Application Note

3Com VCX Connect with SIP Trunking - Configuration Guide

28 May 2009

Table of Contents

Tested versions: Ingate Firewall and SIParator version 4.6.4
Startup Tool version 2.4.2
VCX and VCX Connect 7.1.21c and 8.0.7e1

Revision History:

Revision	Date	Author	Comments
	2009-05-28	Scott Beer	First Draft

1 3Com VCX Connect and Ingate

The 3Com® VCX® Connect IP Communications Platform offers an economical Session Initiation Protocol (SIP) IP telephony and messaging platform. This platform delivers powerful phone features and supports multimedia communications through devices, such as SIP-based video phones. The platform supports organizations with up to 250 phone users.

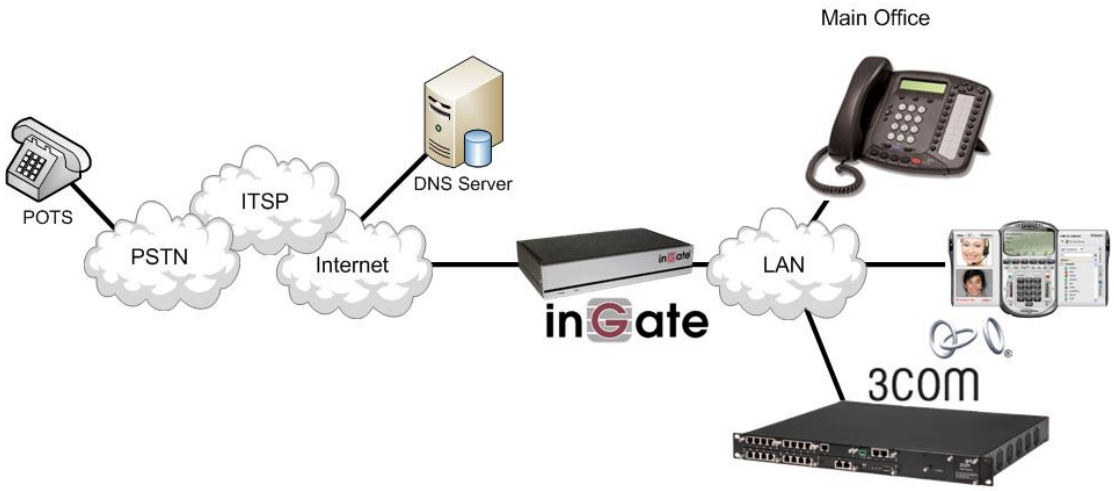
The platform's practical design and affordability allow businesses to replace antiquated PBXs with Voice Over IP (VoIP) solutions that

- Handle unified voicemail and email messaging.
- Support a full range of IP phones.
- Interoperate with the PSTN.

Migration from legacy PBXs to cost-effective IP-based telephony is facilitated by numerous VoIP gateway options. As well, redundant configuration options help ensure business continuity even in the event of power or network disruption.

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 and other live communications, based on 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 3Com VCX Connect 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 3Com VCX Connect IP Communications Platform 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.

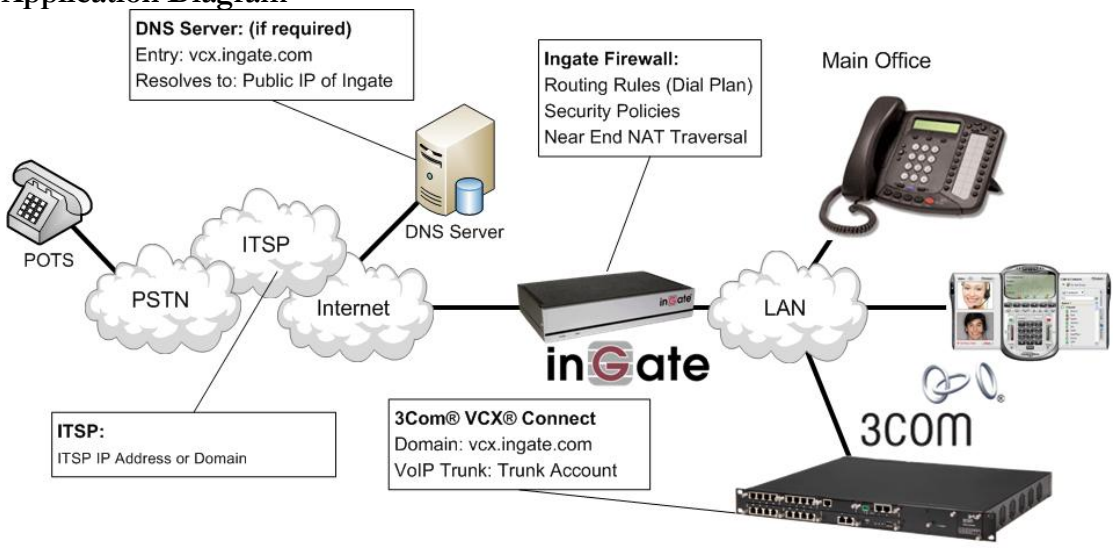
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

The Internet Telephony Service Provider can be of any vendor, located anywhere across the Internet or any remote private networks.

Requirements:

- 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 3Com Icon to focus your attention to specific 3Com VCX Connect setup instructions. These instructions are specific to the Ingate & 3Com 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 3Com VCX Connect. 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

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

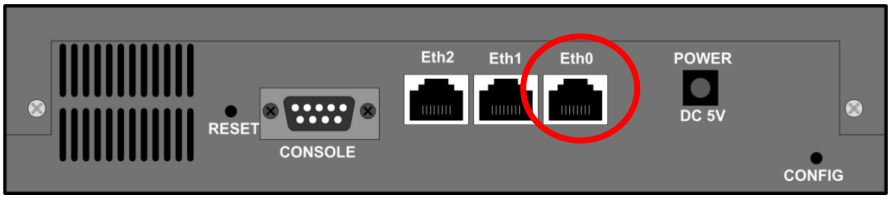
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

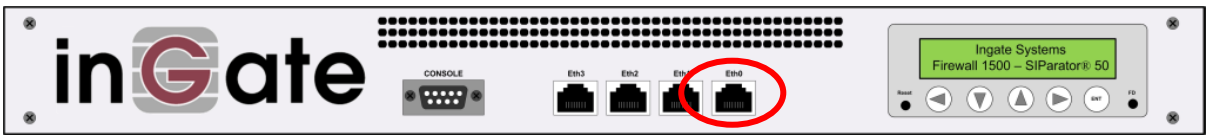
Configuration Steps:

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.

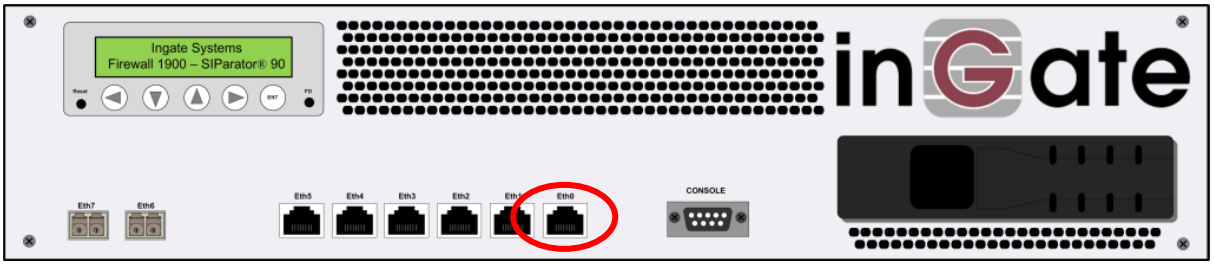
Ingate 1190 Firewall and SIParator 19 (Back)



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

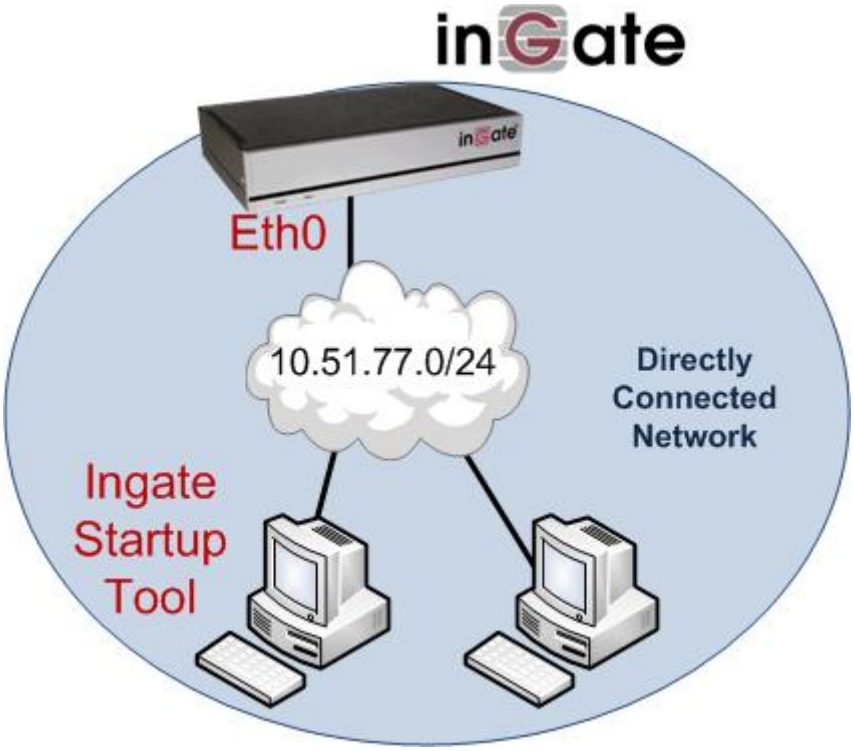


Ingate 1900 Firewall and SIParator 90



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

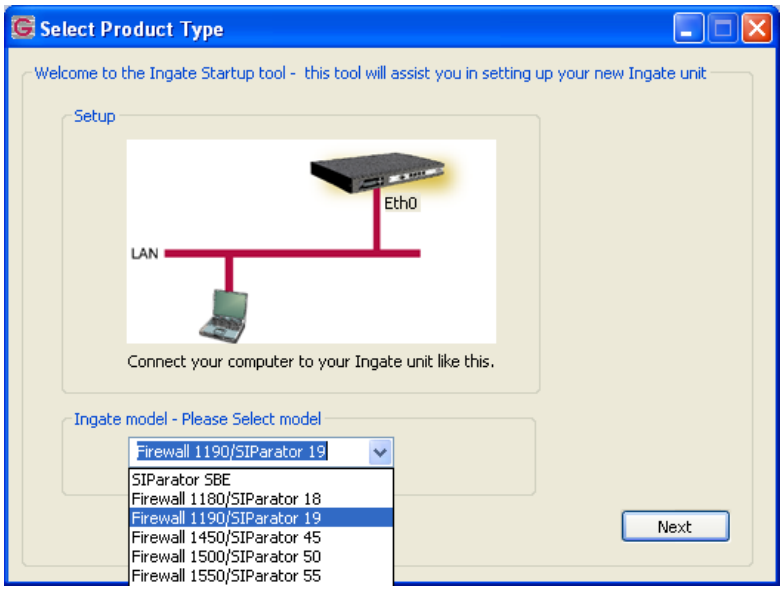
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

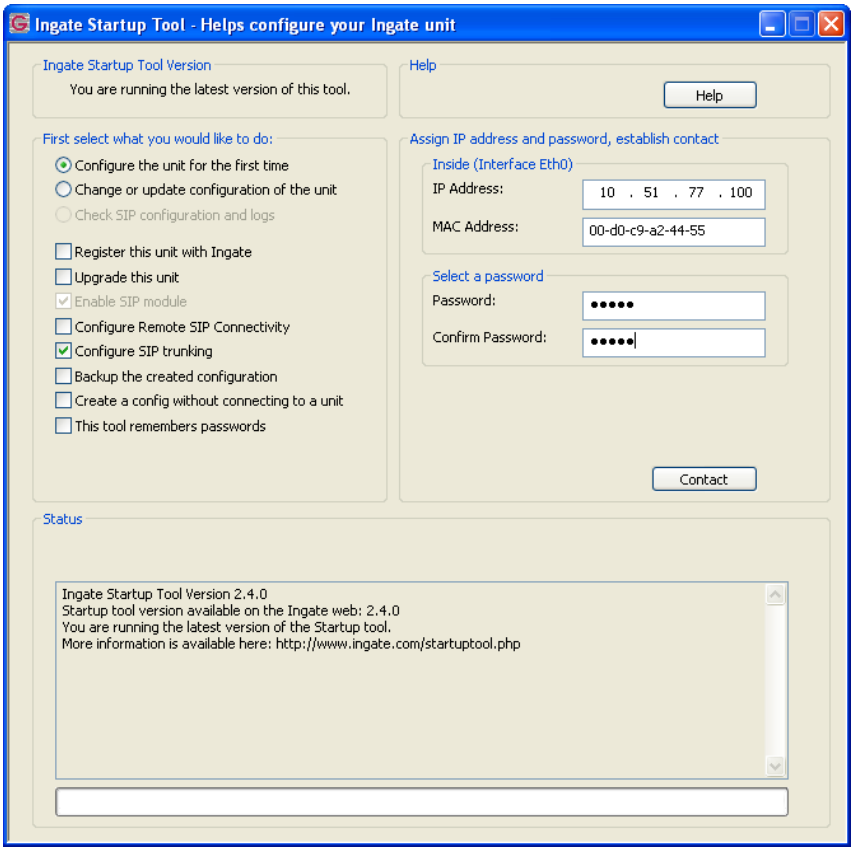
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: "Change or Update Configuration".

Configuration Steps:

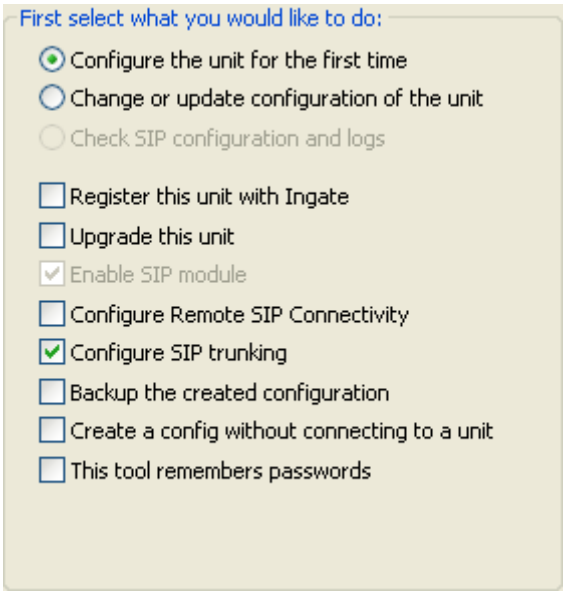
1) Launch the Startup Tool.
2) Select the Model type of the Ingate Unit, and then click Next.



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



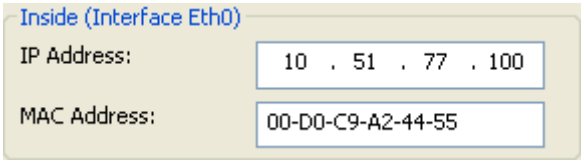
4) Other Options in the "Select first what you would like to do",



a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between the 3Com server and ITSP.

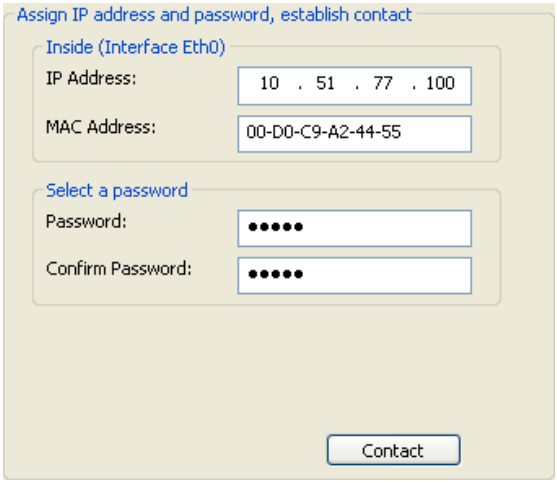
b. Select "Register this unit with Ingate" if you want the tool to connect with www.ingate.com to register the unit. If selected, consult the Startup Tool – Getting Started Guide.
c. Select "Upgrade this unit" if you want the tool to connect with www.ingate.com to download the latest software release 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.



6) In the "Select a Password", enter the Password to be assigned to 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 find the Ingate unit on the network, assign the IP Address and Password.



8) Proceed to Section 4.3: Network Topology.

4.2 Change or Update Configuration

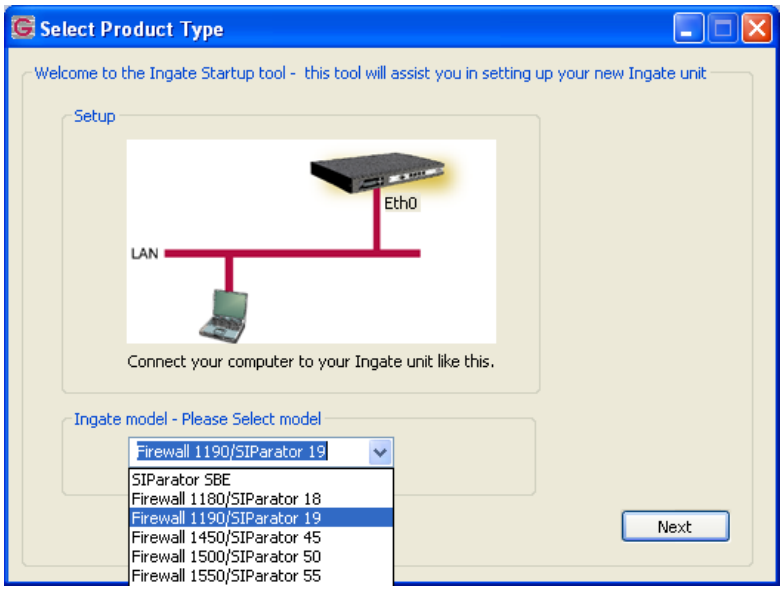
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

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.

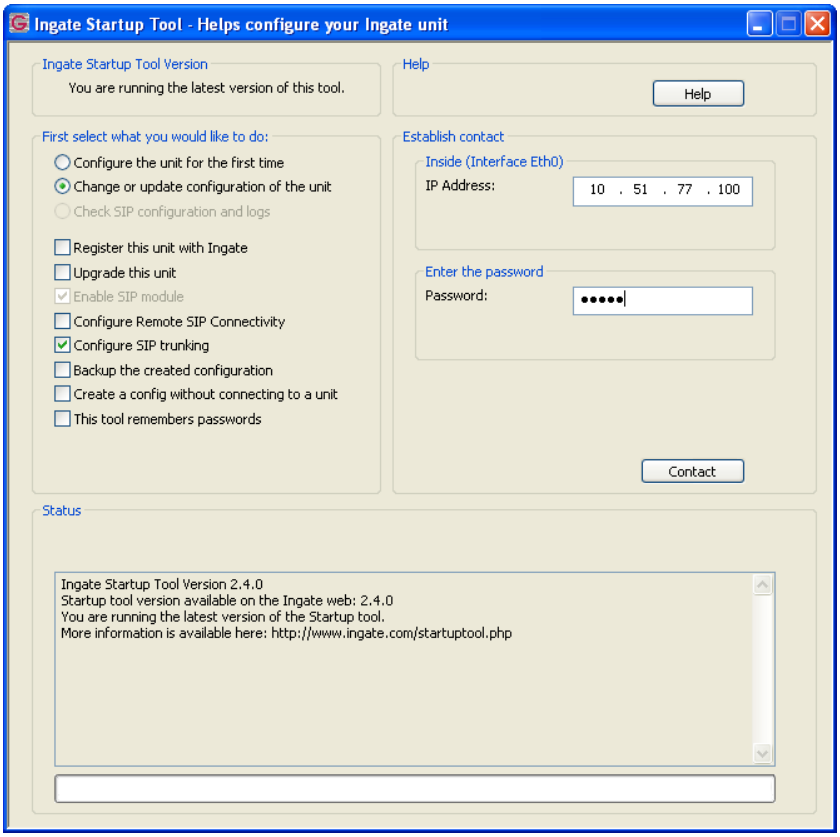
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: "Configure the Unit for the First Time".

Configuration Steps:

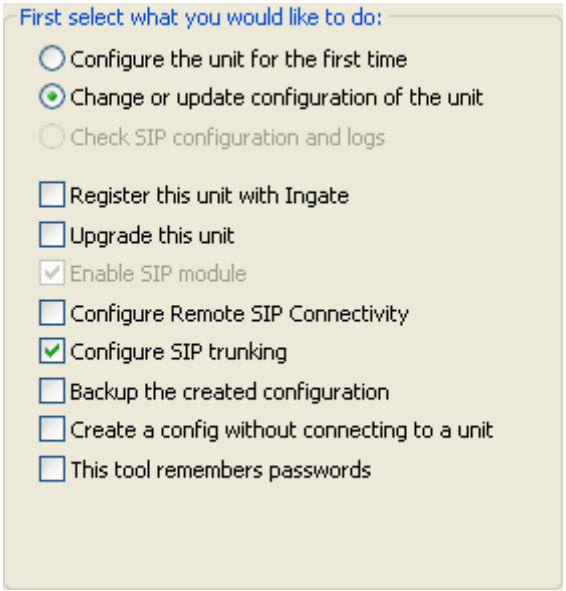
1) Launch the Startup Tool.
2) Select the Model type of the Ingate Unit, and then click Next.



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



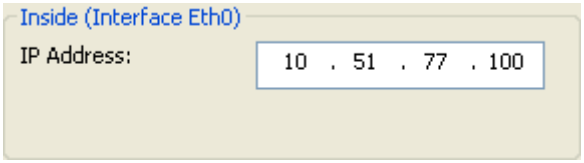
4) Other Options in the "Select first what you would like to do",



a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between the 3Com server 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.



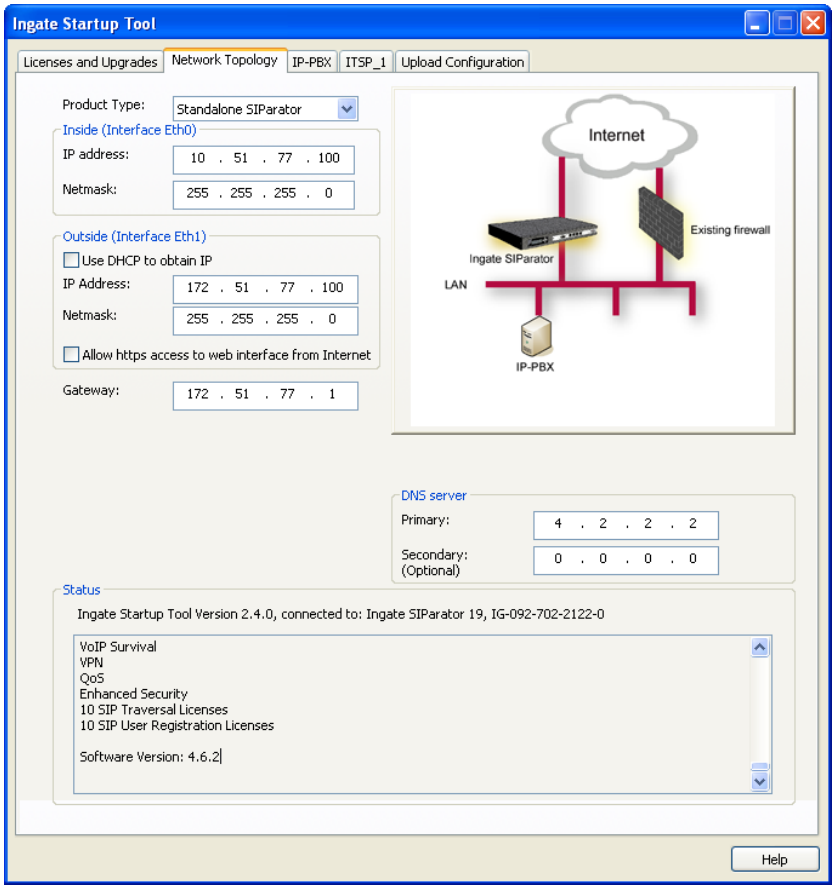
6) In the "Enter a Password", enter the Password of the Ingate unit.

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.

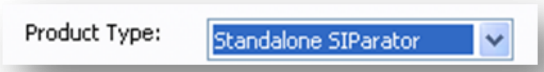
4.3 Network Topology

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.



Configuration Steps:

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

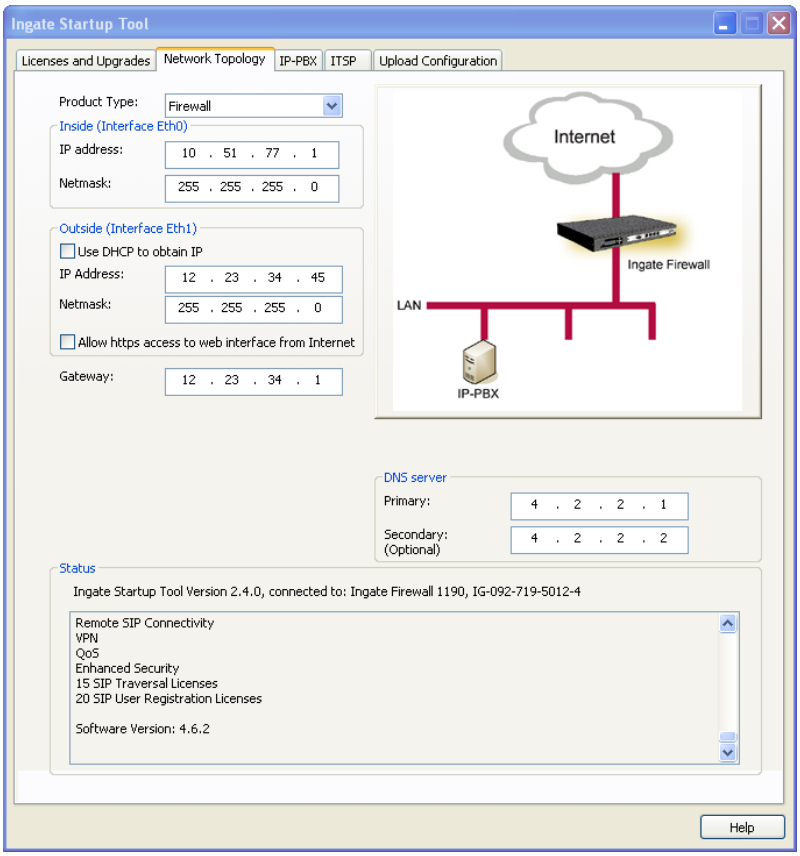


Hint: Match the picture to the network deployment.

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

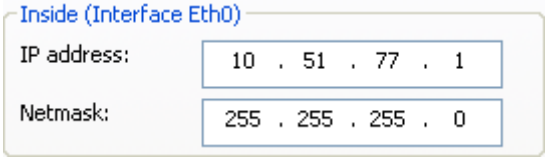
When deploying an Ingate Firewall, there is only one way the Firewall can be installed. The Firewall must be the Default Gateway for the LAN; it is the primary edge device for all data and voice traffic out of the LAN to the Internet.



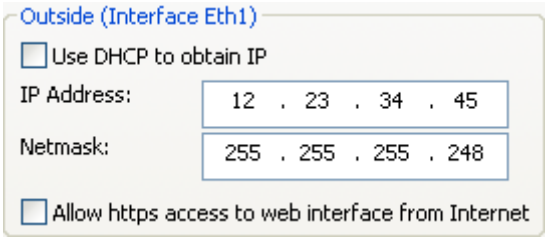
Configuration Steps:

1) In Product Type, select "Firewall".

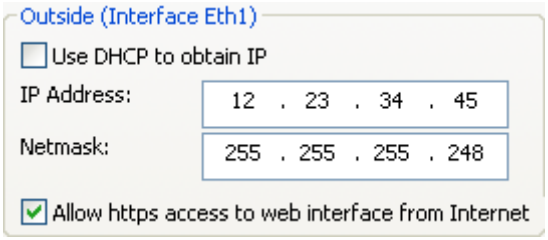
2) Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.



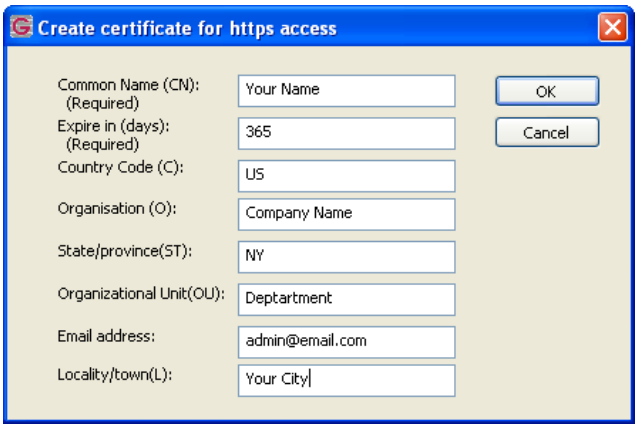
3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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



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"

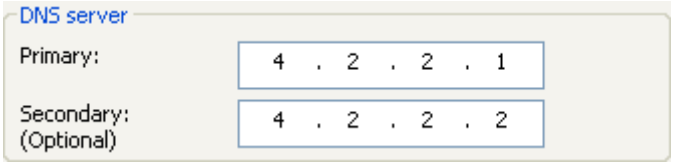


   b. Create a Private Certificate for https access, enter the corresponding information required to generate a certificate.



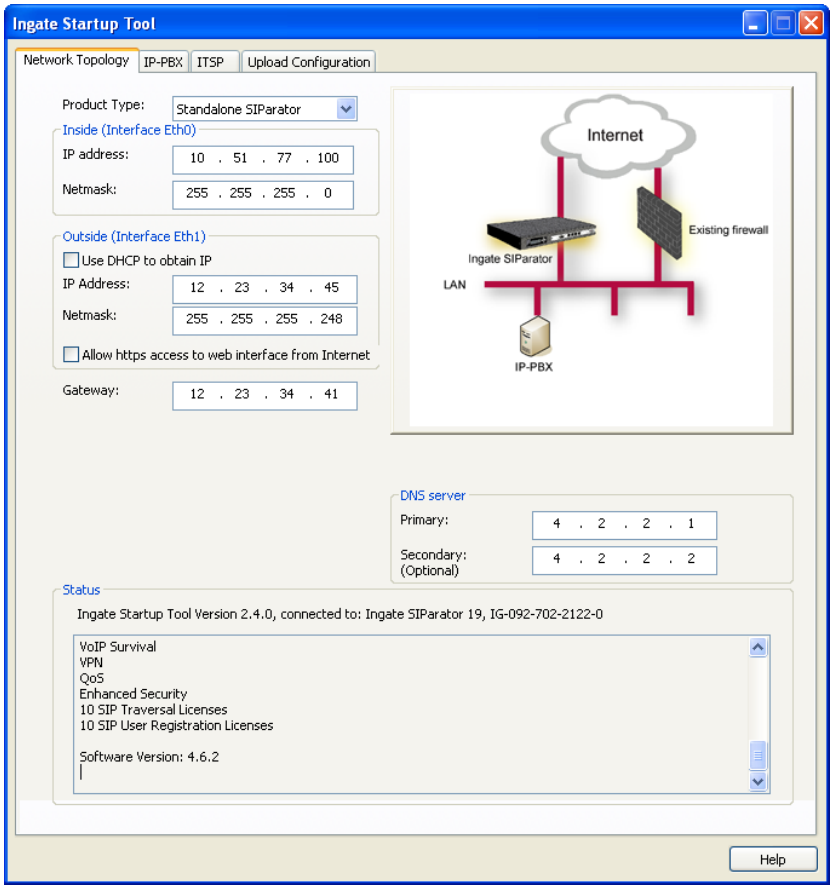
5) Enter the Default Gateway for the Ingate Firewall. The Default Gateway for the Ingate Firewall will always be an IP Address of the Gateway within the network of the outside interface (Eth1).

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.



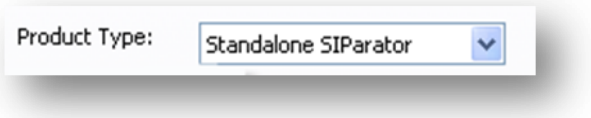
4.3.2 Product Type: Standalone

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.

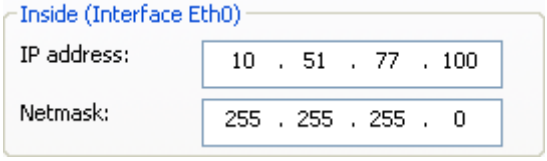


Configuration Steps:

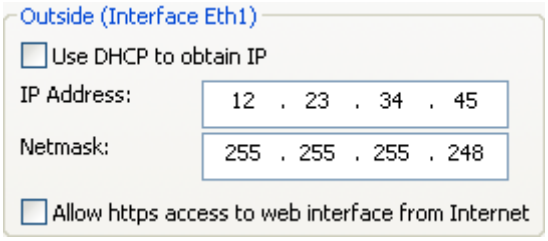
1) In Product Type, select "Standalone SIParator".



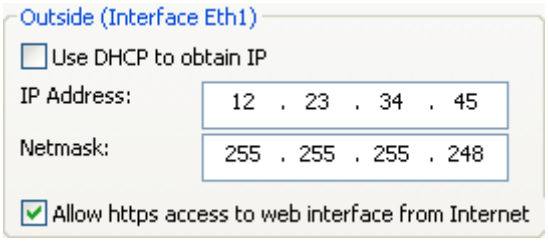
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



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 DCHP.

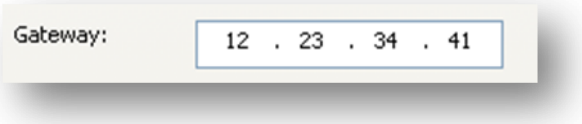


4) **Optional:** To configure Secure Web (https) from the Internet to the Ingate Unit for remote administration,
   c. Select "Allow https access to web interface from Internet"



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

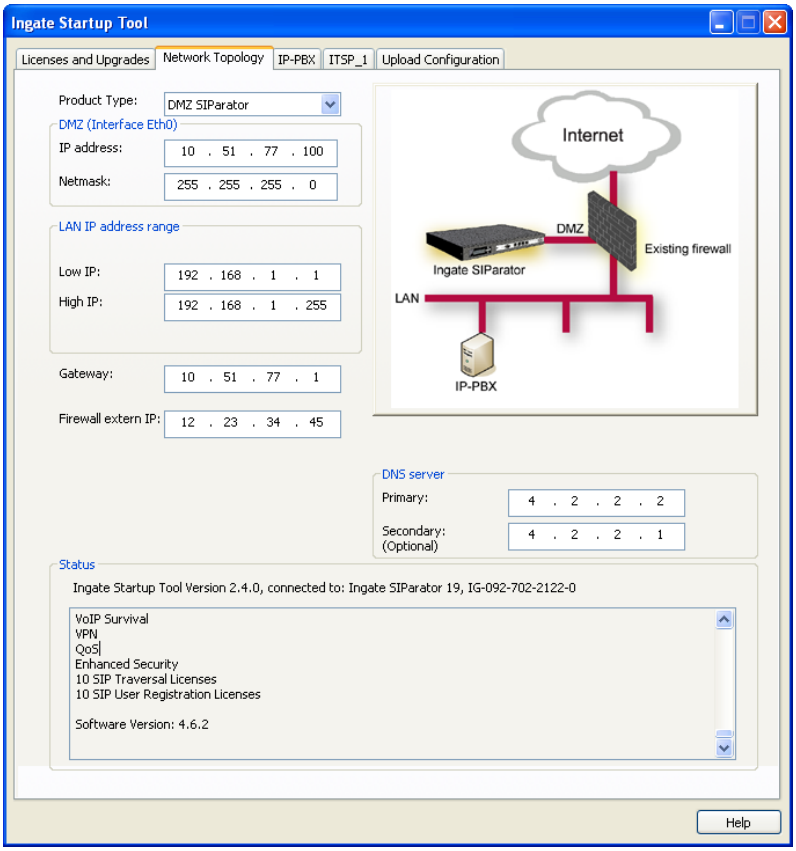
5) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.

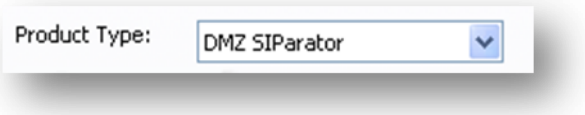
4.3.3 Product Type: DMZ SIParator

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.

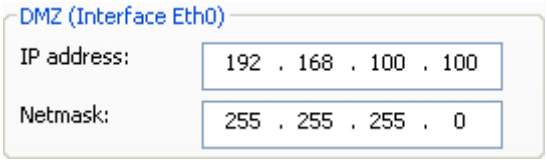


Configuration Steps:

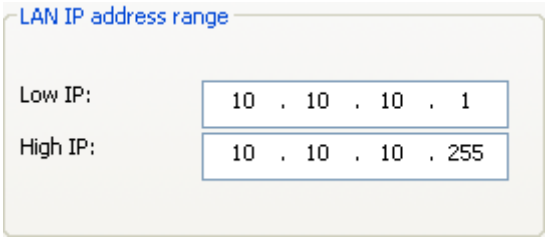
1) In Product Type, select "DMZ SIParator".



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.

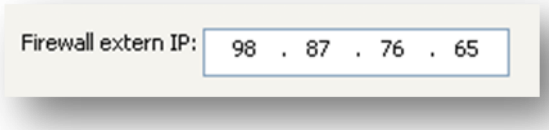


3) Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.

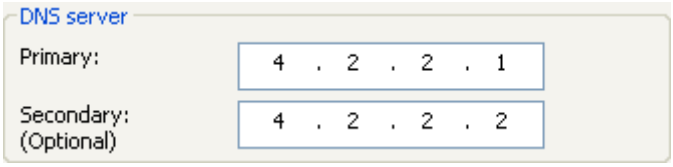


4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

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



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



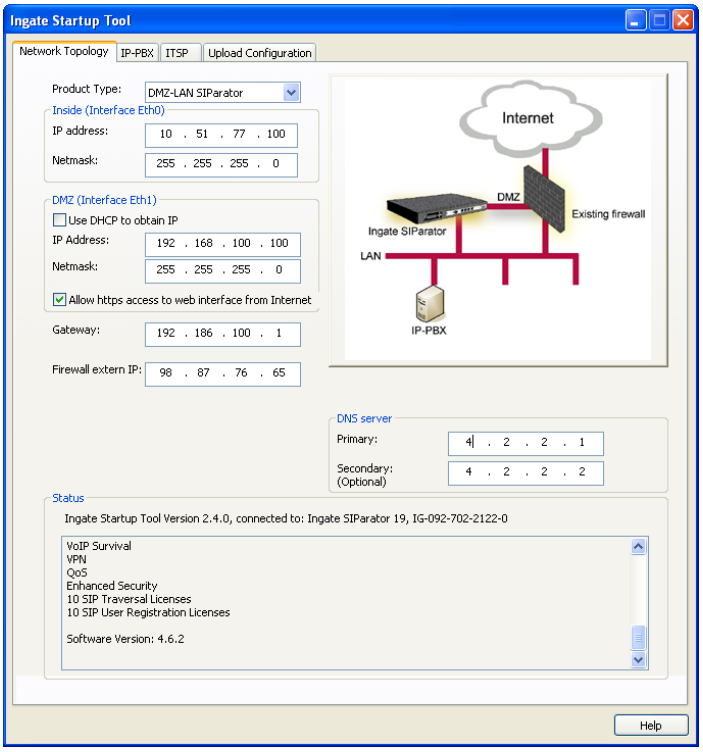
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

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

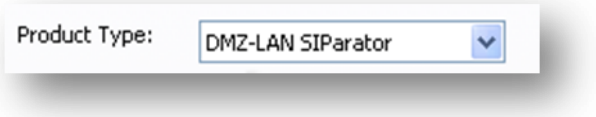
4.3.4 Product Type: DMZ-LAN SIParator

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.

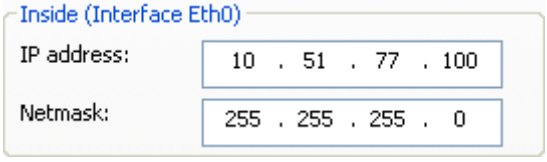


Configuration Steps:

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

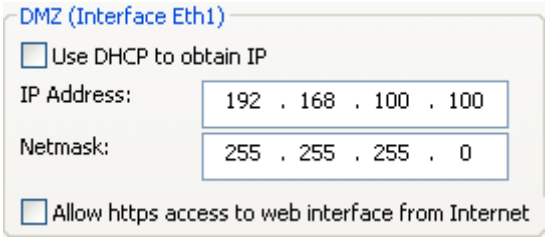


2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



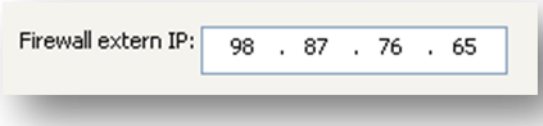
3) Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.

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.

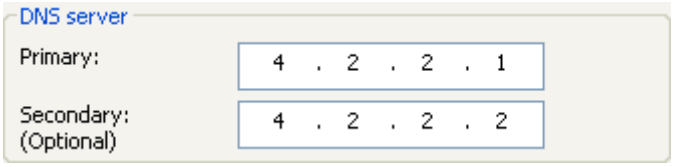


4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

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



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

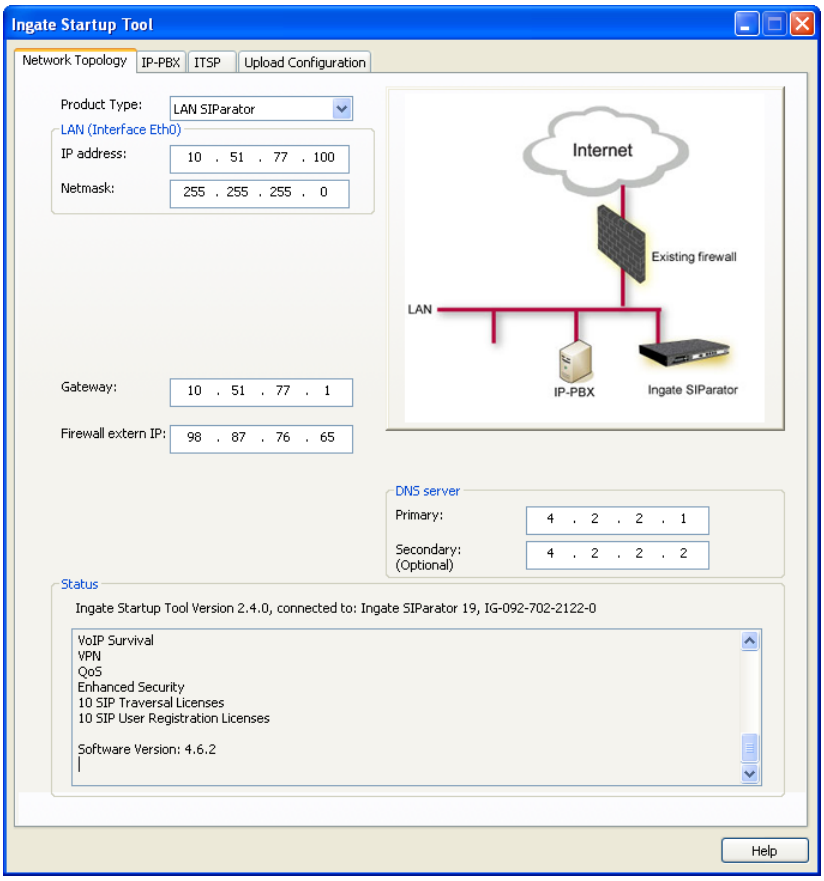


7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

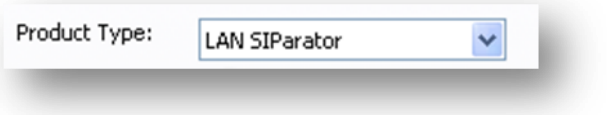
4.3.5 Product Type: LAN SIParator

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.

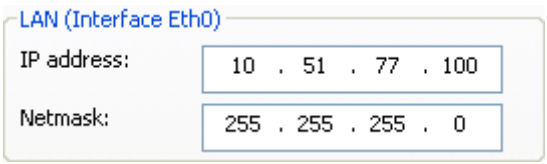


Configuration Steps:

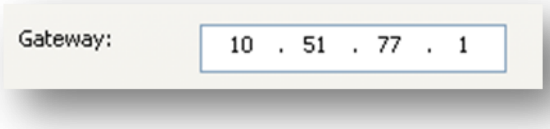
1) In Product Type, select "LAN SIParator".



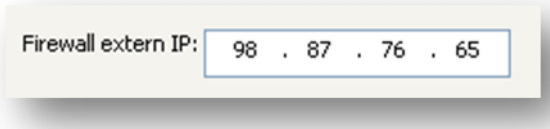
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



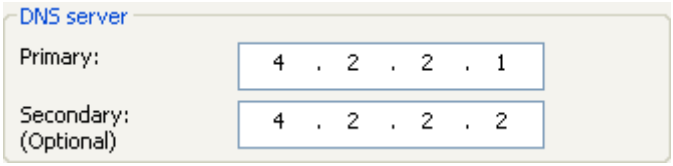
3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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



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



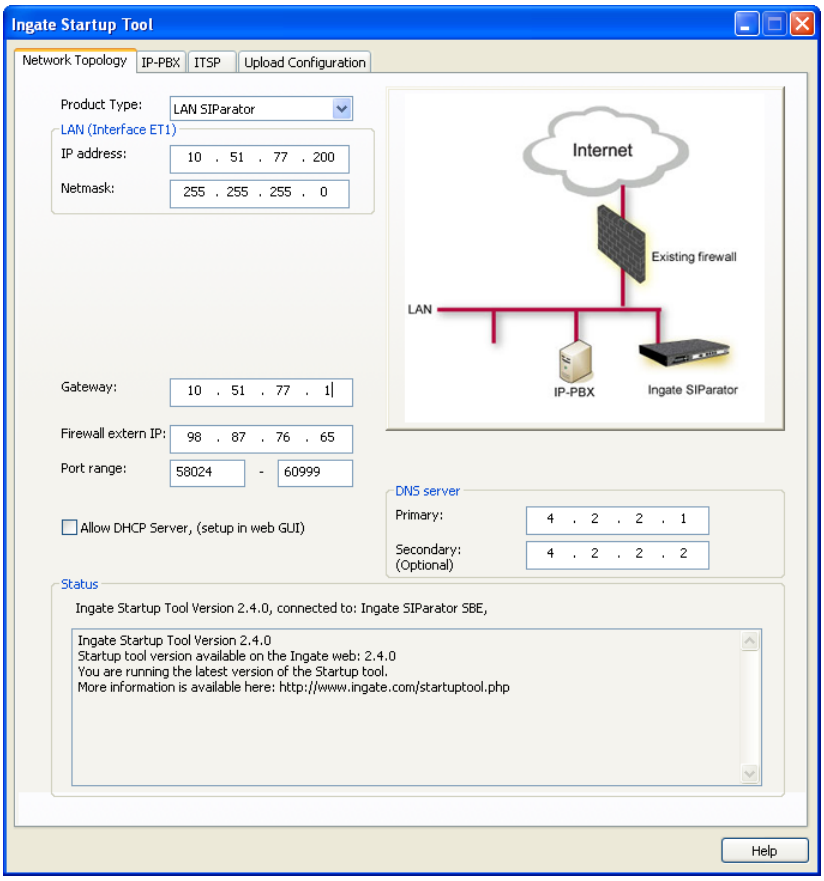
6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

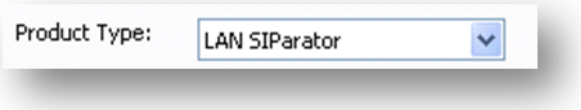
4.3.6 Product Type: LAN SIParator – "*SBE SIParator Only*"

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.

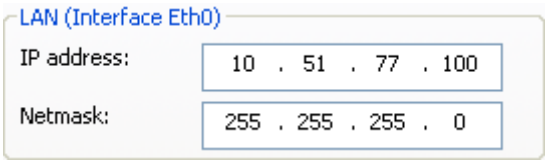


Configuration Steps:

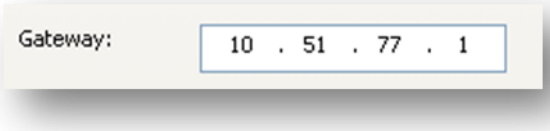
1) In Product Type, select "LAN SIParator".



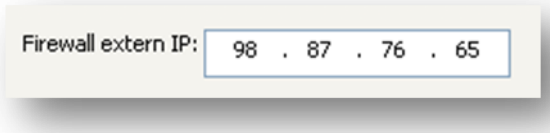
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



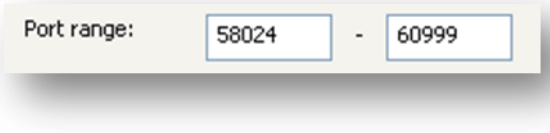
3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



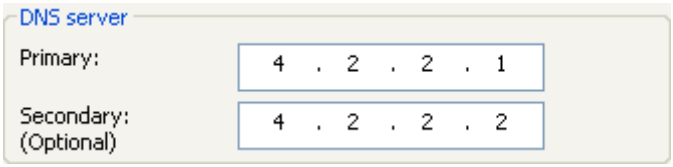
4) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.



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



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



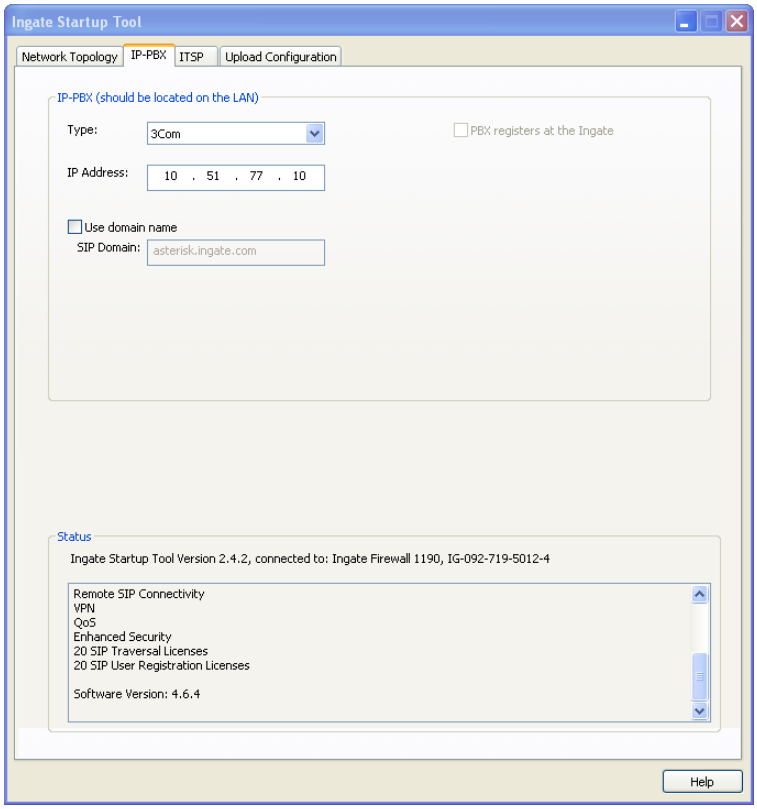
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

On the existing Firewall:

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

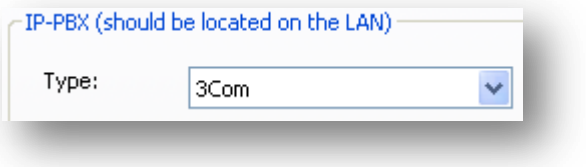
4.4 IP-PBX

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 3Com VCX Connect 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 3Com VCX Connect server.



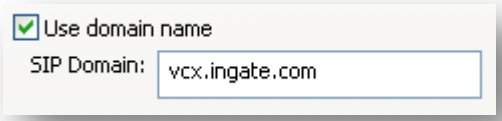
Configuration Steps:

1) In the IP-PBX Type drop down list, select "3Com". Ingate has confirmed interoperability the 3Com VCX Connect, the unique requirements of the testing are contained in the Startup Tool.



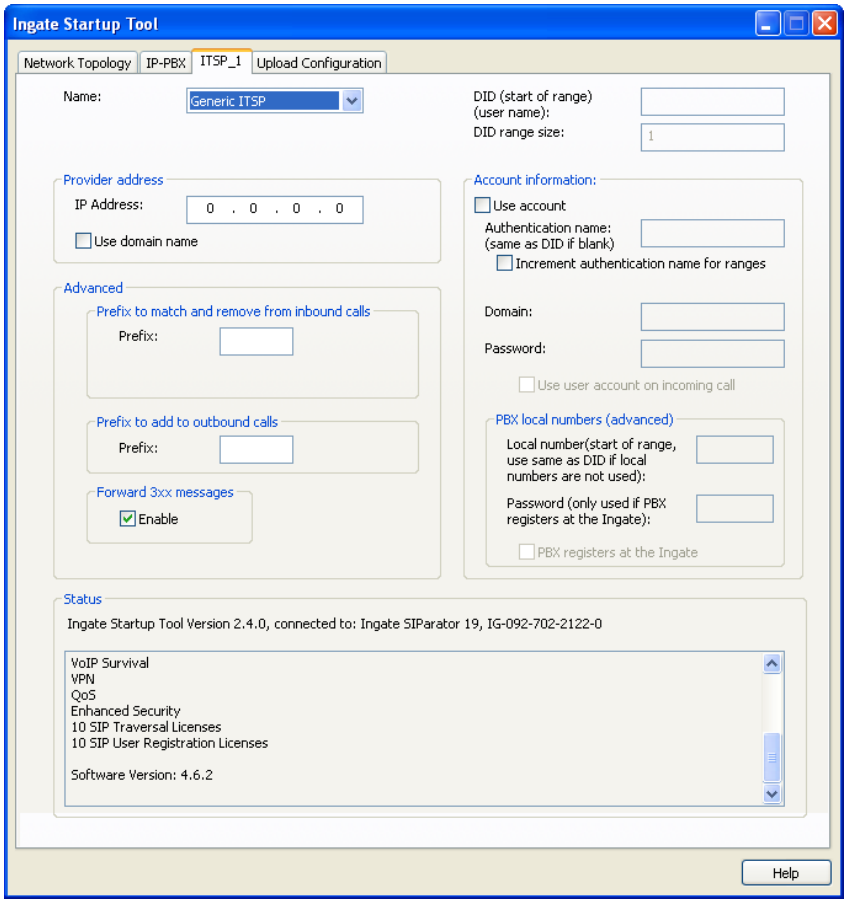
2) Enter the IP Address of the 3Com VCX Connect. The IP Address should be on the same LAN subnet as the Ingate unit.

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



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.



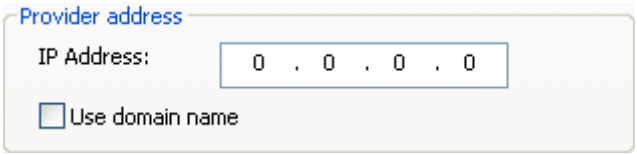
Configuration Steps:

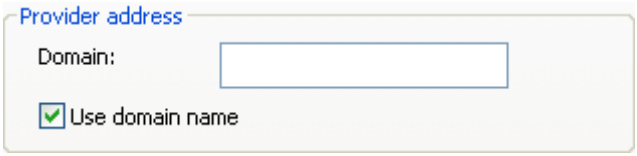
1) In the ITSP drop down list, select the appropriate ITSP vendor. Ingate has confirmed interoperability several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool. If the vendor choice is not seen, select "Generic ITSP".

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.

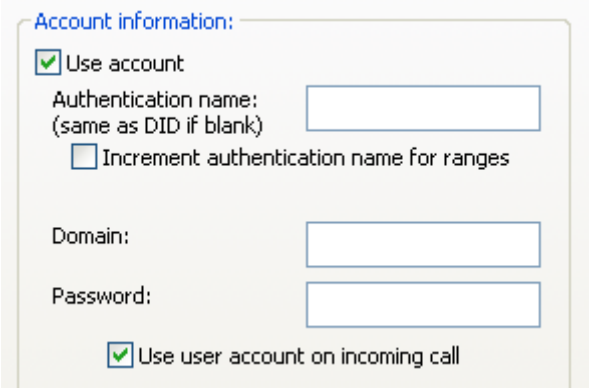
2) Service Providers come in one of two flavors, either they have a trusted IP deployment or they require a Registration account.

   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.

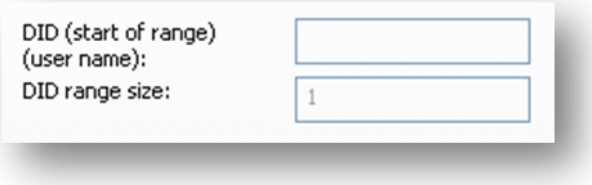




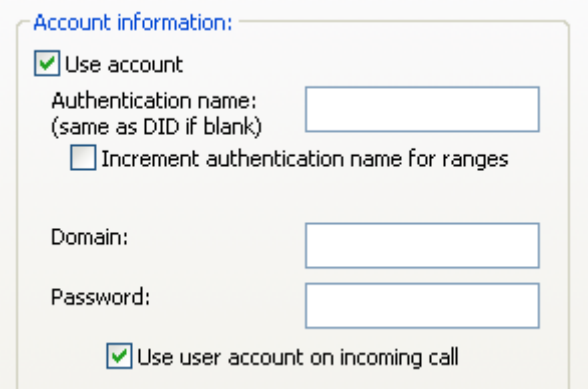
   b. In the case where the Service Provider requires the Ingate to Register with the Service Providers SIP Server or SBC, select "Use Account". When "Use Account" is selected, the Registration Account information from the Service Provider is required. Information such as Username/DID, Service Providers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



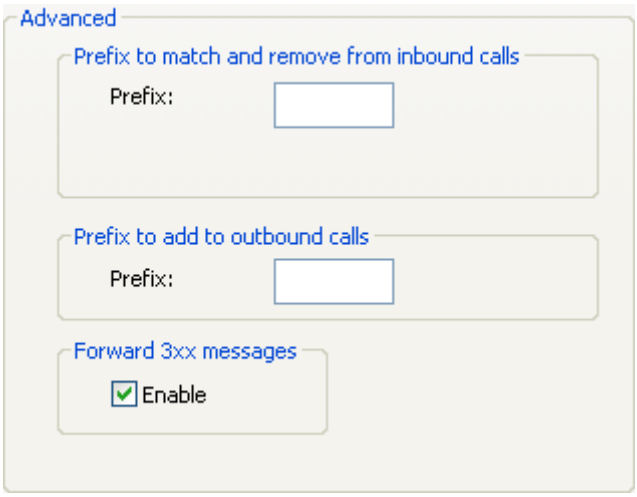
      i. Enter a DID (Username) in which the Ingate will register with the Service Provider. The Startup Tool also has the ability to program a sequential range of DIDs.



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

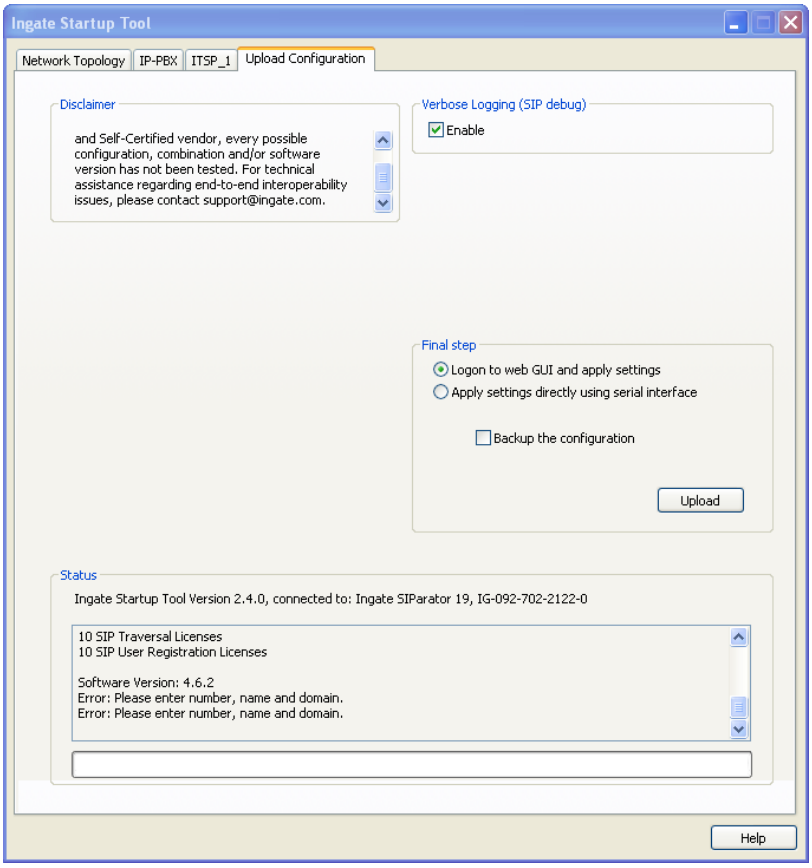


3) The Ingate has the ability to add/remove digits and characters from the Request URI Header. A typical scenario is the addition/removal of ENUM character "+". Many IP-PBX and ITSPs either need to add or remove this character prior to sending or receiving SIP requests. Here you can enter values to Match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



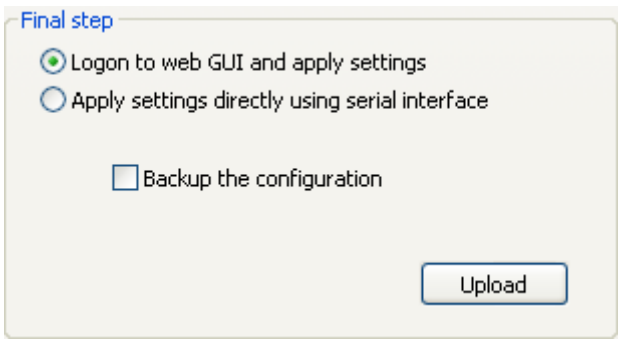
4.6 Upload Configuration

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.

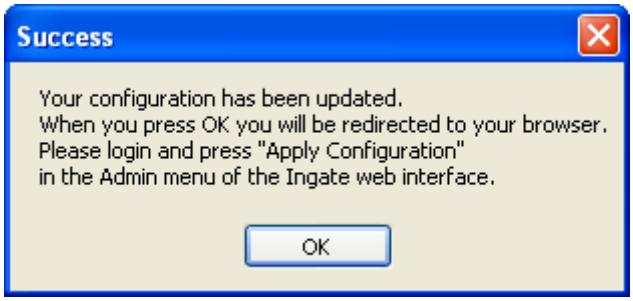


Configuration Steps:

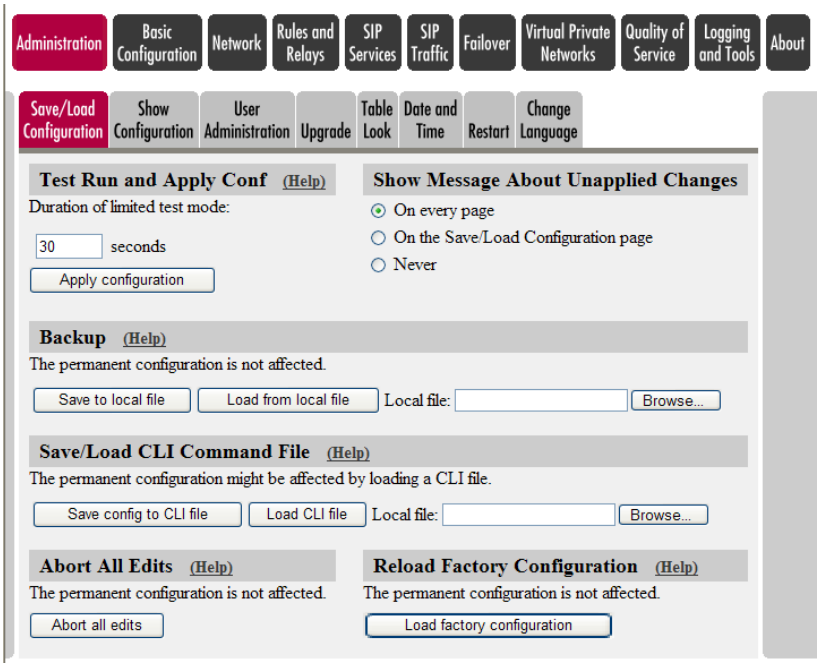
1) Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



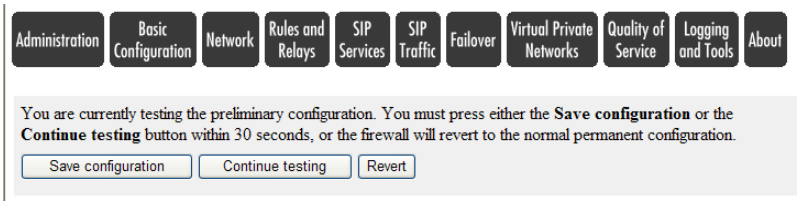
2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



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 3Com VCX Connect Setup

The following configuration details represent the configuration under test. The Ingate SIParator provides Telco communications for all outbound and inbound PSTN calls. In addition the SIParator provided NAT translation services for any remote phones or Teleworkers wanting to register a phone to their work extension.

The VCX is configured with the SIParator IP address as a trusted endpoint. Therefore no authentication or registration is needed between these 2 devices. The SIParator is configured with the both the VCX Primary and Secondary IP addresses as the SIP Proxy. All inbound Telco calls i.e. DID's are redirected by the SIParator to VCX. Remote phone are configured to use the SIParator public IP address as their SIP Proxy address. All phone SIP registrations received by the SIParator are forwarded to the VCX for authentication. Once authenticated these remote phones can make outbound calls using their office extension and receive inbound calls to their office extension at home, all of these calls are carried over their office Telco connection.

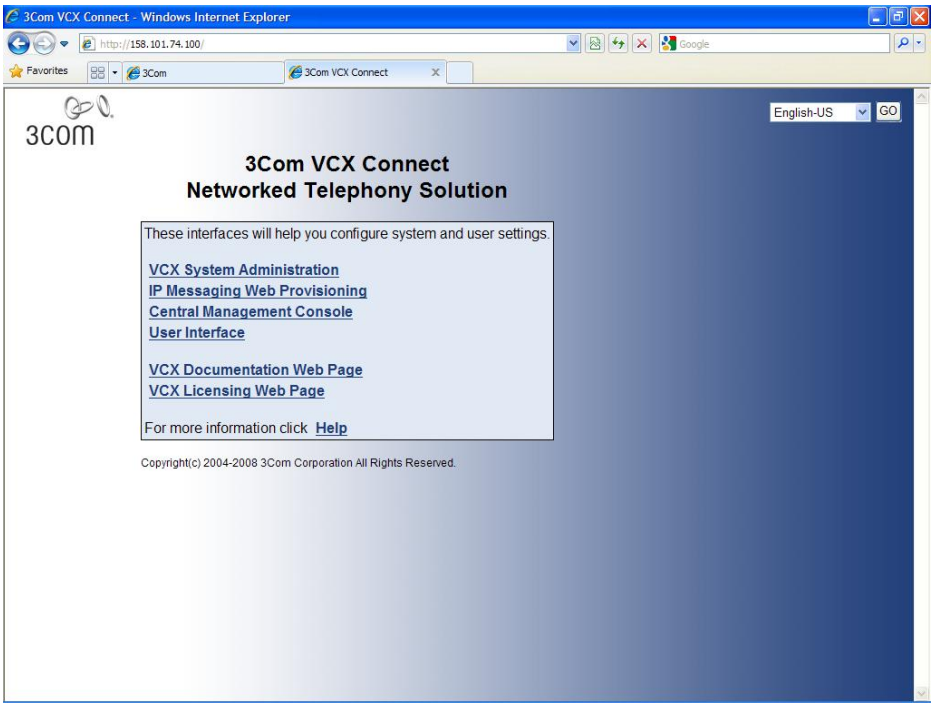
5.1 VCX Configuration

Defining a device on the VCX 8.0.7e as a "Trusted Endpoint" can now be done using the Web interface.

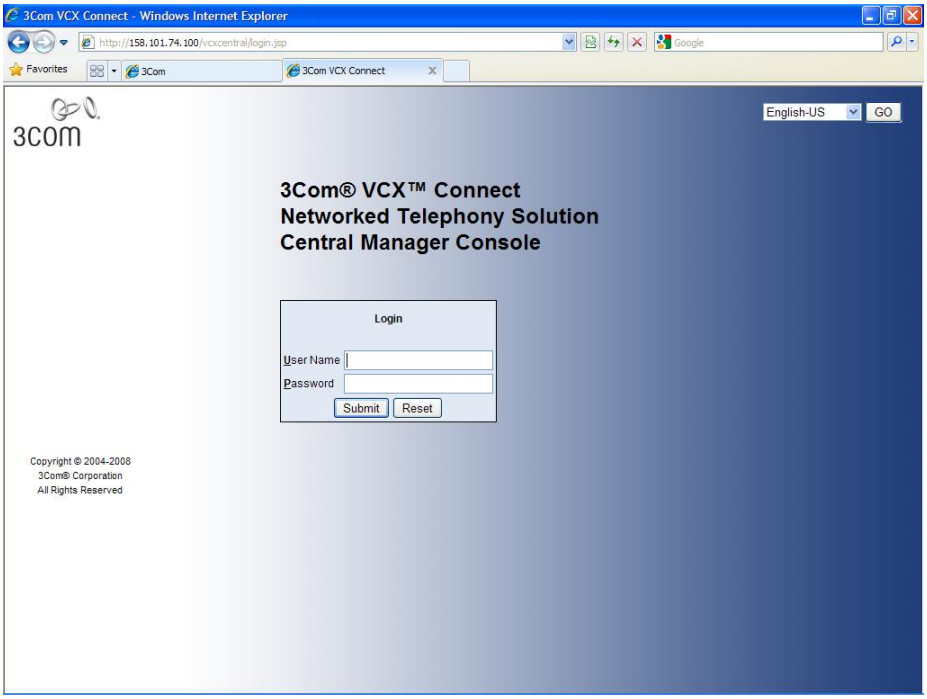
Note: In versions prior to 8.x, creating a trusted endpoint was a 2 step process please refer to documentation for these version for details

Using VCX Web Configuration GUI

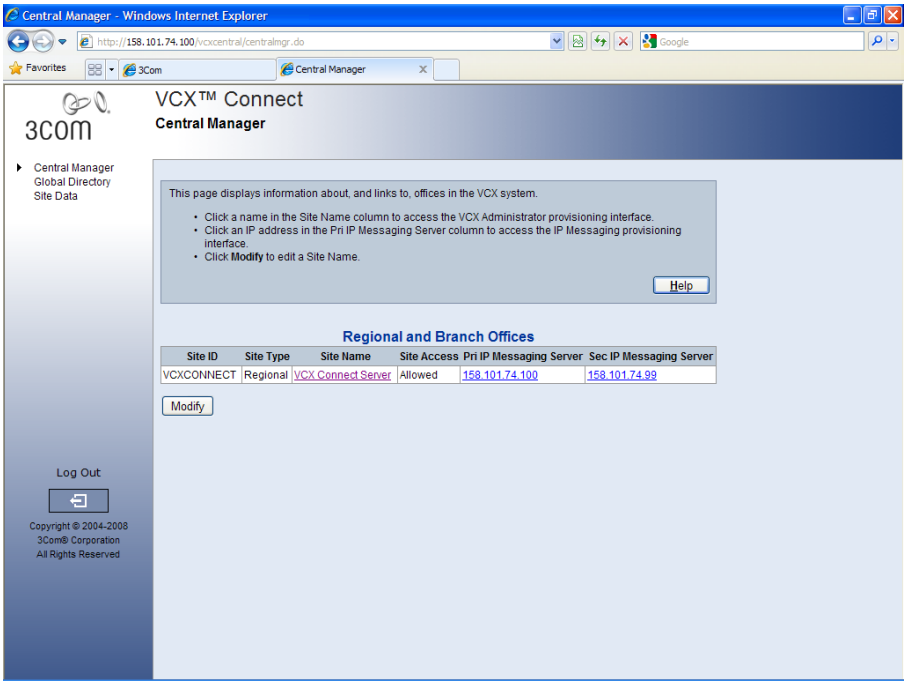
1. Point a browser to VCX Server IP address (e.g.:http://158.101.74.100) The VCX login screen appears. Select the Central Management Console option.



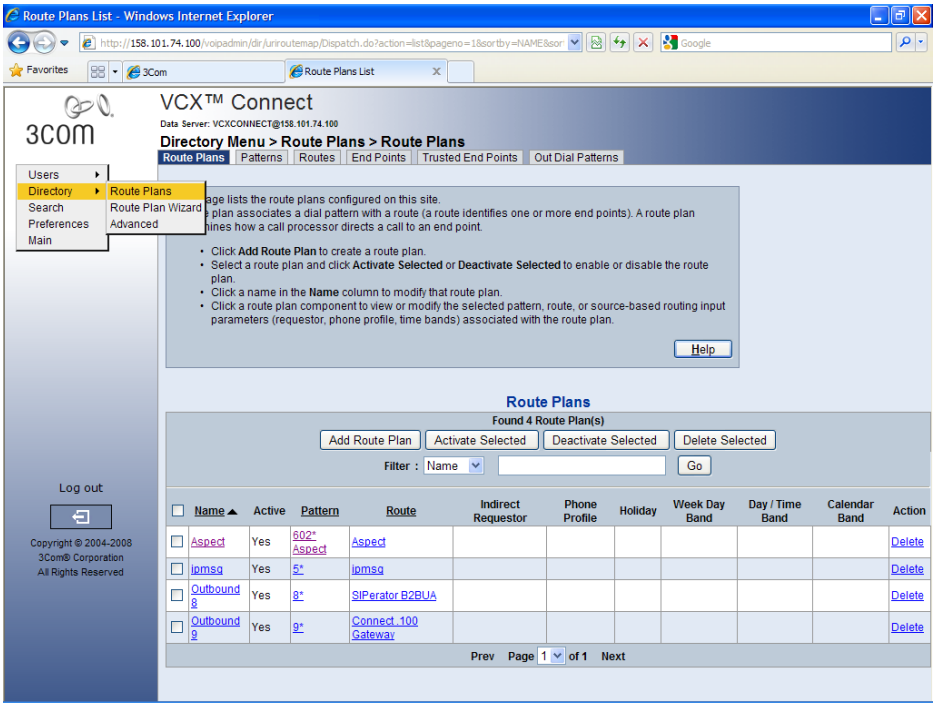
2. Enter a VCX username and password with administrative access. (New VCX installations have a default username **admin** and password **besgroup**.) Click **Submit**.



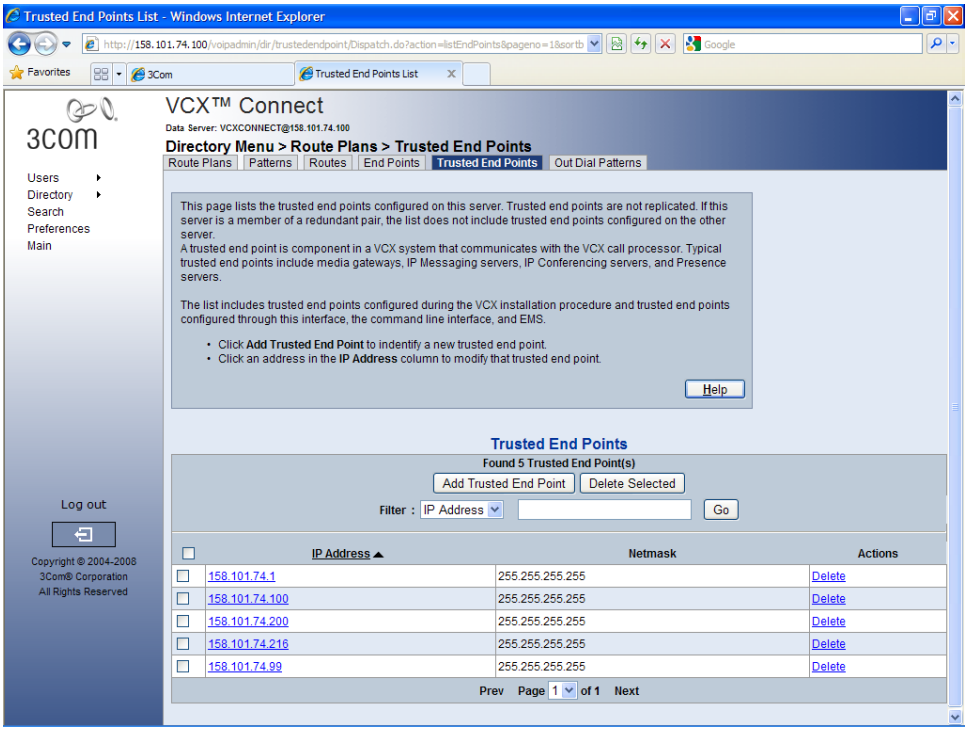
3. Select the site name you wish to work on.



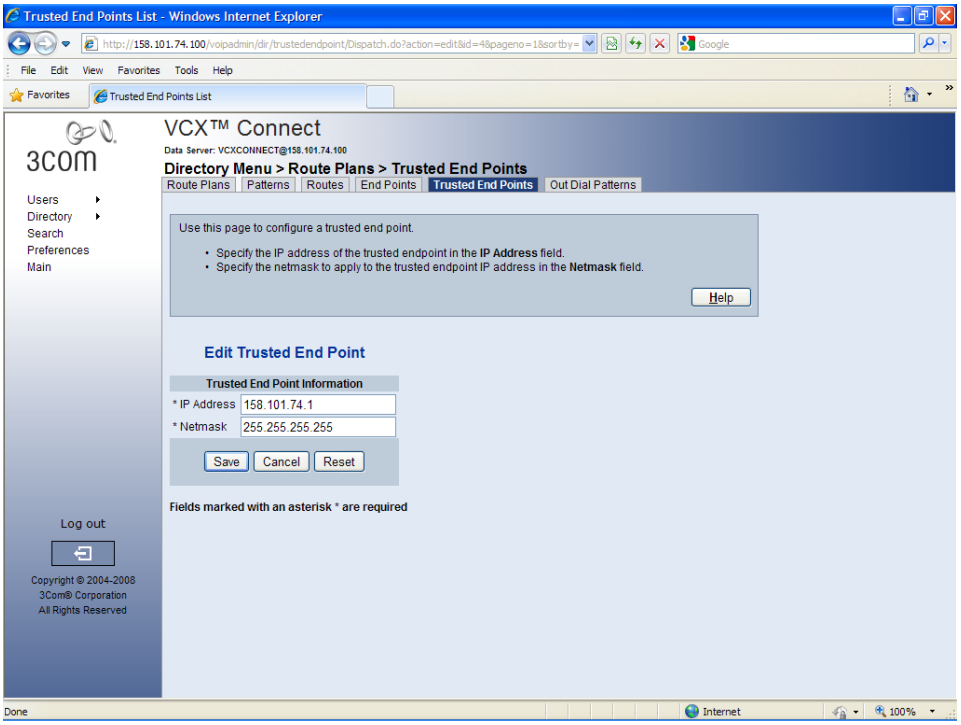
4. Select Directory from the top menu



5. Click "**Trusted End Points**" Tab on Right of the screen to add a device IP addresses

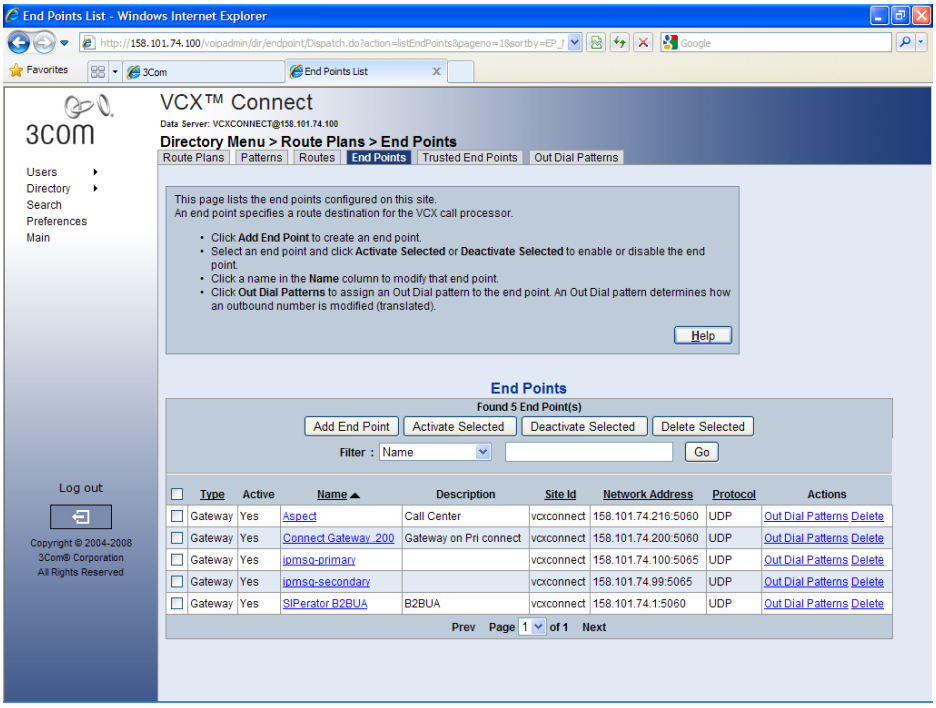


a. Click the **Add Trusted End Point** button.

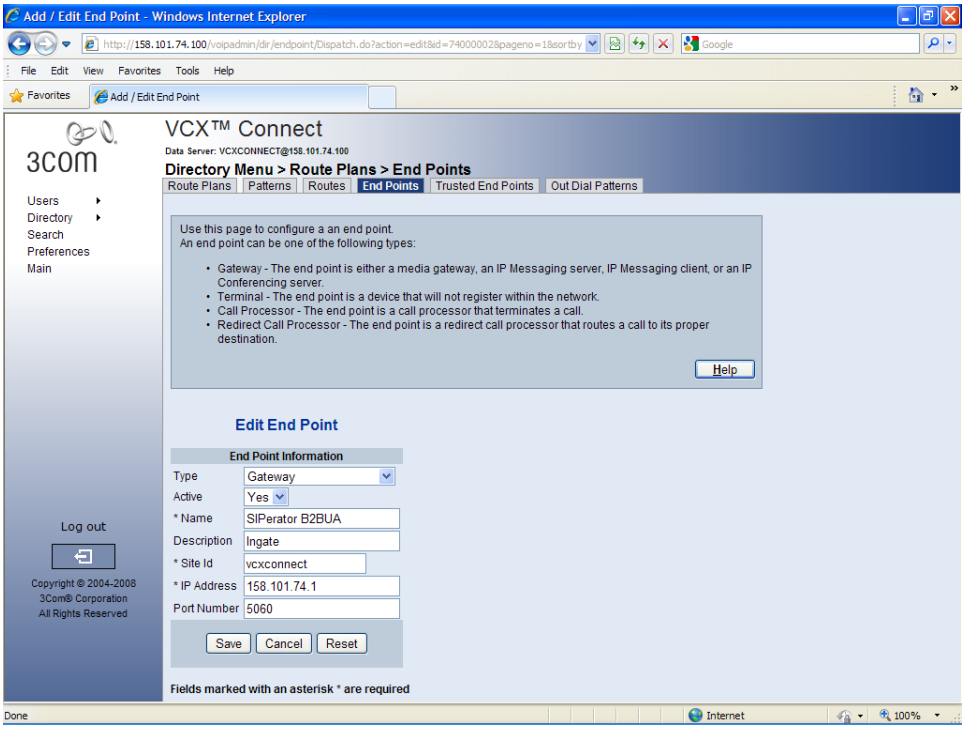


b. Enter the endpoint configuration as follows:
   - **IP Address:** IP address of SIParator
   - **Netmask:** Use Host mask of 255.255.255.255

6. Click "**End Points**" Tab on Right of the screen to add a device name for each i.e. "Aspect" to the list as an endpoint
   a. Select "**Add End Point**" button

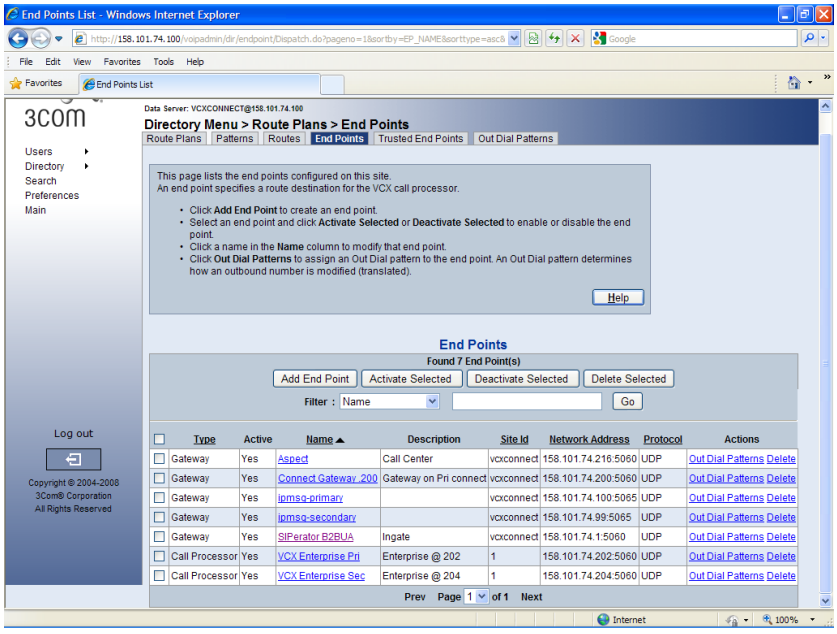


b. The endpoint configuration window is displayed

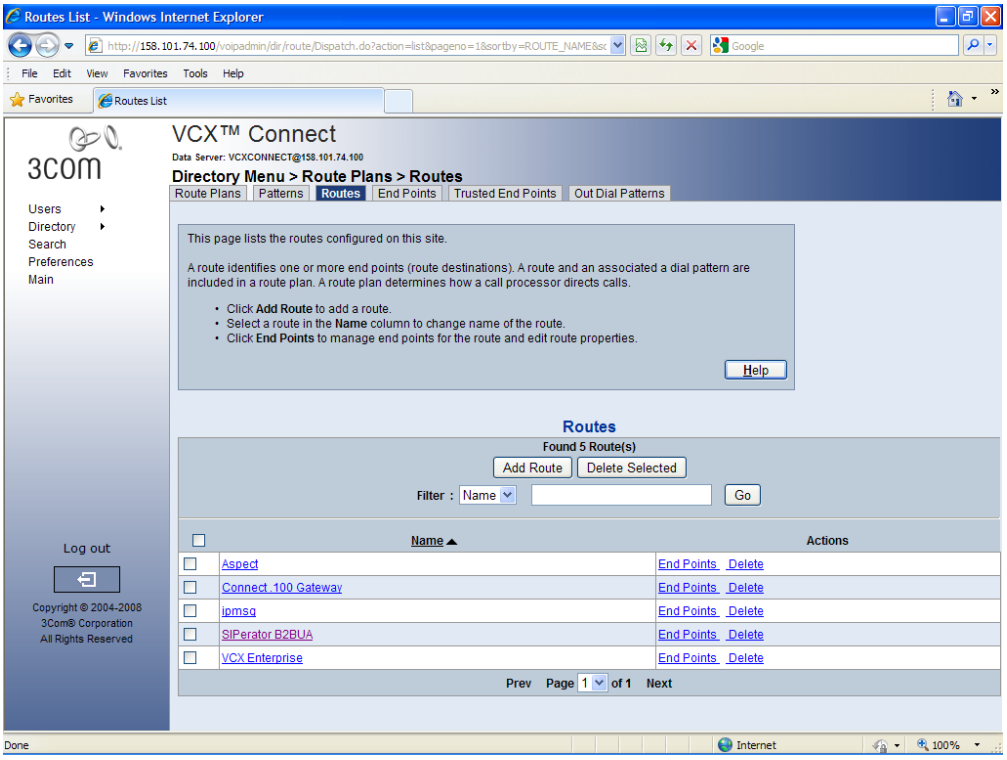


c. Enter the endpoint configuration as follows:
- **Type:** Set to Gateway
- **Active**: Set to Yes.
- **Name:** Enter the name of the device i.e. SIPerator B2BUA
- **Description:** Enter a description of the device i.e. Ingate
- **Site Id:** Enter your VCX site ID.
- **IP Address:** Enter the SIPerator IP address
- **Port Number:** port number (usually 5060)
- Click the **Save** button.

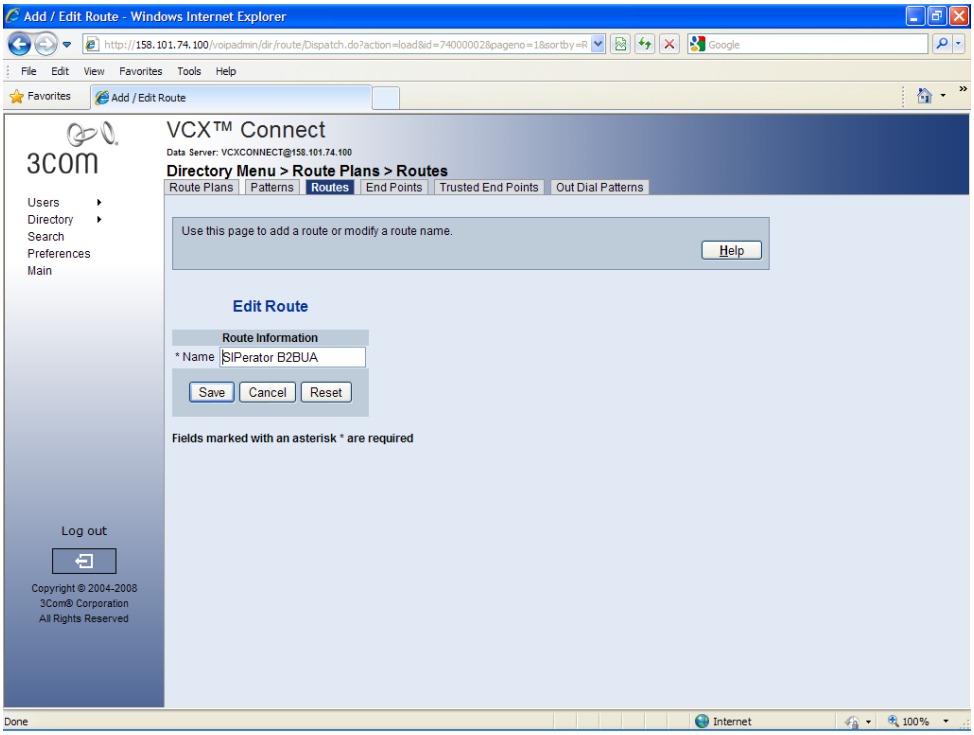
d. The **List of End Points** table appears, listing the new endpoint.



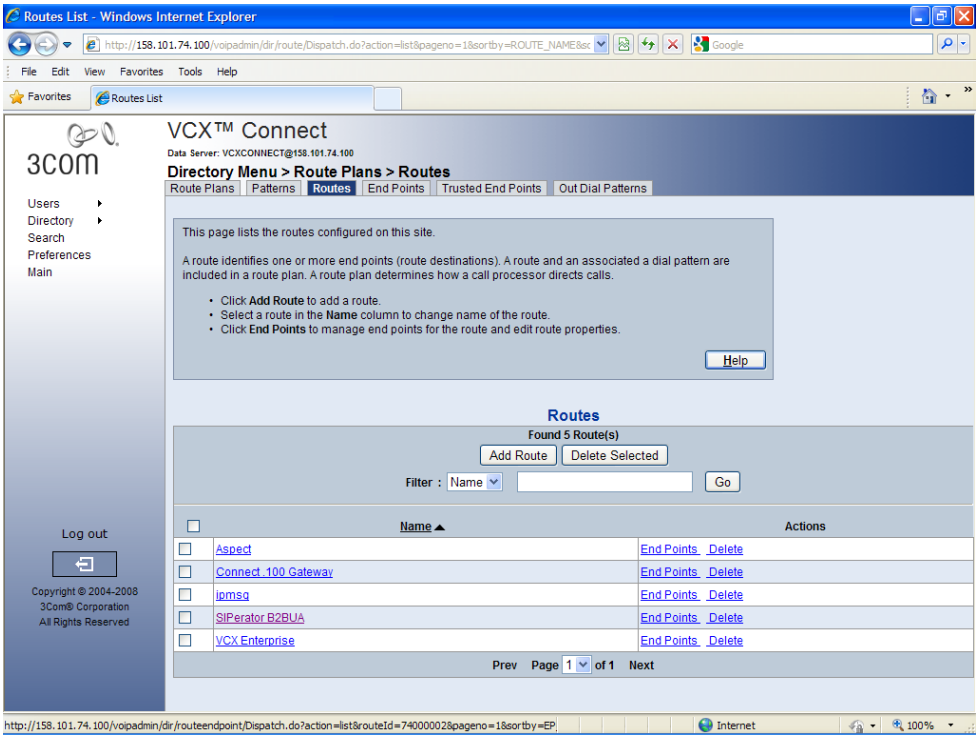
7. Click **Routes** Tab to create a Route with one or more endpoints



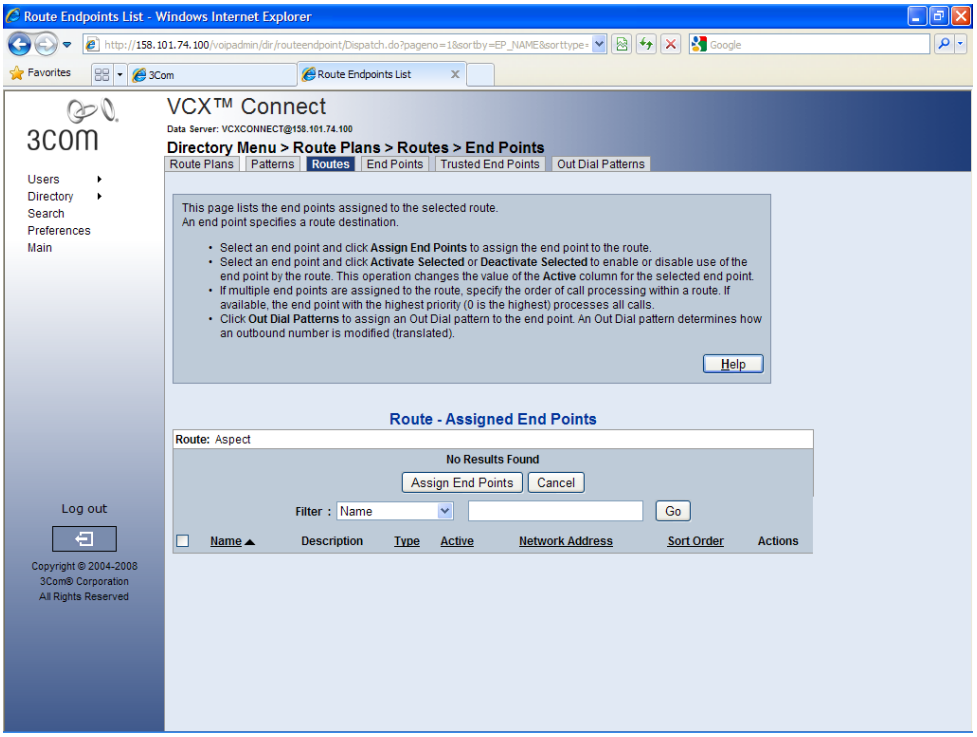
a. Select the "**Add Route**" button and give it a name i.e. SIParator B2BUA and select "**Save**"



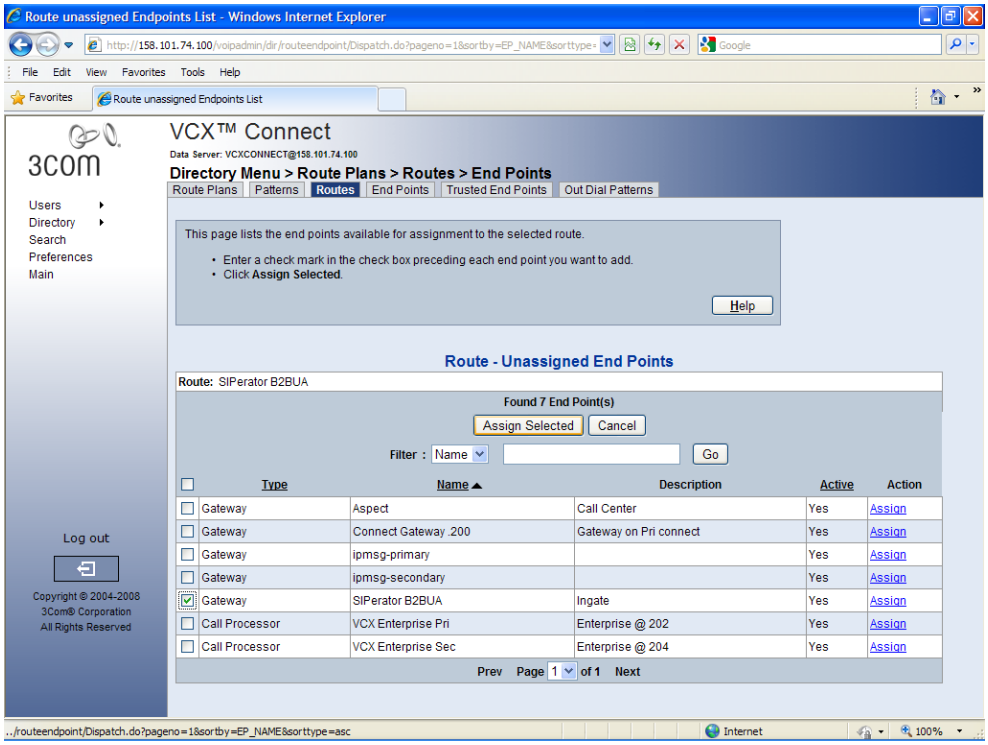
b. Select the "**End Points**" button on Right



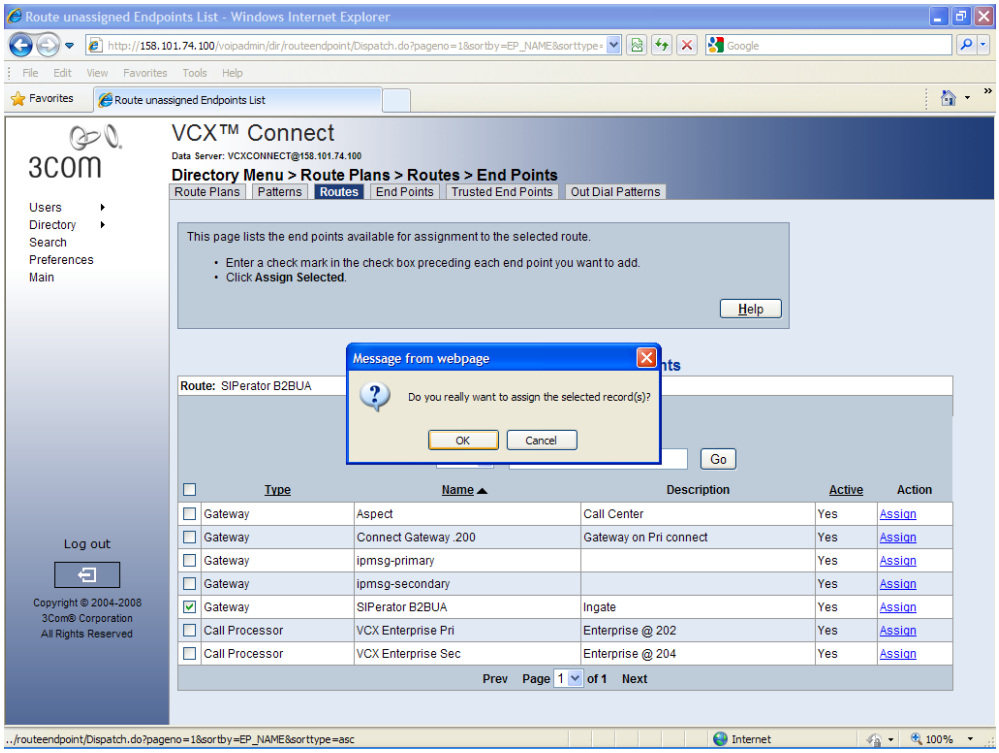
c. Select the "Assign End Points" button



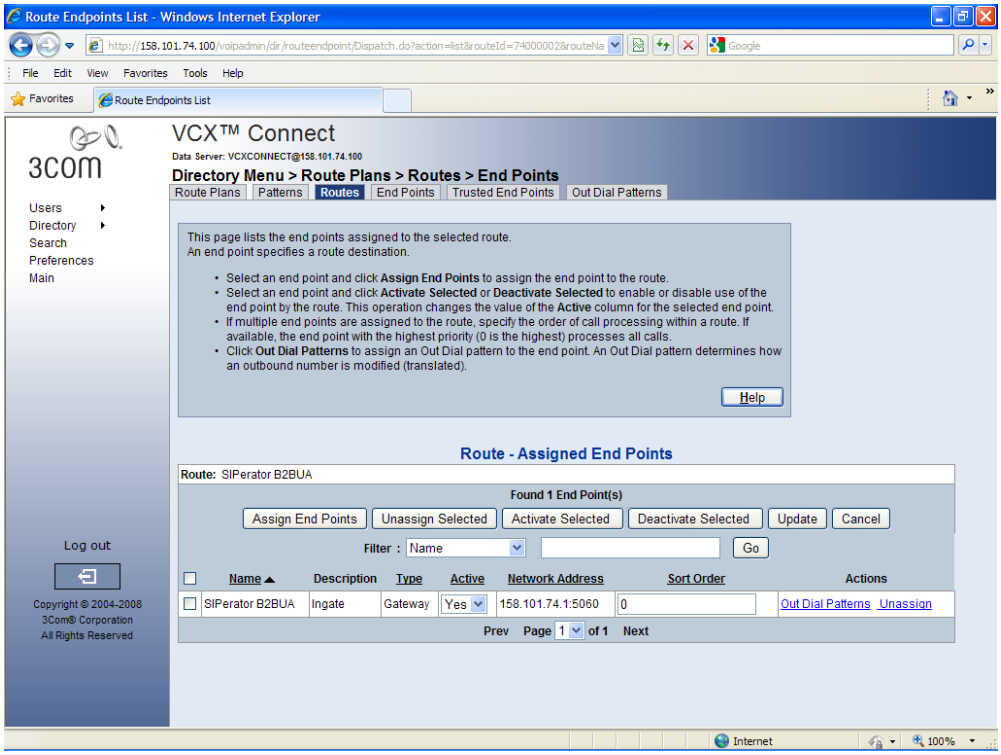
d. From the list of available endpoints put a check mark next to "SIParator B2BUA" and select the "**Assign Selected**" button



e. Confirm the "OK"



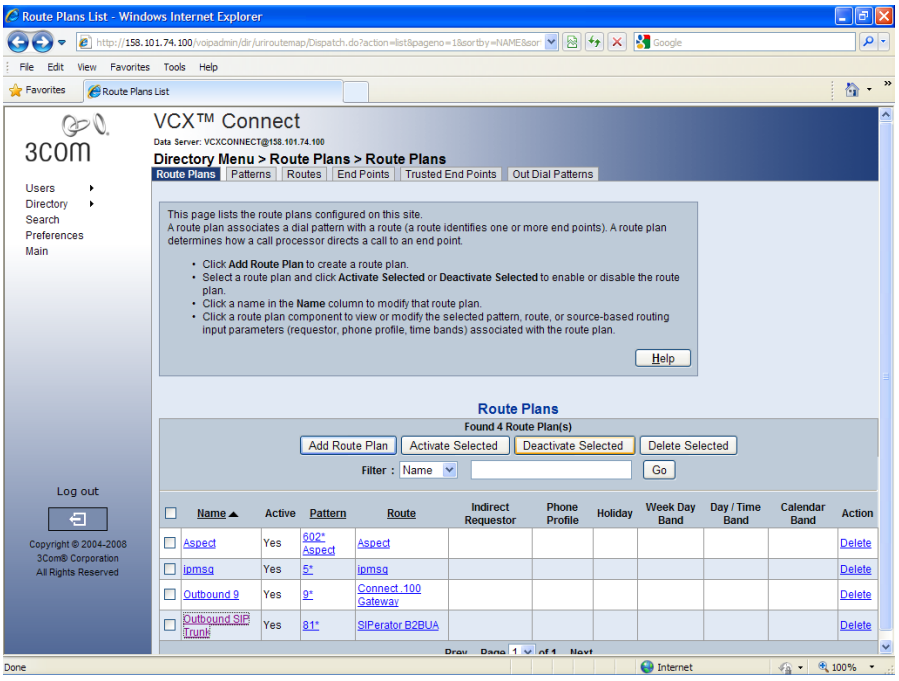
f. The Endpoint "**Aspect**" should be listed as shown

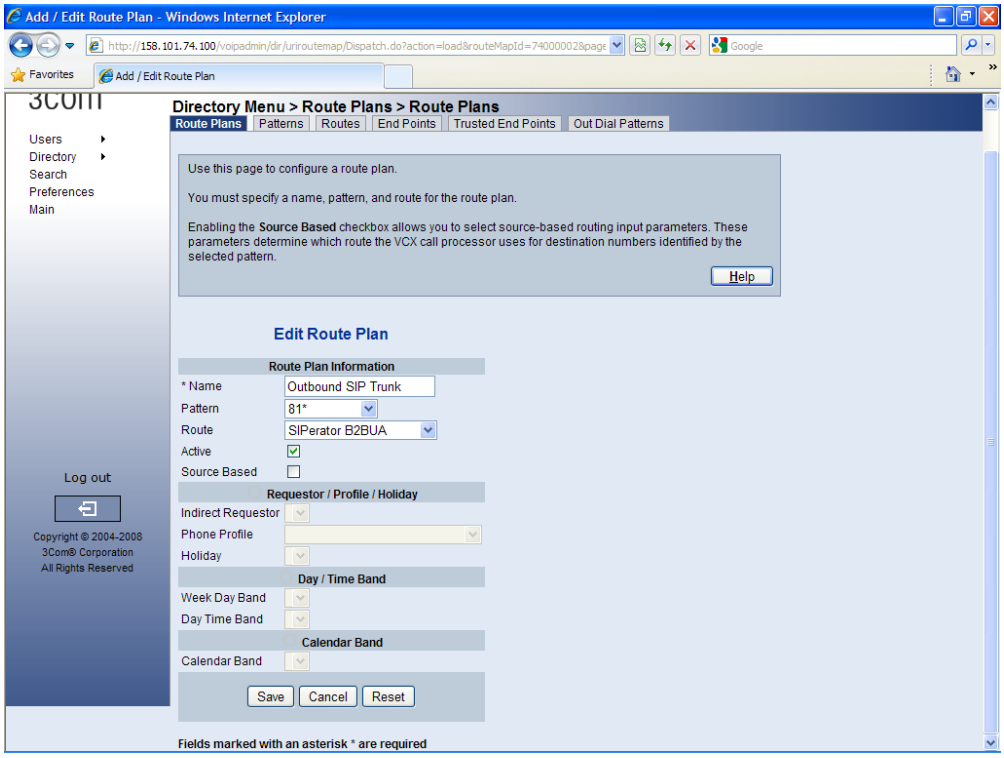


8. Click **Patterns** Tab and create a pattern if needed that a call must match in order for VCX to send the call to the SIParator server.

Note: This step was skipped because the most common patterns are already defined by default on the VCX. Therefore an existing pattern of "**81***" was used in testing

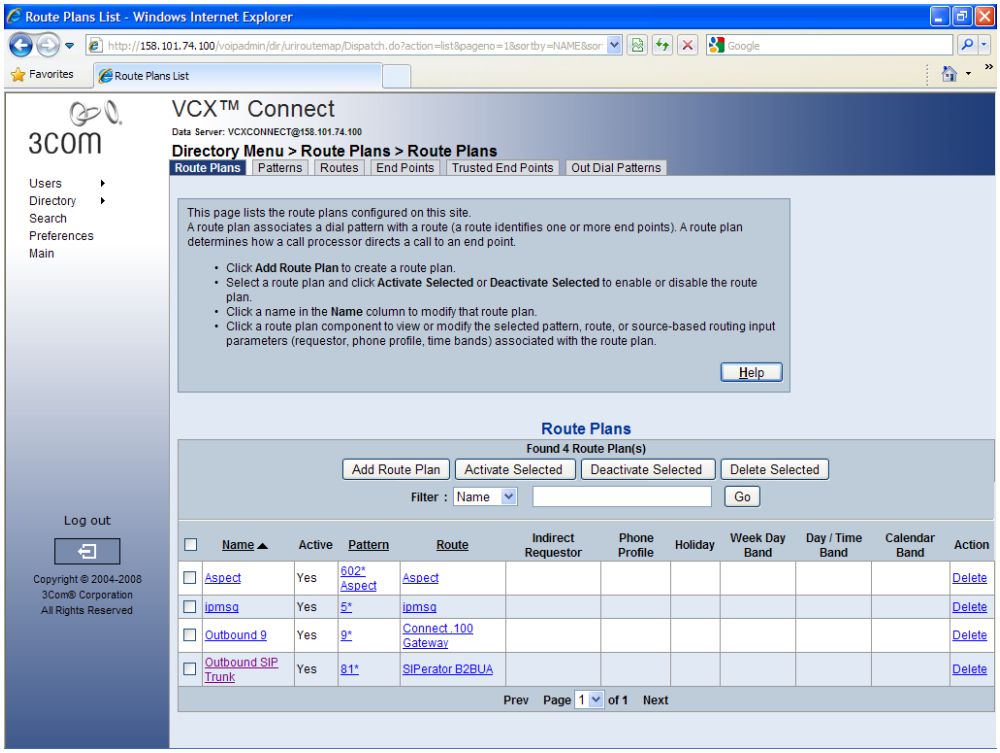
9. Click **Routes** Tab, and create a route that lets VCX send calls to Aspect Unified IP. Click the **Add Route Plan** button.





a. In the Name field, enter a name for the routes i.e. Outbound SIP Trunk
b. Under Pattern field select the pattern "81*"
c. Under Route field select the route "SIParator B2BUA" just created
d. Under Active select the button to enable with a check mark.

10. Click save which will return back to the Routes screen where the route "Aspect" should now be displayed

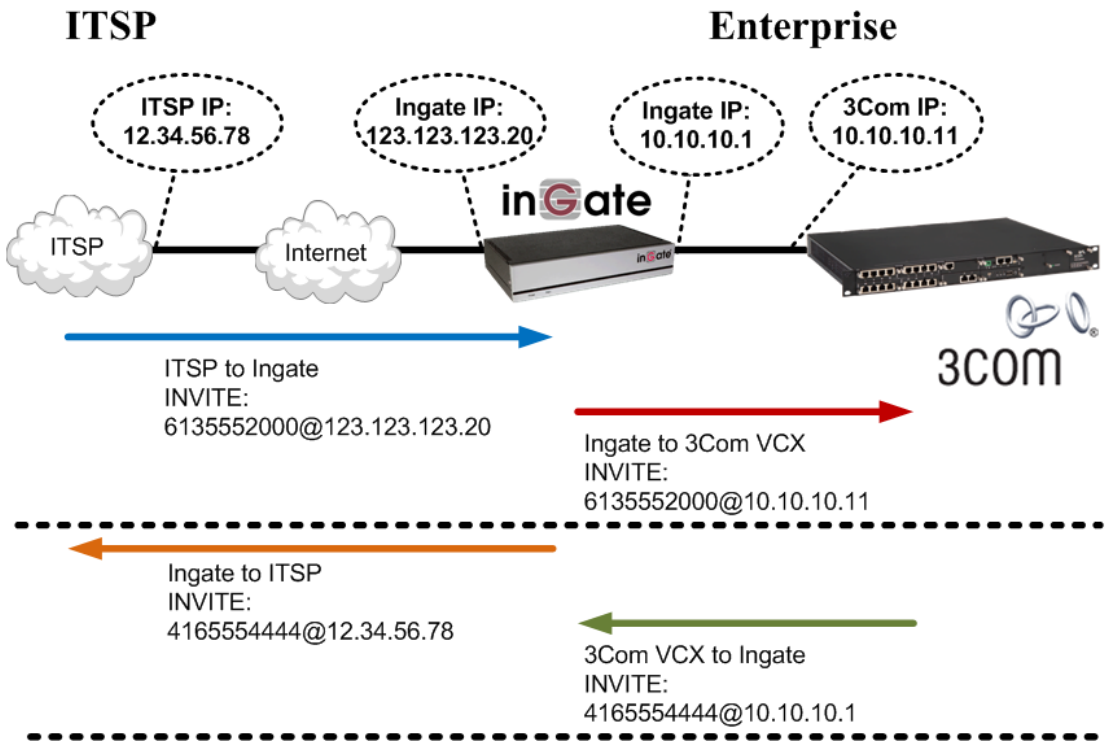


6 Troubleshooting

6.1 Ingate – 3Com VCX Connect Calling

The incoming 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_3Com".

The outgoing call starts at the 3Com, they will deliver a PSTN Number, contained in the Request URI header of a SIP INVITE. Typically the ITSP will send an INVITE to the SIP URI address of "PSTN#@LAN_IP_Address_of_Ingate". The Ingate then processes this through the Dial Plan and forwards the INVITE to the SIP URI address "PSTN#@IP_ITSP".



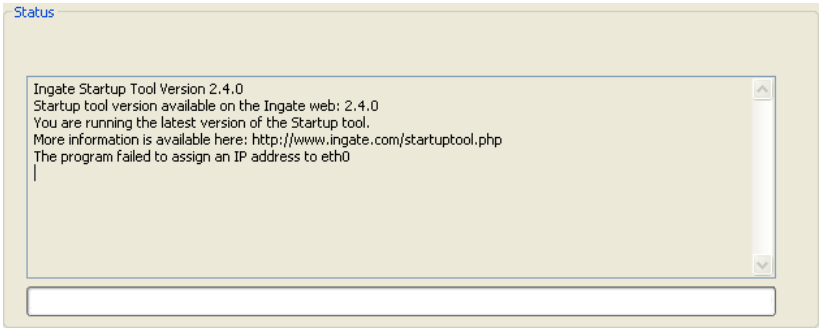
6.2 Startup Tool

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"**.



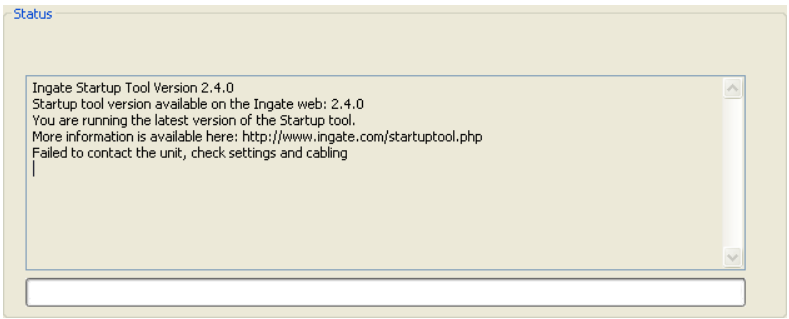
Possible Problems and Resolutions

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…	1) Use the Console Port, please refer to the Reference Guide, section "Installation with a serial cable", and step through the "Basic Configuration". Then you can use the Startup Tool, this time select "Change or Update the Configuration" 2) Factory Default the Database, then try again.

6.2.3 Change or Update Configuration

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

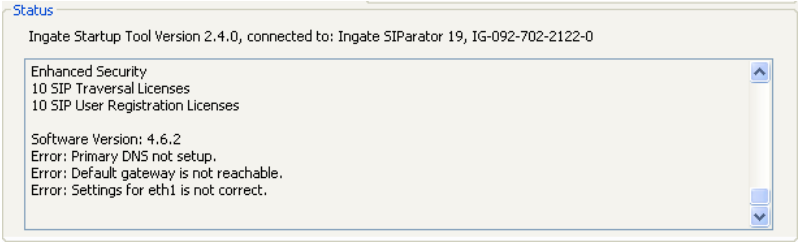


Possible Problems and Resolutions

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…	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.

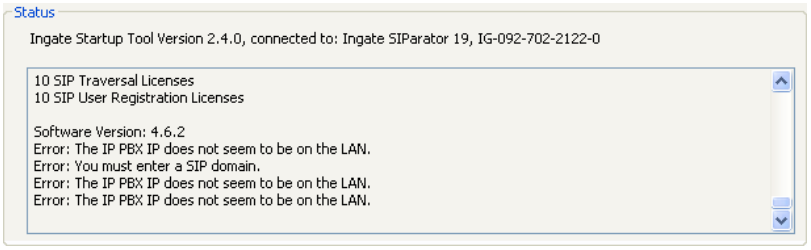


Possible Problems and Resolutions

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.

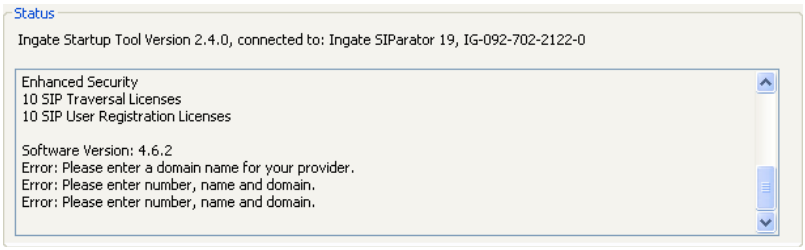


Possible Problems and Resolutions

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.

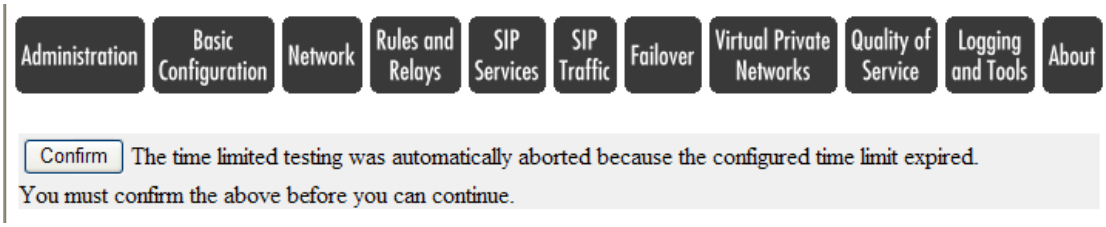


Possible Problems and Resolutions

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 3Com VCX Connect 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 an internal DNS Server to manage internal host names.

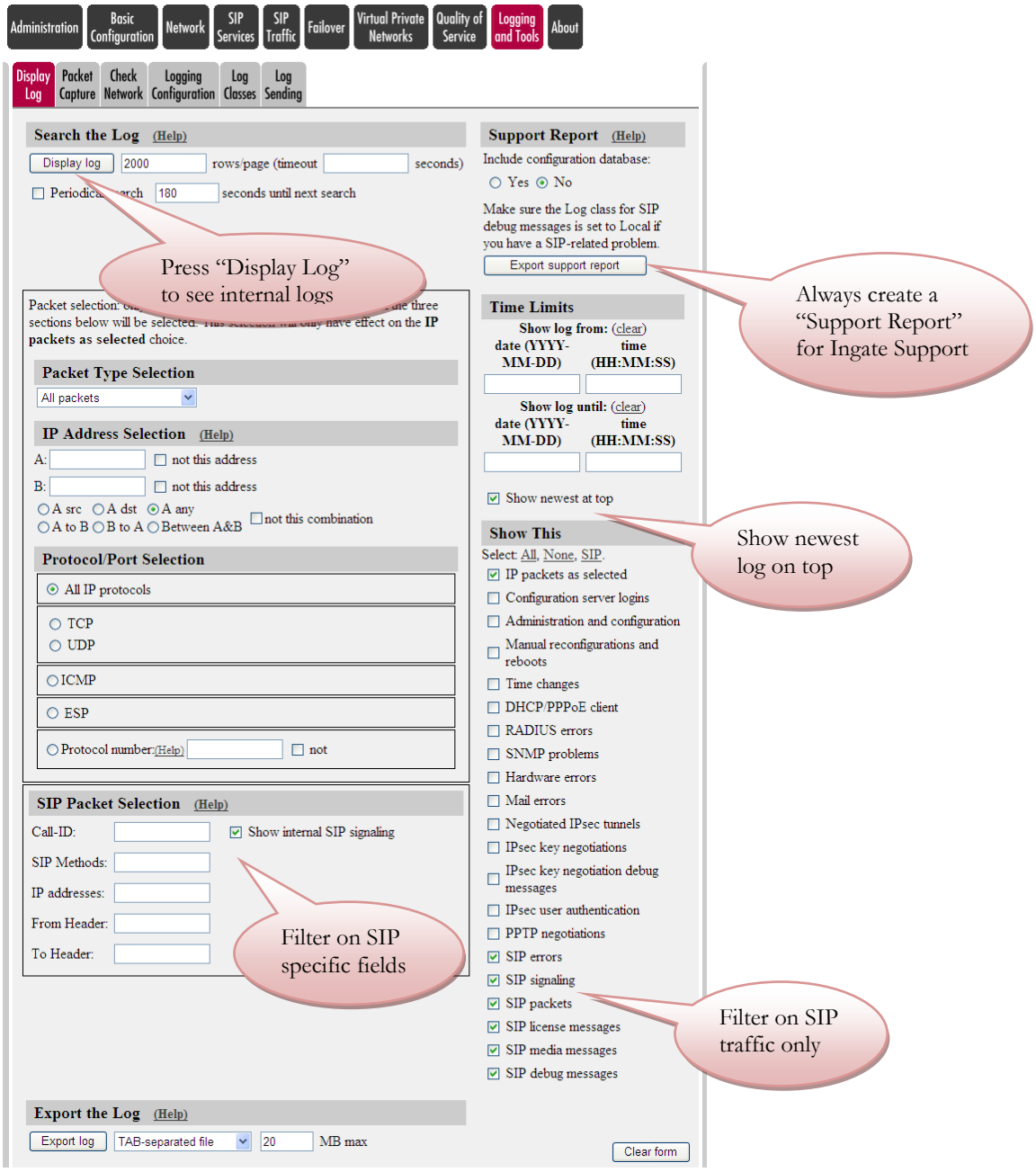
PING tests using a domain is a good test to see if a network can resolve FQDNs.

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

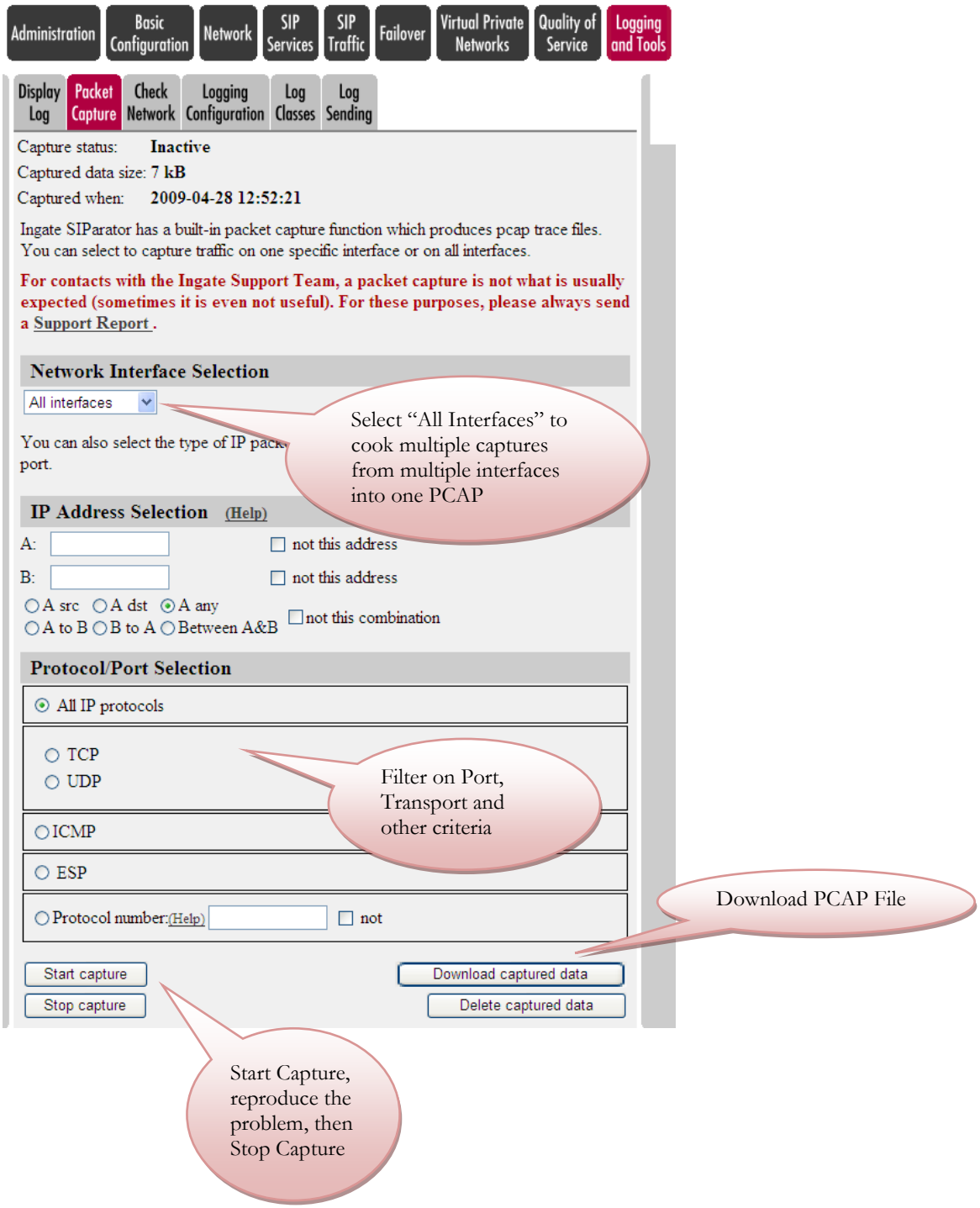
DNS SRV Records
DNS Service Records offer the ability to do Load Balancing and Residency to any SIP Phone deployment. It offers the ability to use one FQDN and break the FQDN into multiple services, one for Web and another for SIP communications.

6.4 Ingate Troubleshooting Tools

6.4.1 Display Logs



6.4.2 Packet Capture



6.4.3 Check Network