		APP NOTE
		TPP-10251 Date : September 2010
Product: ShoreTel | Ingate | Skype		**System version:** ShoreTel 10.x

Skype Connect ™ Getting Started Guide

SIP Trunking allows the use of Session Initiation Protocol (SIP) communications from an Internet Telephony Service Provider (ITSP) instead of the typical analog, Basic Rate Interface (BRI), T1 or E1 trunk connections. Having the pure IP trunk to the Internet Telephony Service Provider allows for more control and options over the communication link. This application note provides the details on connecting the ShoreTel IP phone system through an Ingate box which is connected to both the LAN and WAN and acts as a gateway and security device to the ITSP for SIP Trunking.

Table of Contents

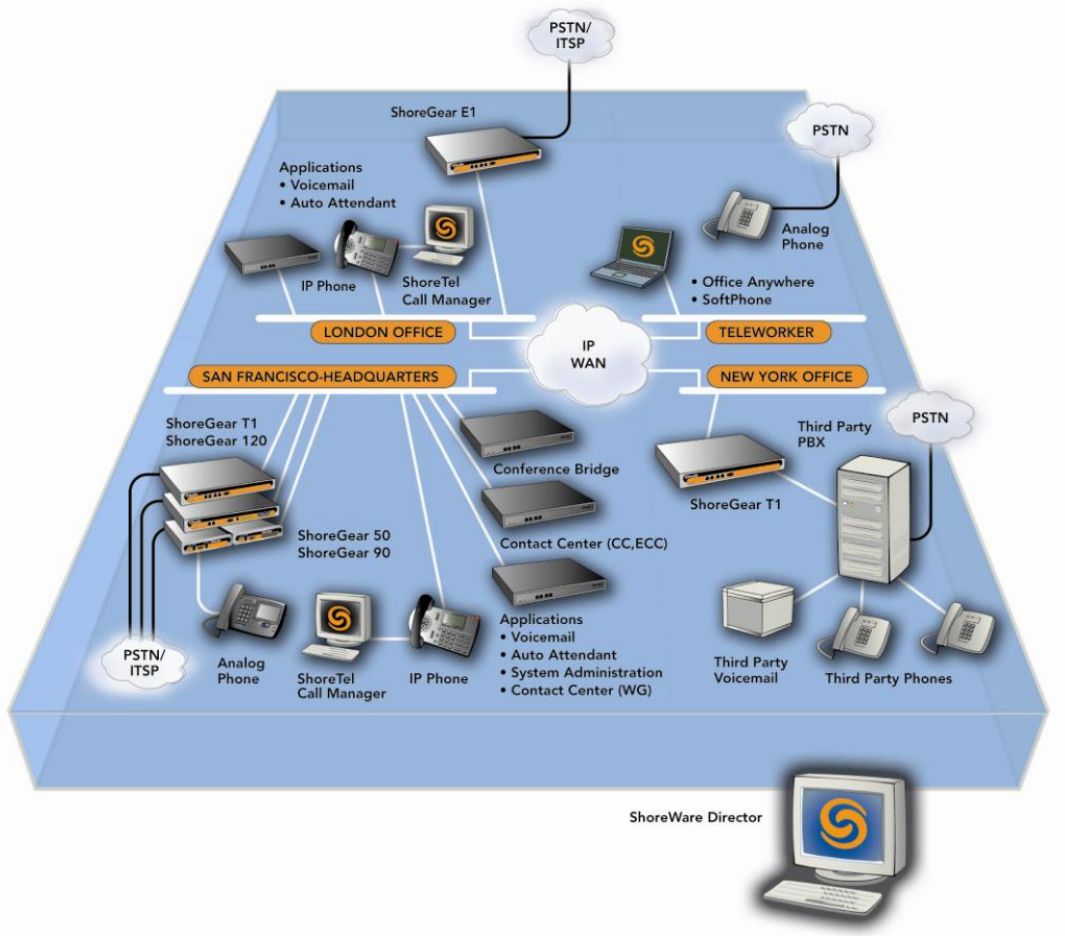
1 INTRODUCTION

This document provides details for connecting the ShoreTel® system through the Ingate SIParator® / Firewall to the ITSP for SIP Trunking to enable audio communications. The document focuses on the network architecture needed to set up these systems to interoperate.

ShoreTel and Ingate have teamed up to build a solid security focused solution, ShoreTel being the IP PBX which sits on the LAN and connects to the Ingate SIParator / Firewall. Providing a solution to allow customers the ability to connect to SIP Trunks offered by different ITSPs in a secure manner is important. The Ingate then is connected to not only the LAN but also the WAN, providing the typical firewall security abilities but also intelligent SIP routing and such SIP features as:

- Registration
- Digest Authentication
- Dial Plan Modification
- Back to Back User Agent (Terminates SIP messaging on both LAN and WAN side)
- Transfer conversion of SIP REFER to SIP reINVITE messaging (critical)
- Quick configuration templates for each of the certified ITSPs

Ingate has two products for this solution, the Ingate Firewall and Ingate SIParator. From a SIP functionality point of view they are basically the same. The Ingate Firewall also provides normal data firewalling functionality and is recommended if the enterprise wants to replace the existing firewall. The Ingate SIParator is the solution for those who want the keep an existing firewall when adopting SIP. In this case the Ingate SIParator will co-exist in parallel with the normal data firewall. The routing of SIP traffic to the Ingate SIParator / Firewall can be accomplished in many ways and each will be discussed in this document.



2 SHORETEL CONFIGURATION

The configuration information below shows examples for configuring both the ShoreTel, Ingate and Skype. Even though configuration requirements can vary from setup to setup, the information provided in these steps, along with the Planning and Installation Guide and documentation provided by Ingate and Skype, should prove to be sufficient. However every design can vary and some may require more planning then others.

2.1 OVERVIEW

2.1.1 Version Support

Products are certified via the Technology Partner Certification Process for the ShoreTel system. Table below contains the matrix of Ingate Firewall and Ingate SIParator versions firmware releases certified on the identified ShoreTel software releases.

	Ingate Firewall and Ingate SIParator version				
	4.5.2	4.6.0	4.6.1	4.6.2	4.6.4
ShoreTel 9.1				✓	
ShoreTel 10.2					✓

2.1.2 ShoreTel / Skype Connect Unsupported Features

At the time of this writing, the following features are not supported, though support will be added in an upcoming future release:

- Fax redirect not supported today via SIP Trunks (though direct Direct Inward Dialing (DID) to fax endpoint is supported)
- Support for p-asserted-id - Skype will check contents of P-ID against Online numbers and caller ID and if there is a mismatch we will strip CLI for outbound calls
- Find Me requires G711
- Inbound / Outbound call with Blocked Caller ID is supported by Skype Manager.
- Emergency, 411 and Operator Assistance is not supported.
- ShoreTel introduces support for Music On Hold (MOH) over SIP trunks. The capacity limits of MOH switches will not change (i.e. a switch will still be capable of providing up to 15 streams). However, these streams can be to other switches or to SIP devices, so customers who were not at the switch capacity limit before may now find themselves testing the limits of the switch capacity.
- If the ShoreTel server has a conference bridge 4.2 installed, you should not enable SIP. The conference bridge is not compatible with a ShoreTel system that has SIP enabled due to the dynamic RTP port required for SIP.
- 3-way conference on a SIP trunk call uses Make Me conference ports. A minimum of 3 Make Me ports must be configured to support 3-way conferencing. Make Me conferencing for 4 to 6 parties is not supported.
- A SIP trunk can be a member of a 3-party conference but cannot initiate a 3-way conference (unless the SIP device merges the media streams itself).

- ShoreTel SIP supports basic transfers (i.e. blind transfers) and attended transfers (i.e. consultative transfers).
- Silent Monitoring is not supported on a SIP trunk call.
- Barge-In is not supported on a SIP trunk call.
- Call recording is not supported on a SIP trunk call. Call recording requires presence of a physical trunk in the call.
- Call redirection by SIP devices is not supported.
- Park/Unpark is not supported on a SIP trunk call. This is planned for a future release.
- Extension Assignment is not supported on SIP trunks. Outbound trunk hunting will automatically avoid SIP trunks when placing the call to the Extension Assignment user. The call to the Extension Assignment user cannot be a SIP trunk; however, the call to the external party can be a SIP trunk.
- Silence detection on trunk-to-trunk transfers is not supported since it requires a physical trunk.
- Fax (and modem) redirection is not supported with SIP trunks as only physical trunks can detect fax tones.
- ShoreTel SIP supports two codecs - G.711 and G.729.
- G.711 SIP devices that do not support RFC 2833 DTMF cannot send DTMF digits to Voicemail (VM) or Auto-Attendants (AA).
- G.729 only SIP devices cannot talk to VM/AA unless they are configured as Teleworkers or configured in remote site.

2.2 SHORETEL CONFIGURATION

This section describes the ShoreTel system configuration to support SIP Trunking. The section is divided into general system settings and trunk configurations (both group and individual) needed to support SIP Trunking.

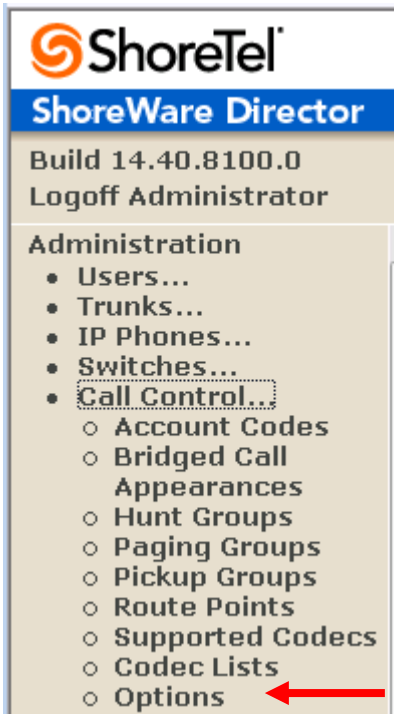
Note: ShoreTel basically just points its Individual SIP Trunks to the Ingate SIParator.

The first settings to address within the ShoreTel system are the general system settings. These configurations include the Call Control, the Site and the Switch settings. If these items have already been configured on the system, skip this section and go on to the "ShoreTel System Settings – Trunk Groups" section below.

2.2.1 Call Control Settings

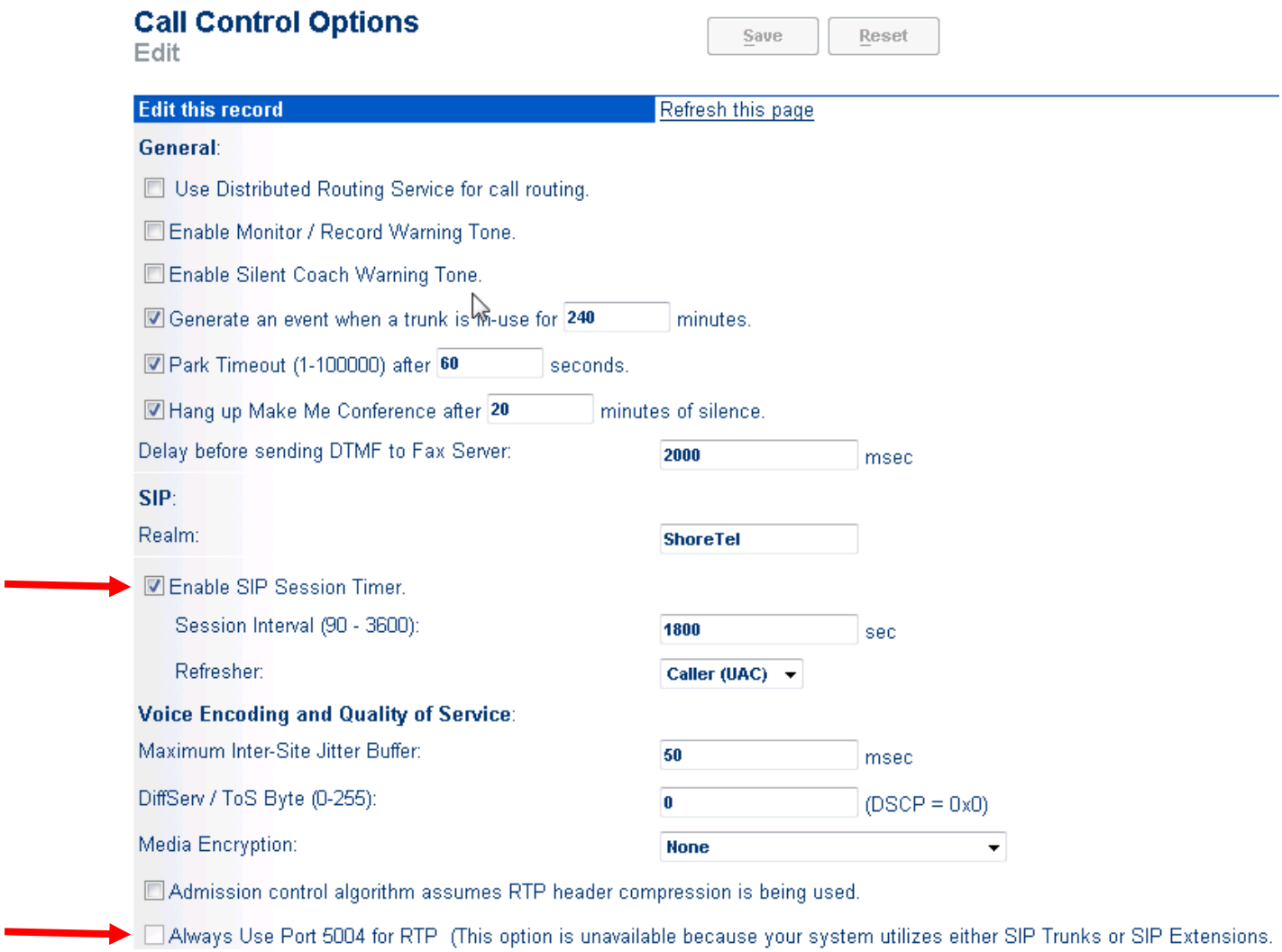
The first settings to configure within ShoreWare Director are the Call Control Options. To configure these settings for the ShoreTel system, log into ShoreWare Director and select "Administration" then "Call Control" followed by "Options".

Administration Call Control Options



The "Call Control Options" screen will then appear.

Call Control Options



Within the "Call Control Options" screen, confirm that the appropriate settings are made for the "Enable SIP Session Timer", "Intra-Site Calls", "Inter-Site Calls" and "Always Use Port 5004 for RTP" fields.

The first step is to make sure that the "Enable SIP Session Timer" box is checked. Next the Session Interval Timer needs to be set. The recommended setting for "Session Interval" is 1800 seconds. The last item to select is the appropriate refresher (from the pull down menu) for the SIP Session Timer. The "Refresher" field will be set either to "Caller (UAC)" [User Agent Client] or to "Callee (UAS)" [User Agent Server]. If the "Refresher" field is set to "Caller (UAC)", the Caller's device will be in control of the session timer refresh. If "Refresher" is set to "Callee (UAS)", the device of the person called will control the session timer refresh.

Note: Unchecking the box for "Always Use Port 5004 for RTP" is required for implementing SIP on the ShoreTel system. For SIP configurations, Dynamic User Datagram Protocol (UDP) must be used for RTP Traffic. If the box is unchecked, MGCP will no longer use UDP port 5004; MGCP and SIP traffic will use dynamic UDP ports. Once this parameter is unchecked, make sure that "everything" (IP Phones, ShoreGear Switches, ShoreWare Director, Distributed Voice Services / Remote Servers, Conference Bridges and Contact Centers) is "fully" rebooted – this is a "one time only" item. By not performing a full system reboot, one way audio will probably occur during initial testing.

2.2.2 Sites Settings

The next settings to address are the administration of sites. These settings are modified under the ShoreWare Director by selecting "Administration", then "Sites".

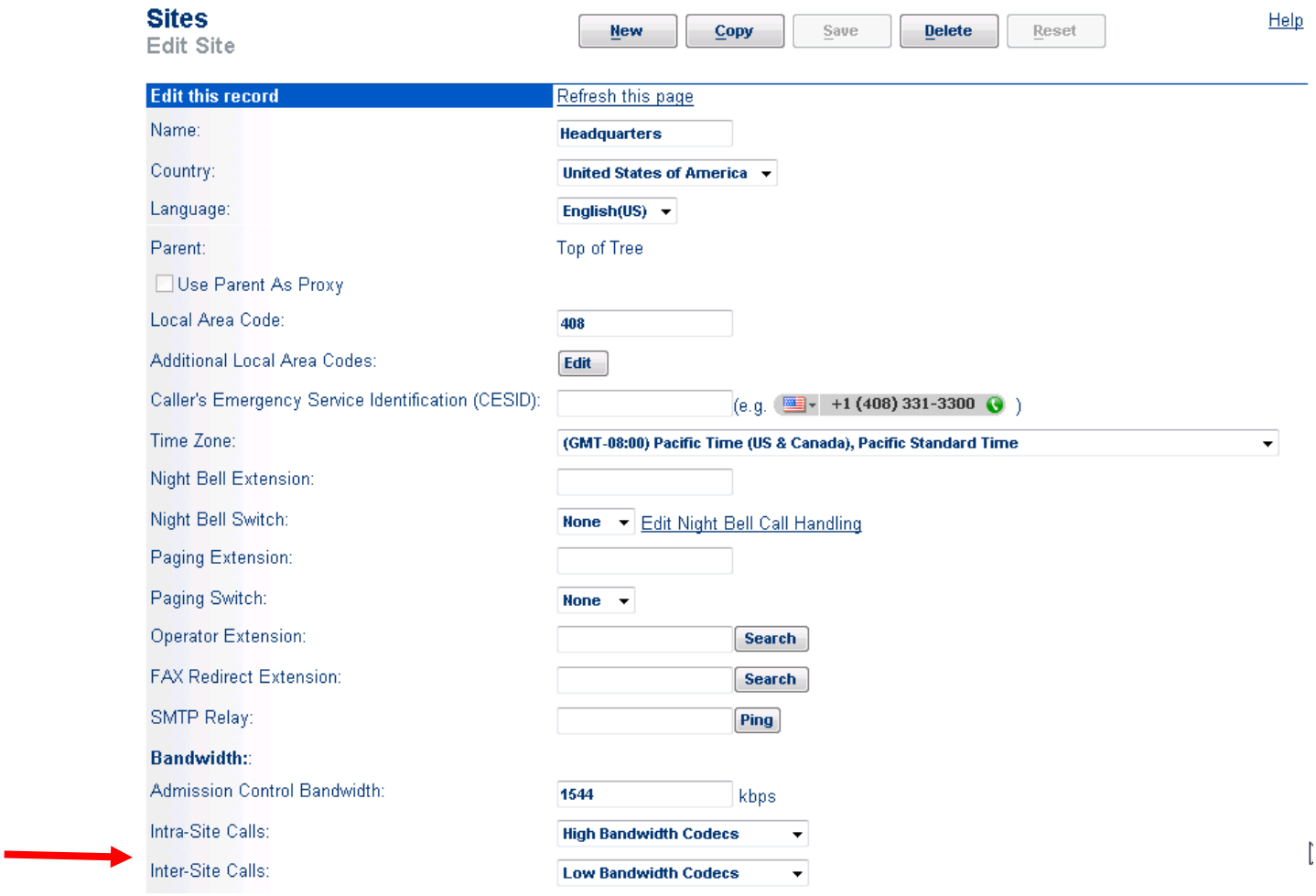
Administration Site

This selection brings up the "Sites" screen. Within the "Sites" screen, select the name of the site to configure. The "Edit Site" screen will then appear. The only change required to the "Edit Site" screen is to the "Admission Control Bandwidth" field.

Note: Bandwidth of 1024 is just an example. Please see the Planning and Installation Guide for additional information on setting Admission Control Bandwidth.

Sites Edit screen – Admission Control Bandwidth

The Admission Control Bandwidth defines the bandwidth available to and from the site. This is important as SIP devices will be counted against the site bandwidth. Bandwidth needs to be set appropriately based on site setup and configuration with the Skype SIP Trunking. See the *ShoreTel Planning and Installation Guide* for more information.



The next settings to verify are the "Intra-Site Calls" and the "Inter-Site Calls" settings under the "Sites" page in Director. For the Intra-Site Calls, verify that the desired audio bandwidth is selected for the CODEC for calls within the system. The settings should then be confirmed for the desired audio bandwidth CODEC for Inter-Site calls (calls between sites).

Note: SIP uses both G.711 and G.729 CODECs. The CODEC setting will be negotiated to the highest CODEC supported (fax requires G.711 at minimum).

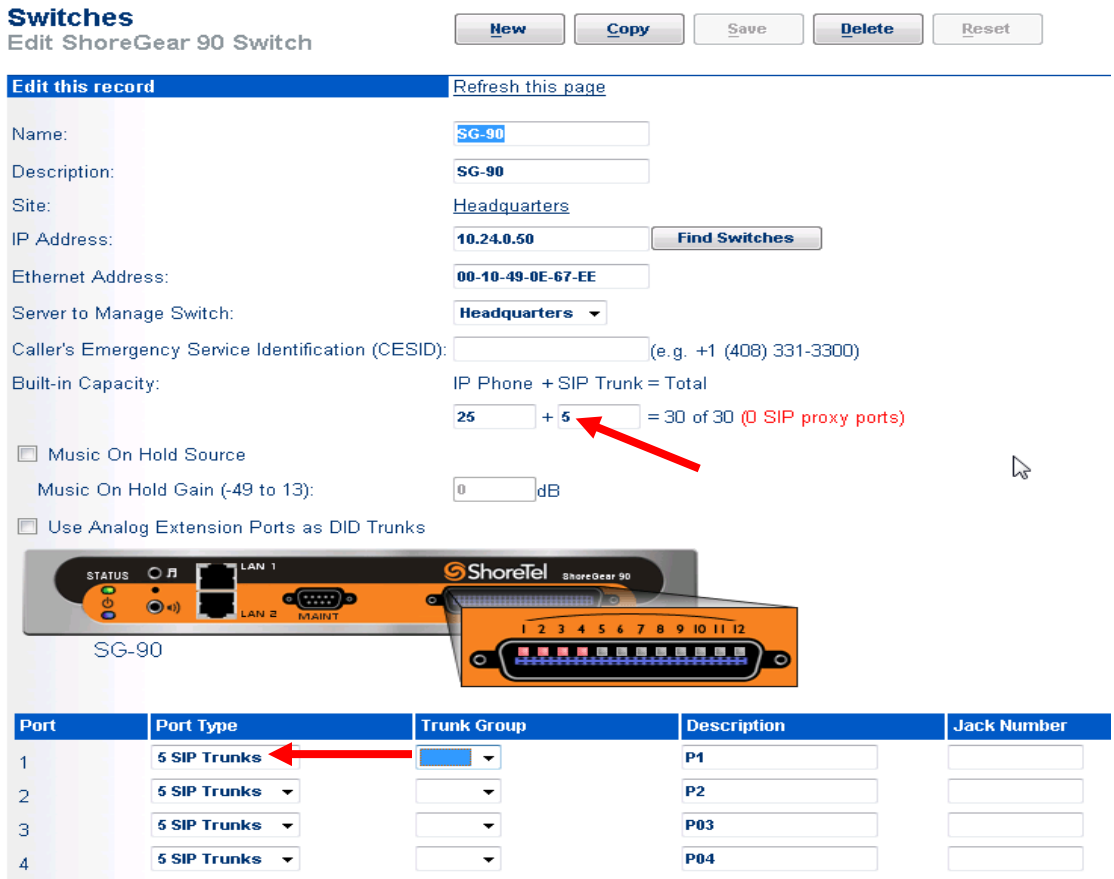
2.2.3 Switch Settings - Allocating Ports

The final general settings to input are the ShoreGear switch settings. These changes are modified by selecting "Administration", then "Switches" in ShoreWare Director.

Administration Switches

This action brings up the "Switches" screen. From the "Switches" screen simply select "Primary "and then the name of the switch to configure. The "Edit ShoreGear ···Switch" screen will be displayed. Within the "Edit ShoreGear ···Switch" screen, select the desired number of SIP Trunks from the ports available. You can set this under the "Built –in Capacity "or select "5 SIP Trunks "under the port type.

ShoreGear Switch Settings



Each port designated as a SIP Trunk enables the support for 5 individual trunks.

2.2.4 System Settings – Trunk Groups

ShoreTel Trunk Groups support both Dynamic and Static SIP endpoint Individual Trunks.

Note: A ShoreGear switch can only support one Trunk Group with Dynamic IP addressing.

In trunk planning, the following need to be considered.

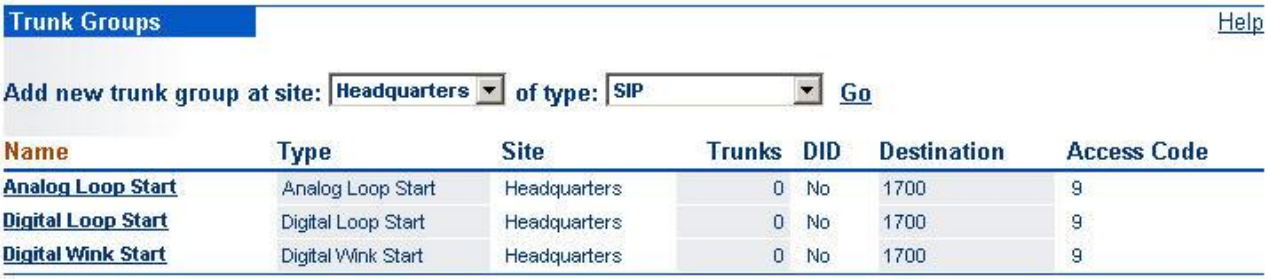
1. Are the SIP devices using DHCP or Static IP?
2. Are the SIP devices endpoints (like Attached Technology Attachments (ATAs), Conference Phone or WiFi handset) or non-endpoint devices like an ITSP?

If the SIP Trunk Groups have already been configured on the system, skip down to the "ShoreTel System Settings - Individual Trunks" section. The settings for Trunk Groups are changed by selecting "Administration", then "Trunks" followed by "Trunk Groups" within ShoreWare Director.

Administration Trunk Groups

This selection brings up the "Trunk Groups" screen.

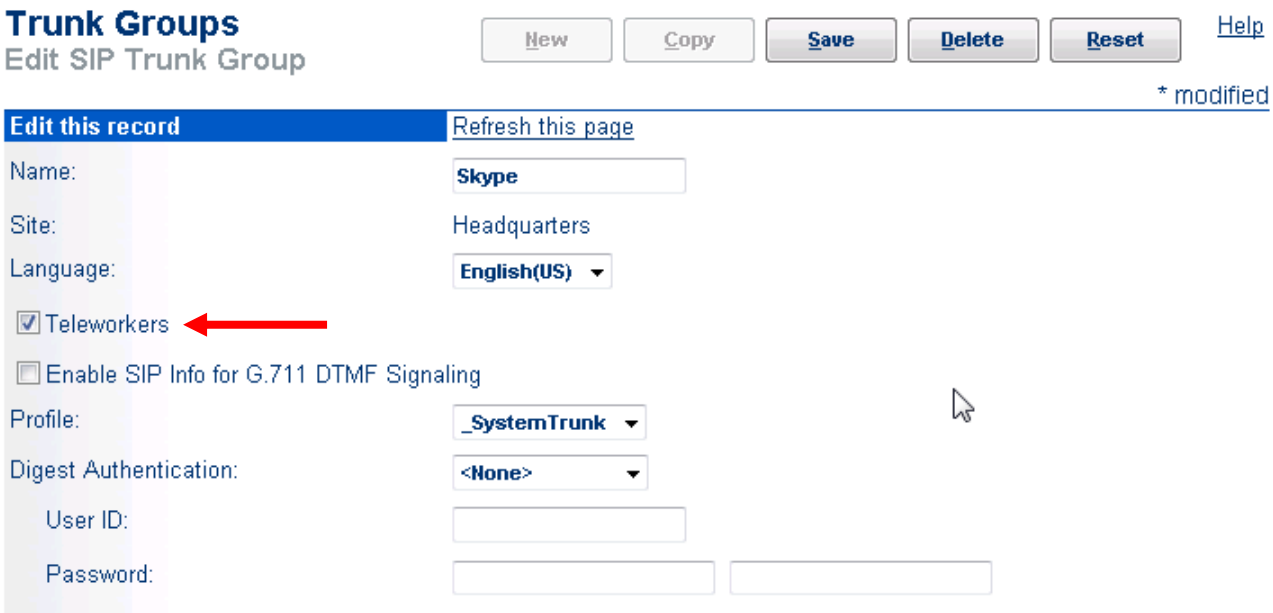
Trunk Groups Settings



Name	Type	Site	Trunks	DID	Destination	Access Code
Analog Loop Start	Analog Loop Start	Headquarters	0	No	1700	9
Digital Loop Start	Digital Loop Start	Headquarters	0	No	1700	9
Digital Wink Start	Digital Wink Start	Headquarters	0	No	1700	9

From the pull down menus on the "Trunk Groups" screen, select the site desired and select the "SIP" trunk type to configure and click on the "Go" link from "Add new trunk group at site:". The "Edit SIP Trunk Group" screen will appear.

SIP Trunk Group Settings



For the Ingate SIP Trunking, the trunks need to be configured as inter-site trunks (trunks between sites). The trunks will also be configured as static.

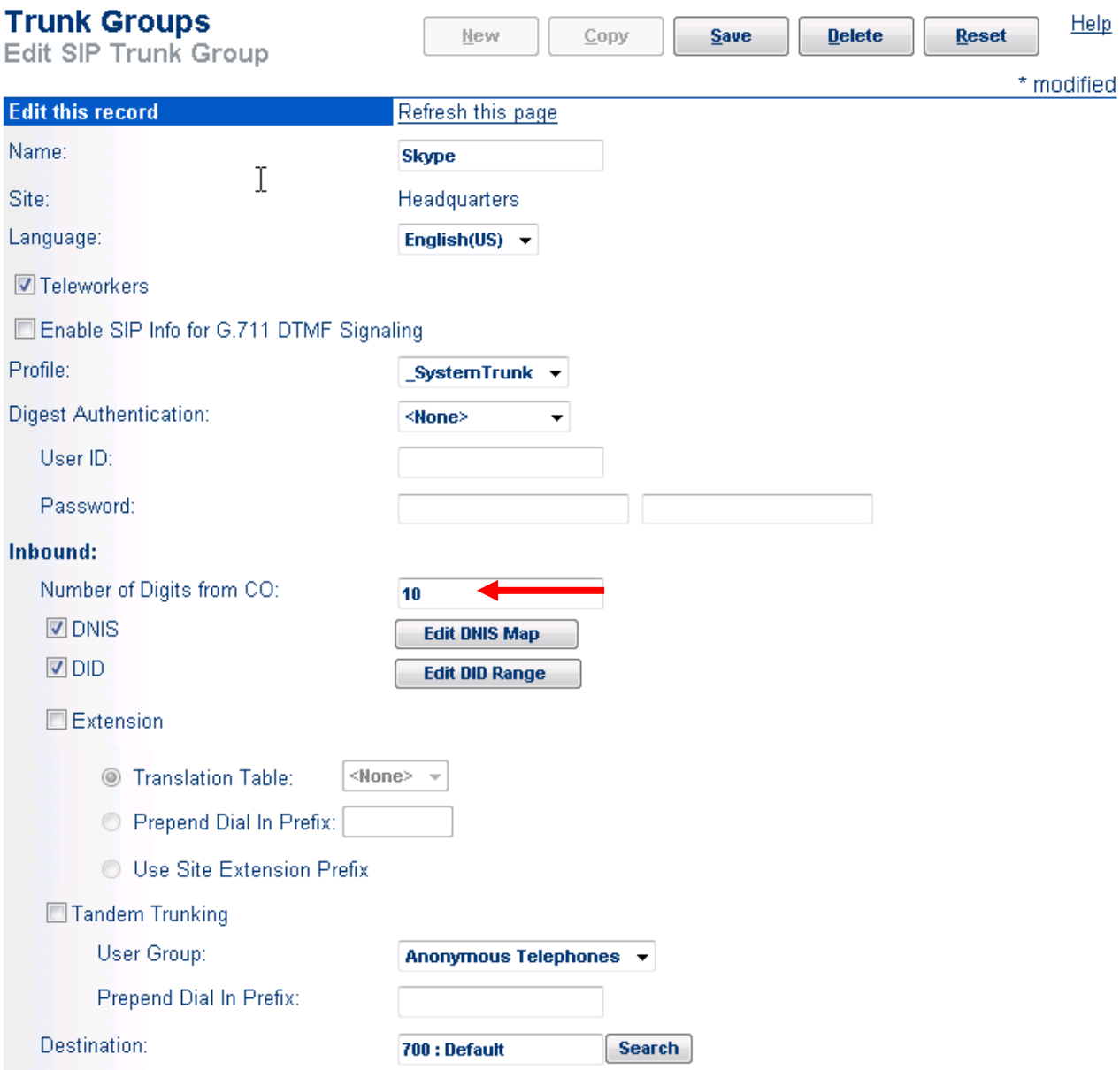
The next step within the "Edit SIP Trunks Group" screen is to input the name for the trunk group. In the example in Figure 9, the name "SIP" has been created. The next step is to verify the setting of the "Teleworker" check box. The "Teleworker" check box needs to be checked since the trunk groups have been configured as inter-site. Once this box is checked, it will count against the site bandwidth.

The "Enable Digest Authentication" field is not required when connecting to an Ingate box.

The "Enable SIP Info for G.711 DTMF Signaling" box should not be checked. Enabling SIP info is currently only used with tie trunks between ShoreTel systems.

The next item to change in the "Edit SIP Trunks Group" screen is to make the appropriate settings for the "Inbound:" fields.

Inbound

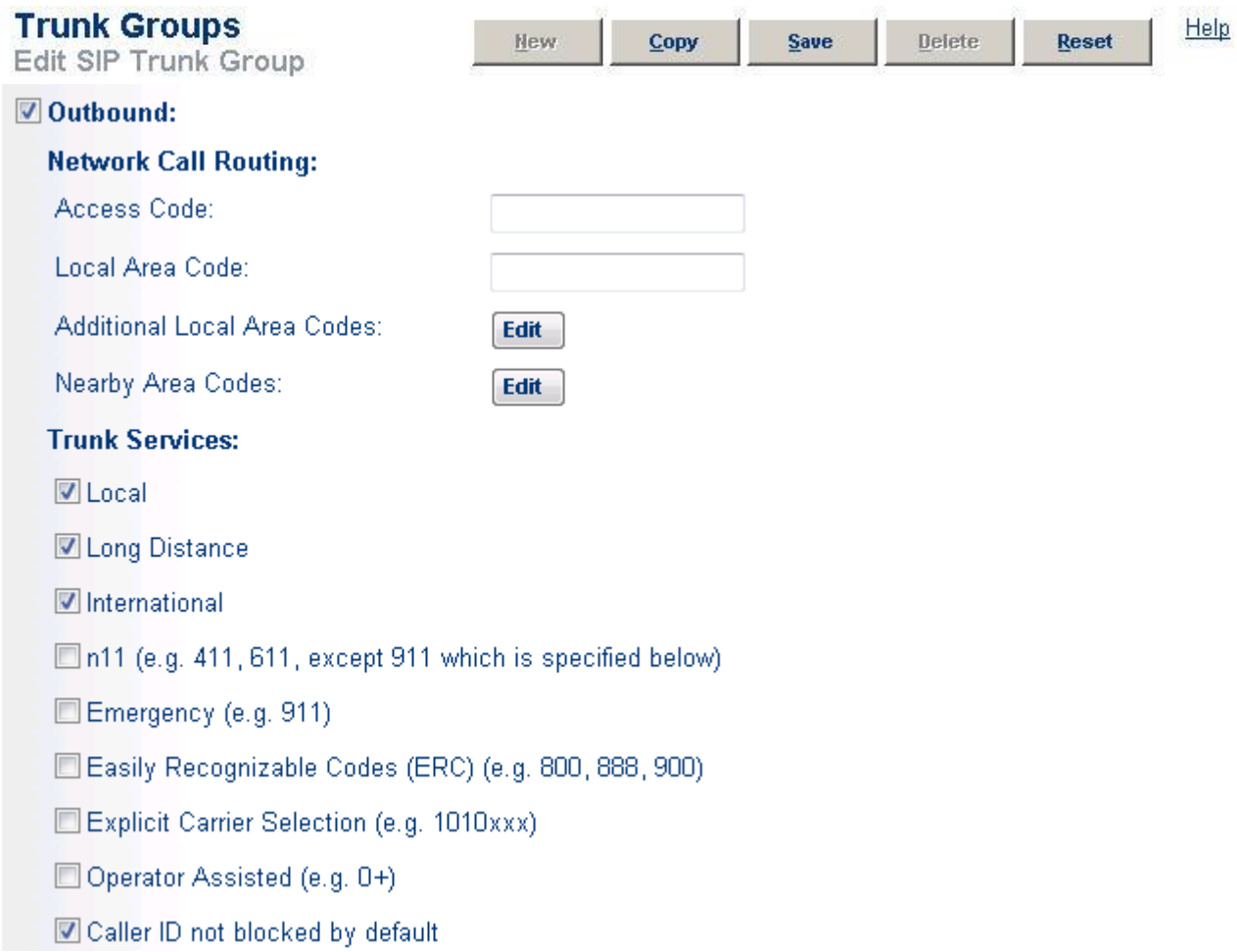


Within the "Inbound:" settings ensure the "Number of Digits from CO" is set to 11 and ensure the "DNIS" or "DID" box is checked, along with the Extension parameter (see Planning and Installation Guide for further information on configuration).

Tandem Trunking is not required unless you plan on routing incoming SIP trunk calls out other ShoreTel trunks.

Note: This section is configured no different then any normal Trunk Group

Trunk Services



On the "Trunk Services:" screen, make sure the appropriate services are checked or unchecked based on what the ITSP supports and what features are needed from this Trunk Group.

The last checkbox determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID etc. will impact how information is passed out to the SIP Trunk group.

After these settings are made to the "Edit SIP Trunk Group" screen, press the "Save" button to input the changes.

This completes the settings needed to set up the trunk groups on the ShoreTel system.

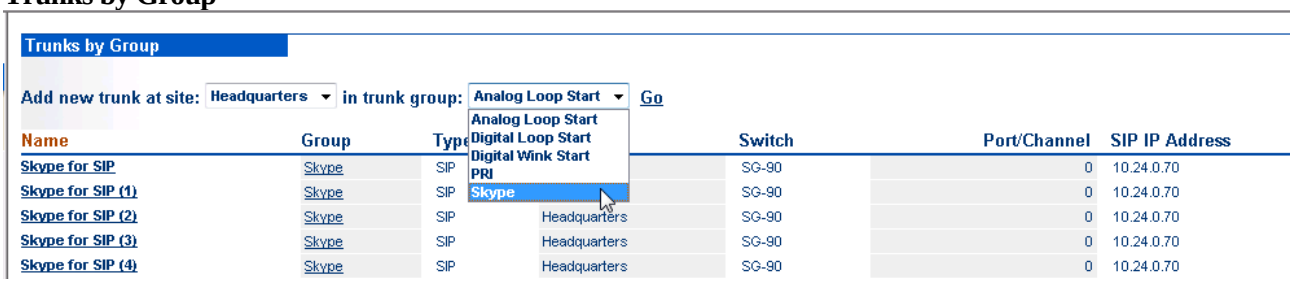
2.2.5 System Settings – Individual Trunks

This section covers the configuration of the individual trunks. Select "Administration", then "Trunks" followed by "Individual Trunks" to configure the individual trunks.

Individual Trunks

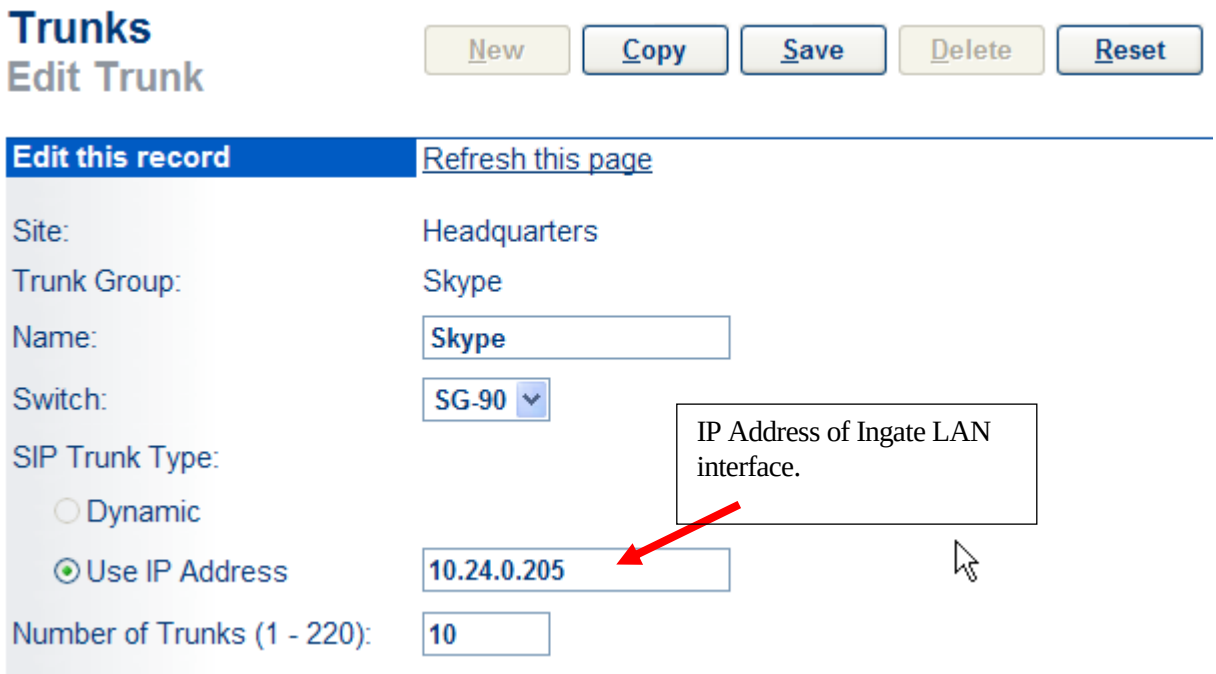
The "Trunks by Group" screen that is used to change the individual trunks settings then appears.

Trunks by Group



Select the site for the new individual trunk(s) to be added and select the appropriate trunk group from the pull down menu in the "Add new trunk at site" area. In this example, the site is "Headquarters" and the trunk group is "SIP". Click on the "Go" button to bring up the "Edit Trunk" screen.

Edit Trunks Screen for Individual Trunks



From the individual trunks "Edit Trunk" screen, input a name for the individual trunks, select the appropriate switch, select the SIP Trunk type and input the number of trunks. When selecting a name, the recommendation is to name the individual trunks the same as the name of the trunk group so that the trunk type can easily be tracked. Select the switch upon which the individual trunk will be created. For the ITSP Trunk, select "Use IP Address" button and input an IP address of the Ingate SIParator product. The last step is to select the number of individual trunks desired (each one supports "one" audio path – example if 5 is input, then 5 audio paths can be up at one time). Once these changes are complete, press the "Save" button to input the changes.

Note: Individual SIP Trunks cannot span networks. SIP Trunks can only terminate on the switch selected. There is no failover to another switch. For redundancy, two trunk groups will be needed with each pointing to another Ingate SIParator – just the same as if PRI were being used.

After setting up the trunk groups and individual trunks, refer to the ShoreTel Product Installation Guide to make the appropriate changes for the User Group settings. This completes the settings for the ShoreTel system side.

3 INGATE CONFIGURATION

3.1 ABOUT

Ingate products are compatible with communications equipment from other vendors and service providers who support the SIP Protocol. The Ingate products are a security device designed to sit on the Enterprise network edge, an ICSA Labs Certified security product, focused on SIP communications security and network security for the Enterprise.

Ingate products are designed to solve the issues related to SIP traversing the NAT (Network Address Translation) which is a part of all enterprise class firewalls. The NAT translates between the public IP address(es) of the enterprise, and the private IP addresses which are only known inside the LAN. These private IP addresses are created to enable all devices to have an IP address, and also provide one of the security layers of the enterprise network. In addition, the Ingate products provide routing rules to assign to SIP traffic flow to ensure only allowed SIP traffic will pass.

3.1.1 Startup Tool

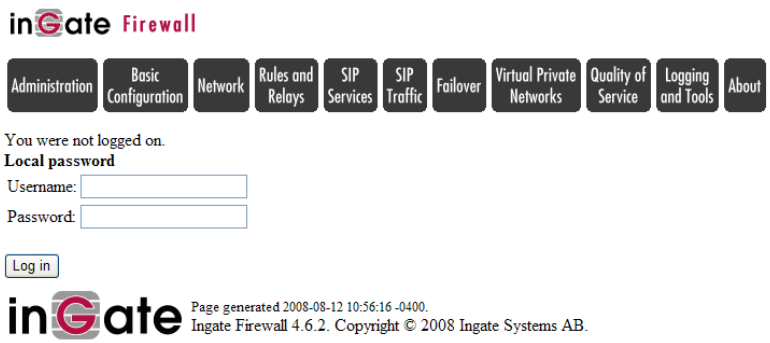
The Ingate Startup Tool is an installation tool for Ingate Firewall® and Ingate SIParator® products, facilitates the "out of the box" set up of SIP Trunking solutions with ShoreTel and various Internet Telephony Service Providers. Designed to simplify SIP trunk deployments, the tool will automatically configure a user's Ingate Firewall or SIParator® to work with ShoreTel and the SIP Trunking service provider of your choice. With the push of a button, the configuration tool will automatically create a SIP trunk deployment designed to the user's individual setup.

Users can select ShoreTel from a drop-down menu and Skype the Internet Telephony Service Provider (ITSP); the configuration tool will automatically apply the correct settings to the Ingate Firewall or SIParator to work seamlessly with that vendor or service provider. A list of SIP Trunking service providers that have demonstrated interoperability with the Ingate products is incorporated into the interface. Please note that not all SIP Trunking service providers listed in this interface have been certified by ShoreTel. Consult the ShoreTel Certified Technology Partner list of vendors for a current list.
(http://www.shoretel.com/partners/technology/certified_partners.html)

The configuration tool is available now as a free download for all Ingate Firewalls and SIParators. It can be found at http://www.ingate.com/startuptool.php. Also available here is a Startup Tool Getting Started Guide to assist in using the Startup Tool.

3.1.2 Web Admin

By default the Ingate units does not come pre-assigned with an IP Address or Password, once these are assigned by the Startup Tool or Console Port, the Ingate units can be administered via the web. Using a Browser, simply enter the IP Address assigned to the unit, this will launch the Web Administration GUI.



3.2 CONNECTING THE INGATE FIREWALL/SIPARATOR

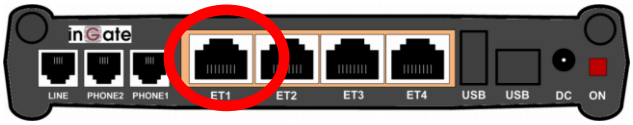
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

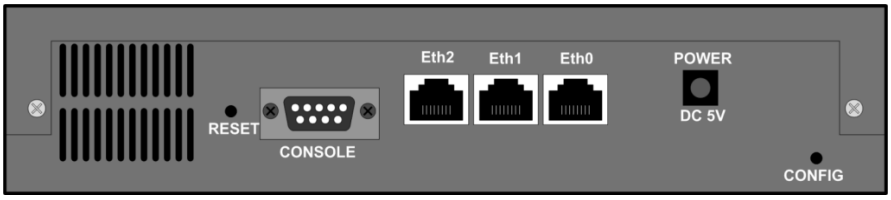
Configuration Steps:

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".

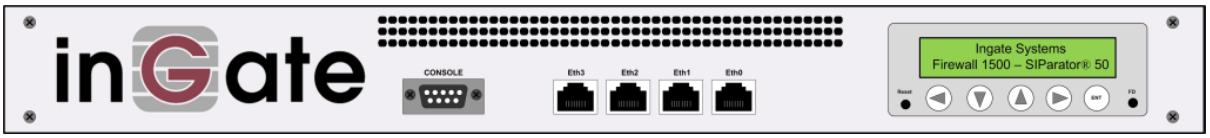
Ingate SIParator SBE (Back)



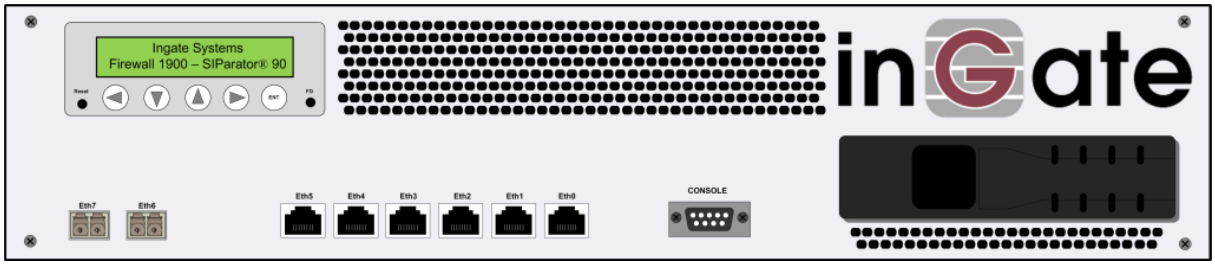
Ingate 1190 Firewall and SIParator 19 (Back)



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

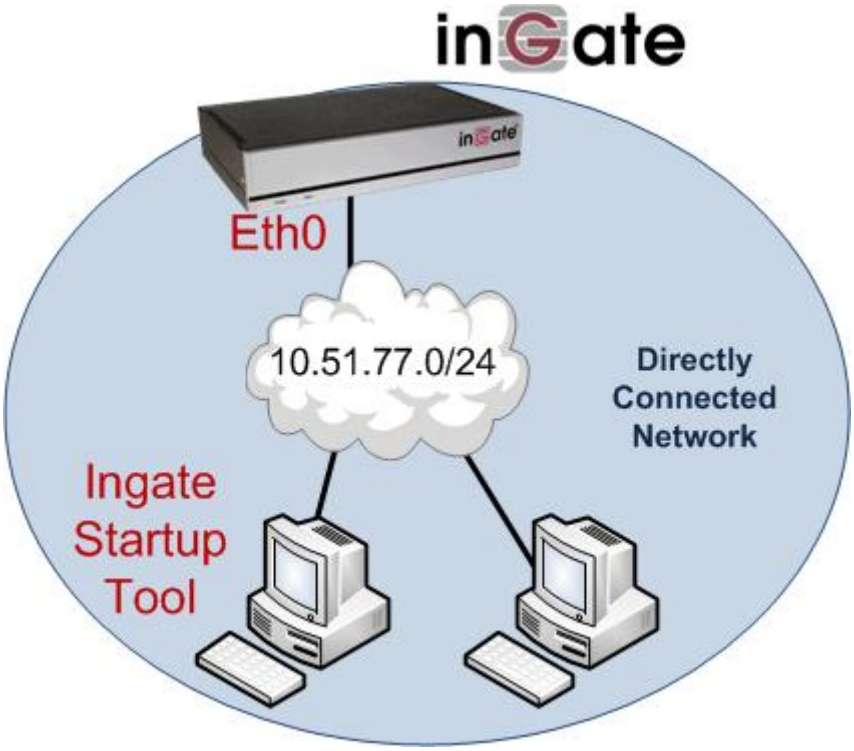


Ingate 1900 Firewall and SIParator 90



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

3.3 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.

3.3.1 Configure the Unit for the First Time

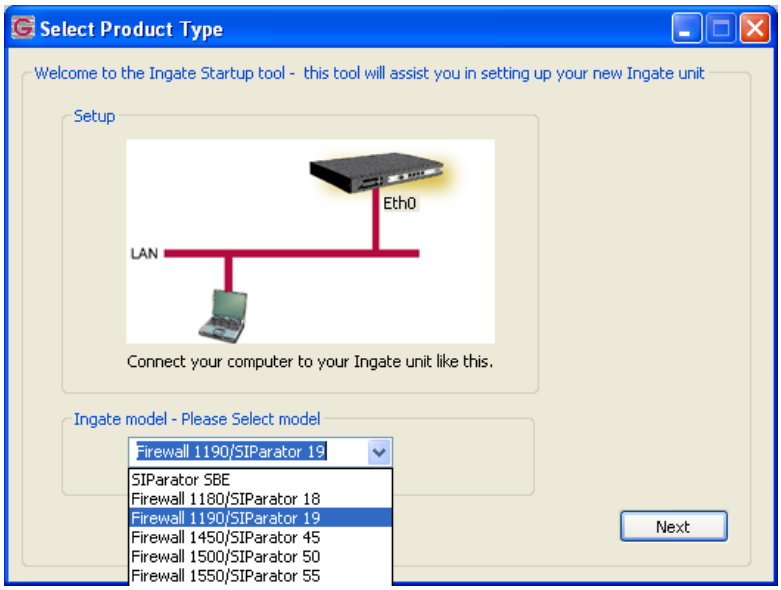
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

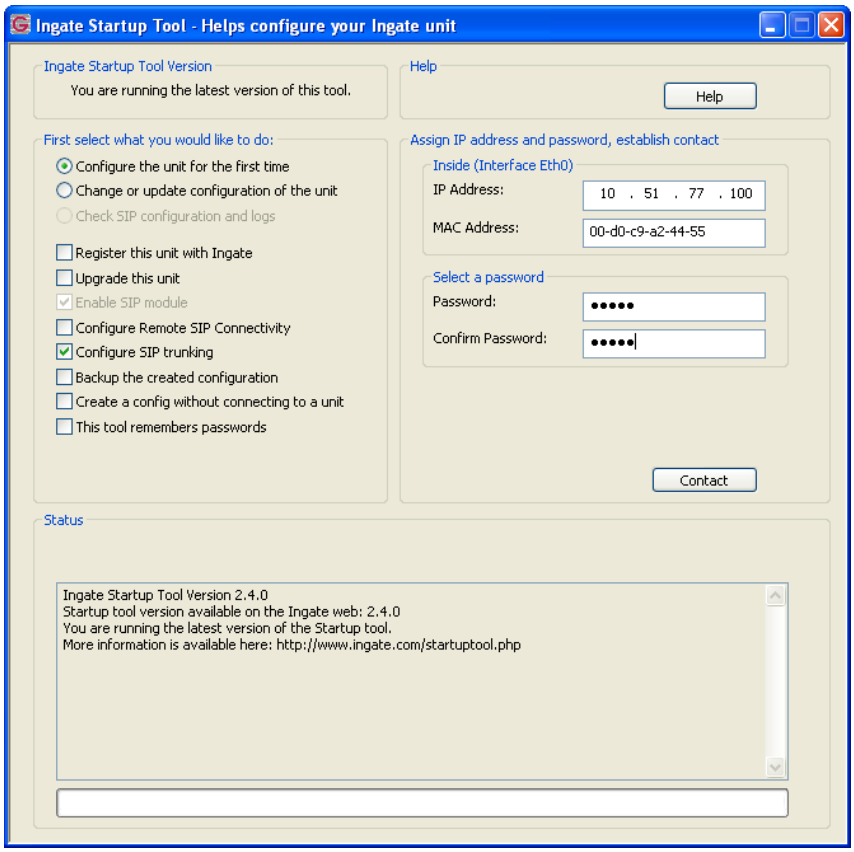
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: "Change or Update Configuration".

Configuration Steps:

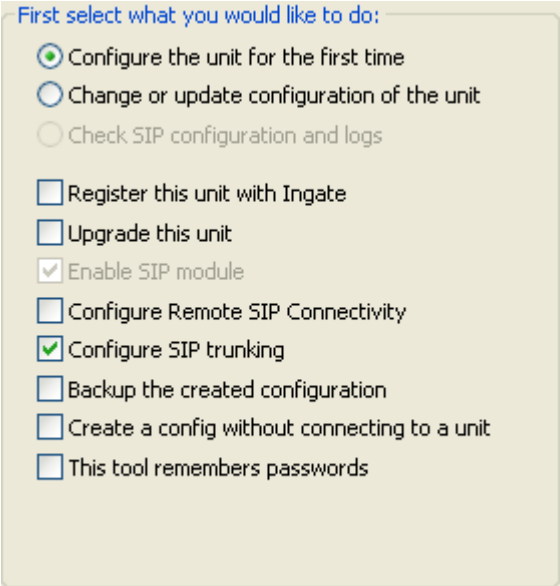
1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.



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



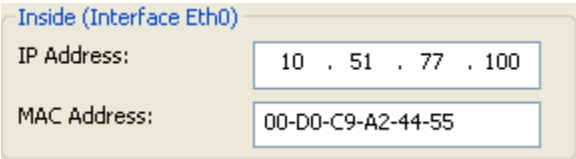
4. Other Options in the "Select first what you would like to do",



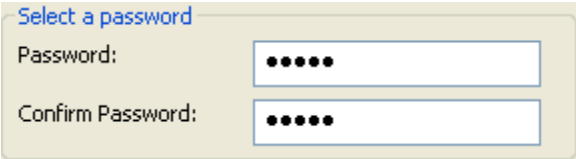
a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

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.

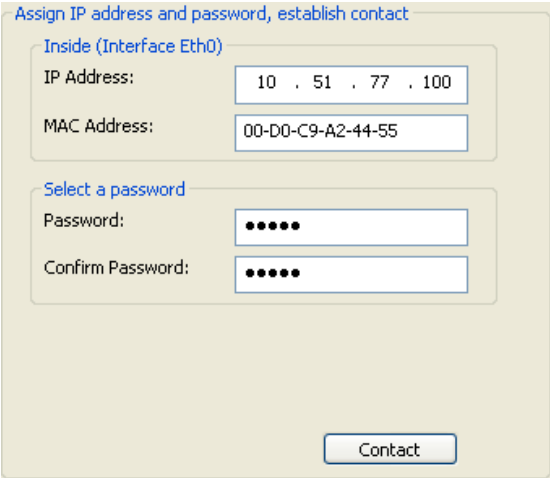
5. In the "Inside (Interface Eth0)",
   a. Enter the IP Address to be assigned to the Ingate Unit.
   b. Enter the MAC Address of the Ingate Unit, this MAC Address will be used to find the unit on the network. The MAC Address can be found on a sticker attached to the unit.



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 3.3.3: Network Topology.

3.3.2 Change or Update Configuration

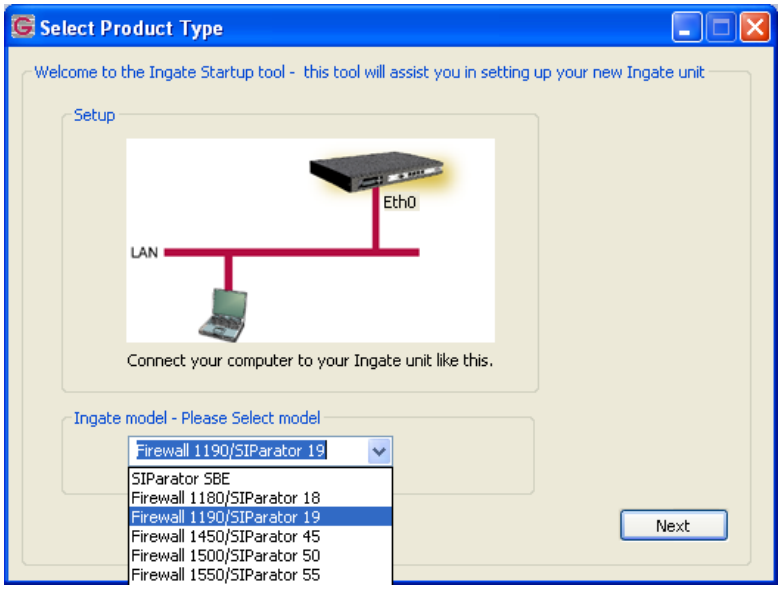
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

In the Startup Tool, when selecting "Change or update configuration of the unit", the Startup Tool will connect directly with the Ingate Unit on the network with the provided IP Address and Password. When completed, the Startup Tool will completely overwrite the existing configuration in the Ingate unit with the new settings.

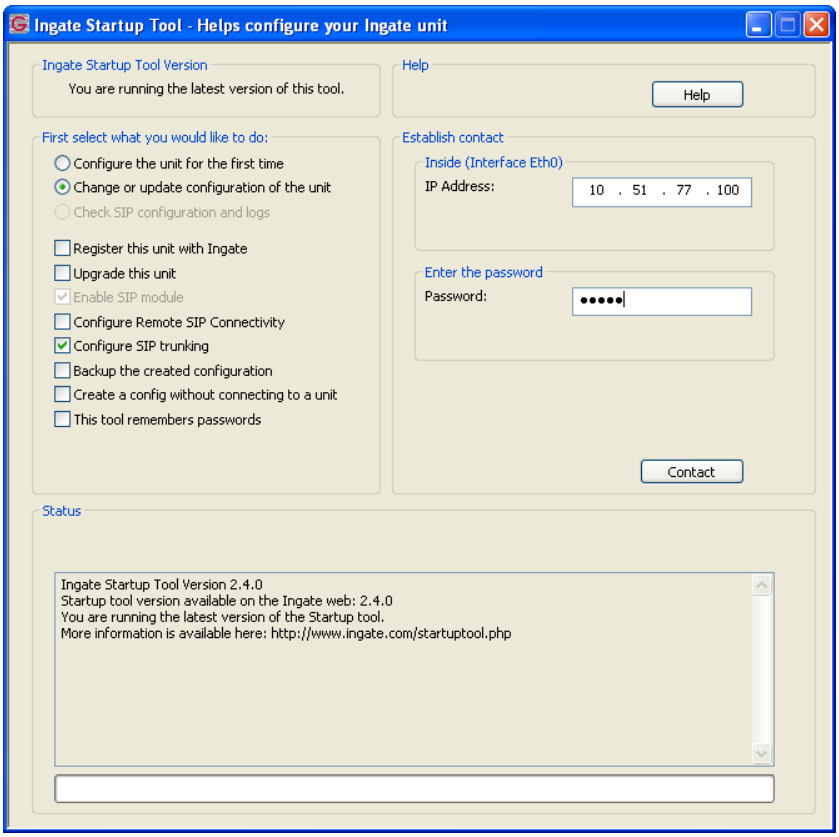
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: "Configure the Unit for the First Time".

Configuration Steps:

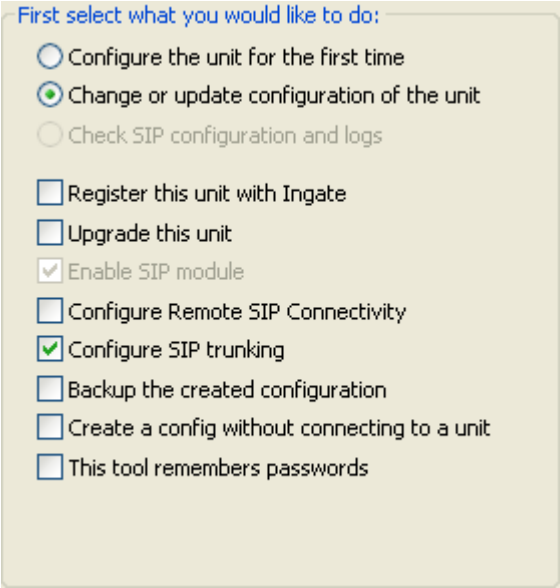
1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.



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



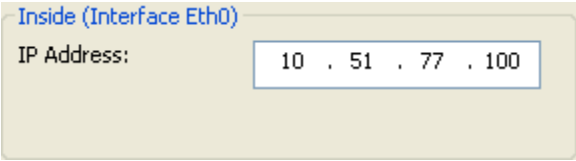
4. Other Options in the "Select first what you would like to do",



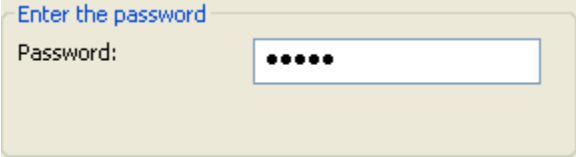
a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
b. Select "Configure Remote SIP Connectivity" if you want the tool to configure Remote Phone access to an IP-PBX

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 "Enter a Password", enter the Password of the Ingate unit.

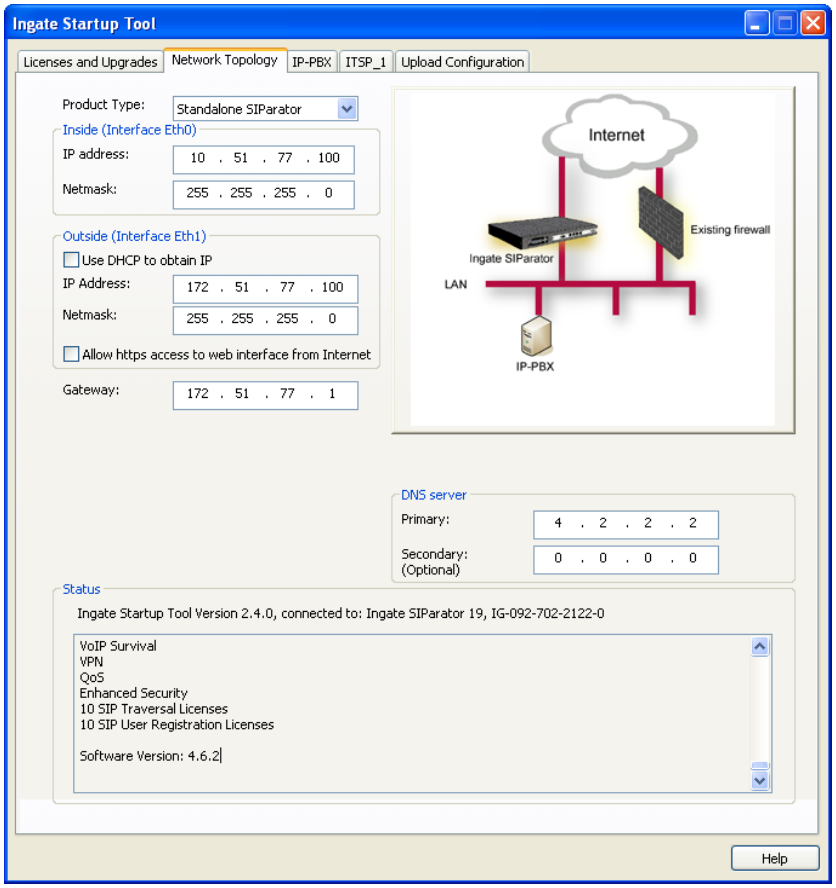


7. Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.

8. Proceed to Section 3.3.3: Network Topology.

3.3.3 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:

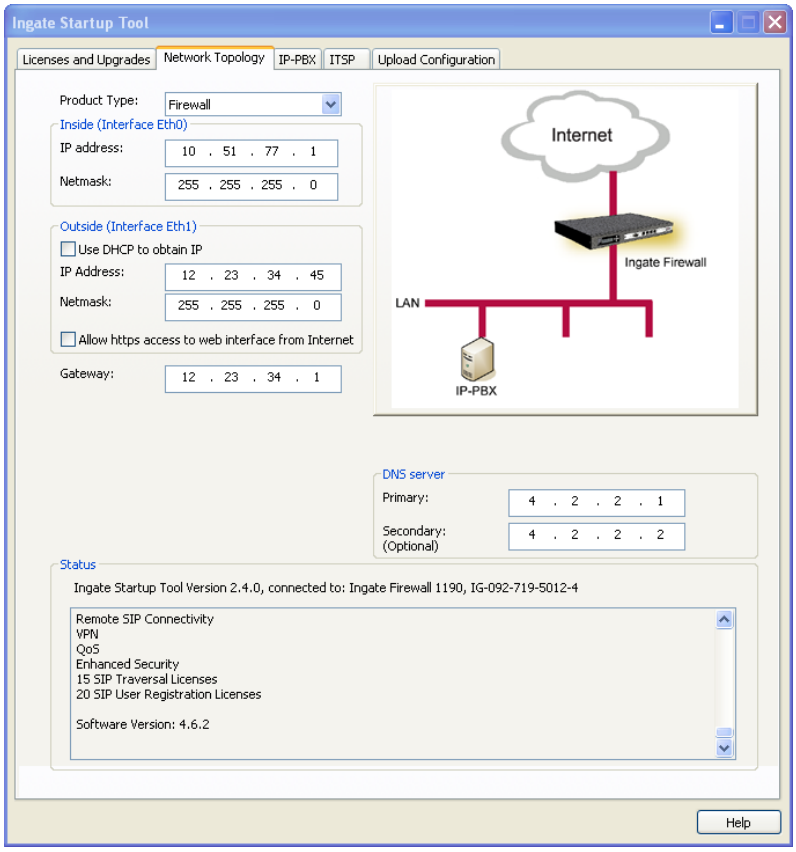
1. In the Product Type drop down list, select the deployment type of the Ingate Firewall or SIParator.

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.

Product Type: Firewall

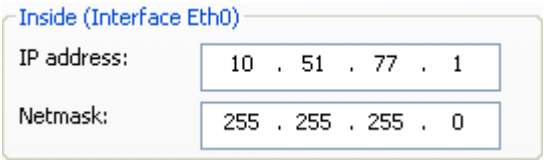
When deploying an Ingate Firewall, there is only one way the Firewall can be installed. The Firewall must be the Default Gateway for the LAN; it is the primary edge device for all data and voice traffic out of the LAN to the Internet.



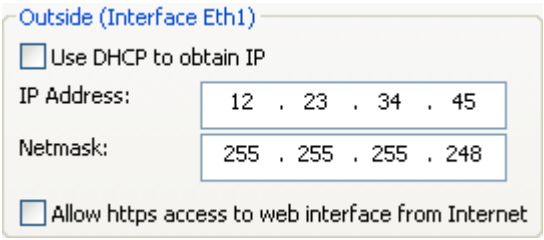
Configuration Steps:

1. In Product Type, select "Firewall".

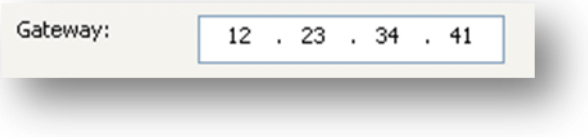
2. Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.



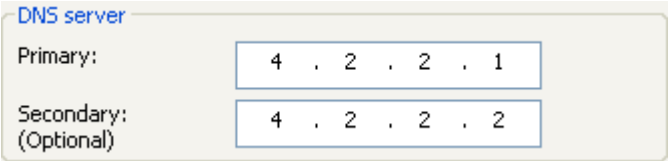
3. Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
    a. A Static IP Address and Netmask can be entered
    b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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



4. 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).



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.

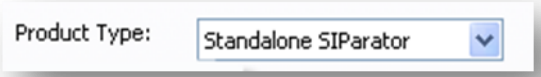


Product Type: Standalone

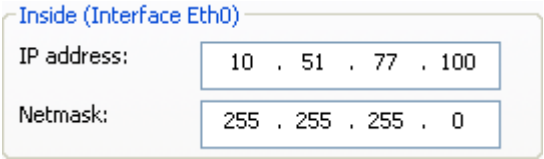
When deploying an Ingate SIParator in a Standalone configuration, the SIParator resides on a LAN network and on the WAN/Internet network. The Default Gateway for SIParator resides on the WAN/Internet network. The existing Firewall is in parallel and independent of the SIParator. Firewall is the primary 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:

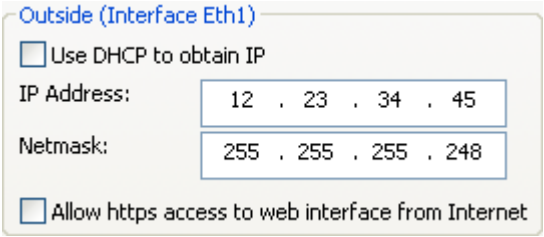
1. In Product Type, select "Standalone SIParator".



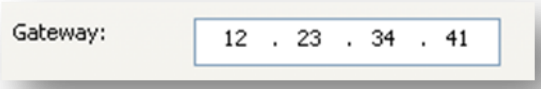
2. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



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.



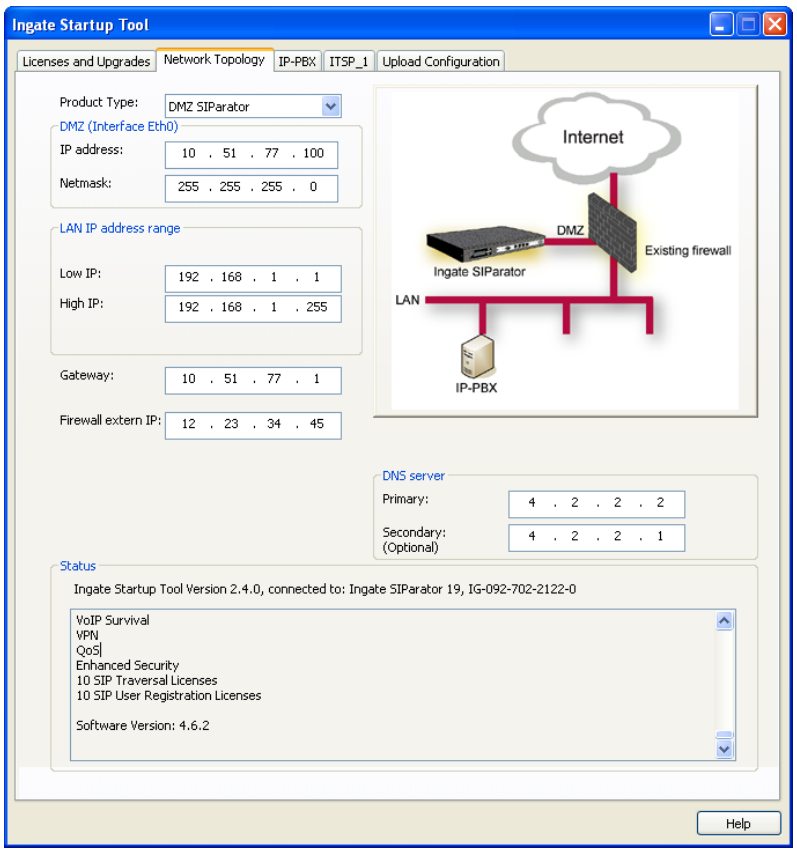
4. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



5. Enter the 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.

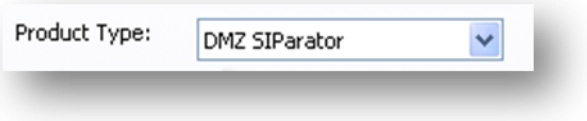
Product Type: DMZ SIParator

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.

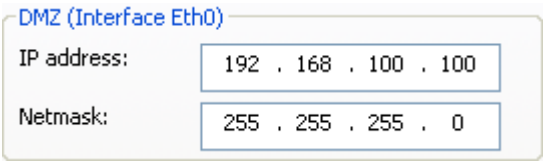


Configuration Steps:

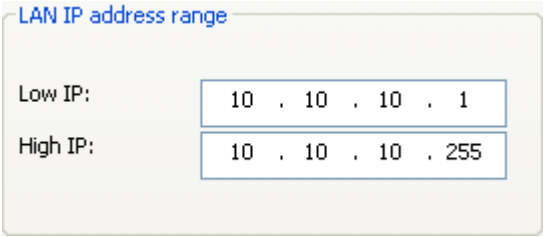
1. In Product Type, select "DMZ SIParator".



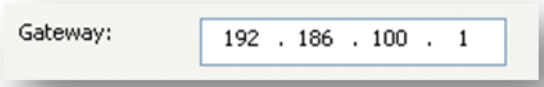
2. Define the IP Address and Netmask of the DMZ (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.



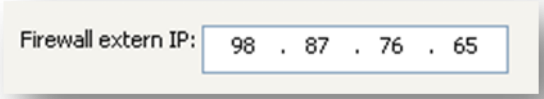
3. Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.



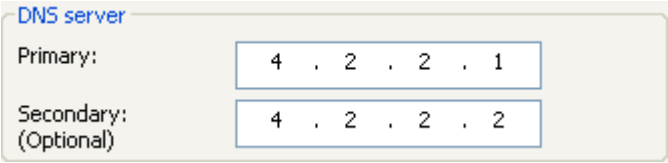
4. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.

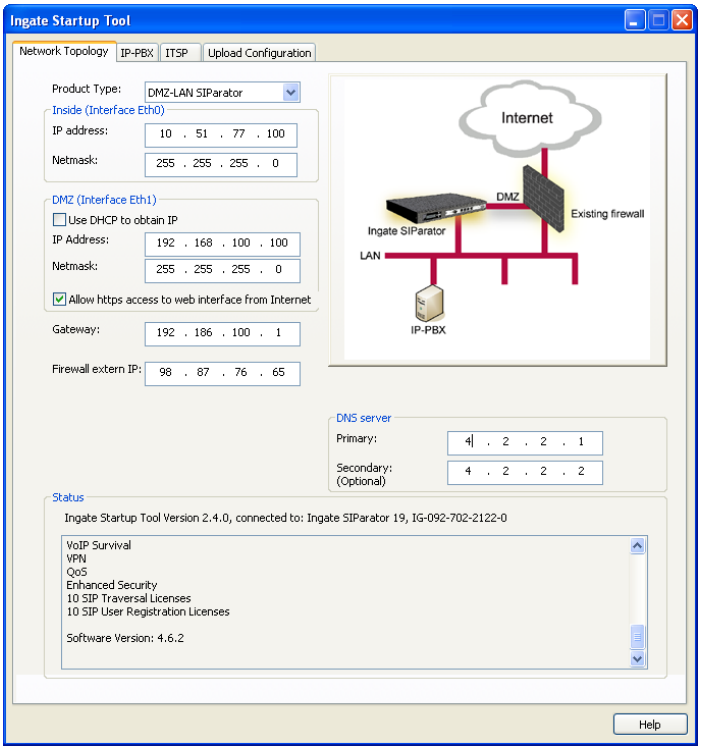


7. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   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.

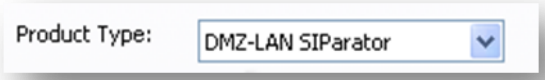
Product Type: DMZ-LAN SIParator

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.

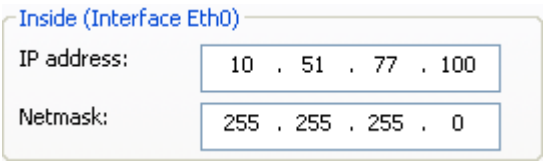


Configuration Steps:

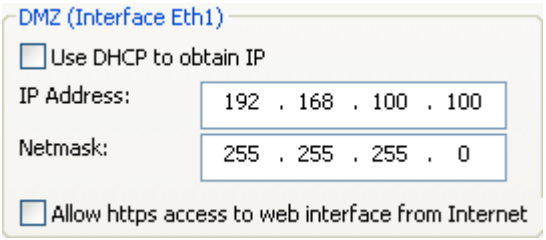
1. In Product Type, select "DMZ-LAN SIParator".



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.

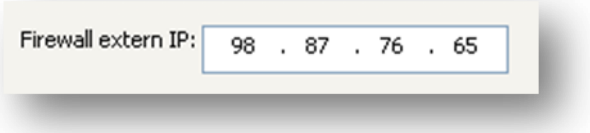


3. Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.
    a. A Static IP Address and Netmask can be entered
    b. Or select "Use DHCP to obtain IP", if you want the Ingate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

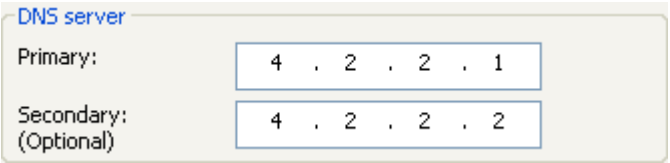


4. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

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.

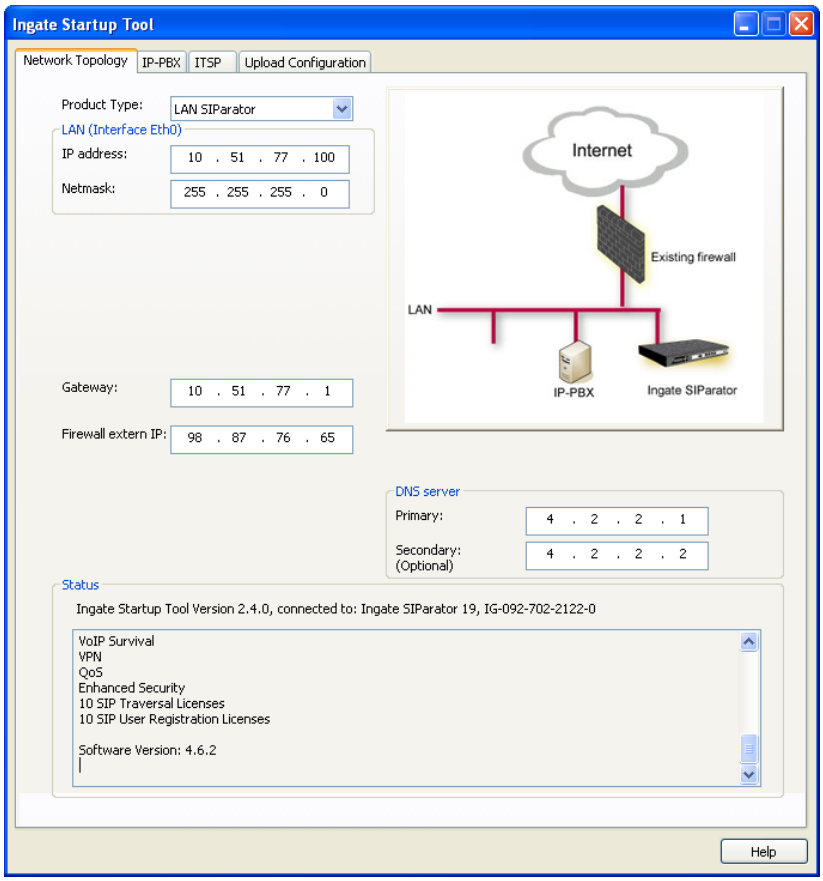


7. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

    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

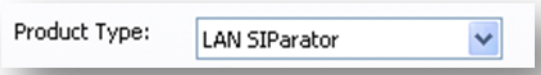
Product Type: LAN SIParator

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.

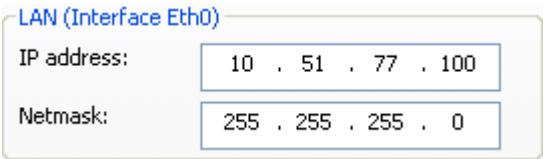


Configuration Steps:

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

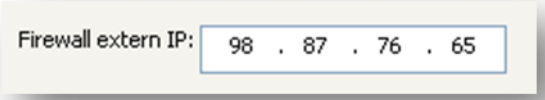


2. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.

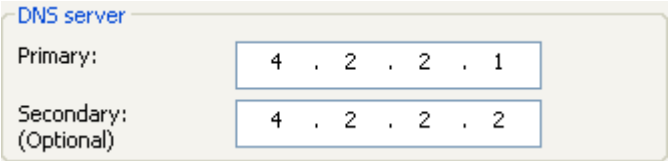


3. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

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.

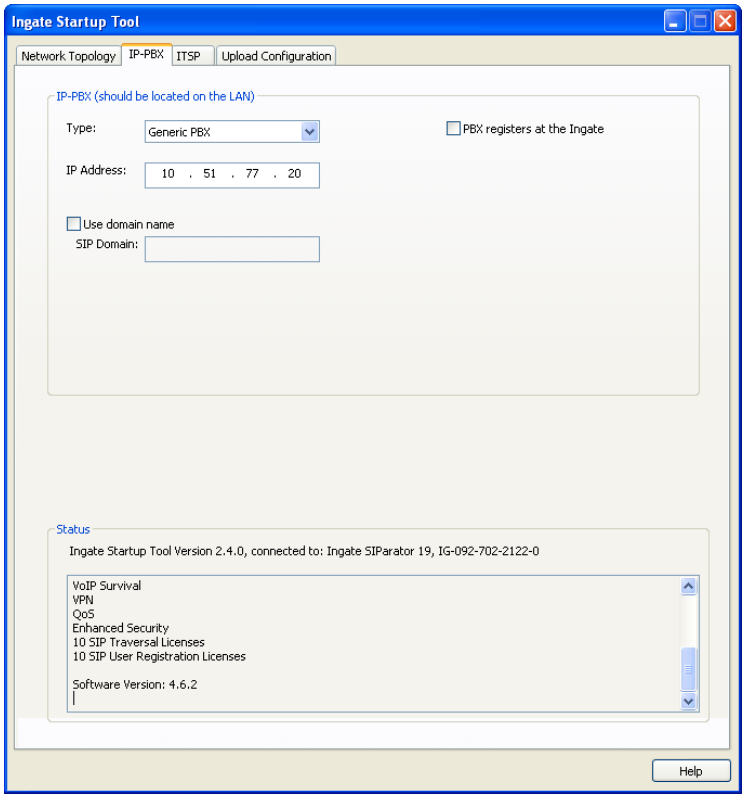


6. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   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

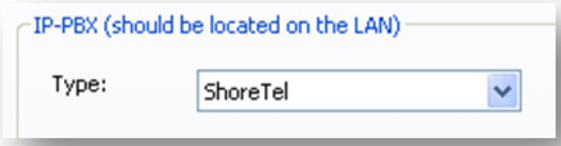
3.3.4 IP-PBX

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 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:

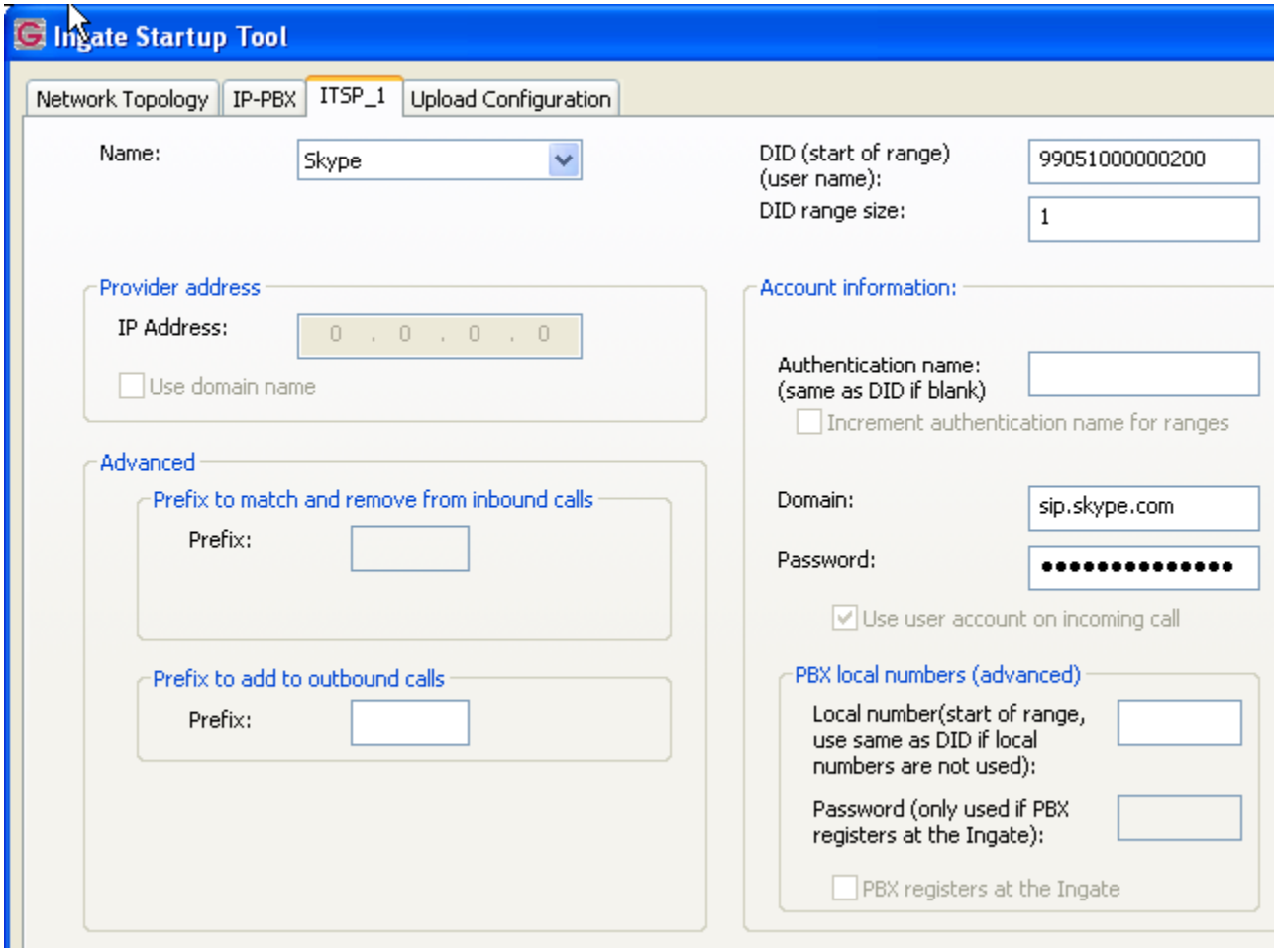
1. In the IP-PBX Type drop down list, select "ShoreTel". Ingate has confirmed interoperability with ShoreTel, the unique requirements of the vendor testing are contained in the Startup Tool.



2. Enter the IP Address of the ShoreTel Shoregear. The IP Address should be on the same LAN subnet as the Ingate unit.

3.3.5 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:

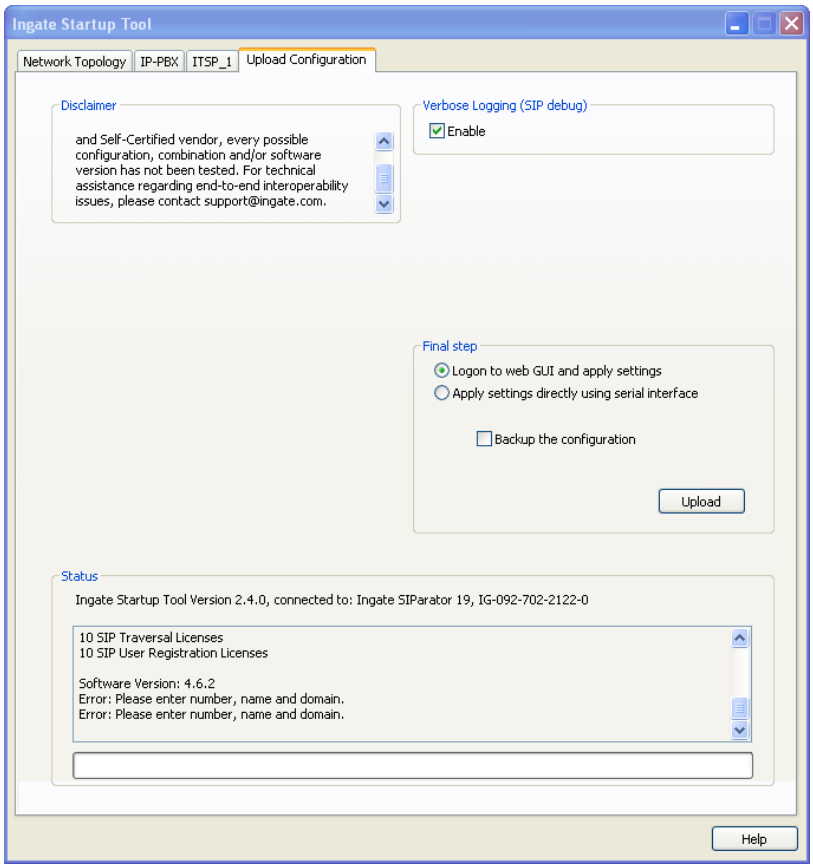
1. In the ITSP drop down list, select Skype as the ITSP vendor. Ingate has confirmed interoperability several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool.

The DID start range will be your Skype SIP user ID. You also need to specify the Skype SIP user password.

This completes the ITSP_1 configuration. Now select the Upload Configuration tab.

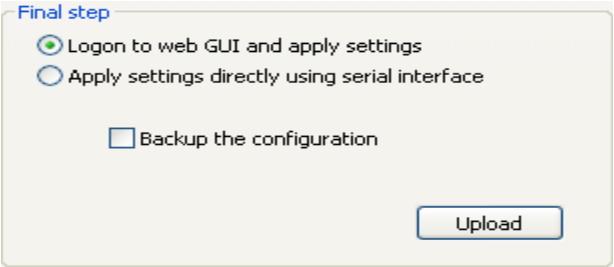
3.3.6 Upload Configuration

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.

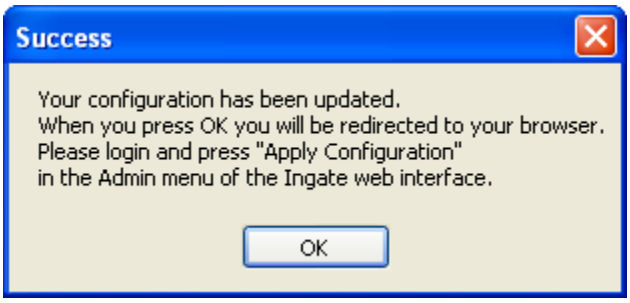


Configuration Steps:

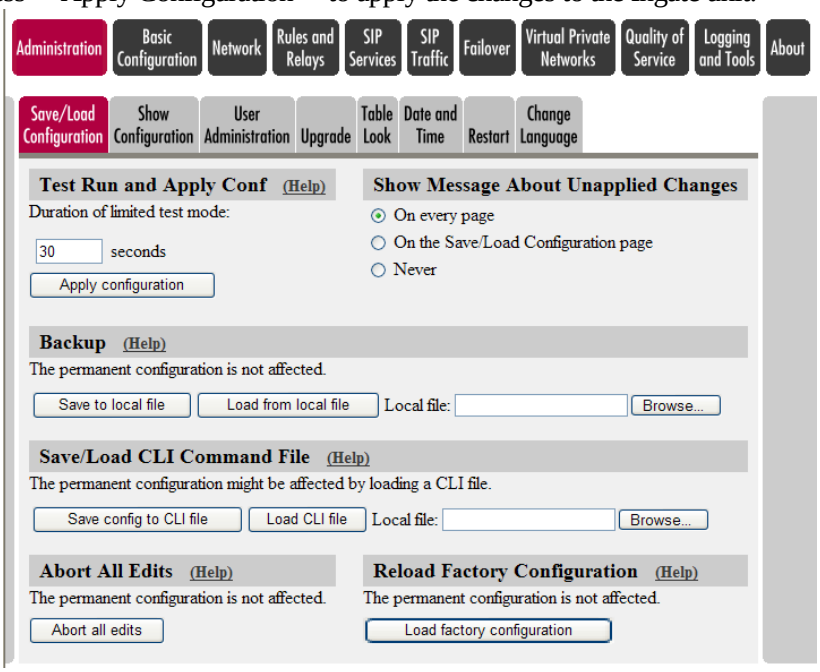
1. Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



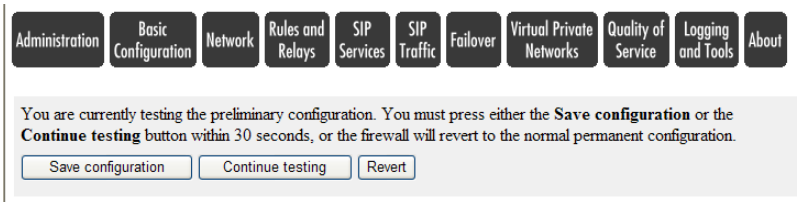
2. When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



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.



3.3.7 Adding additional phone numbers post InGate Startup Tool

Here are the steps to add additional phone numbers and how to make them routable between Skype and ShoreTel. Currently, the Skype for SIP beta will require translation and registration for each User / DID.

Configuration steps

1. Log into Skype Manager and select the "Skype Connect" link under "Your Features". Select "View profile". Select Authentication details. This presents your account information. Here is an example below:

Authentication details

Please choose the method of authentication needed for your PBX.

Registration (Username/password) | **or, IP Authentication**

Your PBX details

SIP User	99051000000200
Public IP address	70.164.124.9
UDP Port	5060

Change PBX details

Use these details to configure your PBX

Skype Connect addresses

Primary	2.sip.skype.com
Secondary	1.sip.skype.com

Skype Connect IP addresses enable traffic for these IP addresses in your firewall

Primary	204.9.161.164

* The new version of the InGate startup tool will no longer make these steps required in the future.

1. Log into InGate. Select the "SIP Traffic " tab and then "Dial Plan". Scroll down to "Matching Request-URI". Click on Add new rows and enter "Inbound " in the Name field. Then select the "- " for the "Tail". Scroll over to "Reg Expr" and add " sip:(.*)@" followed by your public IP address. Example: sip:(.*)@67.203.148.231

Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Inbound			-			sip:(.*)@67.203.1	☐
Outbound			any character		10.24.0.4		☐

2. Scroll down to the "Forward To" section. Click on Add new rows and enter "ShoreTel" in the "Name" field. Then select the "- " for the "Account" field. In the "Reg Expr" field enter sip:$1@10.24.0.92;b2bua where the IP address is your ShoreTel SIP trunk switch.

Forward To (Help)

Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	
ShoreTel	1	-			-	sip:$1@10.24.0.9	☐
Skype	1	99051000000200@sip.skype.com			-		☐

Add new rows 1 groups with 1 rows per group.

3. Scroll down to Dial plan section and select "Add new rows". Renumber the "No." column for "WAN" to 3. Select "Add new rows". Make this new row "No." 2 and select Skype for the "From Header". Select "Inbound" for the "Request URI". Under "Action" select "Forward". Select "ShoreTel" for the "Forward To" field.

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	ShoreTel	Outbound	Forward	Skype			-	-		☐
2	Skype	Inbound	Forward	ShoreTel			-	-		☐
3	WAN	-	Reject	-			-	-		☐

4 TROUBLESHOOTING

4.1 STARTUP TOOL TROUBLESHOOTING

4.1.1 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.

4.1.2 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".

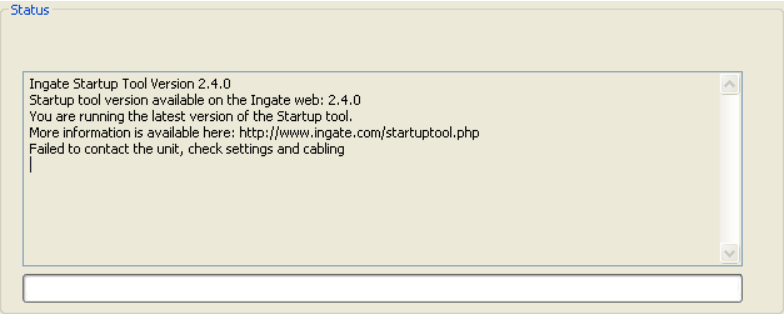
Possible Problems and Resolutions

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.
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.

4.1.3 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.

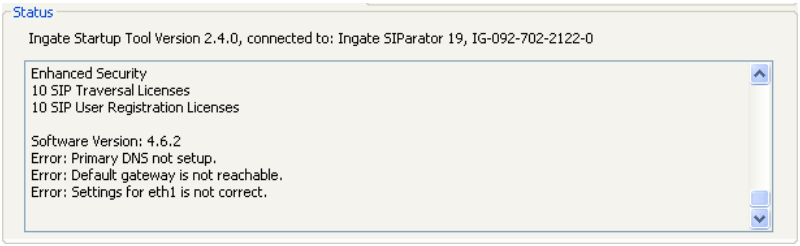


Possible Problems and Resolutions

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".

4.1.4 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.

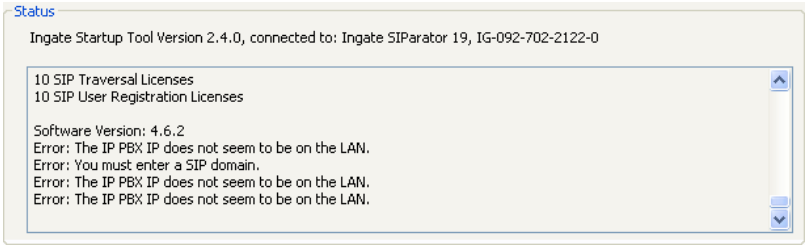


Possible Problems and Resolutions

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

4.1.5 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.

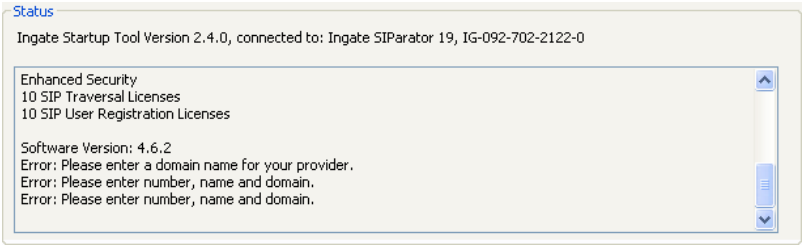


Possible Problems and Resolutions

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.

4.1.6 ITSP

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

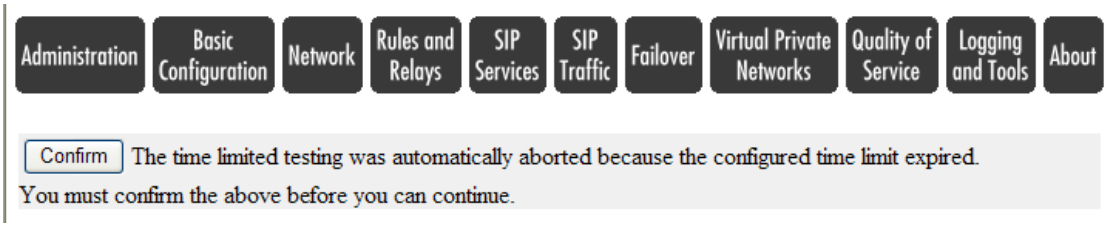


Possible Problems and Resolutions

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"

4.1.7 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.

4.2 INGATE WEB GUI CONFIG

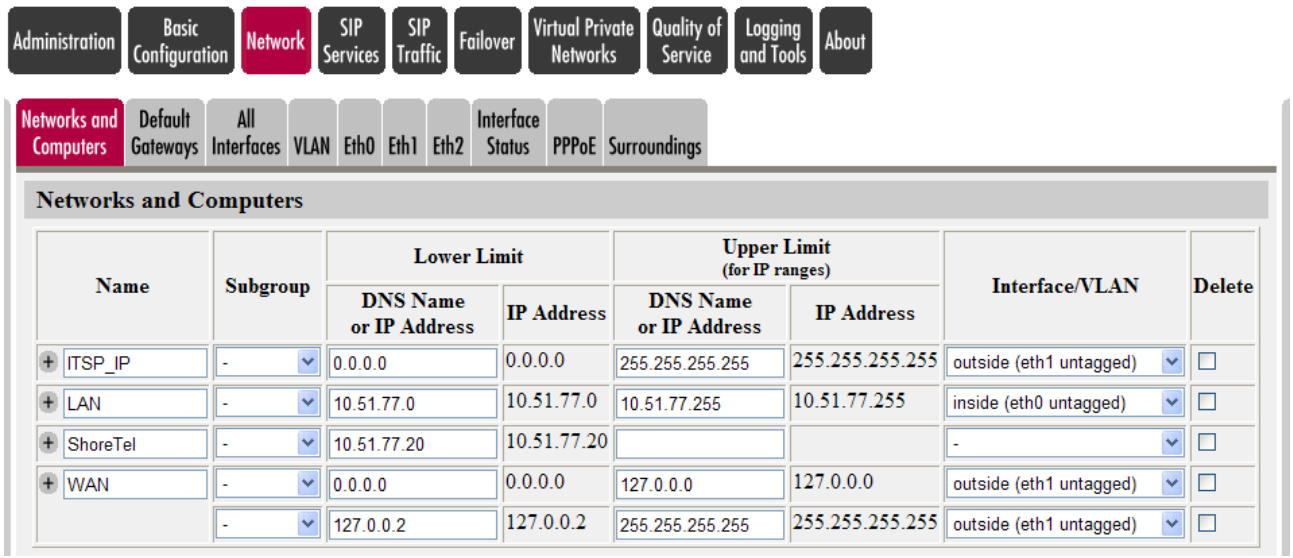
Configure your Ingate Firewall or Ingate SIParator to get basic network connectivity on all applicable interfaces. Please refer to the Reference Guide and other documentation as needed.
Remember to configure the following:

- Assign IP addresses on the inside and outside interface. For DMZ SIParators, use one interface only. (Network -> All Interfaces)
- Assign a default gateway. (Network -> Default Gateway)
- Assign a DNS server address. (Basic Configuration -> Basic Configuration)
- Define the IP subnet allowed to configure the Ingate and the interfaces to use for configuration. (Basic Configuration -> Access Control)

First make these basic settings and apply the configuration to have the unit working in your network environment. Then proceed with the following settings to get SIP Trunking to work with your service provider.

4.2.1 Network - Network and Computers

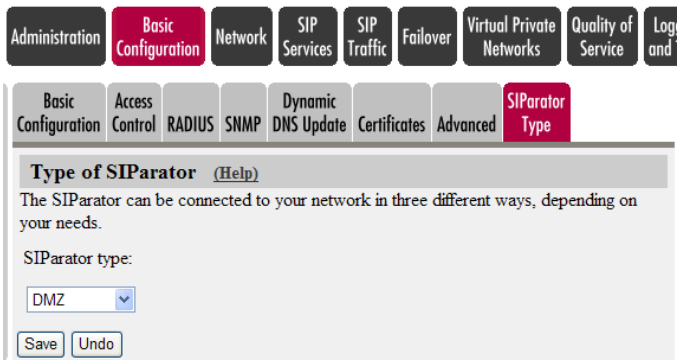
- Add a network for the Service Provider (ITSP IP). If you don't know the IP addresses used, you can put in 0.0.0.0 as lower limit and 255.255.255.255 as upper limit. In this way, requests from any IP address will be accepted.
- Add a network for the LAN (inside IP range).



Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
ITSP_IP	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	☐
LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	☐
ShoreTel	-	10.51.77.20	10.51.77.20			-	☐
WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	☐
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	☐

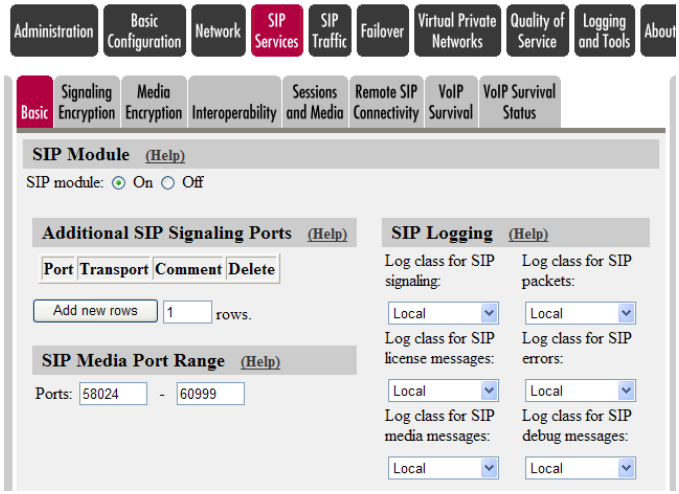
4.2.2 Basic Configuration - SIParator Type (SIParator Only)

Use the appropriate SIParator configuration for your deployment.



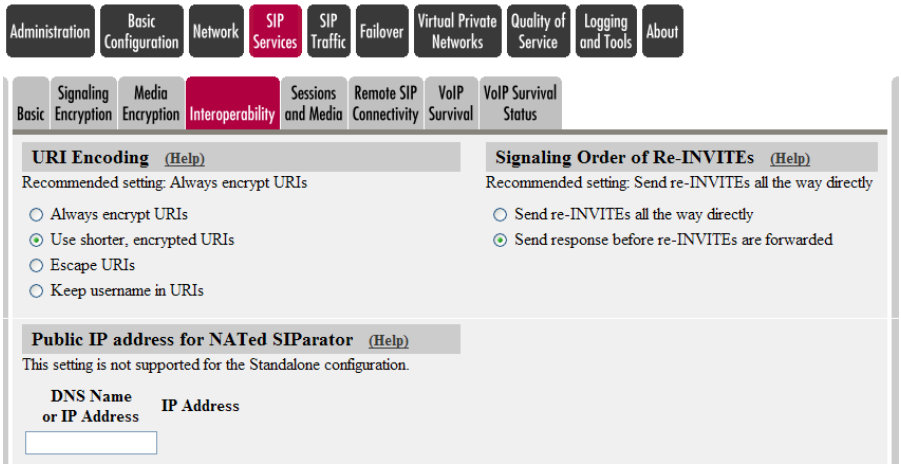
4.2.3 SIP Service - Basic

- SIP Module: On.



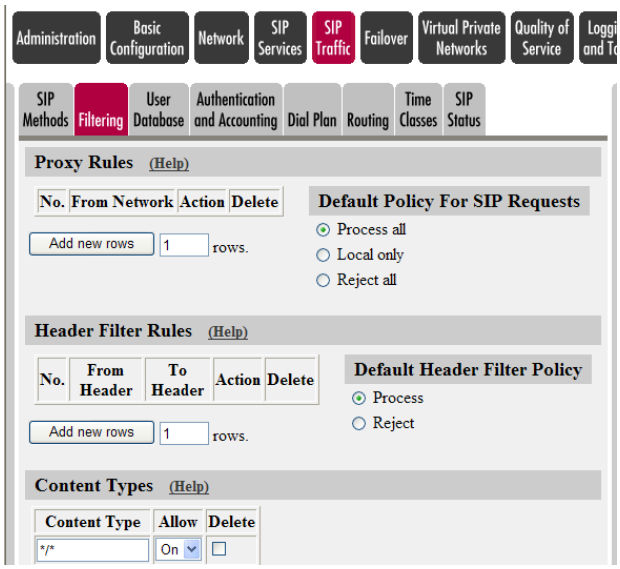
4.2.4 SIP Service – Interoperability

1. URI Encoding – Use shorter, encrypted URI
2. Signaling Order of Re-INVITEs – Send response before re-INVITE are forwarded
3. Public IP address for NATed SIParator – Only in DMZ, DMZ/LAN, and LAN configurations, assign the External Firewall Public IP address



SIP Traffic – Filtering

1. Under Proxy Rules, change the Default Policy for SIP Requests to "Process All".
2. Content Type: Add */* and Allow - ON



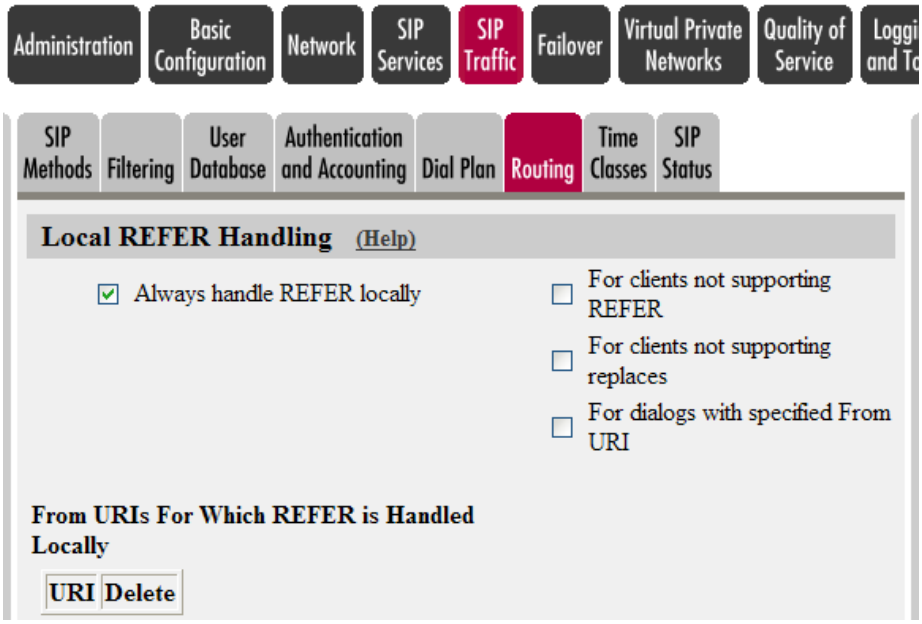
4.2.5 SIP Traffic – User Database

Configure an account with details as provided from the ITSP.

4.2.6 SIP Traffic – Routing

- Local REFER handling: check Always handle REFER locally.

The configuration of the Ingate is now done and the changes must be applied on the Administration page to take effect. **Note:** This can also be done dynamically using the Dial Plan with a Regular Expression in the Forward To, with an expression that looks like "sip:$1@10.51.77.20;b2bua", the ";b2bua" indicates to the Ingate to use the Local REFER handling.



4.2.7 SIP Traffic – Dial Plan

Configure the Dial Plan according to the picture below.

inGate Firewall Configured by Ingate Startup Tool Version 2.6.4 Log Out

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

SIP Methods | Filtering | Local Registrar | Authentication and Accounting | SIP Accounts | Dial Plan | Routing | SIP Status | IDS/IPS | IDS/IPS Status | SIP Test | SIP Test Status

Use Dial Plan (Help)

- On
- Off
- Fallback

Emergency Number (Help)

911

Matching From Header (Help)

Name	Use This ... Username	Use This ... Domain	... Or This Reg Expr	Transport	Network	Delete Row
LAN	*	*		UDP	LAN	☐
ShoreTel	*	*		UDP	ShoreTel	☐
Skype	*	*		UDP	ITSP_IP	☐
WAN	*	*		Any	WAN	☐

Add new rows 1 rows.

Matching Request-URI (Help)

Name	Use This ... Prefix	Use This ... Head	Use This ... Tail	Use This ... Min. Tail	Use This ... Domain	... Or This Reg Expr	Delete Row
Inbound			-			ɔ:(.*)@67.203.148	☐
Outbound			any character		10.24.0.4		☐

Add new rows 1 rows.

Forward To (Help)

Name	Subno.	Use This ... Account	... Or This Replacement Domain	... Or This Port	... Or This Transport	... Or This Reg Expr	Delete Row
ShoreTel	1	-			-	sip:$1@10.24.0.9	☐
Skype	1	99051000000200@sip.skype.com			-		☐

Add new rows 1 groups with 1 rows per group.

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix Forward	Add Prefix ENUM	ENUM Root	Time Class	Comment	Delete Row
1	ShoreTel	Outbound	Forward	Skype			-	-		☐
2	Skype	Inbound	Forward	ShoreTel			-	-		☐
3	WAN	-	Reject	-			-	-		☐

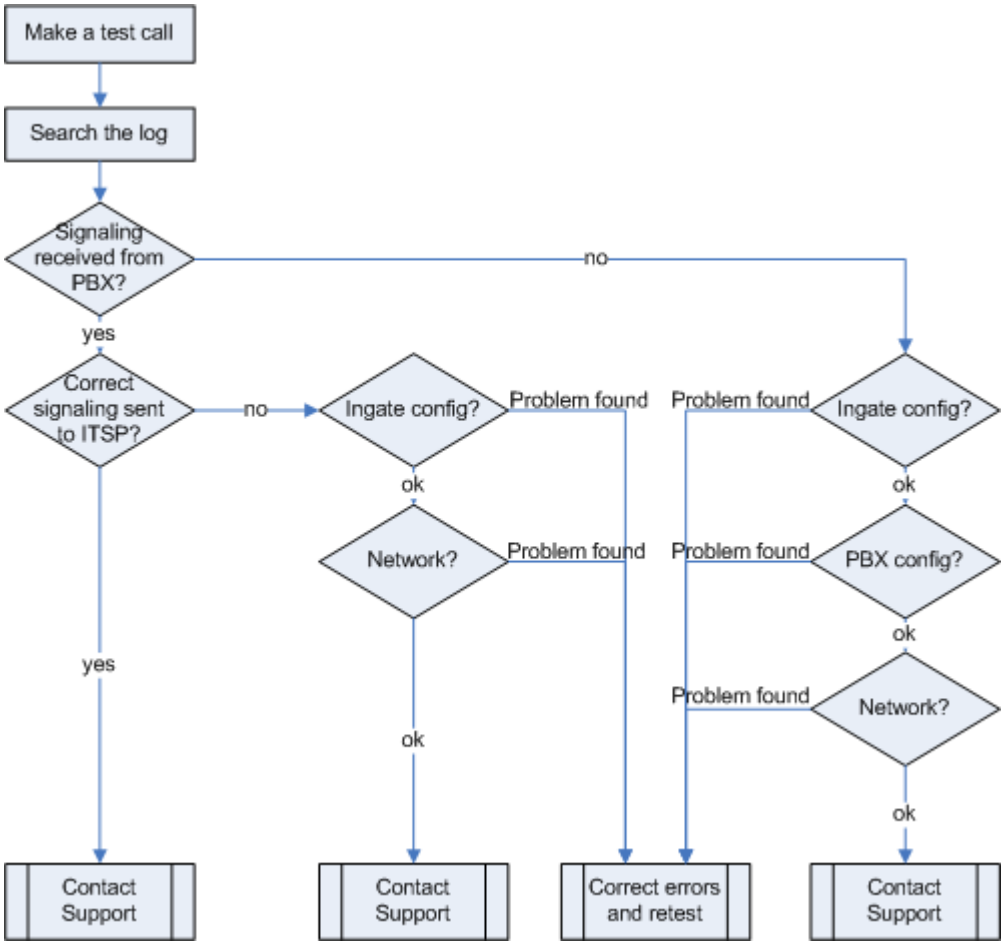
Add new rows 1 rows.

4.3 USING THE INGATE FOR TROUBLESHOOTING

4.3.1 Troubleshooting Outbound Calls

Symptom: When trying to make a call from an internal ShoreTel extension to PSTN, there is no ringing signal on the PSTN phone.

Note: If you get a ringing signal on the PSTN phone, these troubleshooting steps will not help you to find the problem. Please contact your sales representative for support.

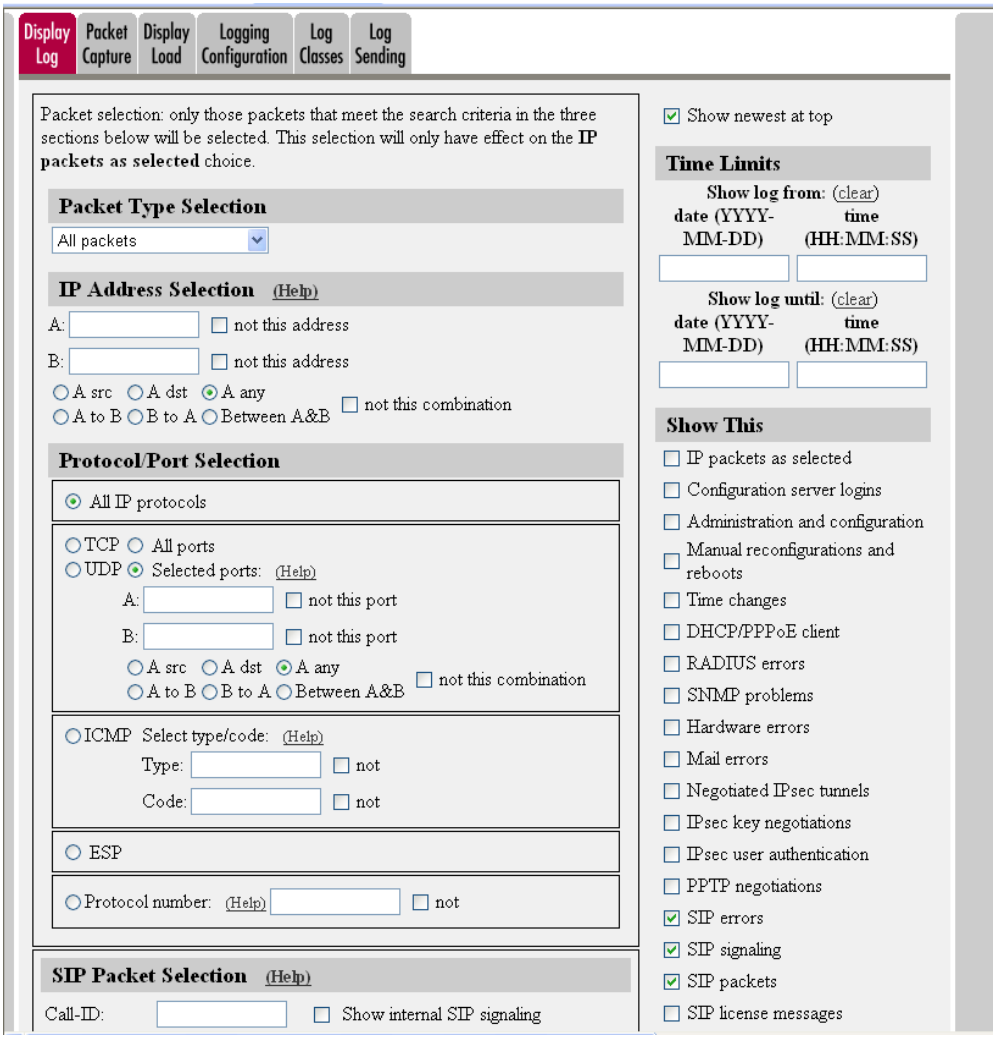


Outbound traffic troubleshooting overview

Get a log for the failing call:

First try to make a call to a PSTN number from a ShoreTel phone and notice the behavior on the ShoreTel phone as well as on the PSTN phone.

Next step is to search the log on the Ingate. Log in to the Ingate box and navigate to the Display Log page. Make necessary settings on this page according to the picture below. Especially make sure that you have the highlighted checkboxes in the correct state.



Then press "Display log" further down on the same page.

You will now see a log of all SIP packets received and sent by the Ingate, with the newest log entry on the top. Ensure the signaling is received from the ShoreTel:

Localize the call initiation from the ShoreTel by searching for "invite sip" in your browser. You should look for the first packet coming from the ShoreTel system that starts with a "recv from <IP address of the ShoreGear switch>" as you can see in the example (only the first lines of the log messages are shown here).

```
>>> Info: sipfw:  recv from 10.100.0.40:5060 via UDP connection 12746:
    INVITE sip:16037914522@10.100.0.13:5060 SIP/2.0
```

If you cannot find a packet like the one above, the problem is in the communication from Shoregear to the Ingate. Follow these steps:

1. Make sure the Ingate SIP module is turned on, SIP Services – SIP Module – On. Retest if you change any setting.
2. Make sure the ShoreTel configuration is correct. Check the IP address pointing at Ingate one extra time. Retest if you change any setting.
3. Make sure there is IP connectivity between the ShoreTel and Ingate. Contact your network administrator for assistance if needed.

If none of the steps above solves the problem, contact your sales representative for support.
Ensure the signaling to the ITSP works:

If you find the incoming packet, you should find a similar packet leaving the Ingate just above (just after in time) the incoming packet. The first rows of the outgoing packet will look something like this:

```
>>> Info: sipfw:  send sf (0x8422820) to 208.49.124.49:5060 via UDP connection 12748:
  INVITE sip:16037914522@208.49.124.49:5060;transport=udp SIP/2.0
```

If you don't see the outgoing packet, something is probably wrong with the Ingate configuration or you lack Internet connectivity:

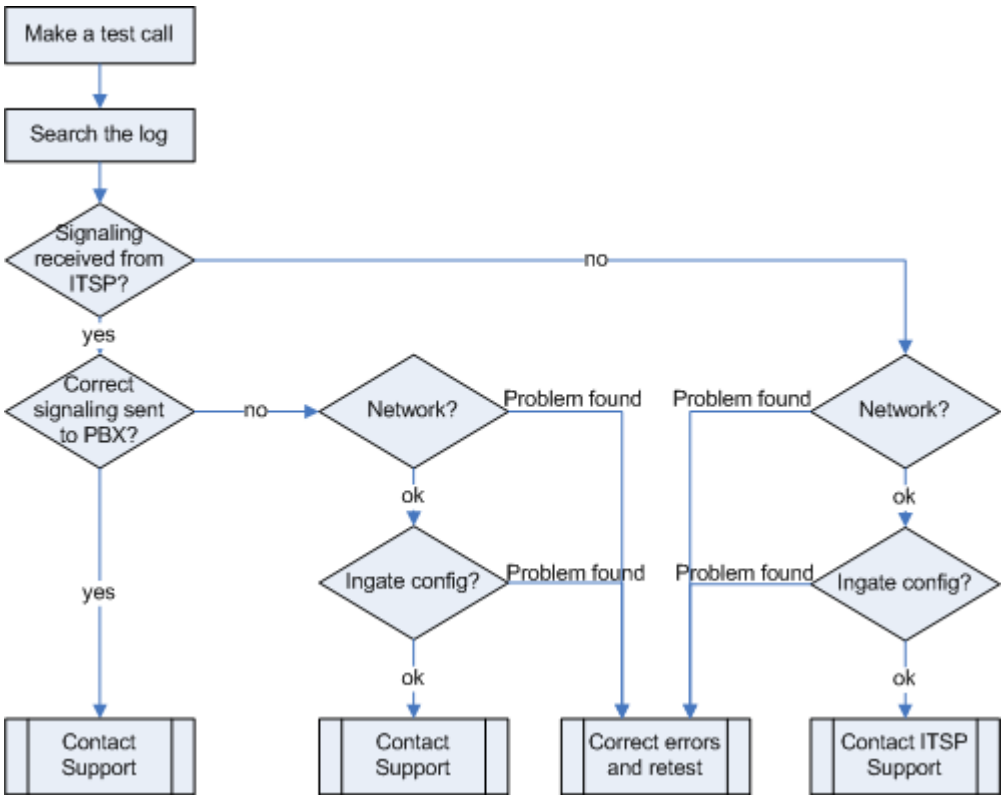
1. Make sure that the Ingate is configured correctly.
2. Make sure the IP connectivity between the Ingate and the ITSP is working. Contact your network administrator for assistance if needed.

If you see a packet sent from the Ingate, verify that it is sent to the IP address provided by the ITSP. If not, correct your configuration and retest.

If none of the steps above solves the problem, contact your sales representative for support.

4.3.2 Troubleshooting Inbound calls

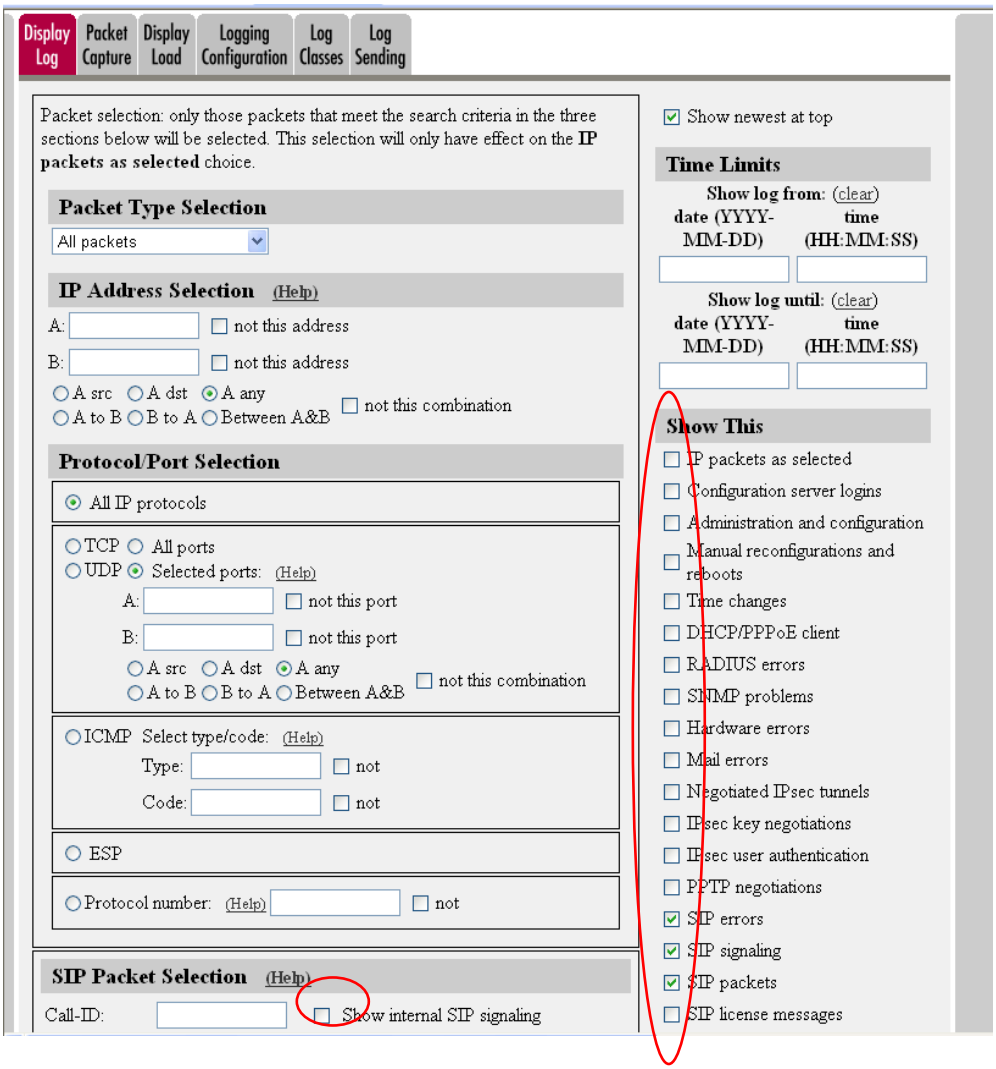
Symptom: When trying to make an inbound call to a ShoreTel phone via the SIP Trunk there is no ringing signal on the ShoreTel phone.
Note: If you get a ringing signal on the ShoreTel phone, these troubleshooting steps will not help you to find the problem. Please contact your sales representative for support.



Get a log for the failing call:

First try to make a call to a ShoreTel phone from a PSTN phone and notice the behavior on the ShoreTel phone as well as on the PSTN phone.

Next step is to search the log on the Ingate. Log in to the Ingate box and navigate to the Display Log page. Make necessary settings on the logging page according to the picture below. Especially make sure that you have the highlighted checkboxes in the correct state.



Then press "Display log" further down on the same page.

You will now see a log of all SIP packets received and sent by the Ingate, with the newest log entry on the top.

Ensure the signaling is received from the ITSP:
Localize the call initiation from the Trunking provider by searching for "invite sip" in your browser. (use Ctrl-F). You should look for the fist packet coming from the ITSP system that starts with a "recv from <IP address of the ITSP>" as you can see in the example (only the first lines of the log are shown below).

```
>>> Info: sipfw:  recv from 208.49.124.49:5060 via UDP connection 12748:
  INVITE sip:6023574058;npdi=yes@193.12.253.37:5060 SIP/2.0
```

If you cannot find a packet like the one above, the problem is in the communication from the ITSP to the Ingate. Follow these steps:

1. Make sure you have IP connectivity between the Ingate and your ITSP. Contact your network administrator for assistance if needed
2. Make sure the Ingate SIP module is turned on, SIP Services – SIP Module – On. Retest if you change any setting.

If you still don't see any packets in the log, contact your ITSP for further troubleshooting.
Ensure correct signaling to the Shoretel PBX:
If you find the incoming packet, you should find a similar packet leaving the Ingate just above (just after in time) the incoming packet. The first lines of the outgoing packet will look something like this:

```
>>> Info: sipfw:  send sf (0x8419848) to 10.100.0.40:5060 via UDP connection 12746:
  INVITE sip:6023574058;npdi=yes@10.100.0.40:5060;transport=udp SIP/2.0
```

If you don't see the outgoing packet, something is probably wrong with the Ingate configuration or you might lack a connection to your LAN where the ShoreTel is located:

1. Ensure you have IP connectivity between ShoreTel and the Ingate. Contact your network administrator for assistance if needed.
2. Make sure your Ingate is configured correctly.

If you see the outgoing packet, make sure the IP address it is sent to is the one used by the Shoregear switch.
If the call still fails after executing the steps described above, please contact your sales representative for support.

5 DOCUMENT AND SOFTWARE COPYRIGHTS

5.1 TRADEMARKS

5.2 DISCLAIMER

To be "ShoreTel Certified" means that Technology Partner's product will inter-operate with the ShoreTel system, but ShoreTel does not certify that the features or functionality of Technology Partner's product will perform as specified by Technology Partner nor that Technology Partner's product will meet your specific application needs or requirements. To inter-operate means that Technology Partner's product is able to exchange, use and share information with the ShoreTel system.

5.3 COMPANY INFORMATION

ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085 USA
+1.408.331.3300
+1.408.331.3333 fax