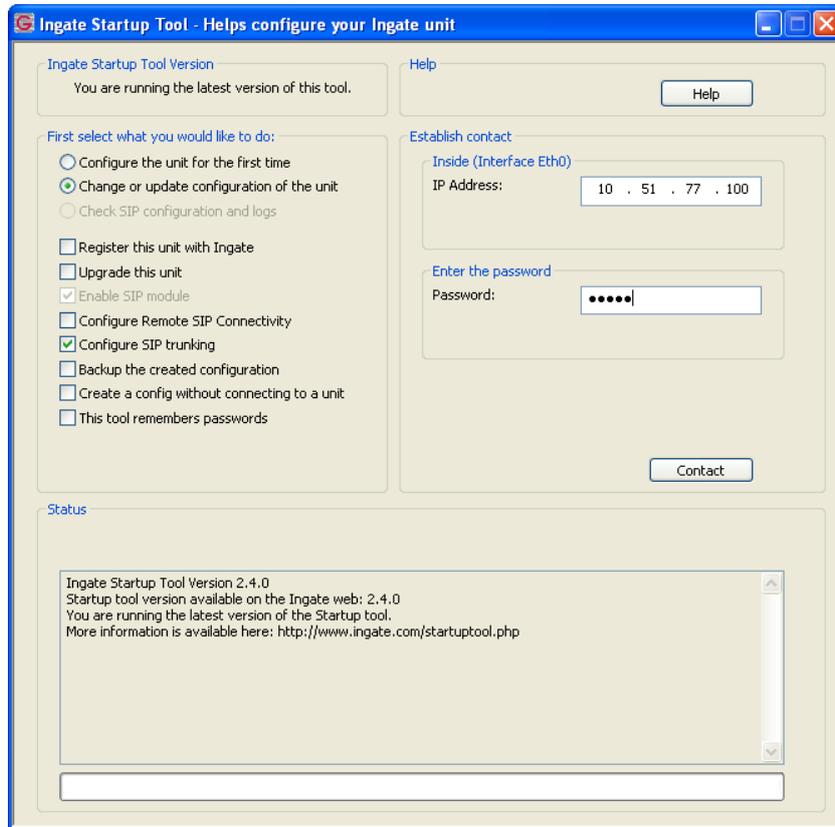
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: “Configure the Unit for the First Time”.

Configuration Steps:

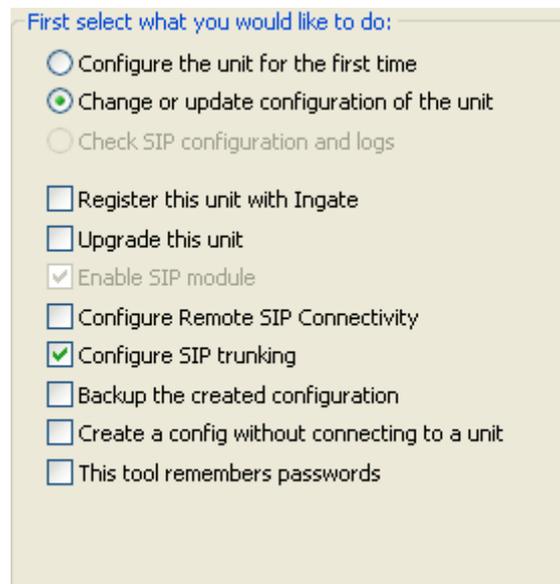
- 1) Launch the Startup Tool
- 2) Select the Model type of the Ingate Unit, and then click Next.



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



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



- a. Select “Configure SIP Trunking” if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.

- 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 of the Ingate Unit.

Inside (Interface Eth0)

IP Address:

- 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:

Enter the password

Password:

Contact

- 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 has IP address '10 . 51 . 77 . 100' and Netmask '255 . 255 . 255 . 0'. The 'Outside (Interface Eth1)' section has 'Use DHCP to obtain IP' unchecked, IP Address '172 . 51 . 77 . 100', Netmask '255 . 255 . 255 . 0', and Gateway '172 . 51 . 77 . 1'. 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 network diagram on the right shows an 'Ingate SIParator' connected to a LAN with an 'IP-PBX' and an 'Existing firewall' connected to the 'Internet'.

Configuration Steps:

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

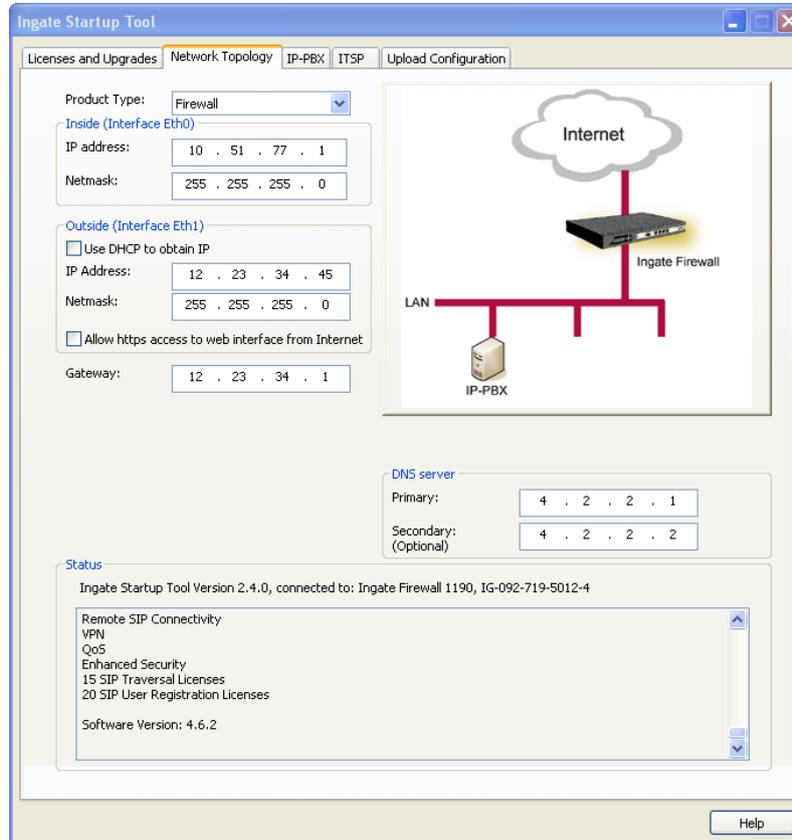


Hint: Match the picture to the network deployment.

- 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.

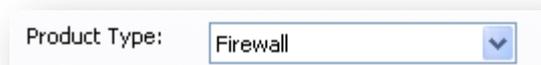
4.3.1 Product Type: Firewall

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.

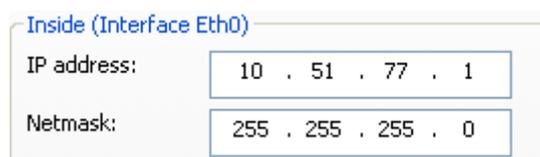


Configuration Steps:

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



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



- 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): Department

Email address: admin@email.com

Locality/town(L): Your City

OK Cancel

- 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.

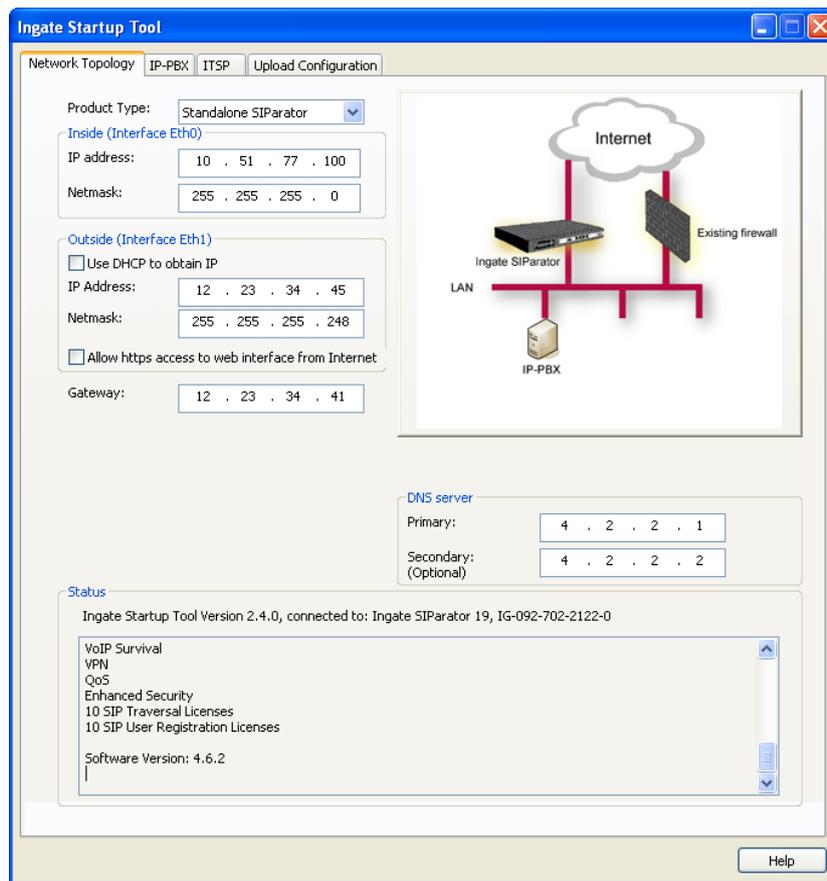
DNS server

Primary: 4 . 2 . 2 . 1

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

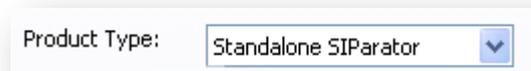
4.3.2 Product Type: Standalone

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.

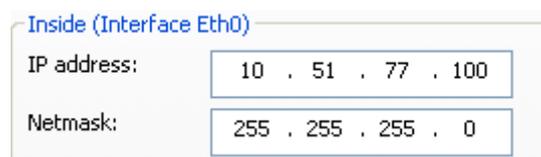


Configuration Steps:

- 1) In Product Type, select “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.



- 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.

- 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”

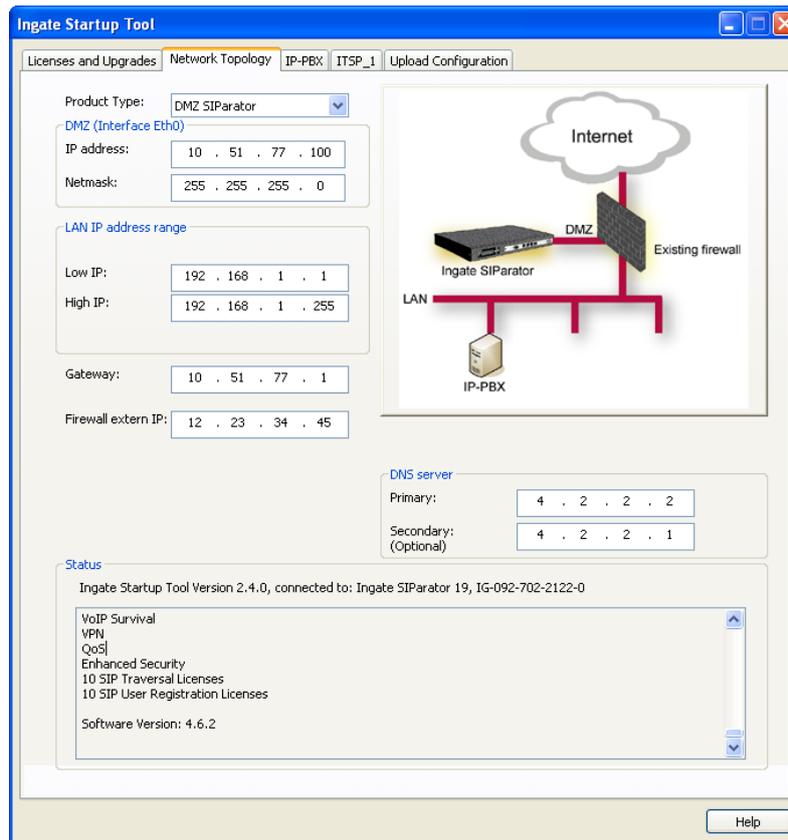
- d. Create a Private Certificate for https access, enter the corresponding information required to generate a certificate.

- 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.

- 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.

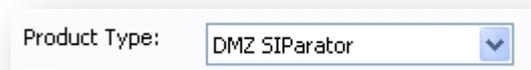
4.3.3 Product Type: DMZ SIParator

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.

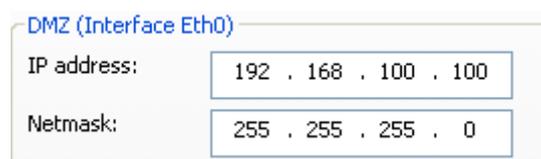


Configuration Steps:

- 1) In Product Type, select “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.



- 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

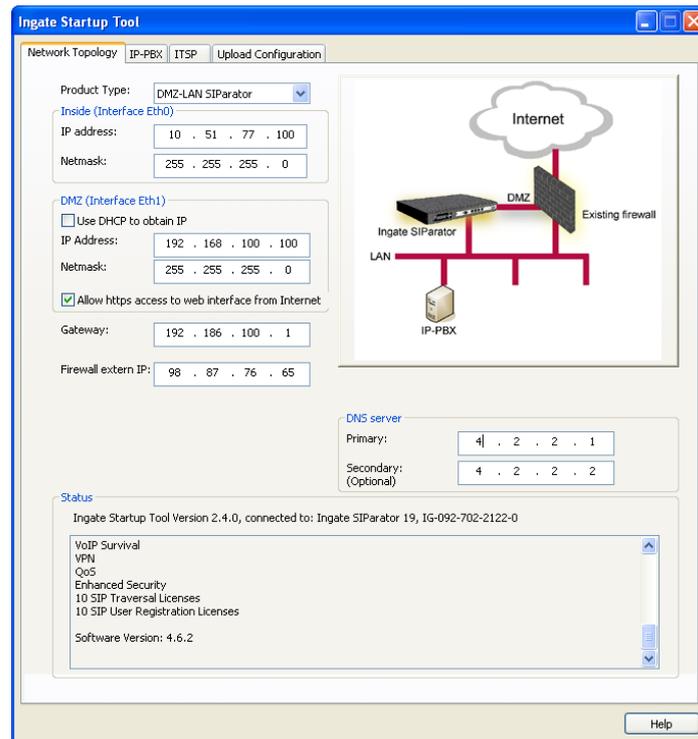
- 7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

- 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
- 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.

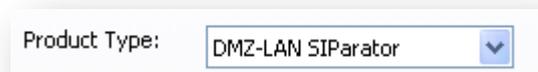
4.3.4 Product Type: DMZ-LAN SIParator

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.

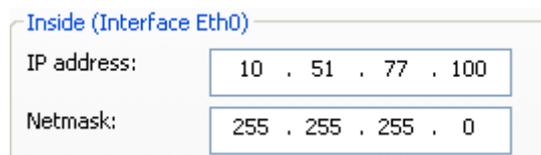


Configuration Steps:

- 1) In Product Type, select “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.



- 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

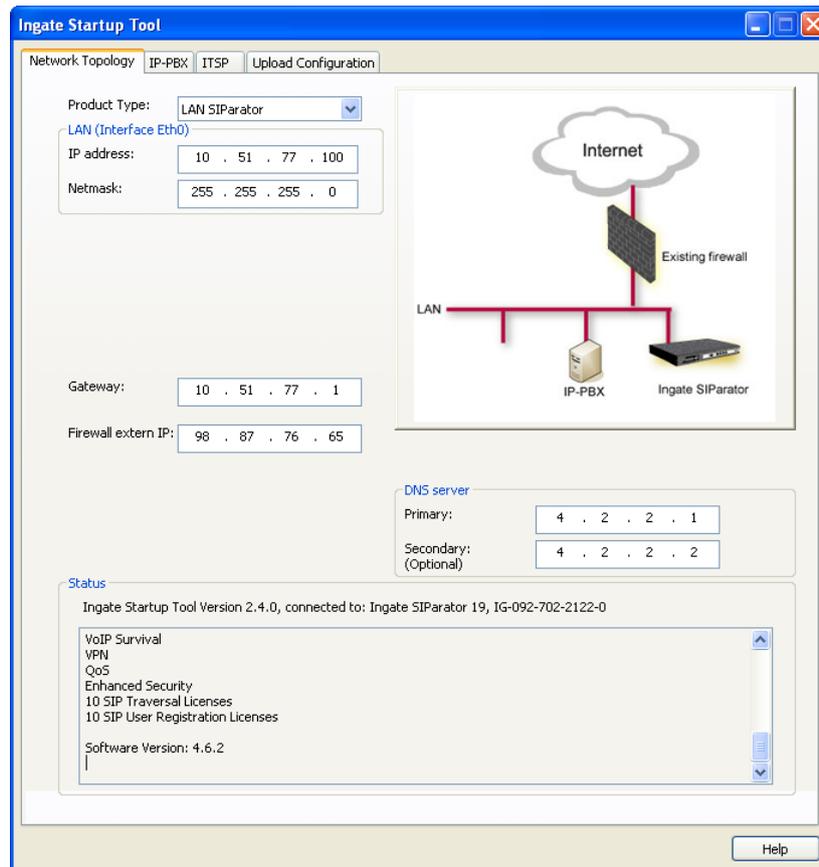
- 7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

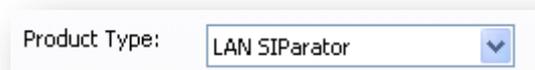
4.3.5 Product Type: LAN SIParator

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.

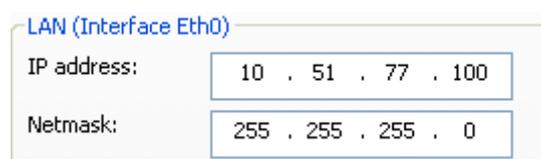


Configuration Steps:

- 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 Firewalls 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 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"/>

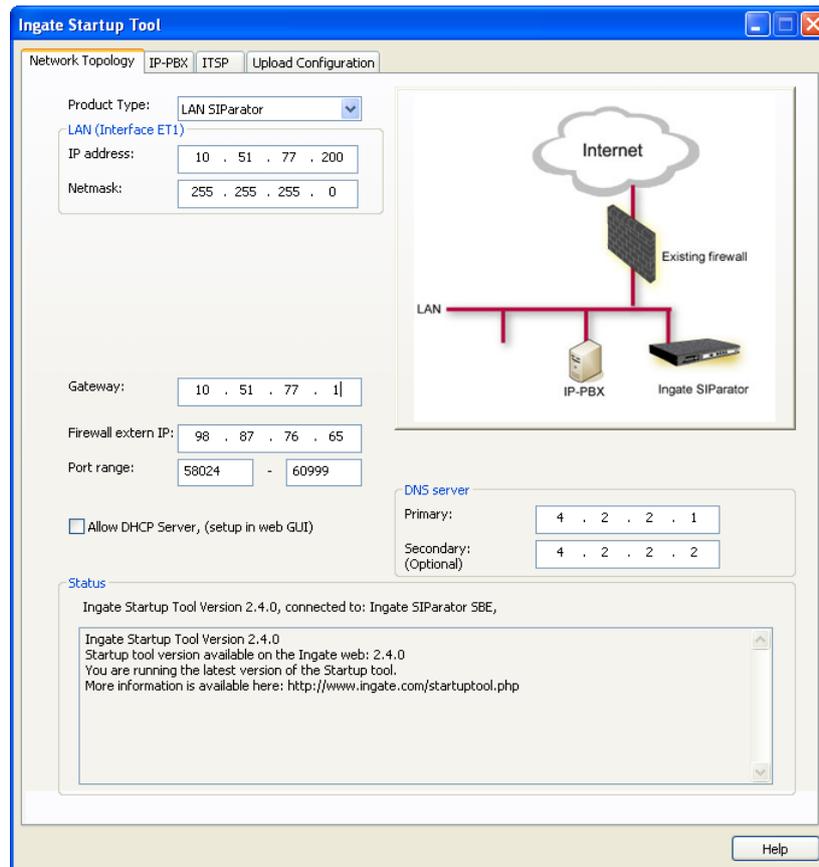
- 6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

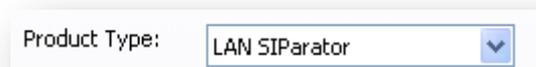
4.3.6 Product Type: LAN SIParator – “SBE SIParator Only”

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.

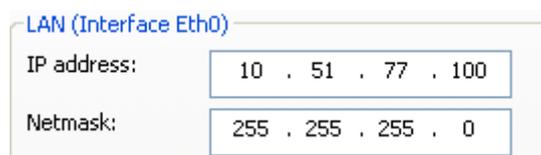


Configuration Steps:

- 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 Firewalls IP Address on the DMZ network.

Gateway:

- 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:

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

Port range: -

- 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:

Secondary:
(Optional)

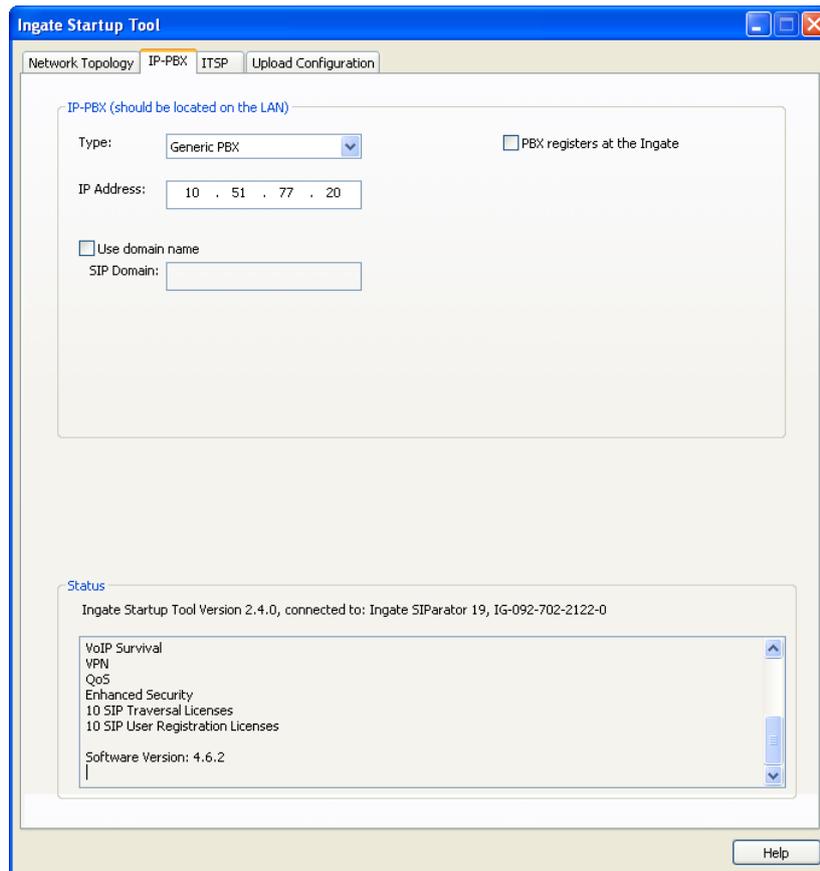
- 7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

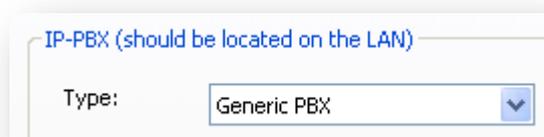
4.4 IP-PBX

The IP-PBX section is where the IP Addresses and Domain location are provided to the Ingate unit. The configuration of the Mitel 3300 ICP (IP-PBX) will allow for the Ingate unit to know the location of the Mitel 3300 ICP as to direct SIP traffic for the use with SIP Trunking. The IP Address of the Mitel 3300 ICP 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 Mitel 3300 ICP.



Configuration Steps:

- 1) In the IP-PBX Type drop down list, select "Mitel". Ingate has confirmed interoperability with the Mitel 3300 ICP, the unique requirements of the Mitel 3300 testing are contained in the Startup Tool.



- 2) Enter the IP Address of the Mitel 3300 ICP. The IP Address should be on the same LAN subnet as the Ingate unit.

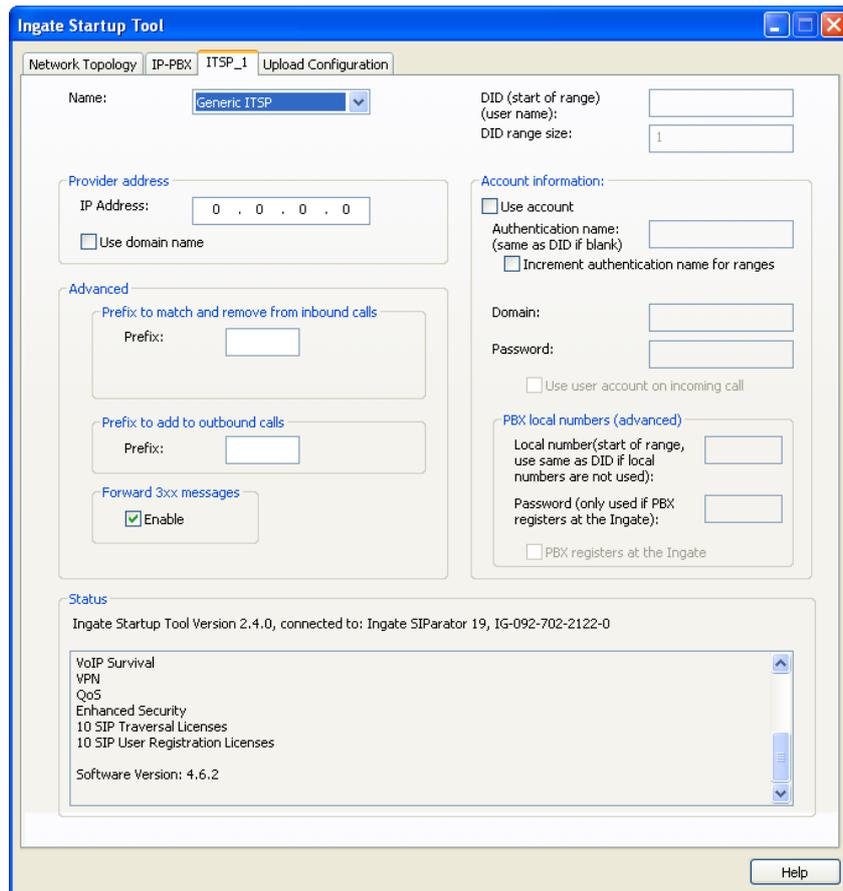
IP Address:

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

Use domain name
SIP Domain:

4.5 ITSP

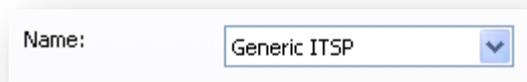
The ITSP section is where all of the attributes of the SIP Trunking Service Provider are programmed. Details like the IP Addresses or Domain, DIDs, Authentication Account information, Prefixes, and PBX local number. The configuration of the ITSP will allow for the Ingate unit to know the location of 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 a 'Use domain name' checkbox. The 'Advanced' section has three fields for 'Prefix' (inbound, outbound, and 3xx messages) and a checked 'Enable' checkbox for 'Forward 3xx messages'. The 'Account information' section includes 'DID (start of range)', 'DID range size', 'Use account' checkbox, 'Authentication name', 'Domain', 'Password', and 'Use user account on incoming call' checkbox. The 'PBX local numbers (advanced)' section includes 'Local number', 'Password', and 'PBX registers at the Ingate' checkbox. The 'Status' section 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, 10 SIP User Registration Licenses, and Software Version: 4.6.2. A 'Help' button is at the bottom right.

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".



A close-up of the 'Name' dropdown menu in the configuration tool. The dropdown is open, showing 'Generic ITSP' as the selected option.

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:

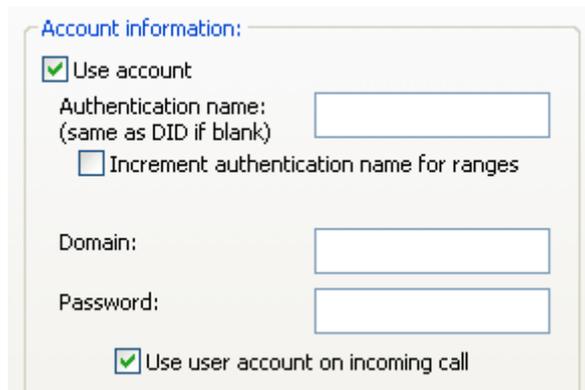
Use user account on incoming call

- 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)

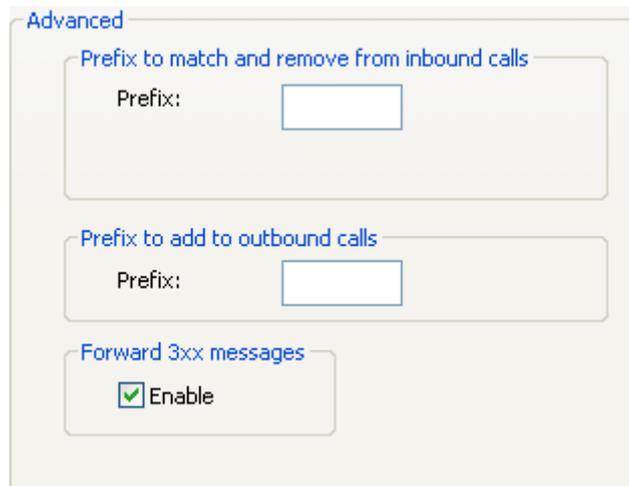
Increment authentication name for ranges

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

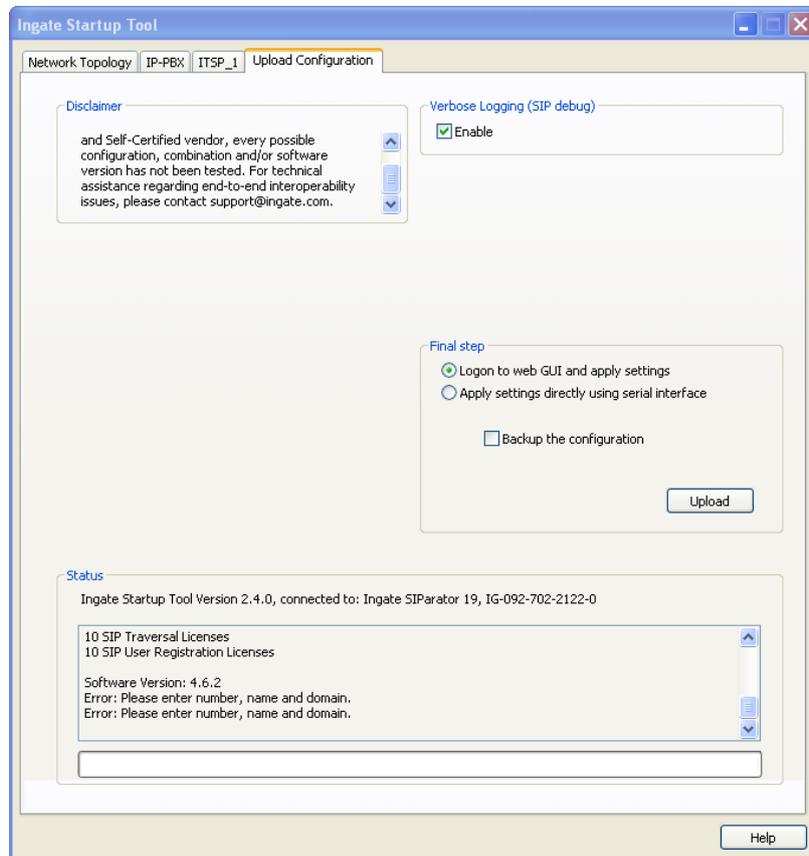
Prefix:

Forward 3xx messages

Enable

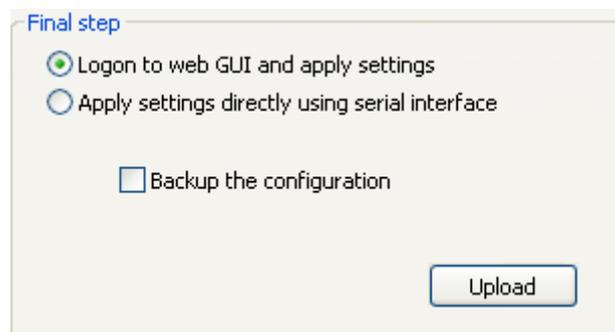
4.6 Upload Configuration

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.

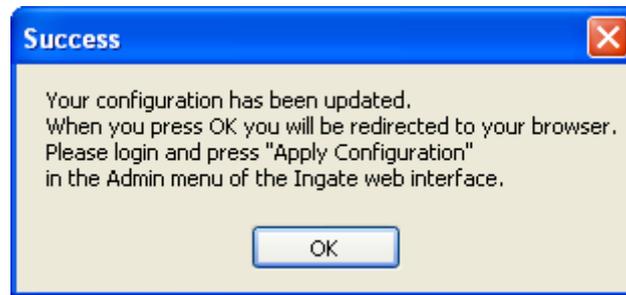


Configuration Steps:

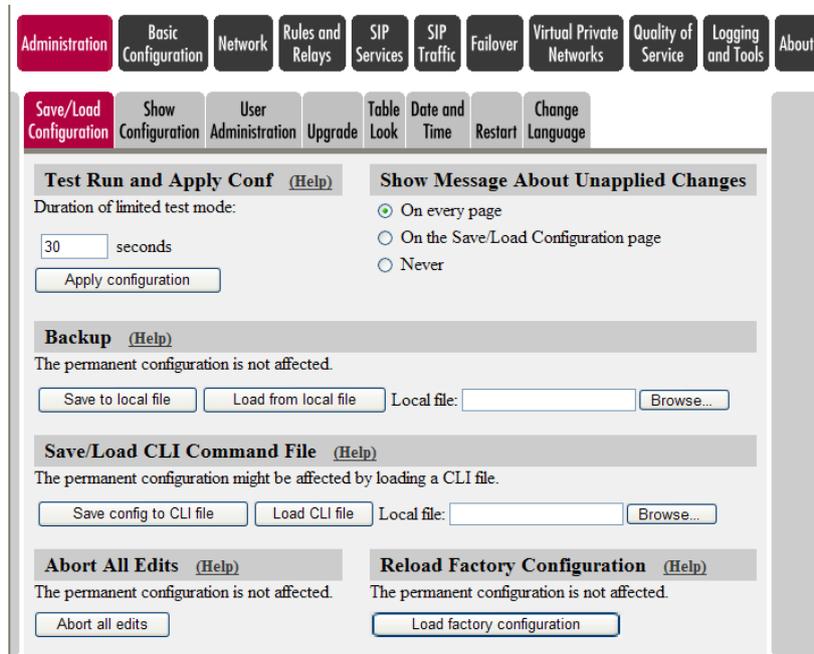
- 1) Press the “Upload” button. If you would like the Startup Tool to create a Backup file also select “Backup the configuration”. Upon pressing the “Upload” button the Startup Tool will push a database into the Ingate unit.



- 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.

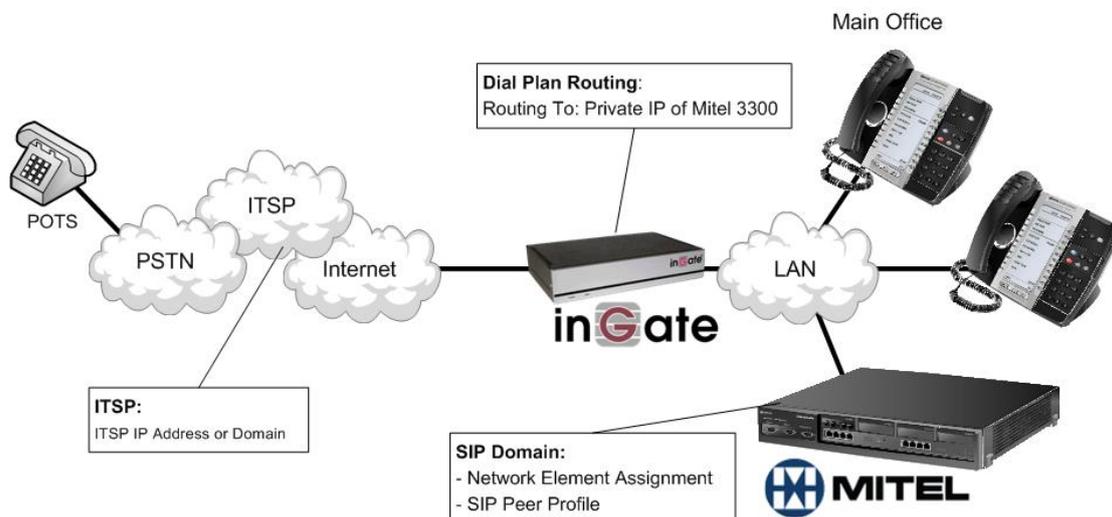


5 Mitel 3300 ICP Setup



The Mitel 3300 ICP will require configuration in the Network Element Assignment, SIP Peer Profile, SIP Peer Profile Assignment by Incoming DID, Automatic Route Selection, Trunk Service Assignment, ...

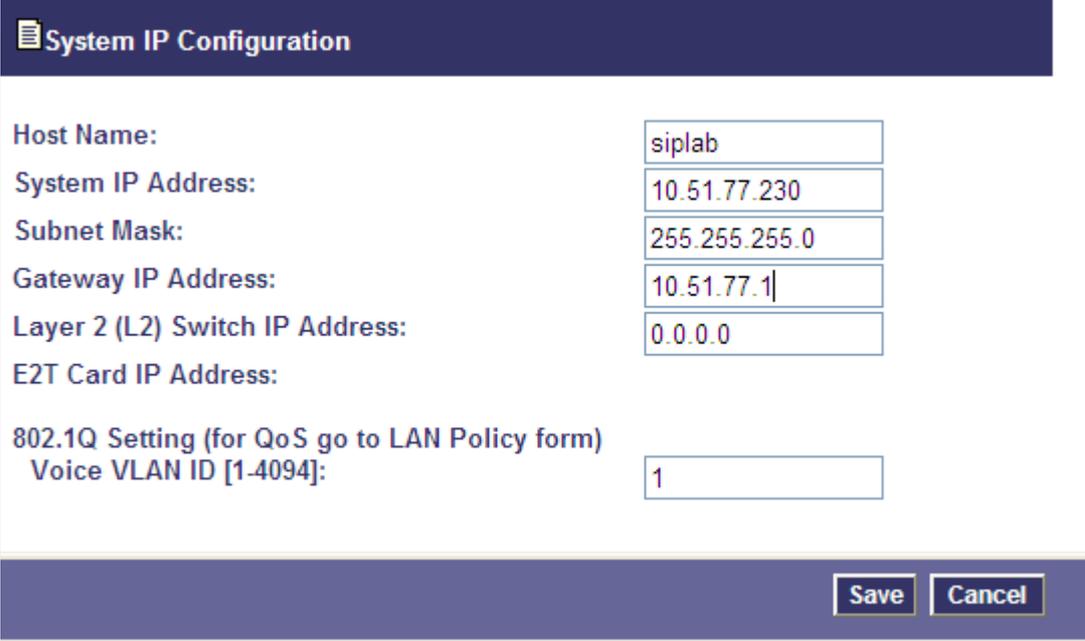
In general, the Mitel 3300 ICP will send SIP Traffic to the public IP address of the Service Provider directly, the typical setup on the Mitel 3300 ICP will have the Service Provider information, the Ingate Firewall and SIParators will provide SIP Security and Routing capabilities to the Mitel 3300 ICP.



5.1 System IP Configuration

The System IP Configuration is where the Mitel 3300 ICP is assigned its IP Address, Mask and Default Gateway. As well as its Host Name, which in combination with its Domain forms a Fully Qualified Domain Name (FQDN). This FQDN is the SIP Domain of the Mitel 3300 ICP, and the 3300 ICP will respond to the SIP Domain for any SIP Traffic.

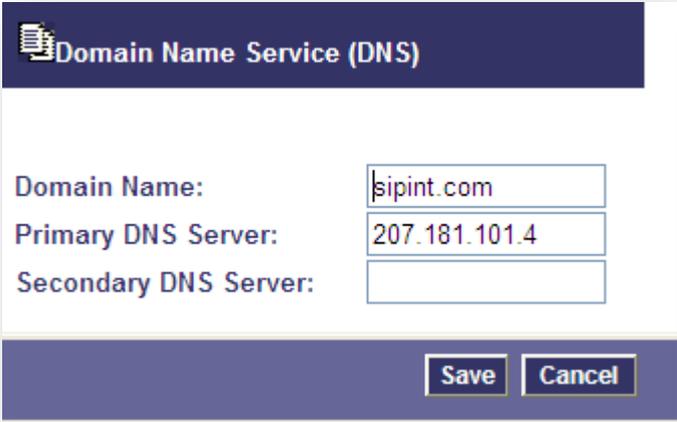
DNS features like DNS A Lookup, and DNS SRV Records can make the Mitel 3300 ICP more resilient in failover scenarios.



The screenshot shows a dialog box titled "System IP Configuration". It contains several input fields for network settings:

Host Name:	siplab
System IP Address:	10.51.77.230
Subnet Mask:	255.255.255.0
Gateway IP Address:	10.51.77.1
Layer 2 (L2) Switch IP Address:	0.0.0.0
E2T Card IP Address:	
802.1Q Setting (for QoS go to LAN Policy form) Voice VLAN ID [1-4094]:	1

At the bottom right of the dialog are "Save" and "Cancel" buttons.



The screenshot shows a dialog box titled "Domain Name Service (DNS)". It contains three input fields for DNS settings:

Domain Name:	sipint.com
Primary DNS Server:	207.181.101.4
Secondary DNS Server:	

At the bottom right of the dialog are "Save" and "Cancel" buttons.

5.2 Network Element Assignment

The purpose of the Network Element Assignment is to identify the location of the SIP Peer (the ITSP) for the SIP Trunks to connect to, the SIP Peer can be either the ITSP's Session Border Controller (SBC) or if there is no SBC the SIP Peer can be the SIP Server itself. This information is provided by the Carrier, as each Carrier implements SIP Trunking slightly differently.



The screenshot shows a configuration window titled "Network Element Assignment". The fields are as follows:

Name:	ATT
Type:	Other
FQDN or IP Address:	207.242.225.200
Local:	False
Version:	
Zone:	2
SIP Peer:	<input checked="" type="checkbox"/>
SIP Peer Specific	
SIP Peer Transport:	UDP
SIP Peer Port:	5060
External SIP Proxy FQDN or IP Address:	
External SIP Proxy Transport:	
External SIP Proxy Port:	0
SIP Registrar FQDN or IP Address:	
SIP Registrar Transport:	
SIP Registrar Port:	0

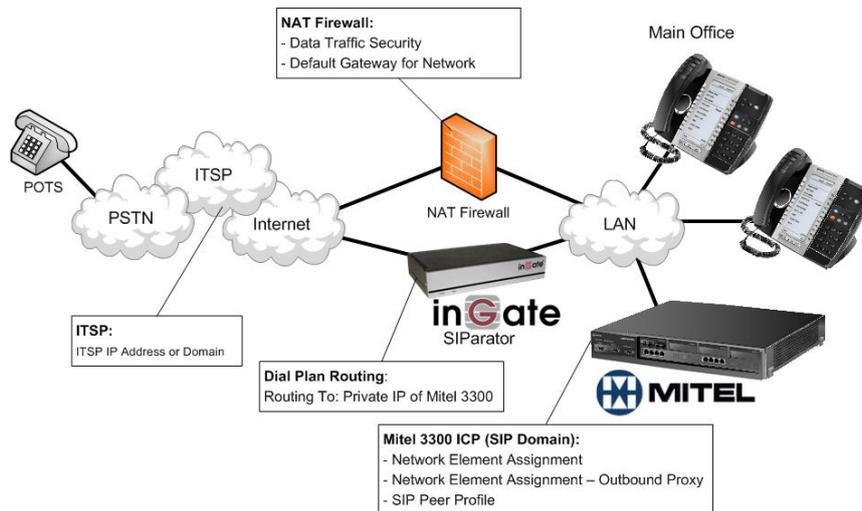
At the bottom right, there are "Save" and "Cancel" buttons.

Configuration Steps:

- 1) **Name:** Provide a unique name to identify the Outbound Proxy.
- 2) **Type:** Select "Other"
- 3) **FQDN or IP Address:** Provide the FQDN or Public IP address of the ITSP.
- 4) Select "SIP Peer"
- 5) **SIP Peer Transport:** Select "UDP" (or TCP depending on ITSP)
- 6) "SIP Peer Port" field, enter "5060"
- 7) **(Optional) SIP Registrar FQDN or IP Address:** Provide the FQDN or Public IP address of the ITSP.
- 8) **(Optional): SIP Registrar Transport:** Select "UDP" (or TCP depending on ITSP)
- 9) **(Optional): SIP Registrar Port:** Enter "5060"
- 10) Press SAVE.

5.2.1 Outbound Proxy with SIParator

An Outbound Proxy is required to route to a destination via a different path from that of the Default Gateway. In many Enterprise campuses there are usually more than one Firewall to connect to one or multiple Carriers and/or Internet or other Service Providers. As when PCs, Servers and all the general Data & Internet traffic go through the Default Gateway firewall, the SIP Trunking application may have an Ingate SIParator to a different Service Provider for the purpose of managing the SIP traffic.



The Mitel 3300 ICP can provision an Outbound Proxy in the Network Element Assignment.

The screenshot shows the 'Network Element Assignment' configuration window. The fields are as follows:

Name:	SIParator
Type:	Outbound Proxy
FQDN or IP Address:	10.51.77.100
Local:	False
Version:	
Zone:	1
Outbound Proxy Specific	
Outbound Proxy Transport Type:	UDP
Outbound Proxy Port:	5060

Buttons: Save, Cancel

Configuration Steps:

- 1) **Name:** Provide a unique name to identify the Outbound Proxy.
- 2) **Type:** Select "Outbound Proxy"
- 3) **FQDN or IP Address:** Provide the IP address of the SIParator.
- 4) **Outbound Proxy Transport Type:** Select "UDP"
- 5) **Outbound Proxy Port:** Enter "5060"
- 6) Press SAVE.

5.3 SIP Peer Profile

SIP Peer Profile is required to configure the SIP Protocol settings and behaviors for the Network Element - SIP Peer. This form contains all the required settings to finalize the connectivity to the SIP Peer. SIP Protocol settings such as the Local Account Info, the associated Outbound Proxy Server, Timer, and other configurable Options.

The Local Account Information is where the Telephone Number of the SIP Trunk is defined. This can also be a range of Numbers or Multiple different numbers associated with this SIP Peer. If the Mitel 3300 ICP is Registering with the SIP Peer the Ingate Firewall will show this registration in the SIP STATUS page of the Web Config Tool. This Local Account Info forms the Incoming Request-URI, the Mitel 3300 ICP will match this Request-URI to ensure that the incoming call is meant for itself.

SIP Peer Profile

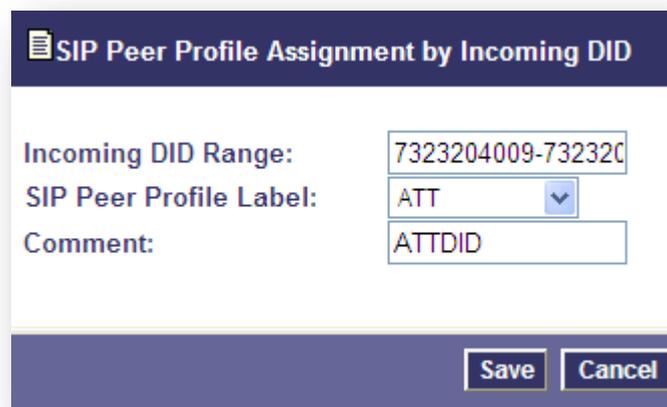
SIP Peer Profile Label:	<input type="text" value="ATT"/>
Network Element:	<input type="text" value="ATT"/>
Local Account Information	
Registration User Name:	<input type="text" value="7323204009.732320"/>
Address Type:	<input type="radio"/> FQDN: siplab13.sipint.com <input checked="" type="radio"/> IP Address: 66.46.196.195
Outbound Proxy Server:	<input type="text" value="SIPParator"/>
Calling Line ID	
Default CPN:	<input type="text" value="7323204009"/>
Restriction:	<input type="checkbox"/>
Policies	
Trunk Service:	<input type="text" value="4"/>
Interconnect Restriction:	<input type="text" value="1"/>
Maximum Simultaneous Calls:	<input type="text" value="5"/>
Session Timer:	<input type="text" value="0"/>
Zone:	<input type="text" value="2"/>
SMDR Tag:	<input type="text" value="0"/>
NAT Keepalive:	<input type="checkbox"/>
Enable Mitel Proprietary SDP:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Use P-Asserted Identity Header:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Use Restricted Character Set For Authentication:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Disable Reliable Provisional Responses:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Use Alternate Destination Domain:	<input checked="" type="radio"/> No <input type="radio"/> Yes
FQDN or IP Address:	<input type="text"/>
Ignore Incoming Loose Routing Indication:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Suppress Use of SDP Inactive Media Streams:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Enable Special Re-invite Collision Handling:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Enable sending '+' for E.164 numbers:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Force sending SDP in initial Invite message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Use To Address in From Header on Outgoing Calls:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Force Answer - send SDP in initial Invite:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Prevent the Use of IP Address 0.0.0.0 in SDP Messages:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Use P-Preferred Identity Header:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Route Call Using To Header:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Private SIP Trunk:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Public Calling Party Number Passthrough:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Use Diverting Party Number as Calling Party Number:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Build Contact Using Request URI Address:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Renegotiate SDP To Enforce Symmetric Codec:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Repeat SDP Answer If Duplicate Offer Is Received:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Allow Peer To Use Multiple Active M-Lines:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Authentication	
User Name:	<input type="text"/>
Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
Authentication Option for Incoming Calls:	<input type="text" value="No Authentication"/>

Configuration Steps:

- 1) **SIP Peer Profile Label:** Enter a unique label.
- 2) **Network Element:** Select the Network Element Assignment Label for the ITSP
- 3) **Local Account Information - Registration Username:** Enter the ITSP provide Username, such as a DID or account name/number
- 4) **Address Type:** Select either the FQDN or IP Address, this will be used by the Mitel 3300 to identify its SIP Domain.
- 5) **Outbound Proxy Server:** Outbound Proxy Server is where the Network Element for the Ingate SIParator is assigned when there is an Outbound Proxy required for an alternate Carrier and/or Internet or other Service Provider access route. If you are using an Ingate SIParator and have programmed its location in Network Element Assignment, select it here.
- 6) **Calling Line ID – Default CPN:** Outgoing Default CLID, enter a DID.
- 7) **Various Policies:** Specific to Mitel 3300 ICP and Carrier requirements, there is nothing here specific to Ingate requirements, only ITSP requirements.
- 8) **Authentication – Username:** (Optional) Used to provide a Username/Account for the use in Registration.
- 9) **Authentication – Password:** (Optional) Used to provide a Password for the use in Registration.

5.4 SIP Peer Profile Assignment by Incoming DID

SIP Peer Profile Assignment by Incoming DID is used to identify DIDs and DID ranges of the incoming calls.



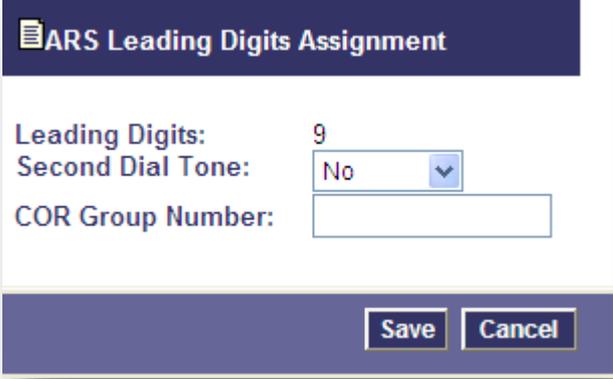
The screenshot shows a configuration dialog box titled "SIP Peer Profile Assignment by Incoming DID". It contains three input fields: "Incoming DID Range" with the value "7323204009-732320", "SIP Peer Profile Label" with a dropdown menu showing "ATT", and "Comment" with the value "ATTDID". At the bottom right, there are "Save" and "Cancel" buttons.

Configuration Steps:

- 1) Incoming DID Range: Enter the DID or DID range for the incoming calls
- 2) SIP Peer Profile Label: Assign the SIP Peer Profile for these incoming calls

5.5 ARS Setup

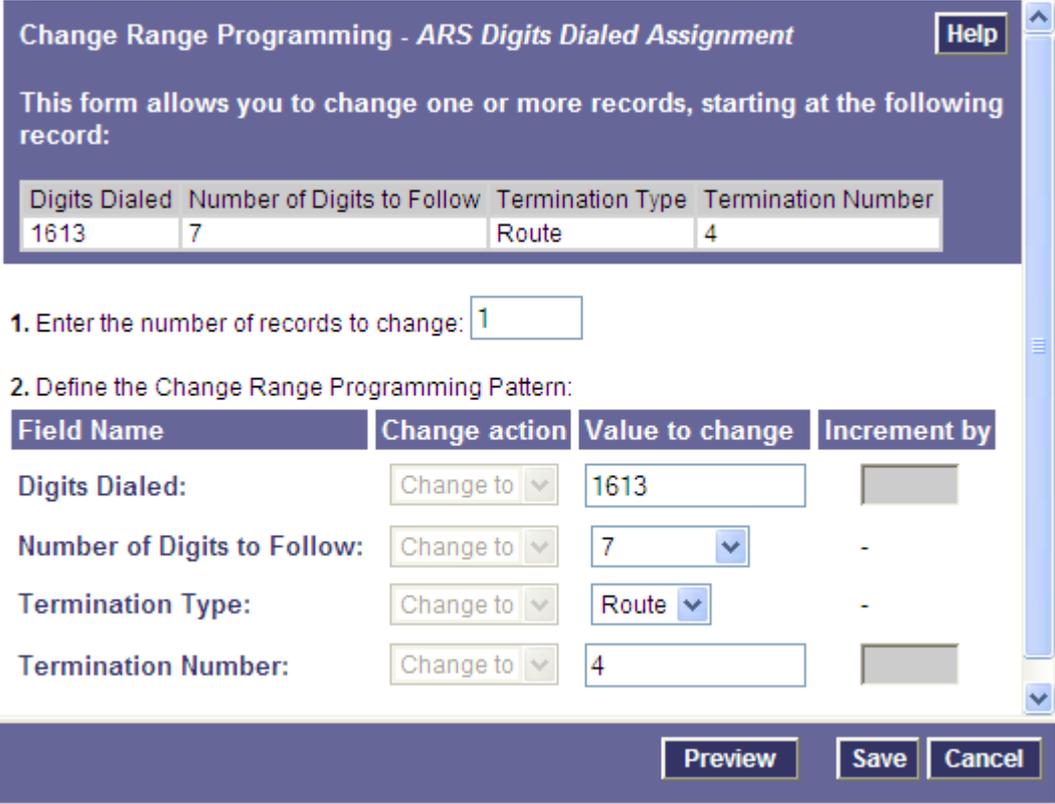
ARS includes a number of different forms, but all are defining a route for callers to dial out the SIP Trunk to the ITSP.



The form is titled "ARS Leading Digits Assignment". It contains three fields: "Leading Digits" with a text input containing "9", "Second Dial Tone" with a dropdown menu set to "No", and "COR Group Number" with an empty text input. At the bottom right, there are "Save" and "Cancel" buttons.

Configuration Steps:

- 1) Enter a Leading Digit of 9 (or some other value)



The form is titled "Change Range Programming - ARS Digits Dialed Assignment". It includes a "Help" button in the top right. Below the title, it states: "This form allows you to change one or more records, starting at the following record:"

Digits Dialed	Number of Digits to Follow	Termination Type	Termination Number
1613	7	Route	4

1. Enter the number of records to change:

2. Define the Change Range Programming Pattern:

Field Name	Change action	Value to change	Increment by
Digits Dialed:	Change to	<input type="text" value="1613"/>	<input type="text"/>
Number of Digits to Follow:	Change to	<input type="text" value="7"/>	-
Termination Type:	Change to	<input type="text" value="Route"/>	-
Termination Number:	Change to	<input type="text" value="4"/>	<input type="text"/>

At the bottom right, there are "Preview", "Save", and "Cancel" buttons.

- 2) Under ARS Digits Dialed Assignment, define the Digits dialed and select a Route Assignment.

Route Assignment

Route Number: 4

Routing Medium: SIP Trunk

Trunk Group Number: [disabled]

SIP Peer Profile: ATT

COR Group Number: 1

Digit Modification Number: 2

Digits Before Outpulsing: [dropdown]

Route Type: [dropdown]

Compression: Off

Save Cancel

- 3) In Route Assignment,
 - a. Routing Medium: Select SIP Trunk
 - b. SIP Peer Profile: Select the SIP Peer Profile to send outgoing call to.

Trunk Service Assignment

Trunk Service Number: 4

Release Link Trunk: No

Class of Service: 4

Class of Restriction: 1

Baud Rate: 300

Intercept Number: 1

Non-dial In Trunks Answer Point - Day: [text input]

Non-dial In Trunks Answer Point - Night 1: [text input]

Non-dial In Trunks Answer Point - Night 2: [text input]

Dial In Trunks Incoming Digit Modification - Absorb: 6

Dial In Trunks Incoming Digit Modification - Insert: [text input]

Trunk Label: ATT

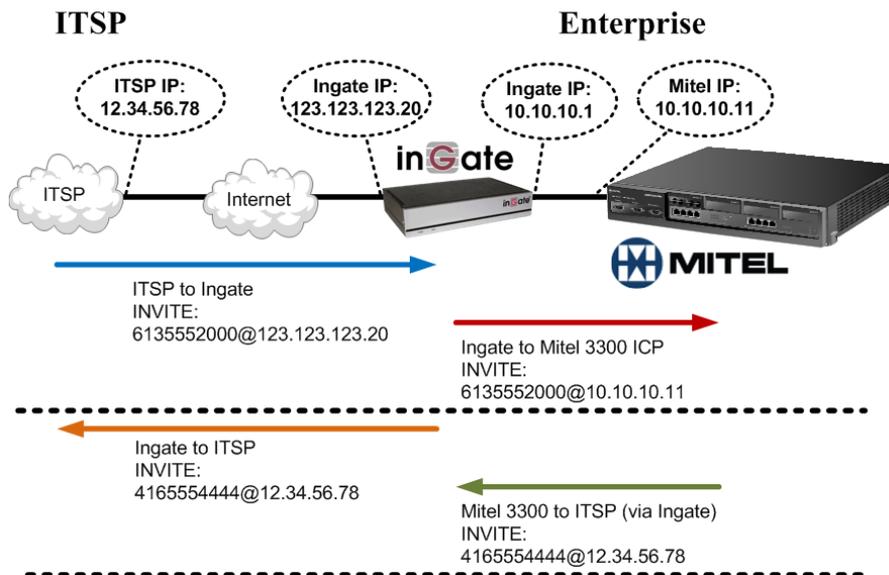
Save Cancel

- 4) Trunk Service Assignment, Dial In Trunks Incoming Digit Modification – Absorb is used for incoming calls to indicate there are incoming digits and to absorb any number of digits. Ensure there is a value to accept the number of incoming digits of the DID from the ITSP.

6 Troubleshooting

6.1 Ingate – Mitel 3300 ICP 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@IP_Address_Mitel”.



6.2 Startup Tool

6.2.1 Status Bar

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



6.2.2 Configure Unit for the First Time

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



Possible Problems 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"> 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 Tool 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.

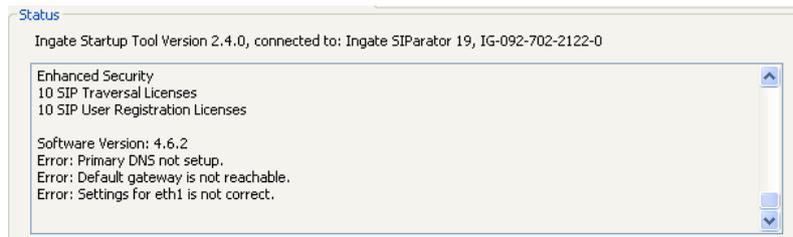


Possible Problems and Resolutions

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"> 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.

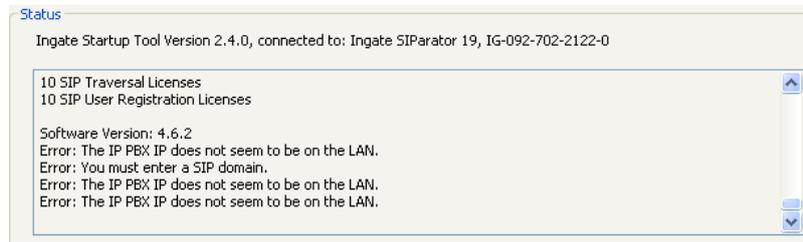


Possible Problems and Resolutions

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.

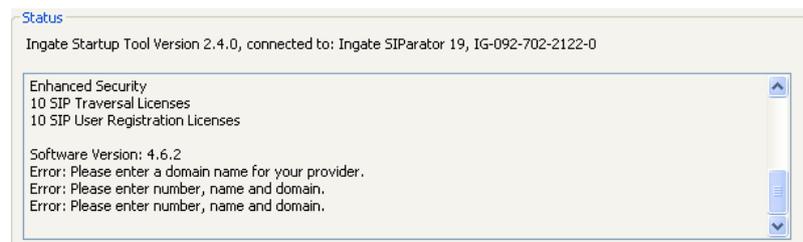


Possible Problems and Resolutions

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.

6.2.6 ITSP

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



Possible Problems 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"

6.2.7 Apply Configuration

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



Possible Problems 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.

6.3 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.