Application Note

Avaya QE - Configuration Guide

17 July 2008

Table of Contents

Tested versions: Ingate Firewall and SIParator version 4.6.2
Startup Tool version 2.4.0

Revision History:

Revision	Date	Author	Comments
	2008-07-17	Scott Beer	1st draft

1 Avaya Quick Edition and Ingate Products

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 Avaya QE as the IP-PBX and a SIP Trunking service provider of your choice, and sets up all the routing needed to enable remote users to access and use the Avaya QE solution. Thanks to detailed interoperability testing, Ingate has been able to create this tool with pre-configured set ups for the Avaya QE and various 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/startuptool.php

Avaya Quick Edition is a simple yet sophisticated phone system for small businesses or small branch offices of enterprises. It delivers big business communications capabilities - including a host of call handling and mobility features, voicemail, and auto attendants - to help small offices work more efficiently and serve customers better. With Quick Edition, all the intelligence is built into the phones, simplifying set-up and ongoing management.

Look for the Avaya ONE-X Quick Edition Icon 

to focus your attention to specific Avaya QE setup instructions. These instructions are specific to the Ingate & Avaya QE deployment.

2 Connecting the Ingate Firewall/SIParator

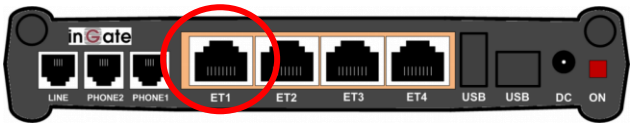
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

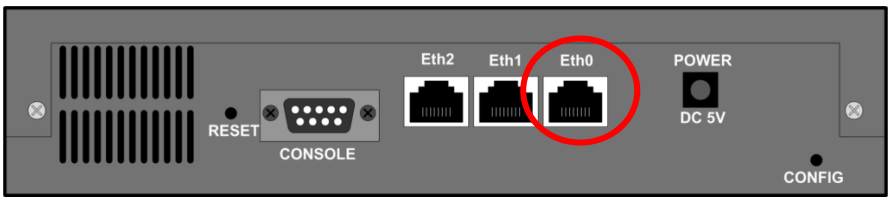
Configuration Steps:

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".

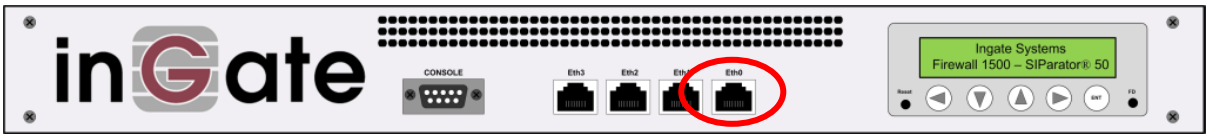
Ingate SIParator SBE (Back)



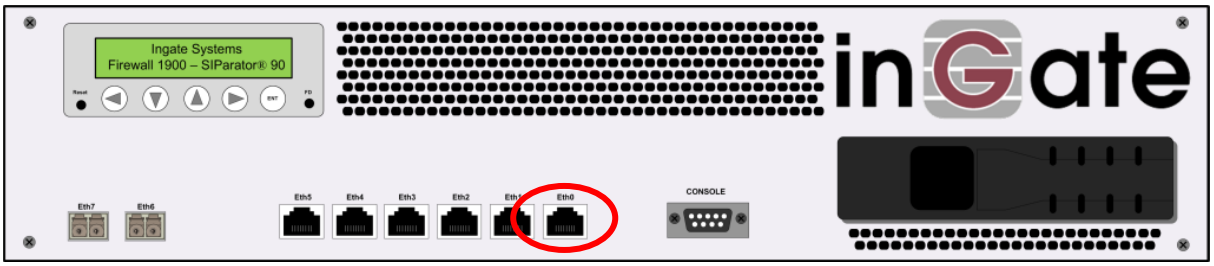
Ingate 1190 Firewall and SIParator 19 (Back)



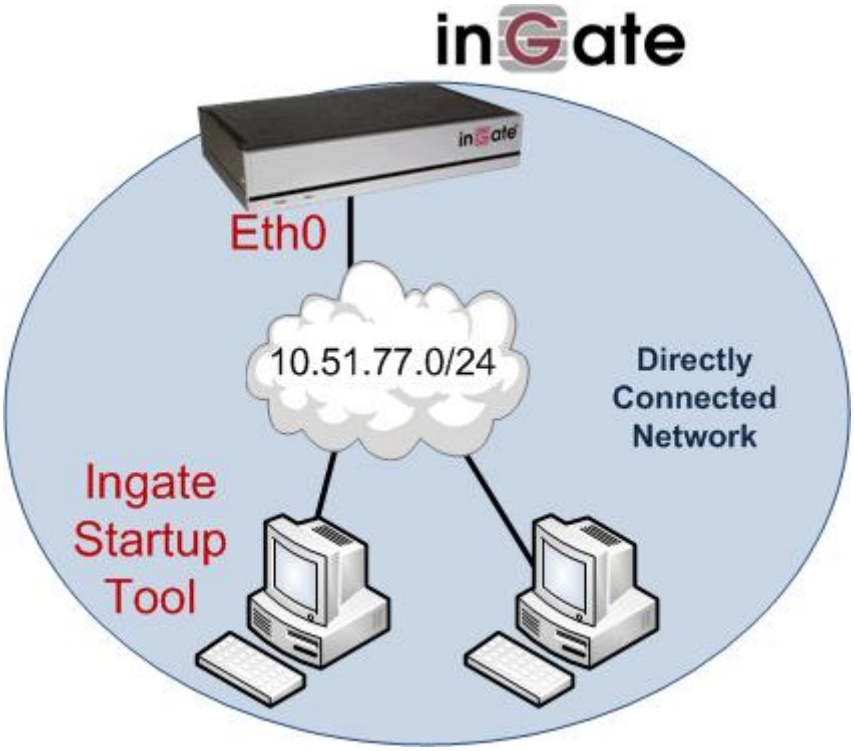
Ingate 1500/1550/1650 Firewall and SIParator 50/55/65



Ingate 1900 Firewall and SIParator 90



3) The PC/Server with the Startup Tool should be located on the same LAN segment/subnet. Preferably 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.



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

3 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.

3.1 Configure the Unit for the First Time

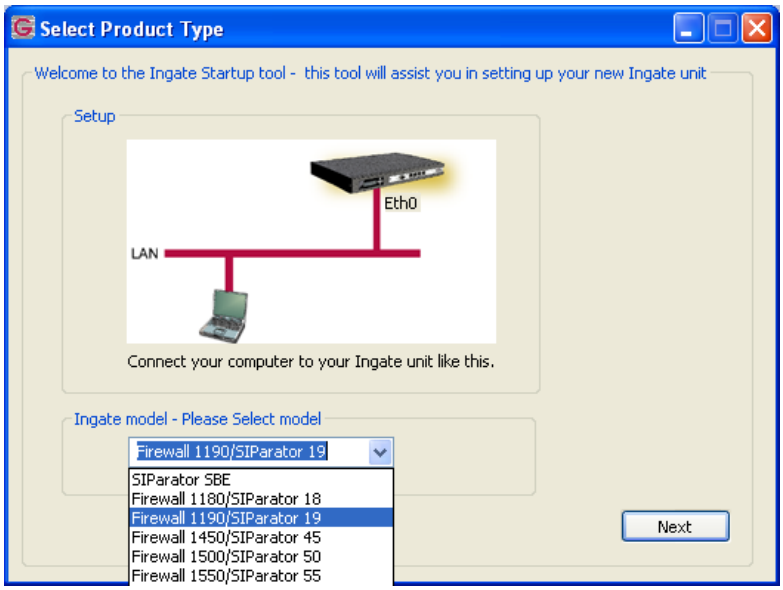
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

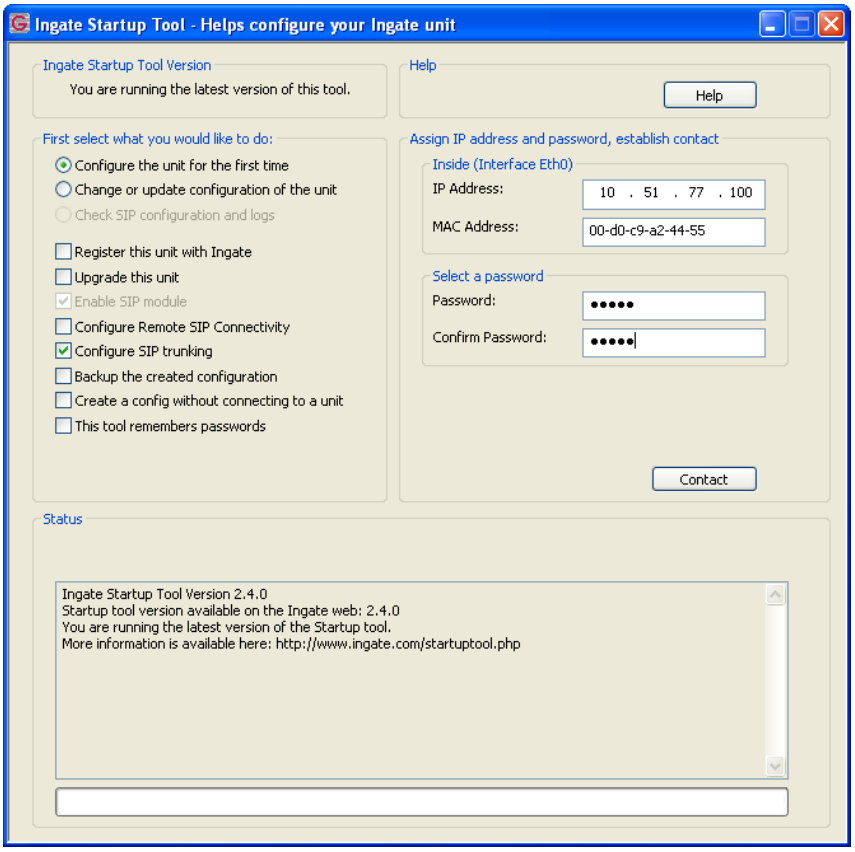
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: "Change or Update Configuration".

Configuration Steps:

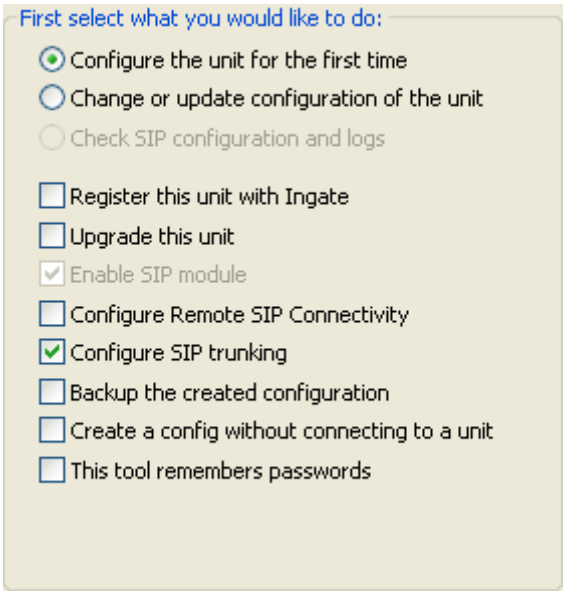
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



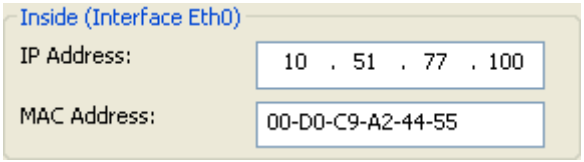
4) Other Options in the "Select first what you would like to do",



a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

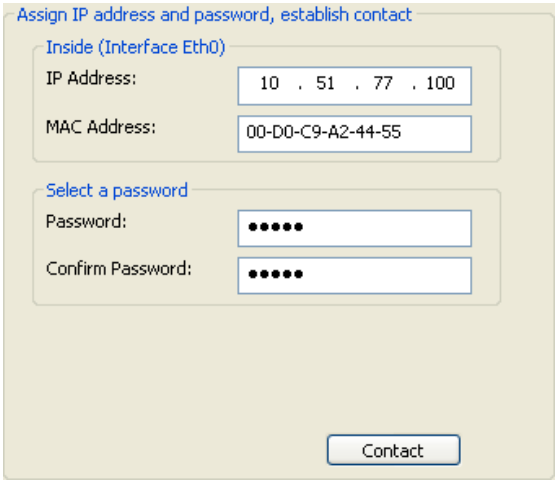
c. Select "Register this unit with Ingate" if you want the tool to connect with www.ingate.com to register the unit. If selected, see Section 4.3: Licenses and Upgrades.
d. Select "Upgrade this unit" if you want the tool to connect with www.ingate.com to download the latest software release and upgrade the unit. If selected, see Section 4.3: Licenses and Upgrades.
e. Select "Backup the created configuration" if you want the tool to apply the settings to an Ingate unit and save the config file.
f. Select "Creating a config without connecting to a unit" if you want the tool to just create a config file.
g. 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.



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 4.4: Network Topology.

3.2 Change or Update Configuration

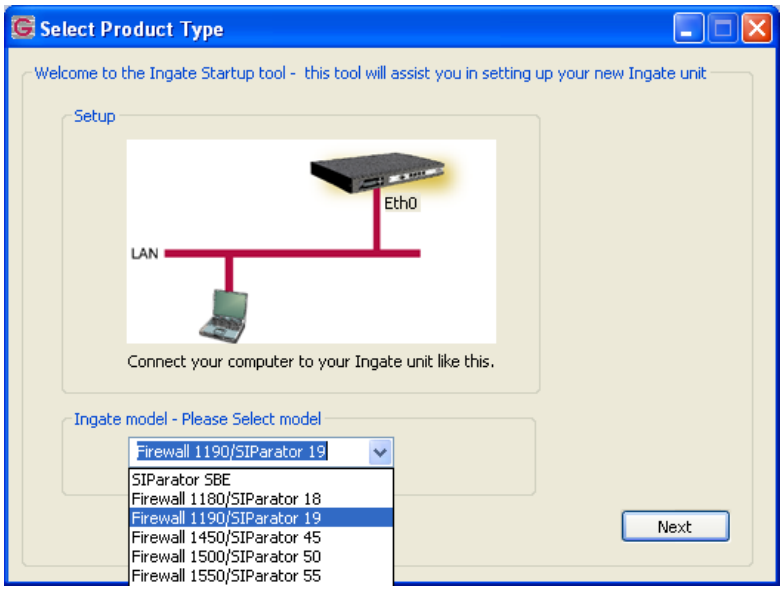
The "Change or update configuration of the unit" setting in the Startup Tool, the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

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.

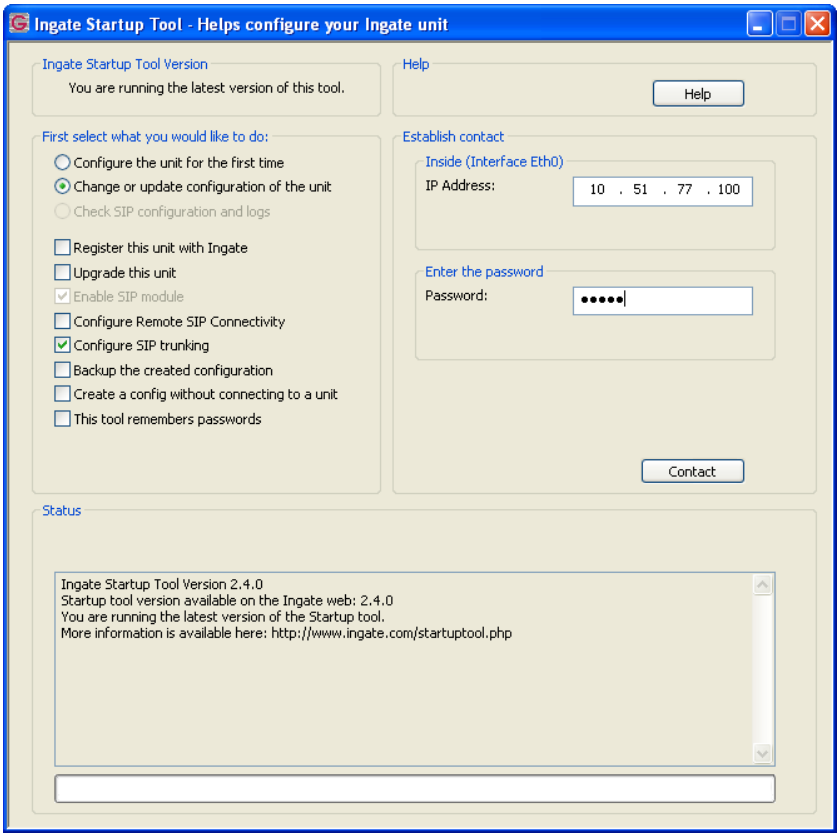
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: "Configure the Unit for the First Time".

Configuration Steps:

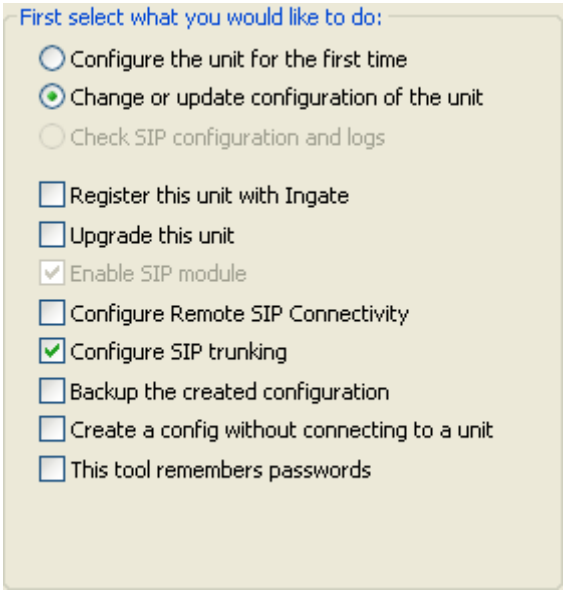
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



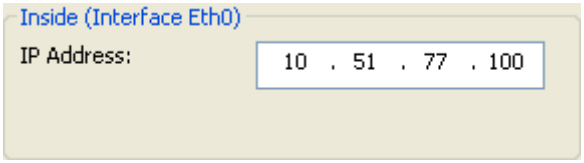
4) Other Options in the "Select first what you would like to do",



a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

c. Select "Register this unit with Ingate" if you want the tool to connect with www.ingate.com to register the unit. If selected, see Section 4.3: Licenses and Upgrades.
d. 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, see Section 4.3: Licenses and Upgrades.
e. Select "Backup the created configuration" if you want the tool to apply the settings to an Ingate unit and save the config file.
f. Select "Creating a config without connecting to a unit" if you want the tool to just create a config file.
g. 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.



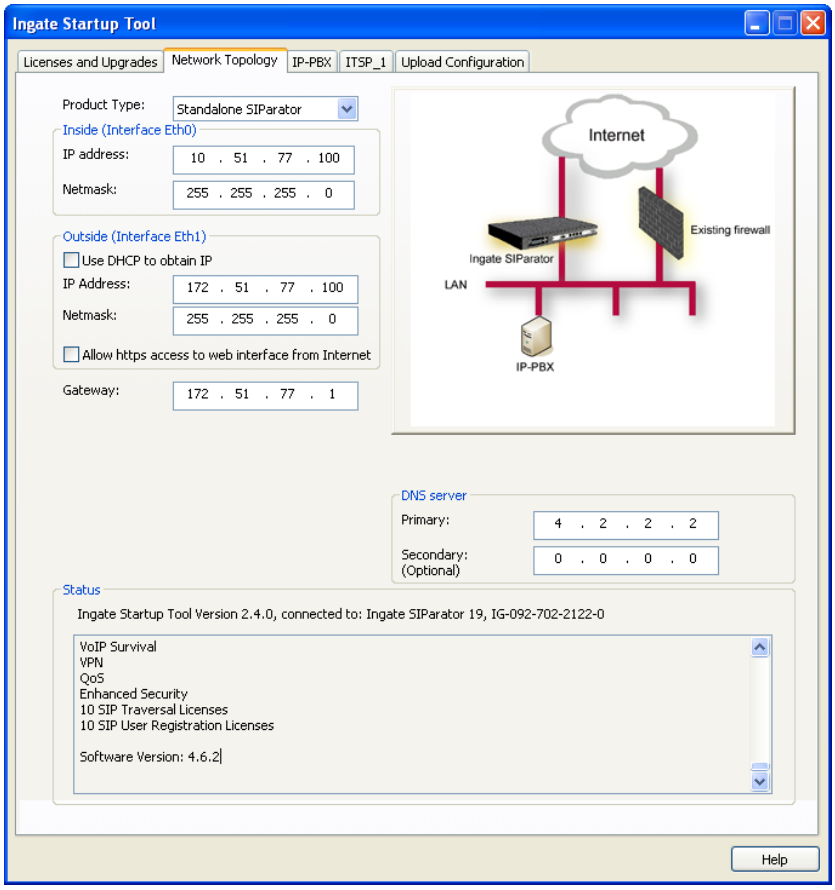
6) In the "Select a Password", enter the Password of the Ingate unit.

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 4.4: Network Topology.

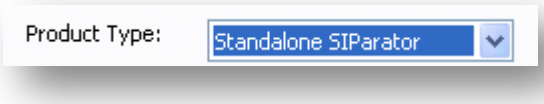
3.3 Network Topology

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.

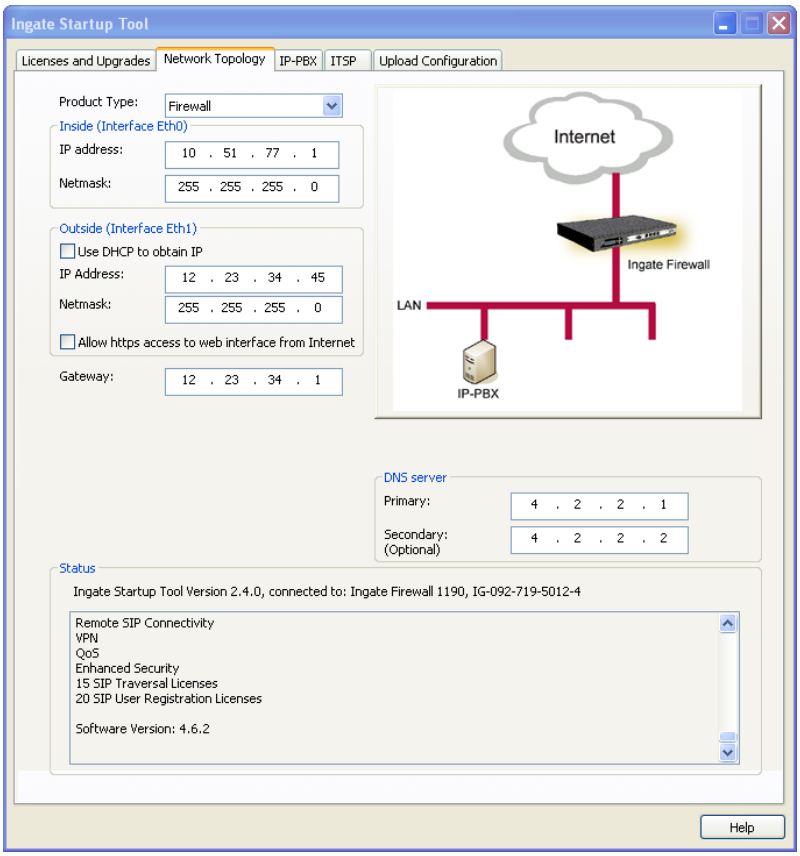


Hint: Match the picture to the network deployment.

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.

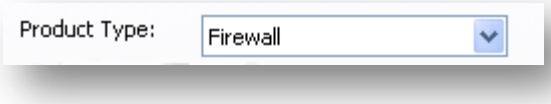
3.3.1 Product Type: Firewall

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.

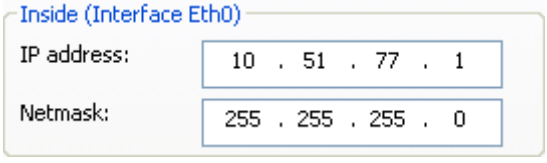


Configuration Steps:

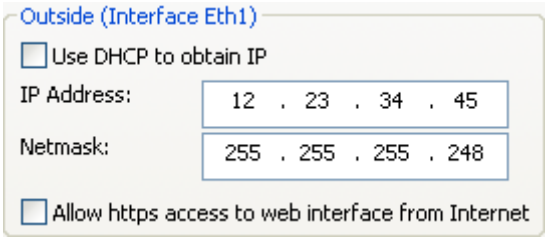
1) In Product Type, select "Firewall".



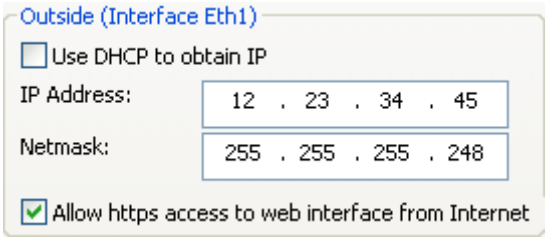
2) Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.



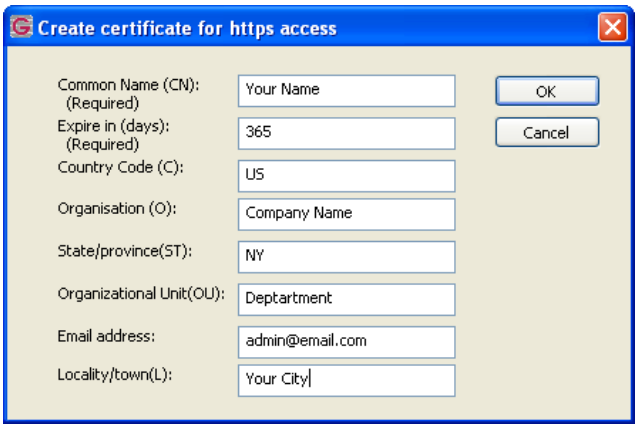
3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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



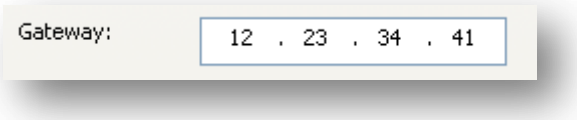
4) **Optional:** To configure Secure Web (https) from the Internet to the Ingate Unit for remote administration,
   a. Select "Allow https access to web interface from Internet"



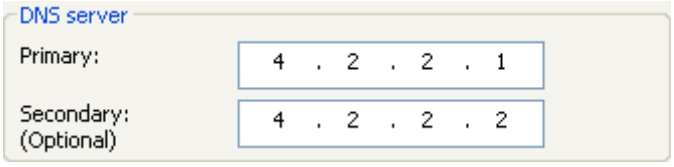
   b. Create a Private Certificate for https access, enter the corresponding information required to generate a certificate.



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).

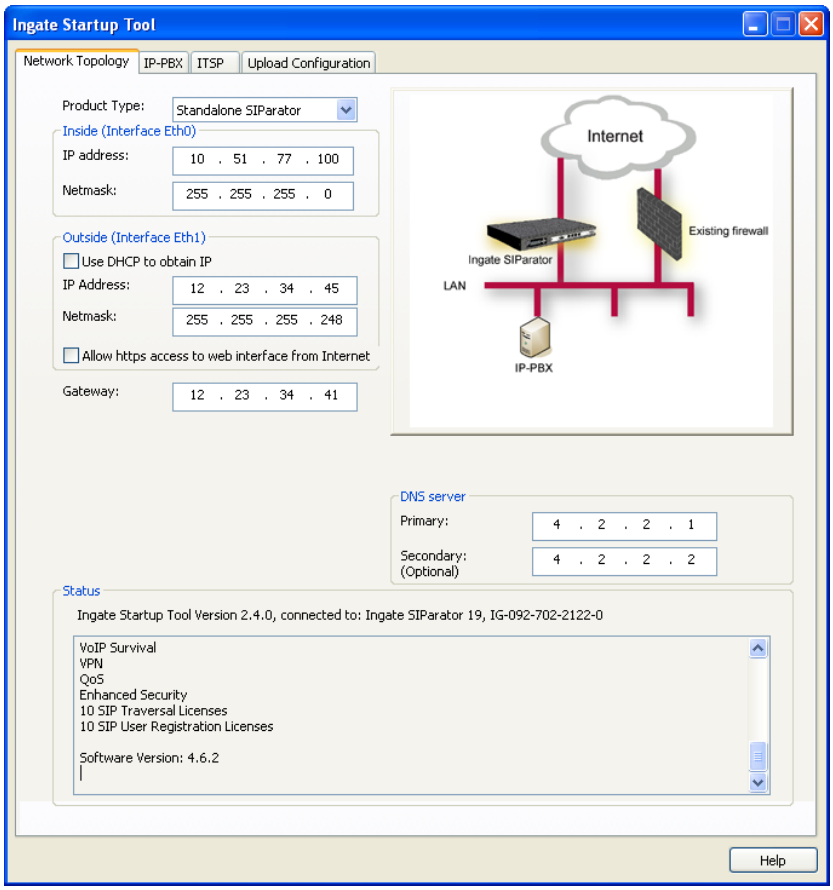


6) Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.



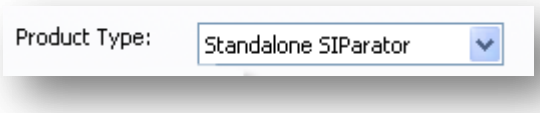
3.3.2 Product Type: Standalone

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.

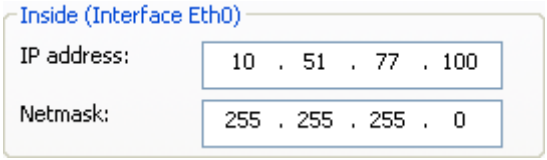


Configuration Steps:

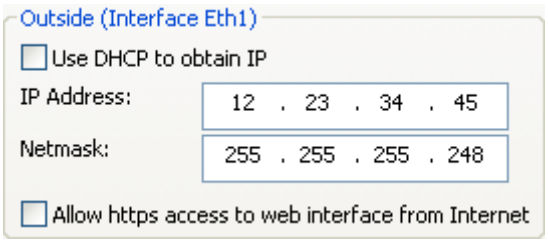
1) In Product Type, select "Standalone SIParator".



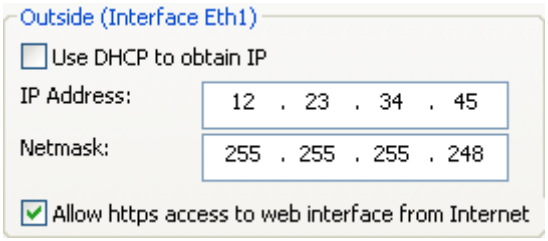
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



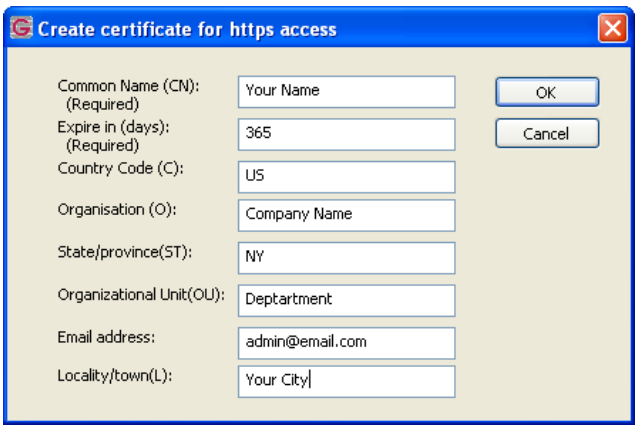
3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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



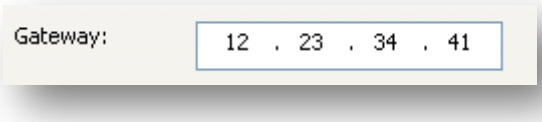
4) **Optional:** To configure Secure Web (https) from the Internet to the Ingate Unit for remote administration,
   c. Select "Allow https access to web interface from Internet"



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



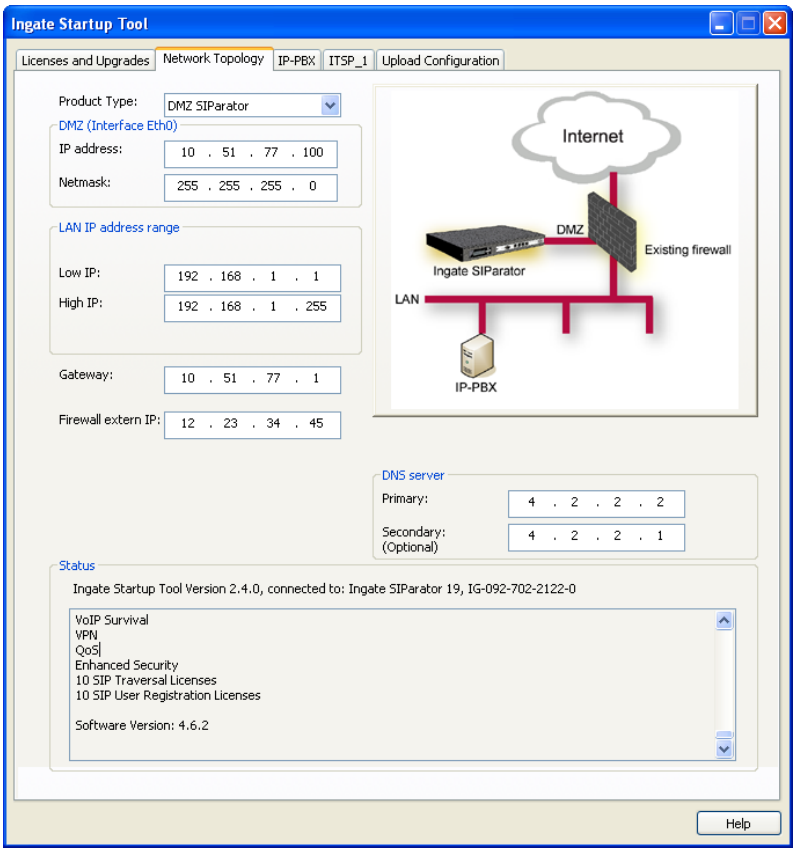
5) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.

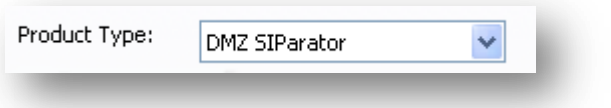
3.3.3 Product Type: DMZ SIParator

When deploying an Ingate SIParator in a DMZ configuration, the Ingate resides on a DMZ network connected to an existing Firewall. 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.

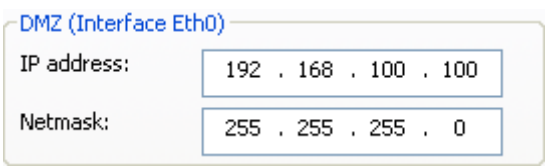


Configuration Steps:

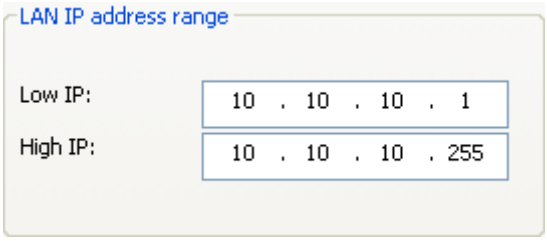
1) In Product Type, select "DMZ SIParator".



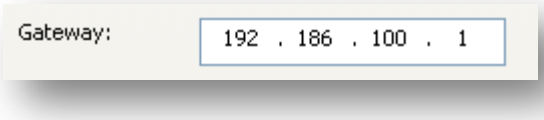
2) Define the IP Address and Netmask of the DMZ (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.



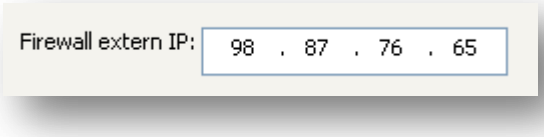
3) Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.



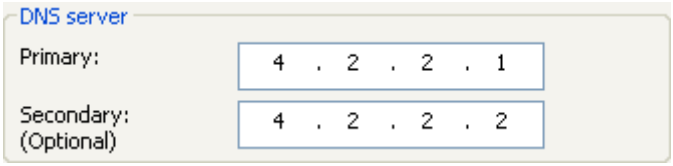
4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.



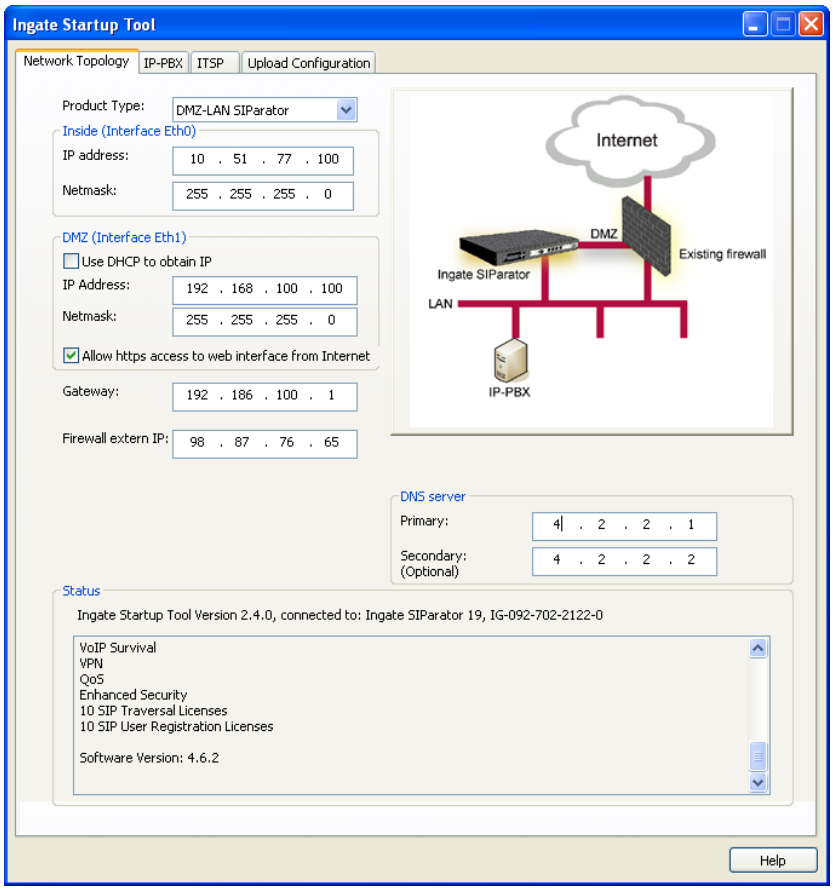
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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.

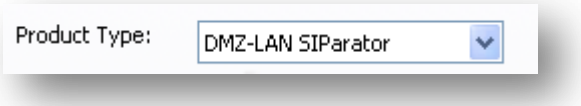
3.3.4 Product Type: DMZ-LAN SIParator

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. 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.

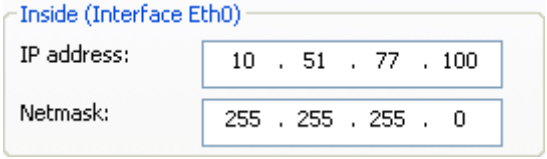


Configuration Steps:

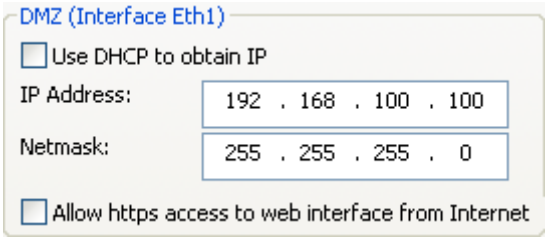
1) In Product Type, select "DMZ SIParator".



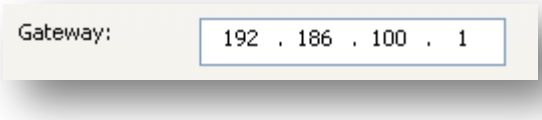
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



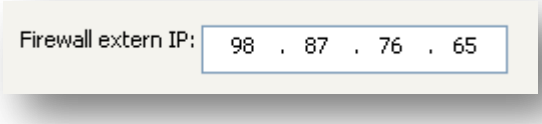
3) Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.
    a. A Static IP Address and Netmask can be entered
    b. Or select "Use DHCP to obtain IP", if you want the Ingate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



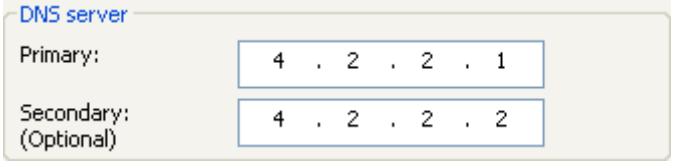
4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.

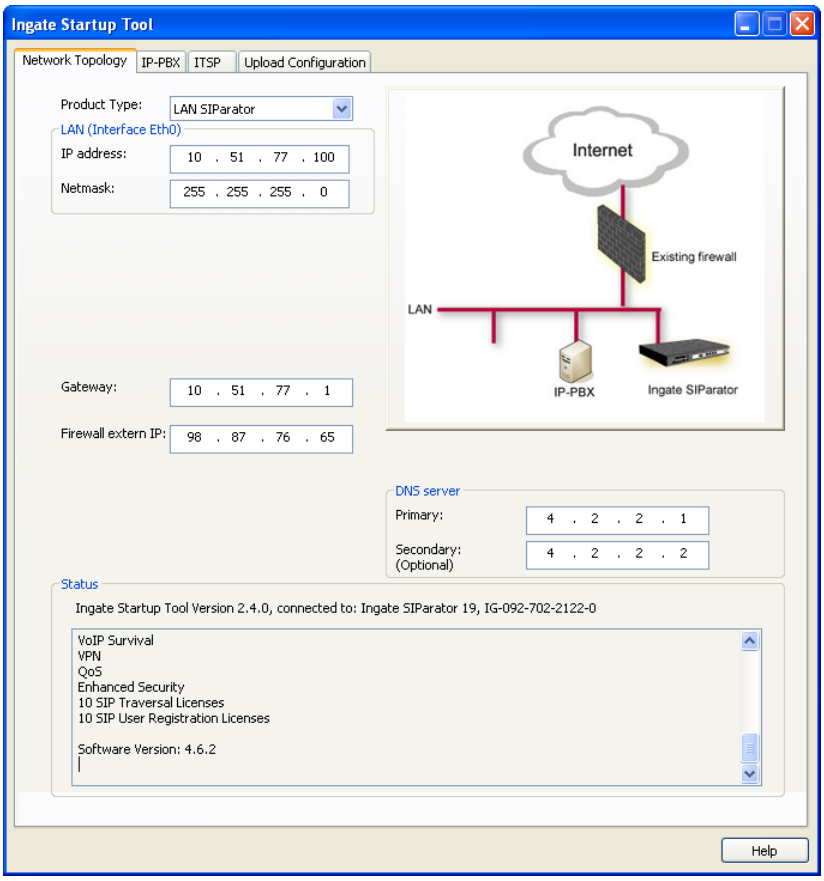


7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

    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

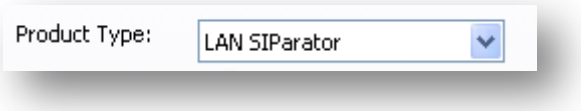
3.3.5 Product Type: LAN SIParator

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.

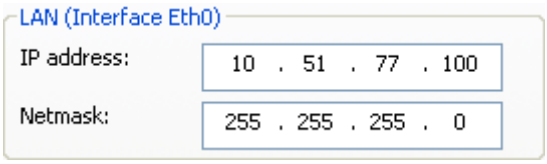


Configuration Steps:

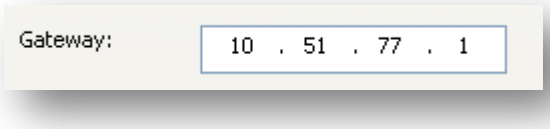
1) In Product Type, select "LAN SIParator".



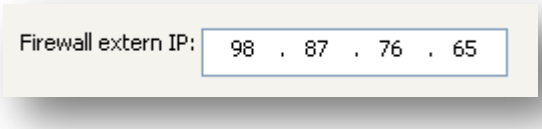
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



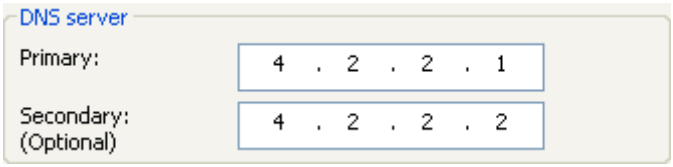
3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.



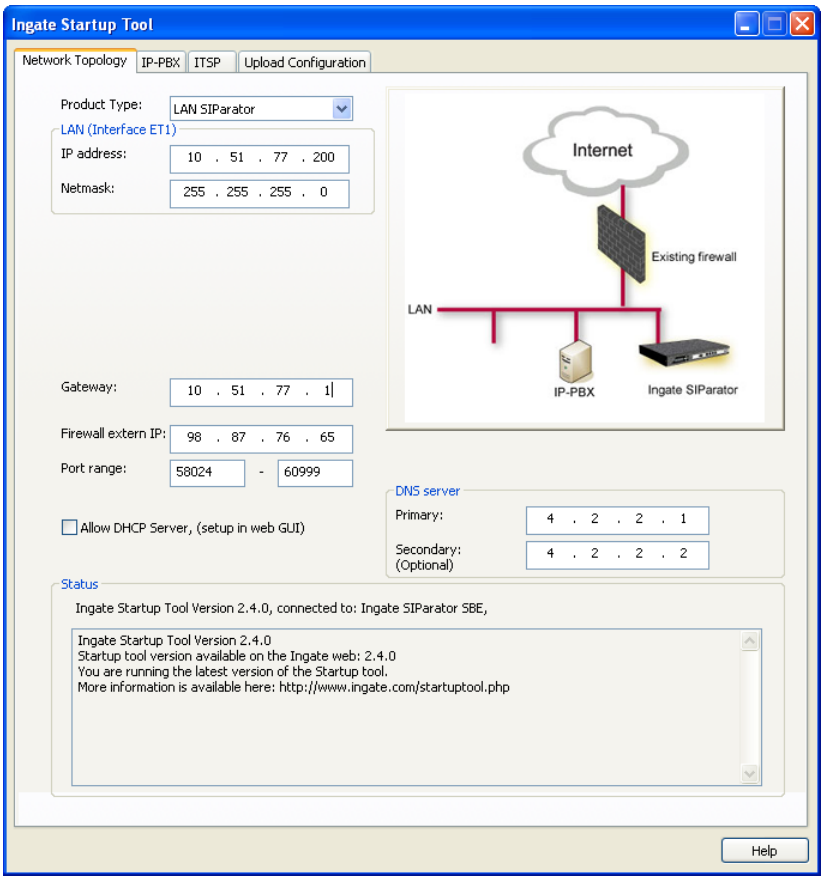
6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

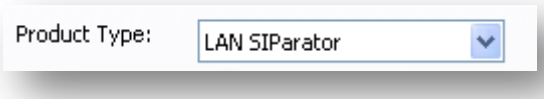
3.3.6 Product Type: LAN SIParator – "*SBE SIParator Only*"

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.

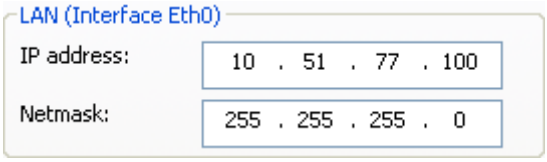


Configuration Steps:

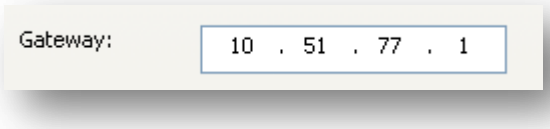
1) In Product Type, select "LAN SIParator".



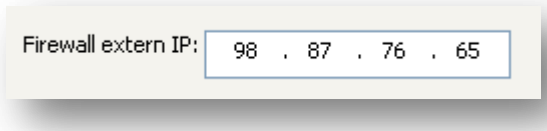
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



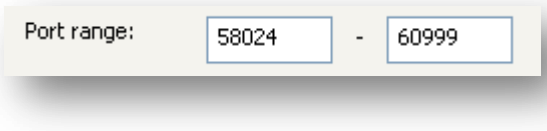
3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



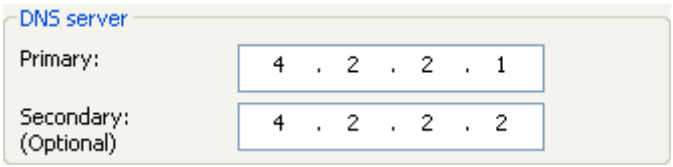
4) Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT.



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.



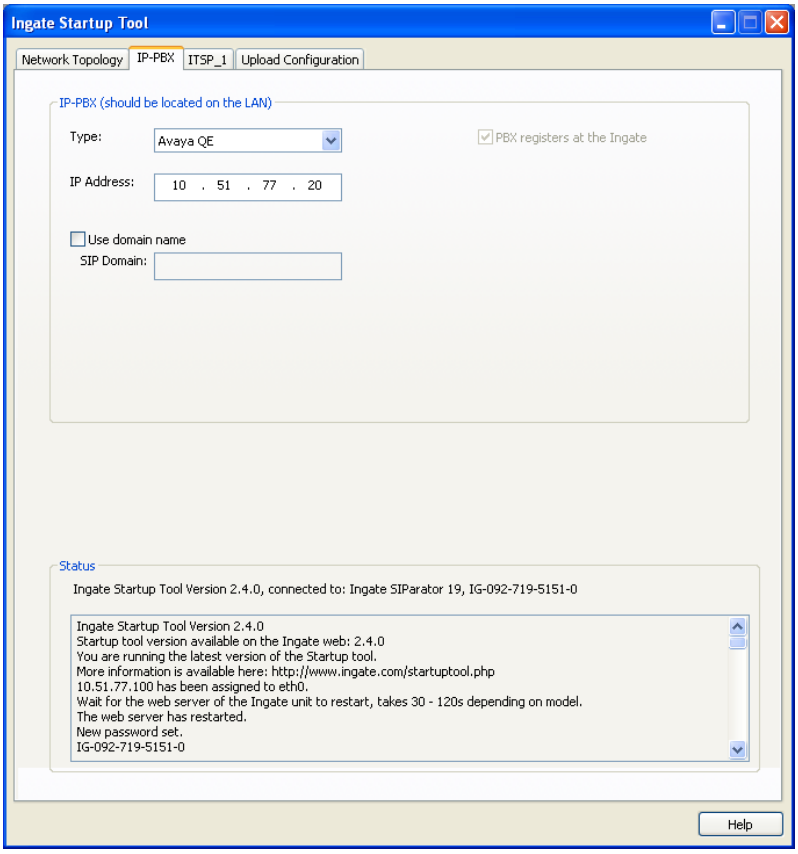
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

3.4 IP-PBX Setup for Avaya QE

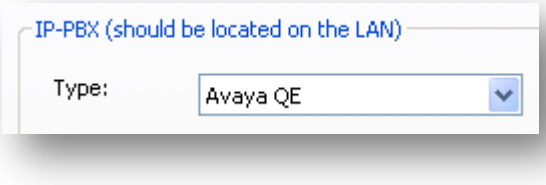
The IP-PBX section is where the IP Addresses and Domain location are provided to the Ingate unit. The configuration of the IP-PBX will allow for the Ingate unit to know the location of the IP-PBX as to direct SIP traffic for the use with SIP Trunking and Remote Phones. The IP Address of the IP-PBX must be on the same network subnet at the IP Address of the inside interface of the Ingate unit. Ingate has confirmed interoperability several of the leading IP-PBX vendors.



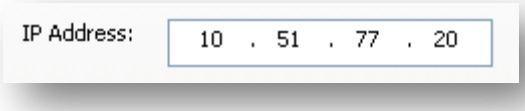
Configuration Steps:

AVAYA one-X™ Quick Edition

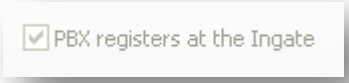
1) In the IP-PBX Type drop down list, select the Avaya QE. Ingate has confirmed interoperability with the Avaya QE solution. The unique requirements of the Avaya QE testing are contained in the Startup Tool.



2) Enter the IP Address of any Avaya QE phone. The IP Address should be on the same LAN subnet as the Ingate unit.

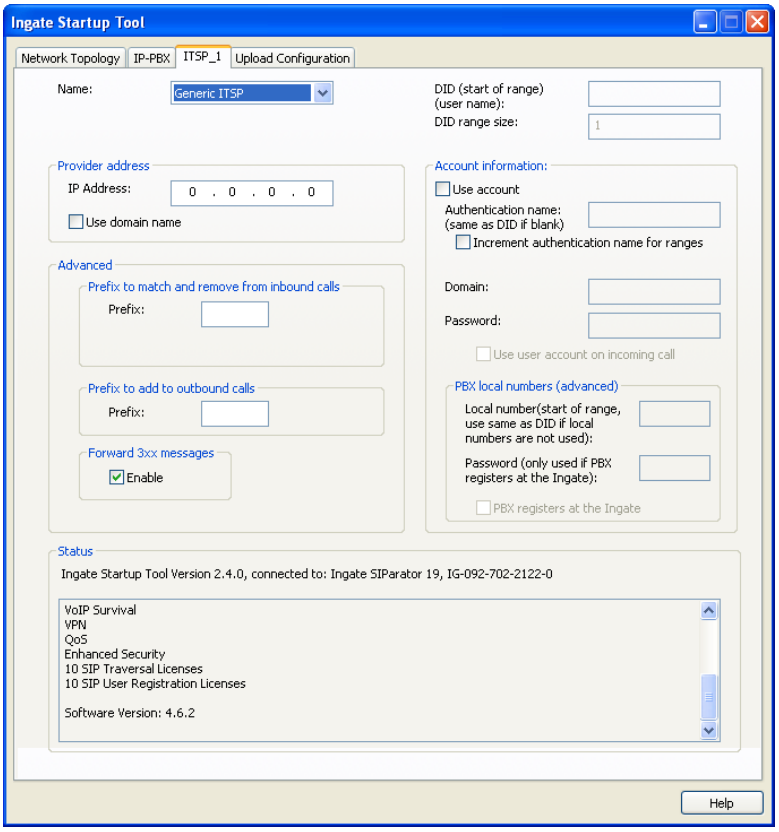


3) When Avaya QE is selected as the IP-PBX type, then the option "PBX registers at the Ingate" is automatically selected. When is option is enabled, the Ingate Registrar is enabled, later on the ITSP configuration, Avaya QE Identities are assigned on the Registrar and associated to the incoming call characteristics. So the Avaya QE registers to the Ingate and the Ingate sends the incoming call to these registered users/identities.



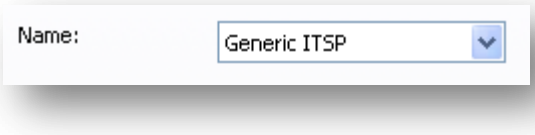
3.5 ITSP for Avaya QE

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:

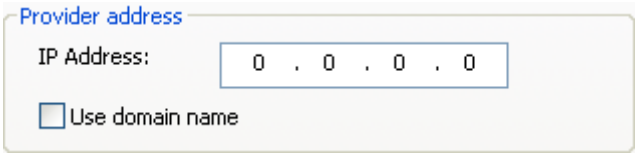
1) In the ITSP drop down list, select the appropriate ITSP vendor. Ingate has confirmed interoperability several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool. If the vendor choice is not seen, select "Generic ITSP".

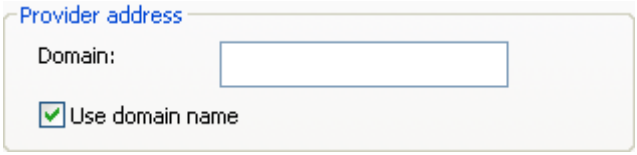


When you select a specific ITSP vendor, the Startup Tool will have the individual connection requirements predefined for that ITSP, the only additional entries may be the specific site requirements.

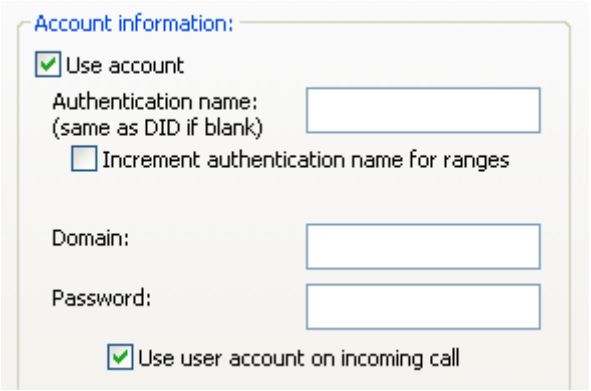
2) Service Providers come in one of two flavors, either they have a trusted IP deployment or they require a Registration account.

   a. In the case where the Service Provider uses a Trusted IP deployment, all which 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.

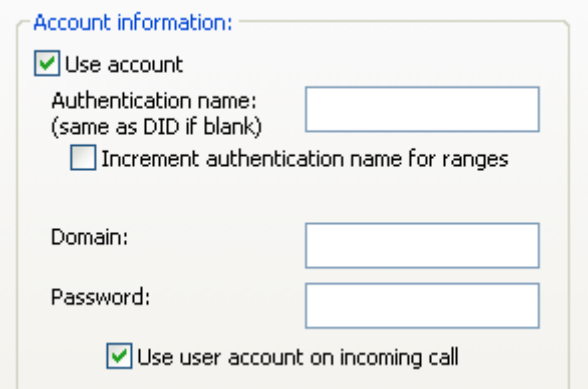




   b. In the case where the Service Provider requires the Ingate to register with the Service Providers SIP Server or SBC, select "Use Account". When "Use Account" is selected, the Registration Account information from the Service Provider is required. Information such as Username/DID, Service Providers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



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

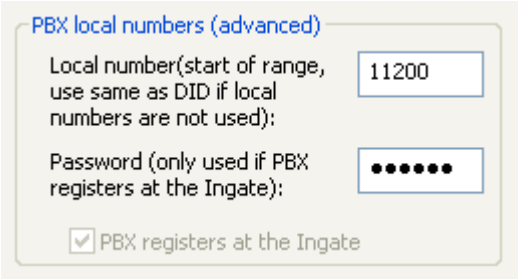


AVAYA one-X™ Quick Edition

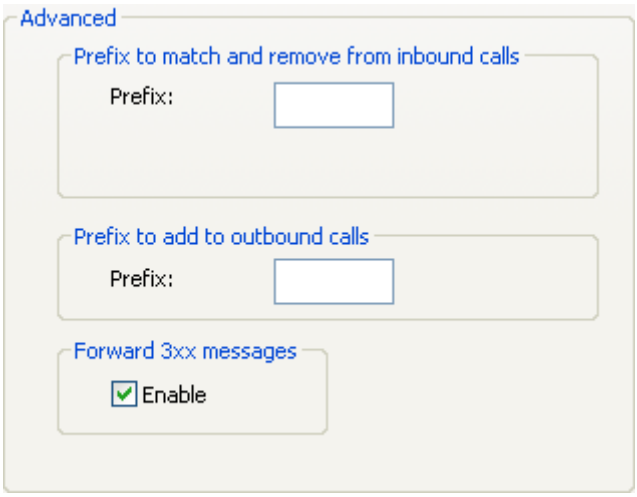
c. Enter a DID (Username) from the Service Provider. These DIDs will be directed from the Ingate to the registration Identities from the Avaya QE. The Startup Tool also has the ability to program a sequential range of DIDs.

AVAYA one-X™ Quick Edition

d. The Avaya QE requires the use of Ingate's Registrar, where the Avaya QE registers Local Identities on the Ingate. The Ingate will direct calls to these registered Identities. Here enter the start of the range of Identity being registered to the Ingate from the Avaya QE.

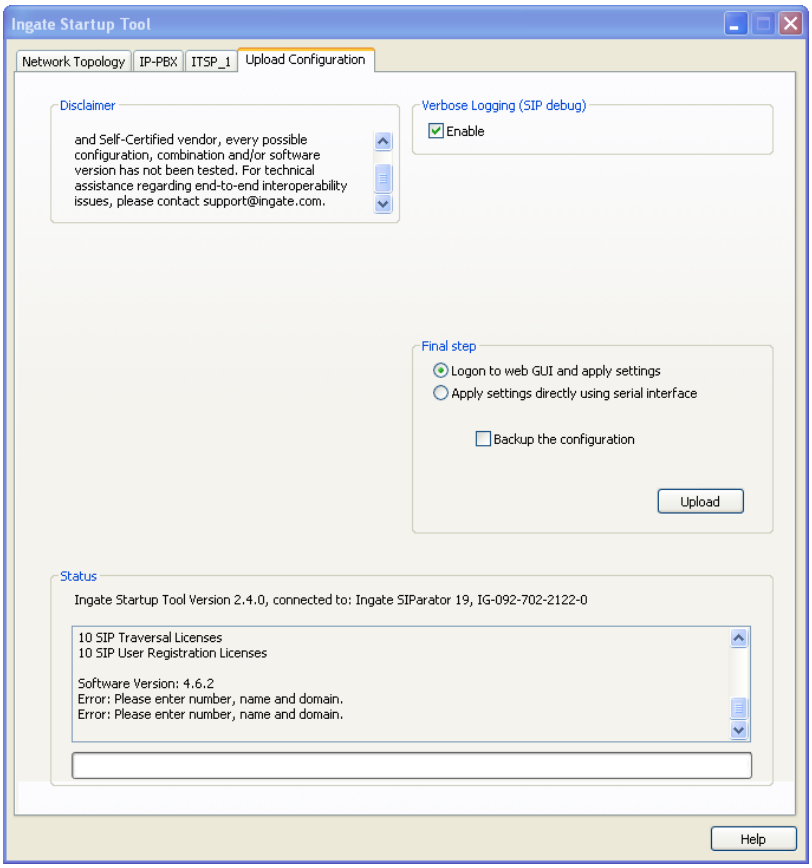


3) The Ingate has the ability to add/remove digits and characters from the Request URI Header. A typical scenario is the addition/removal of ENUM character "+". Many IP-PBX and ITSPs either need to add or remove this character prior to sending or receiving SIP requests. Here you can enter values to Match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



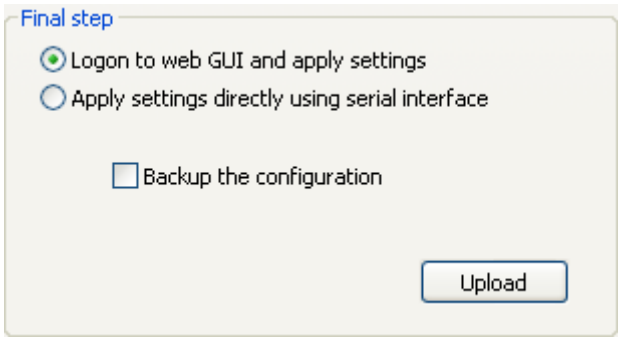
3.6 Upload Configuration

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.

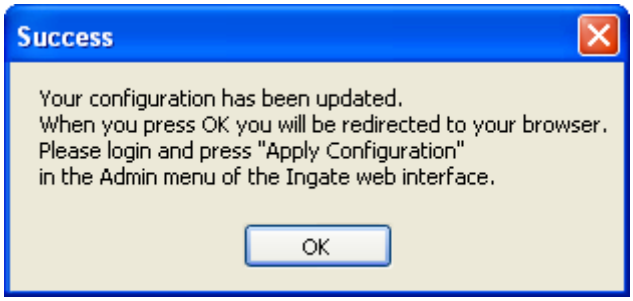


Configuration Steps:

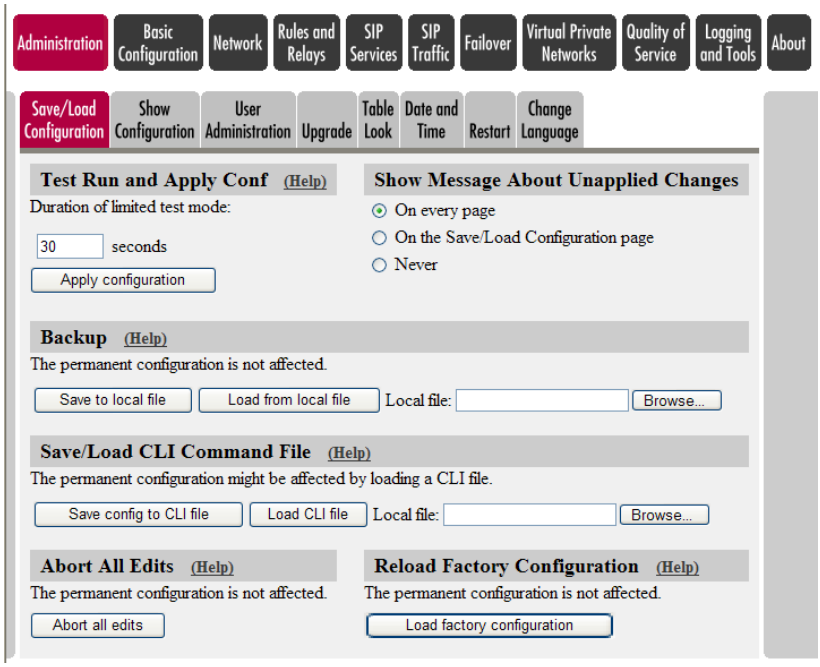
1) Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



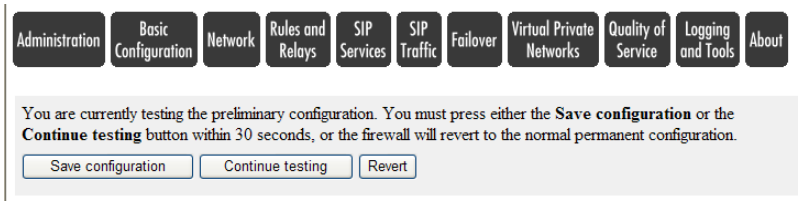
2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



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.



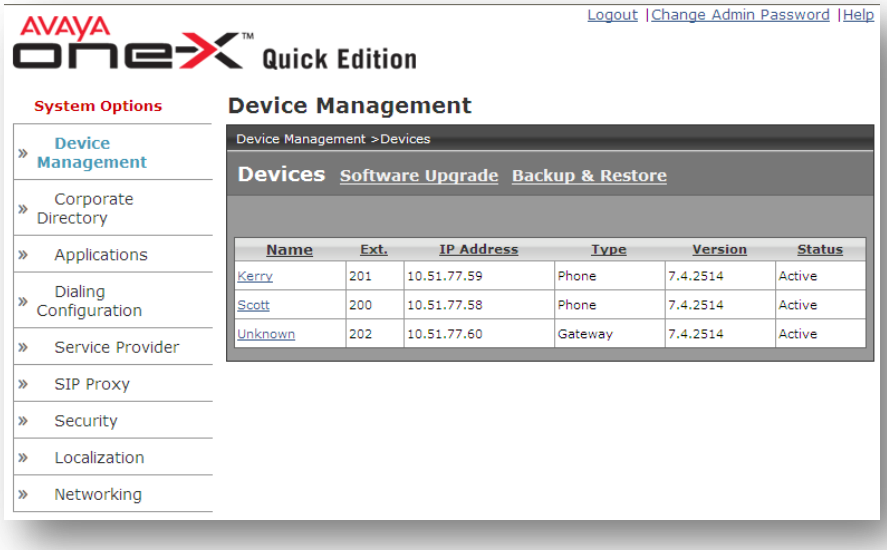
4) A new page will appear after the previous step requesting to save the configuration. Press "Save Configuration" to complete the saving process.



4 Avaya Quick Edition Setup

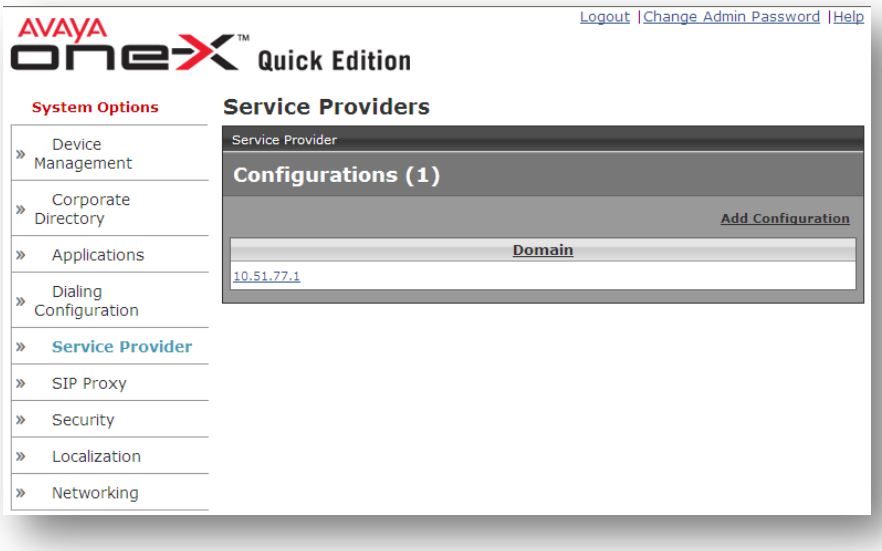
4.1 Device Management

By default the Avaya QE will add devices into the Device Management section as each phone or gateway is connected to the LAN. These are the Extensions of the Avaya QE. Users can call these extensions from their Avaya phones.



4.2 Service Provider

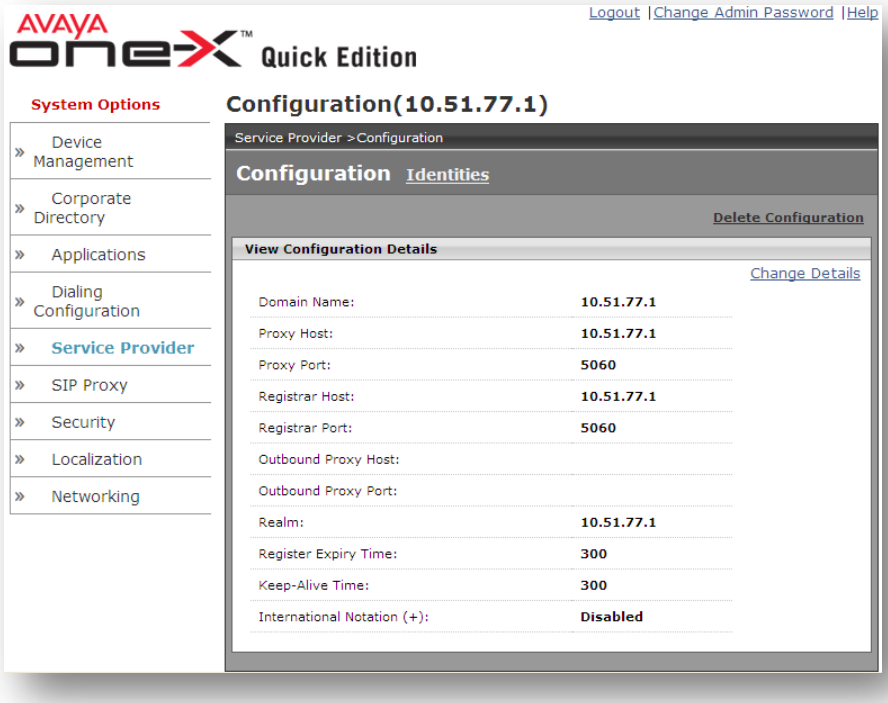
Here is where we add the Ingate Firewall/SIParator information into the Avaya QE.



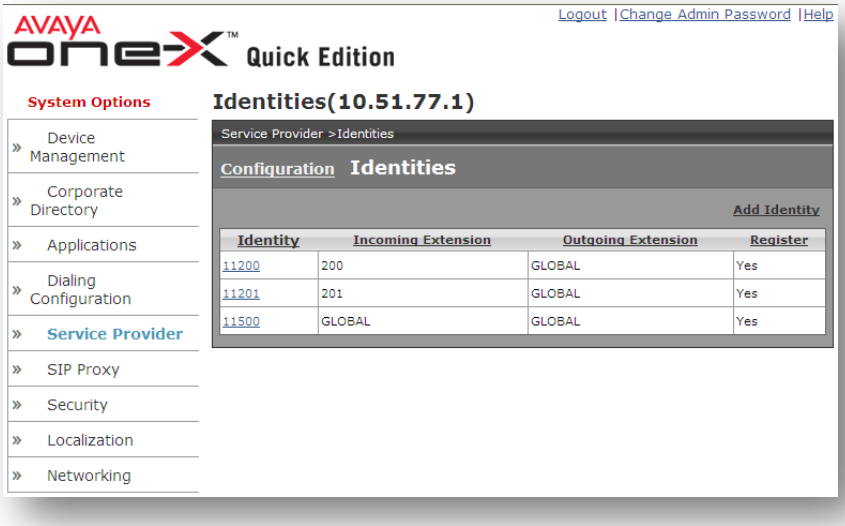
Configuration Steps:

1. In the Service Provider page, press "Add Configuration".

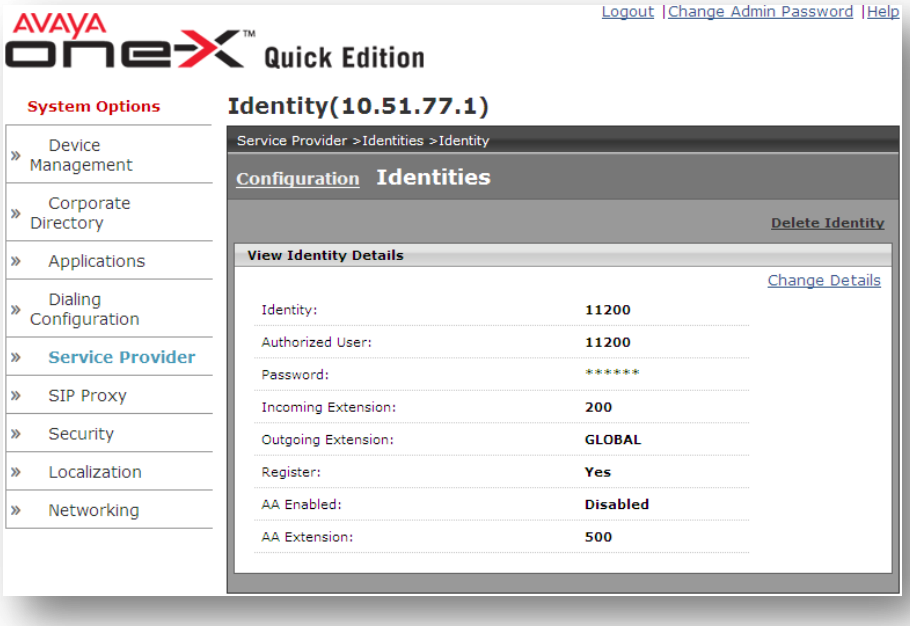
2. Enter the following to configure the Ingate on the Avaya QE:
   a. **Domain Name:** IP Address of the Ingate (or FQDN)
   b. **Proxy Host:** IP Address of the Ingate (or FQDN)
   c. **Proxy Port:** 5060
   d. **Registrar Host:** IP Address of the Ingate (or FQDN)
   e. **Registrar Port:** 5060
   f. **Outbound Proxy Host:** "Blank"
   g. **Outbound Proxy Port:** "Blank"
   h. **Realm:** IP Address of the Ingate (or FQDN)
   i. **Register Expiry Time:** 300 (default)
   j. **Keep-Alive Time:** 300 (default)
   k. **International Notation (+):** Either Disabled or Enabled



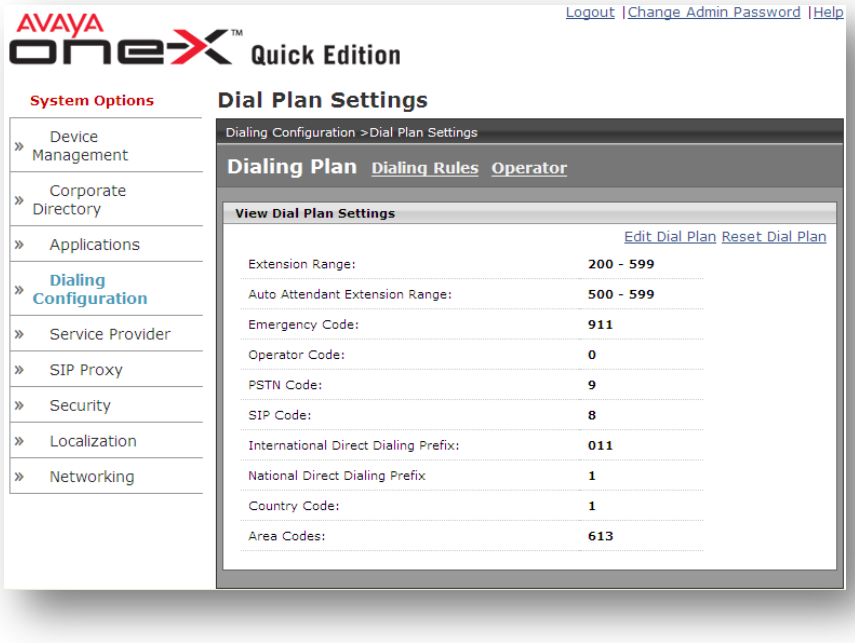
3. Once the Ingate has been added as a Service Provider, Click on "Identities", then "Add Identity".



4. This "Identity" will register to the Ingate and the Avaya QE will associate the identity with an Extension in Device Management. Complete the following:
   a. **Identity:** Enter an Identity that matches the Identity entered in Section 3.5 Configuration Step 2d.
   b. **Authorized User:** Enter the Identity number, same as above.
   c. **Password:** Enter a Password
   d. **Incoming Extension:** Select an Extension from the drop down list, or the Auto Attendant Extension.
   e. **Outgoing Extension:** Select "Global"
   f. **Register:** Select "Yes"
   g. **AA Enabled:** Enable only for Auto Attendant Use, otherwise disable.
   h. **AA Extension:** Select the Auto Attendant Extension number.



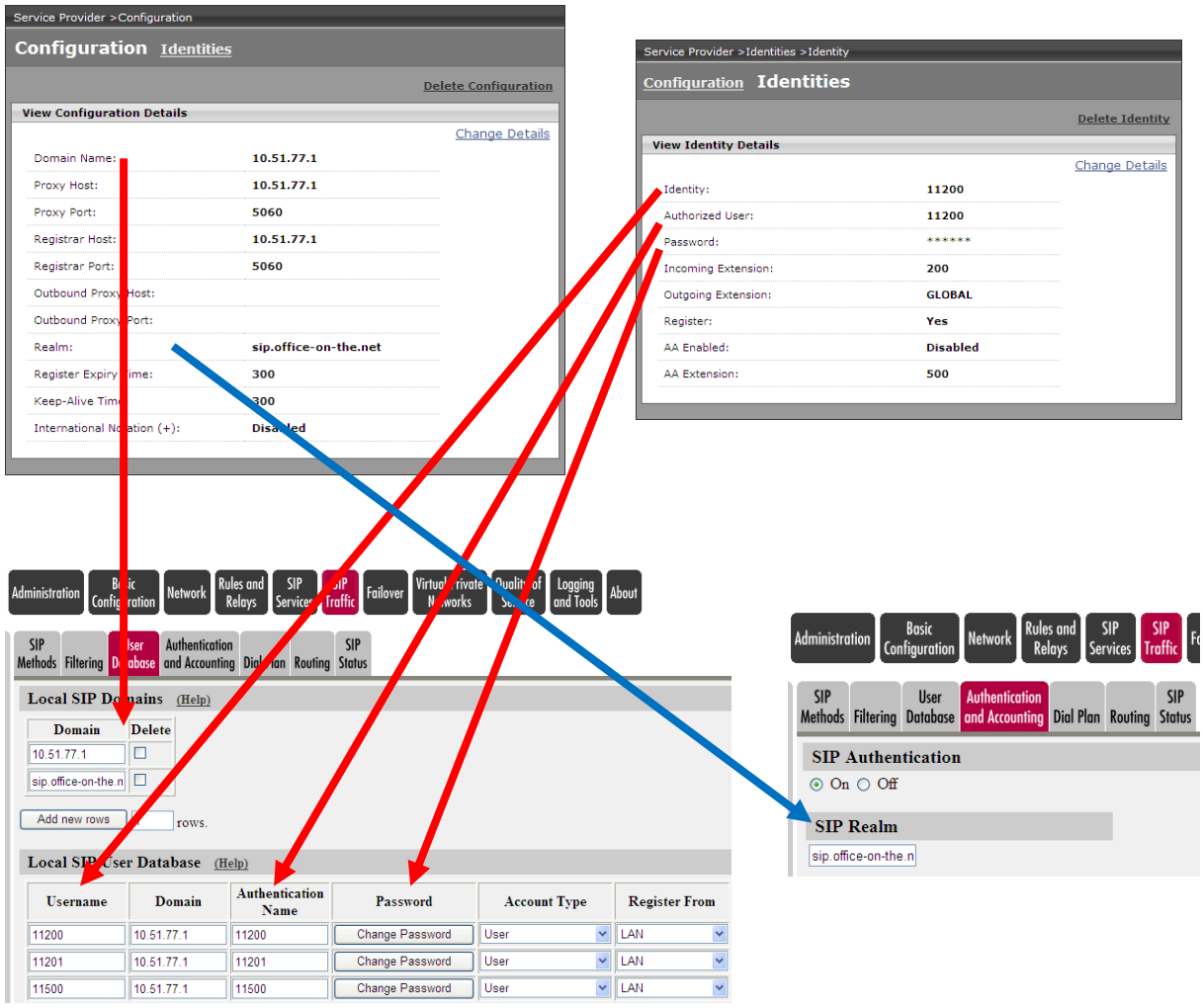
5. Avaya QE Dial Configuration needs no adjustment. Simply, to use the Service Provider, the "8" prefix needs to be dialed from the Avaya phone.



5 Troubleshooting

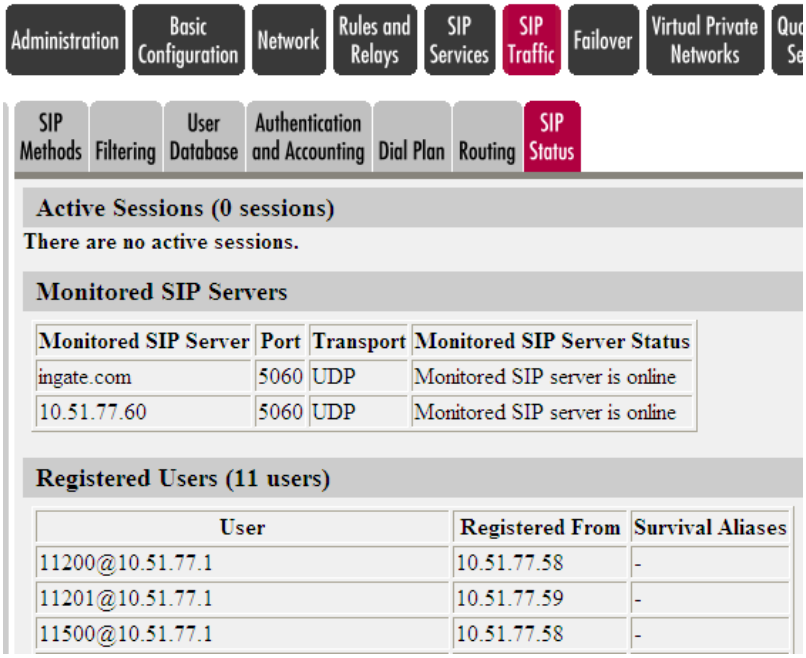
5.1 Avaya QE Identity Registration Information

Here is how the Avaya QE "Identities" register to Ingate's Registrar. The Avaya QE Identities provider Username, Authentication Username, Password and Realm to the Ingate Registrar.



5.2 Registration Status

The successful registration of the Avaya QE Identities can be seen in SIP Traffic -> SIP Status.



5.3 Incoming Routing

Depending on whether the ITSP requirement was for the Ingate to provide Registration or whether the ITSP was a just an IP, depends on whether the Startup Tool creates a Static Registration or a User Routing. For ITSPs that just use IP addresses a Static Route will be created, and if the ITSP requires Registrations, User Routing will be created.

The DID from the ITSP (INVITE Request URI header) will have to match the "Request to User" and then be forwarded to the Registration accounts in the Ingate to route to the Avaya QE.