ShoreTel	Broadvox	Innovation Network App Note IN- 13056 Date : Sept, 2013
Product: ShoreTel | Ingate | Broadvox		**System version:** ShoreTel 13.x

ShoreTel, Ingate & Broadvox for SIP Trunking

SIP Trunking allows the use of Session Initiation Protocol (SIP) communications from Broadvox instead of the typical analog, Basic Rate Interface **(**BRI), T-1 or E-1 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 Broadvox for SIP Trunking.

Table of Contents

ShoreTel tests and validates the interoperability of the Member's solution with ShoreTel's published software interfaces. ShoreTel does not test, nor vouch for the Member's development and/or quality assurance process, nor the overall feature functionality of the Member's solution(s). ShoreTel does not test the Member's solution under load or assess the scalability of the Member's solution. It is the responsibility of the Member to ensure their solution is current with ShoreTel's published interfaces.

The ShoreTel Technical Support organization will provide Customers with support of ShoreTel's published software interfaces. This does not imply any support for the Member's solution directly. Customers or reseller partners will need to work directly with the Member to obtain support for their solution.

Overview

This document provides details for connecting the ShoreTel® system through the Ingate SIParator® / Firewall to Broadvox for SIP Trunking, which enables audio communications. The document specifically focuses on the configuration procedures needed to set up these systems to interoperate.

Broadvox Overview and Contact

Broadvox is a leader in providing customized integrated managed VoIP communication and collaboration solutions to support SMB, Enterprise and Carrier customers. It has deployed one of the largest, full-featured global VoIP networks and is trusted by over 300 telecommunications carriers, ASPs, ISPs and more than 10,000 businesses and 4,000 partners nationwide. Broadvox delivers SIP Trunking, SIP origination and termination services, broadband and Hosted Communications. Broadvox is headquartered in Dallas, Texas. For more information, visit www.broadvox.com.

Contact:
Technical Support:
Email: techsupport@Broadvox.com
Phone: 888-849-9608

Ingate Overview & Contact

INGATE SYSTEMS offers the only fully SIP capable security products offering features important to enterprise adoption of SIP Trunking. The Ingate Firewall® offers a single device to protect the network and manage SIP traffic. The Ingate SIParator® allows the enterprise to adopt SIP without replacing their existing firewall. Both products include a SIP Application Layer Gateway (ALG), proxy and registrar that enable SIP signaling to traverse the firewall, support for dynamic media port management to keep the network safe, encryption for privacy, added routing capabilities to make the installation of SIP Trunks simple and inexpensive, and remote SIP connectivity so that the enterprise can offer SIP services to their remote workers.

NORTH AMERICA
For general sales questions, please contact your reseller or contact Ingate directly at:
Steven Johnson
603-883-6569
Steve@ingate.com
www.ingate.com

Resellers who want to start selling this solution should contact:
Steven Johnson
603-883-6569
Steve@ingate.com
www.ingate.com

EMEA
For general sales questions, please contact your reseller or contact Ingate directly at:
Ingate Systems HQ
+46 86007750

sales@ingate.com
www.ingate.com

Resellers who want to start selling this solution should contact:
Ingate Systems HQ
+46 86007750
sales@ingate.com
www.ingate.com

Architecture Overview

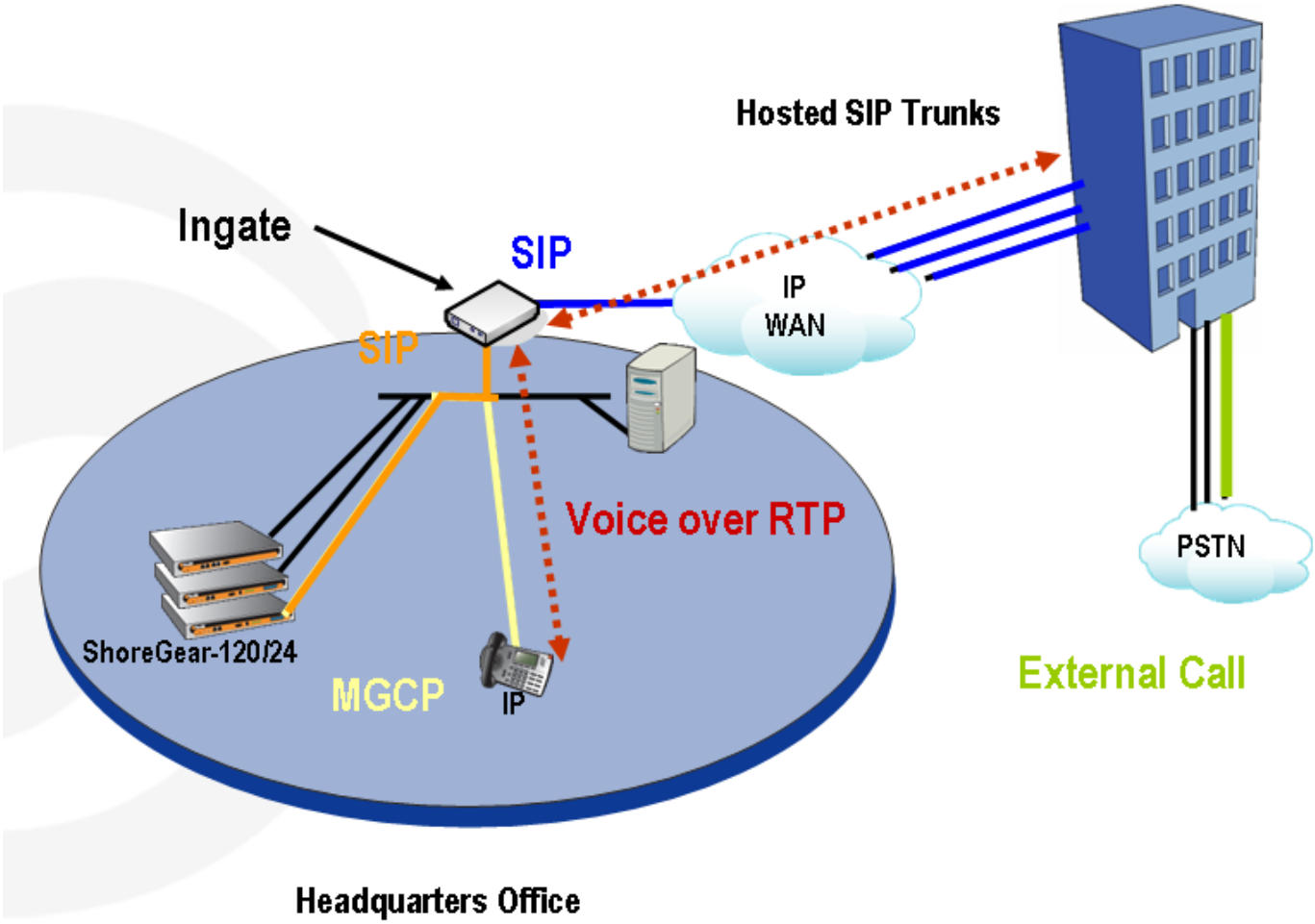
SIP Trunking allows the use of Session Initiation Protocol (SIP) communications from an Internet Telephony Service Provider (ITSP) instead of the typical analog, Basic Rate Interface (BRI), T1 or E1 trunk connections. Having the pure IP trunk to the ITSP allows for more control and options over the communication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

ShoreTel and Ingate have teamed up to build a solid security focused solution, ShoreTel being the IP PBX which resides 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 Broadvox 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 and additionally intelligent SIP routing and SIP features such as:

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

The image below shows a high level drawing of a basic ShoreTel / Ingate / ITSP design. This drawing only represents SIP and Real-time Transfer protocol (RTP) traffic. The next section of this application note covers actual deployment design options.

FIGURE 2 – ARCHITECTURAL OVERVIEW



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. Ingate Firewalls handle both data and voice traffic as a single device. 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 can be accomplished in three primary ways. The first is the most commonly deployed though each configuration offers its own advantages for the enterprise:

- **Configuration 1:** Single leg/DMZ only, Firewall logs all activity
- **Configuration 2:** DMZ/LAN, Reduced load on firewall
- **Configuration 3:** Two legged/Standalone, SIP traffic separate from data traffic

FIGURE 3 – INGATE 3 POSSIBLE CONFIGURATIONS

Requirements, Certification and Limitations

Any Ingate SIParator or Ingate Firewall model will work in this configuration. In a Trunking scenario it is required to have the Ingate SIP Trunking module installed.

A few traversal licenses are included with the Ingate unit at delivery. Typically one traversal license will be needed for each expected concurrent phone call on the SIP Trunk. Additional licenses can be bought via your Ingate reseller.

G711 and G729 are the preferred codec's on Broadvox's network. ShoreTel does not support more than one G729 dialog for a single local switchboard, therefore some call scenarios involving multiple inbound and outbound dialogs will fail if the Ingate is set to pass only G729, even though ShoreTel is set for G729 first and G711 (or any other) second. With this combination ShoreTel will negotiate to use G729 for the first dialog but not for subsequent dialogs. It's in these subsequent dialogs where the chosen codec offered by ShoreTel will be stripped by the Ingate since it's set to pass only G729. The requirement here would be to not set the Ingate to pass only G729, but to setup the Ingate to also include other codec's that are in the chosen ShoreTel codec list.

All outbound calls to the PSTN will require an assigned prefix as per customer's requirements.

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	5.0.1
ShoreTel 13.x	✓

Broadvox network equipment:
Broadvox Fusion Version 1.0

Broadvox Validation Test Results

Basic test plan:

TABLE 1-1: INITIALIZATION AND BASIC CALLS

ID	Name	Description	Results
1.0	Configuration Application Note	Innovation Network Lab will use the configuration application note provided by the vendor to configure the vendor's product to work with the ShoreTel system.	Pass
1.1	Setup and initialization	Verify successful setup and initialization of the SUT	Pass
1.2	Outbound Call (Domestic)	Verify calls outbound placed through the SUT reach the external destination.	Pass
1.3	Inbound Call (Domestic)	Verify calls received by the SUT are routed to the default trunk group destination.	Pass
1.4	Device restart – Power Loss	Verify that the SUT recovers after power loss to the SUT	Pass
1.5	Device restart – Network Loss	Verify the SUT recovers after loss of network link to the SUT.	Pass
1.6	All Trunks Busy – Inbound Callers	Verify an inbound callers hears busy tone when all channels/trunks are in use	Pass
1.7	All Trunks Busy – Outbound Callers	Verify an outbound callers hears busy tone when all channels/trunks are in use	Pass
1.8	Incomplete Inbound Calls	Verify proper call progress tones are provided and proper call teardown for incomplete inbound calls.	Pass

TABLE 1-2: MEDIA AND DTMF SUPPORT

ID	Name	Description	Notes
2.1	Media Support – ShoreTel to SUT	Verify call connection and audio path from a ShoreTel phone to an external destination through the service provider using all supported codes with both sides set to a common codec.	Pass
2.2	Media Support – SIP Reference to SUT	Verify call connection and audio path from a SIP Reference phones to an external destination through the service provider using all supported codes with both sides set to a common codec.	Pass
2.3	Codec Negotiation	Verify codec negotiation between the SUT and the calling device with each side configured for a different codec.	Pass[1]
2.4	DTMF Transmission – Out of Band / In Band	Verify transmission of in-band and out-of-band digits per RFC 2833 for various devices connected to the SUT.	Pass
2.5	Auto Attendant Menu	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the desired extension.	Pass
2.6	Auto Attendant Menu "Dial by Name"	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the desired extension using the "Dial by Name" feature.	Pass
2.7	Auto Attendant Menu checking Voice Mail mailbox	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the Voice Mail Login Extension.	Pass

TABLE 1-3: PERFORMANCE & QUALITY OF SERVICE

ID	Name	Description	Notes
3.1	Voice Quality Service Levels	Verify the SUT can provide a voice quality SLA across the WAN from the customer premises to the SUT SIP gateway.	Not Tested

[1] With some call scenarios ShoreTel does not support more than a single G729 dialog; therefore audio issues occur when the Ingate is set to pass only G729. Here ShoreTel is selecting a different codec for the second dialog of the call which the Ingate removes. The recommendation is to not set the Ingate to pass G729 only, include others or set to pass all codecs.

ID	Name	Description	Notes
3.2	Capacity Test	Verify the service provider interface can sustain services through period of heavy outbound and inbound load.	Pass
3.3	Post Dial Delay	Verify that post dial delay is within acceptable limits.	Pass
3.4	Billing Accuracy	Verify that all test calls made are accurately reflected in the SUT's CDR and billing reports.	Pass

TABLE 1-4: ENHANCED SERVICES AND FEATURES

ID	Name	Description	Notes
4.1	Caller ID Name and Number - Inbound	Verify that Caller ID name and number is received from SIP endpoint device	Pass
4.2	Caller ID Name and Number - Outbound	Verify that Caller ID name and number is sent from SIP endpoint device	Pass
4.3	Hold from SUT to SIP Reference	Verify successful hold and resume of connected call	Pass[2]
4.4	Call Forward - SUT	Verify outbound calls that are being forwarded by the SUT are redirected and connected to the appropriate destination.	Pass
4.5	Call Forward – External PSTN Number	Verify outbound calls that are being forwarded by the SUT are redirected and connected to the appropriate destination.	Pass
4.6	Call Transfer – blind	Verify a call connected from the SUT to the ShoreTel phone can be transferred to an alternate destination.	Pass
4.7	Call Transfer – Consultative	Verify a call connected from the SUT to the ShoreTel phone can be transferred to an alternate destination.	Pass
4.8	Conference – ad hoc	Verify successful ad hoc conference of three parties	Pass
4.9	Inbound DID/DNIS	Verify the SUT provides inbound "dialed number information" and is correctly routed to the configured destination.	Pass
4.10	Outbound 911	Verify that outbound calls to 911 are routed to the correct PSAP for the calling location and that caller ID information is delivered.	Pass
4.11	Operator Assisted	Verify that 0+ calls are routed to an operator for calling assistance.	N/A
4.12	Inbound / Outbound call with Blocked Caller ID	Verify that calls with Blocked Caller ID route properly and the answering phone does not display any Caller ID information.	Pass
4.13	Inbound call to a Hunt Group	Verify that calls route to the proper Hunt Group and are answered by an available hunt group member with audio in both directions using G.729 and G.711 codecs.	Pass

[2] When SIP Bria client version 3.5.2-70364 is assigned as a ShoreTel user extension, file based MoH is not heard to the caller placed on hold by the Bria. This is a known limitation for some 3rd party SIP endpoints.

ID	Name	Description	Notes
4.14	Inbound call to a Workgroup	Verify that calls route to the proper Workgroup and are answered successfully by an available workgroup agent with audio in both directions using G.729 and G.711 codecs.	Pass
4.15	Inbound call to DNIS / DID and leave a voice mail message	Verify that inbound calls to a user, via DID / DNIS, routes to the proper user mailbox and a message can be left with proper audio.	Pass
4.16	Call Forward – "FindMe"	Verify that inbound calls are forwarded to a user's "FindMe" destination.	Pass
4.17	Call Forward Always	Verify that inbound calls are immediately automatically forwarded to a user's external destination.	Pass
4.18	Inbound / Outbound Fax calls	Verify that inbound / outbound fax calls complete successfully.	Pass
4.19	ShoreTel Converged Conferencing Server	Verify that inbound calls are properly forwarded to the ShoreTel Converged Conferencing Server and it properly accepts the access code and you're able to participate in the conference bridge.	Not Tested
4.20	Inbound call to Bridged Call Appearance (BCA) extension	Verify that inbound calls properly presented to all of the phones that have BCA configured and that the call can be answered, placed on-hold and then transferred.	Pass
4.21	Inbound call to a Group Pickup extension	Verify that inbound calls properly presented to all of the phones that have Group Pickup configured and that the call can be answered, placed on-hold and then transferred.	Pass
4.22	Office Anywhere External	Verify that inbound calls are properly presented to the Office Anywhere External PSTN destination.	Pass
4.23	Simul Ring	Verify that inbound calls are properly presented to the desired extension and the "Additional Phones" destinations.	Pass
4.24	MakeMe Conference	Verify that an inbound call can be conferenced with three (or more) additional parties	Pass
4.25	Park / Unpark	Verify that an inbound call can be parked and unparked	Pass
4.26	Call Recording	Verify that external calls can be recorded via the SIP Trunk using ShoreTel Communicator	Pass

ID	Name	Description	Notes
4.27	Silent Monitor / Barge-In / Whisper Page	Verify that external calls can be silently monitored, barged-in and whisper paged via the SUT.	Pass
4.28	Long Duration – Inbound	Verify that an inbound call is established for a minimum of 30 minutes.	Pass
4.29	Long Duration – Outbound	Verify that an outbound call is established for a minimum of 30 minutes.	Pass
4.30	Contact Center	Verify that an inbound call can be established directly to the ShoreTel Contact Center, that all prompts are heard and the agent can answer the call.	Pass
4.31	ShoreTel Mobility Router (SMR)	Verify that the SMR can be used with the SUT	Not Tested

Table 1-5: Security

ID	Name	Description	Notes
5.1	Registration / Digest Authentication	Verify the SUT supports the use of registration / digest authentication for service access for inbound and outbound calls.	N/A

Configuration Overview

The configuration information below shows examples for configuring ShoreTel, Ingate, and Broadvox. Even though configuration requirements can vary from setup to set up, the information provided in these steps, along with the Planning and Installation Guide and documentation provided by Ingate and Broadvox should prove to be sufficient. However, every design can vary and some may require more planning than others. All testing in this document was done using Shoretel 13.2 with file based Music on Hold enabled.

ShoreTel Unsupported Features

Please refer to the ShoreTel Administration Guide, Chapter 18 – Session Initiation Protocol, for general supported and unsupported features when utilizing SIP Trunks.

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.

ShoreTel System Settings – General

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.

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"** (**Figure 4**).

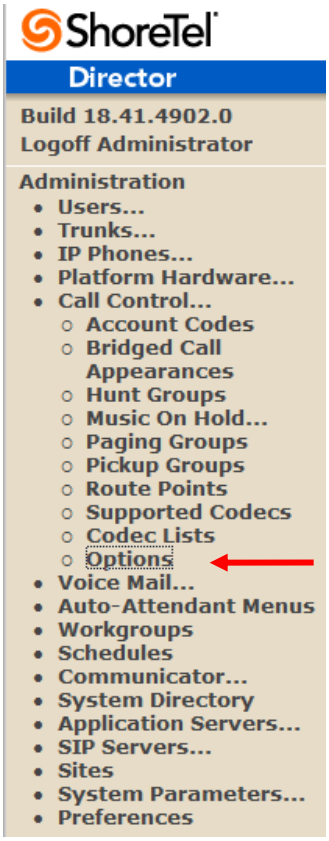


Figure 4 - Administration Call Control Options

The "Call Control Options" screen will then appear (**Figure 5**).

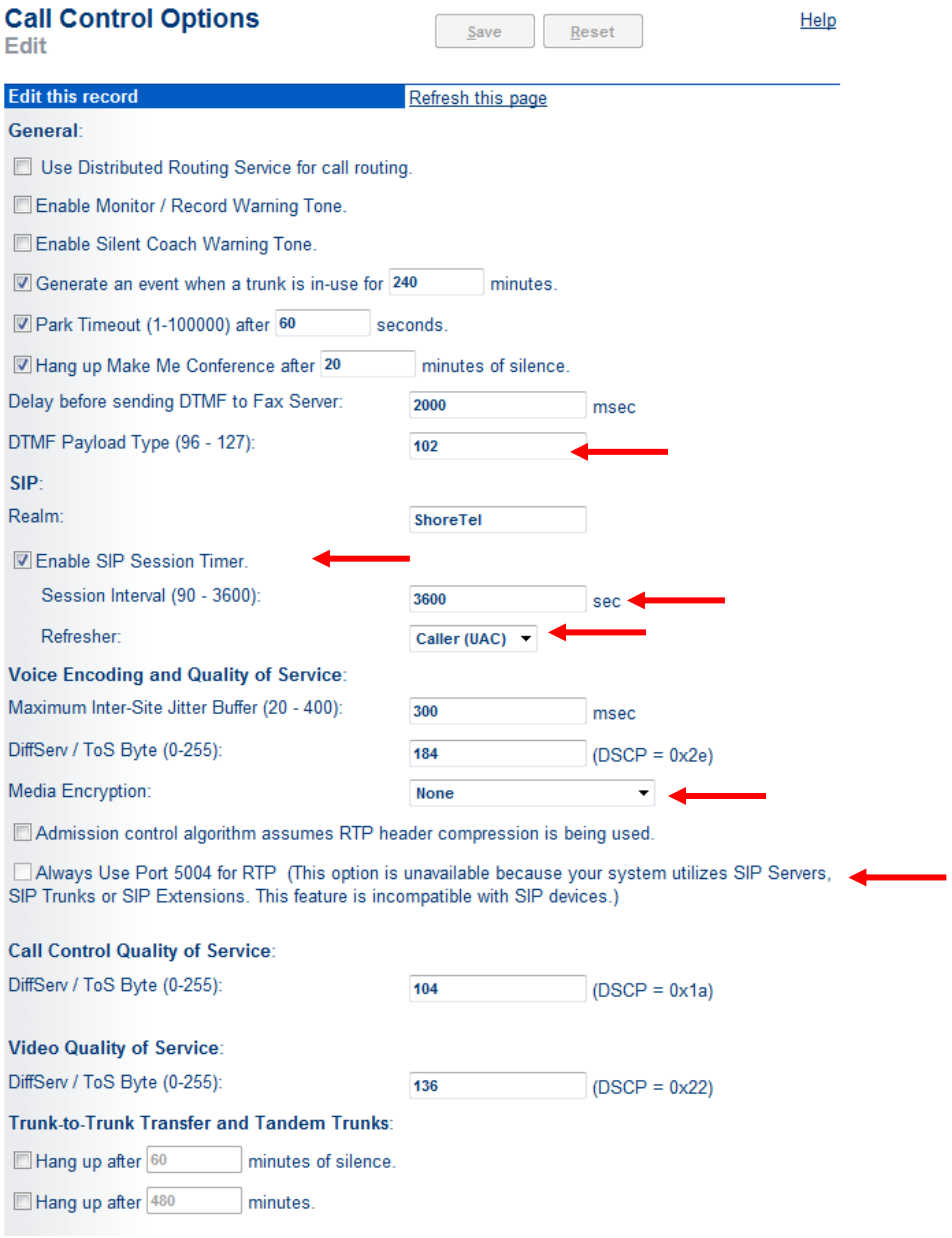


Figure 5 - Call Control Options

In the **"General"** parameters, the **"DTMF Payload Type (96 – 127)"** defaults to a value of "102", and no modification is necessary to interoperate with Broadvox.

Within the "**SIP"** parameters; confirm that the appropriate settings are made for the "**Realm**" "**Enable SIP Session Timer"** and **"Always Use Port 5004 for RTP"** parameters.

The "**Realm**" parameter is used in authenticating all SIP devices. It is typically a description of the computer or system being accessed. Changing this value will require a reboot of all ShoreGear switches serving SIP extensions. It is not necessary to modify this parameter to get the ShoreTel IP PBX system functional with Broadvox. Verify that the "**Enable SIP Session Timer**" box is checked (enabled). Next the Session Interval Timer needs to be set. The recommended setting for **"Session Interval"** is "3600" 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.

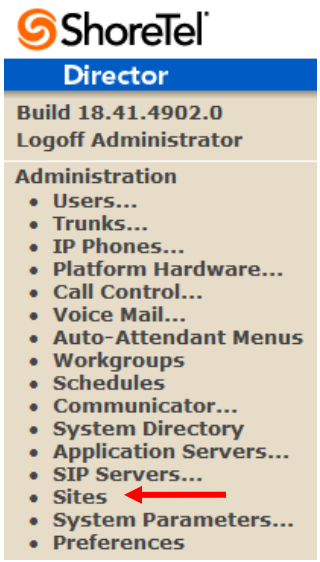
The next settings to verify are the **"Voice Encoding and Quality of Service"**, specifically the **"Media Encryption"** parameter, make sure this parameter is set to "None", otherwise you may experience one-way audio issues. Please refer to ShoreTel's Administration Guide for additional details on media encryption and the other parameters in the "Voice Encoding and Quality of Service" area.

The ShoreTel legacy parameter **"Always Use Port 5004 for RTP"** should be disabled by default, if it's enabled you will need to disable it. Disabling 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 parameter is disabled, Media Gateway Control Protocol (MGCP) will no longer use UDP port 5004; MGCP and SIP traffic will use dynamic UDP ports. Once this parameter is disabled (unchecked), make sure that "everything" (IP Phones, ShoreGear® Switches, ShoreWare Server, Distributed Voice Mail Servers / 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.

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"** (**Figure 6**).

Figure 6 – Site Administration



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 changes required to the "Edit Site" screen is to the **"Admission Control Bandwidth"** and **"Intra-Site / Inter-Site Calls"** parameters (**Figure 7**).

Figure 7 – Site Bandwidth settings

Note: Bandwidth of 2046 is just an example. Please refer to the *ShoreTel 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 trunk calls may be counted against the site bandwidth. Bandwidth needs to be set appropriately based on site setup and configuration with Broadvox's SIP Trunking. See the *ShoreTel Planning and Installation Guide* for more information.

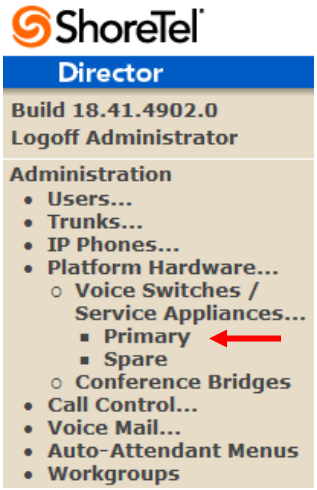
Sites Edit screen - Intra / Inter-Site Calls

By default ShoreTel 13.2 has 11 built-in codecs, these codecs can be grouped as "Codec Lists" and defined in the sites page for "Inter-site" and "Intra-site" calls. Configure the "Intra-Site Calls" option to a "Codec List" that contains the desired codecs and save the change. Codec lists are found under **"Call Control "**, then **"Codec Lists"**. The site that the SIP Trunk Group belongs to will determine which "Intra-Site" Codec List will be utilized be sure to move the desired codec up the list for higher priority. Please refer to the *ShoreTel Planning and Installation Guide* for additional information.

Switch Settings – Allocating Ports for SIP Trunks

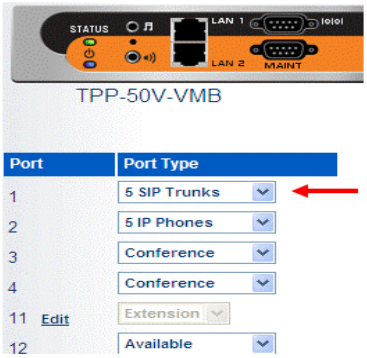
The final general settings to input are the ShoreGear switch settings. These changes are modified by selecting **"Administration"**, then **"Platform Hardware…",** then **"Voice Switches / Service Appliances…"** followed by **"Primary"** in ShoreWare Director (**Figure 8**).

Figure 8 - Administration Switches



This action brings up the **"Switches"** screen. From the "Switches" screen simply select 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 (**Figure 9**).

Figure 9 - ShoreGear Switch Settings



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

Note: If you would like Music On Hold (MOH) to be played when calls are on hold, then the MOH source needs to be connected to the same ShoreGear switch where the SIP Trunks are provisioned. File based Music on Hold doesn't require a physical connection to the switch and is accomplished by placing specially formatted WAV files on the HQ server. See the System Administration guide for more information.

ShoreTel 13 adds an additional option to the "Port Type" of half-width ShoreGear switches. The new selection is "SIP Media Proxy", it ensures that the ShoreTel system that is using SIP Trunks have feature parity with PRI trunks. These include RFC 2833 DTMF detection for Office Anywhere External or Simultaneous Ring calls, three party mesh conferencing (without needing to configure "MakeMe" conference ports), call recording, Silent Monitoring, Barge-In, Whisper Page, and Invites with no SDP and when there's no common codec between ITSP and the local extension. For further information on "SIP Media Proxy" please refer to Chapter 18 of the ShoreTel 13 System Administration Guide.

ShoreTel System Settings – Trunk Groups

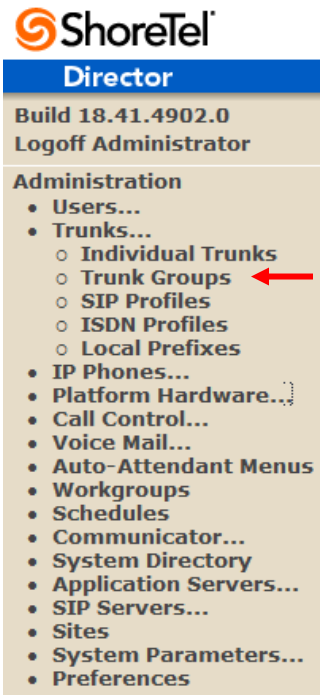
ShoreTel Trunk Groups only support Static IP Addresses for Individual Trunks.

In trunk planning, the following needs to be considered.

- Ingate SIParator LAN and WAN interfaces should always be configured to use a "Static" IP Address.

The settings for Trunk Groups are changed by selecting **"Administration",** then **"Trunks"** followed by **"Trunk Groups"** within ShoreWare Director (**Figure 10**).

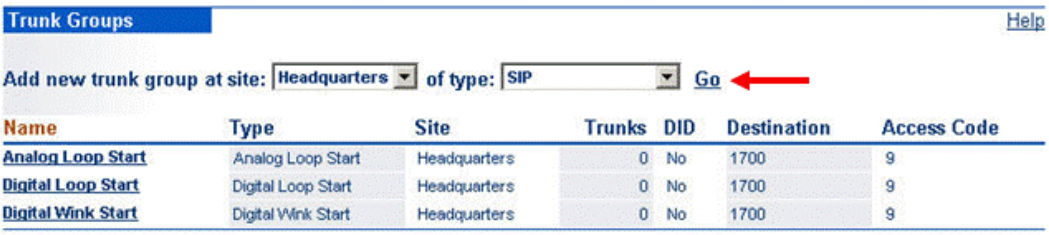
Figure 10 – Administration Trunk Groups



Administration Trunk Groups

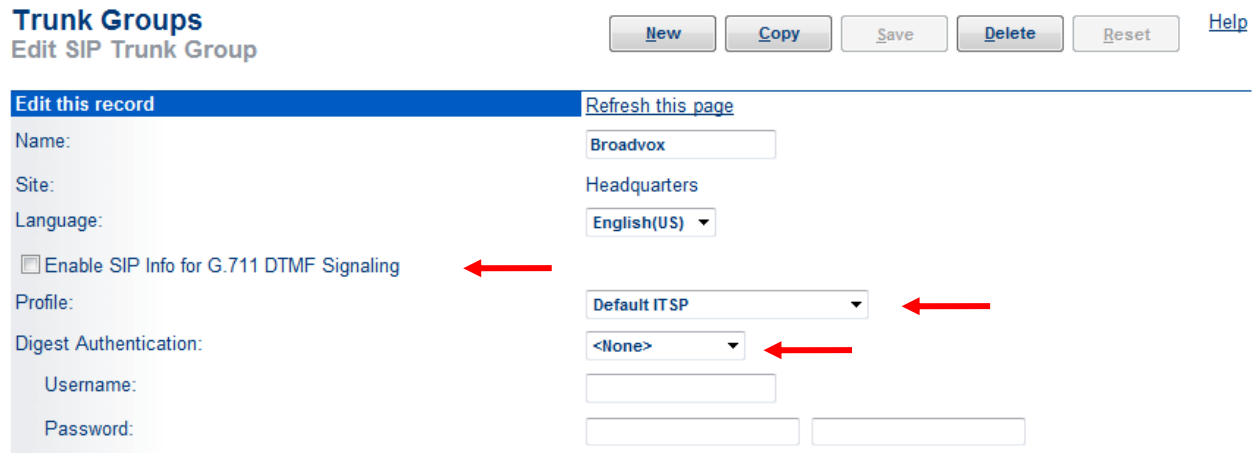
This selection brings up the "Trunk Groups" screen (**Figure 11**).

Figure 11 - Trunk Groups Settings



From the pull down menus on the "Trunk Groups" screen, select the site desired and select the **"SIP"** trunk type to configure. Then click on the **"Go"** link from **"Add new trunk group at site"**. The "Edit SIP Trunk Group" screen will appear (**Figure 12**).

Figure 12 – Edit SIP Trunk Group



The next step within the "Edit SIP Trunks Group" screen is to input the name for the trunk group. In the example in Figure 12, the name "Broadvox " has been created.

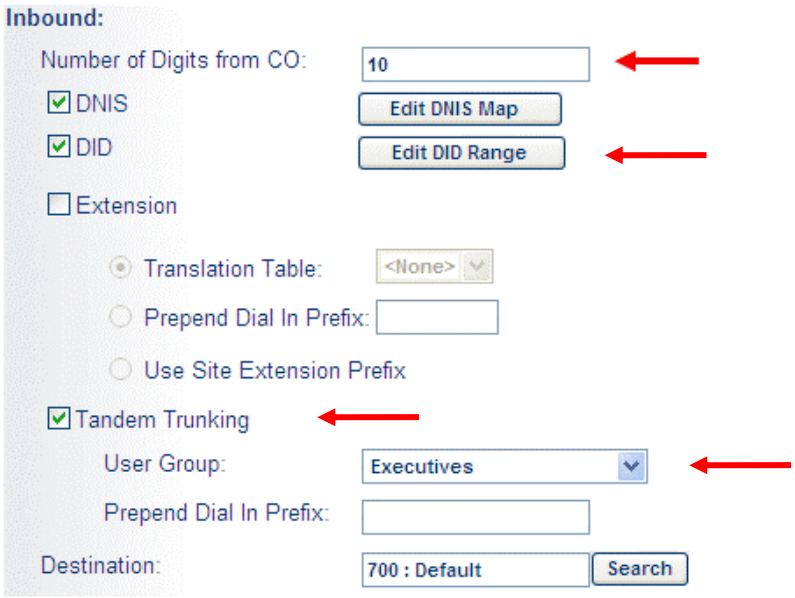
The **"Enable SIP Info for G.711 DTMF Signaling"** parameter should not be enabled (checked). Enabling SIP info is currently only used with SIP tie trunks between ShoreTel systems.

The **"Profile:"** parameter should be left at a default setting of "Default ITSP", it is not necessary to modify this parameter when connecting to Broadvox SIP Trunking via an Ingate SIParator. If there's another setting defined, click on the down arrow (pull-down menu) and select "Default ITSP".

The **"Enable Digest Authentication"** parameter defaults to "<None>" and modification is not required when connecting to Broadvox SIP Trunking.

The next item to change in the "Edit SIP Trunks Group" screen is to make the appropriate settings for the **"Inbound:"** parameters. (**Figure 13**).

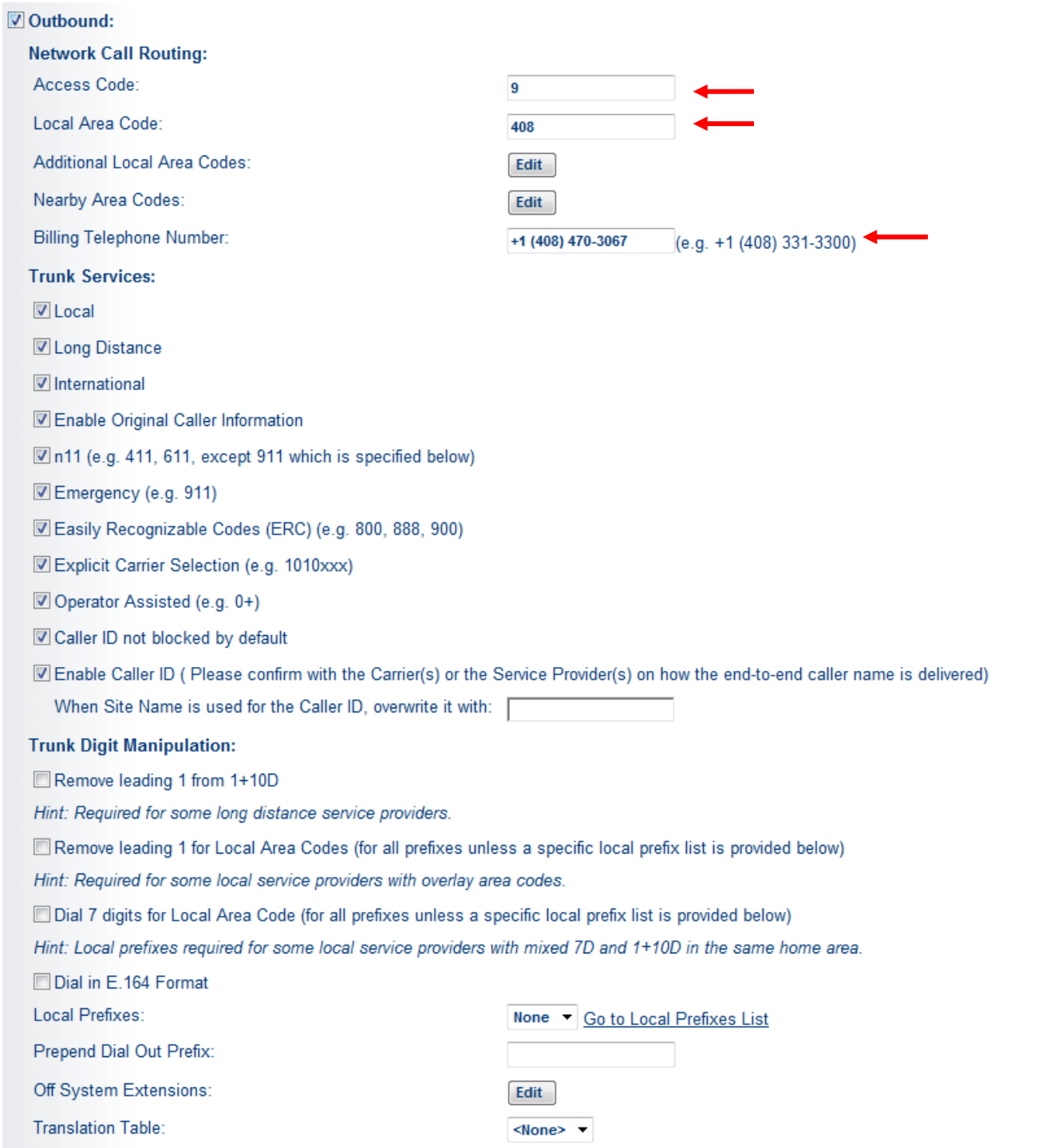
Figure 13 – Inbound



Within the **"Inbound:"** settings, ensure the **"Number of Digits from CO:"** is configured to a value of "**10"**, this is the number of digits that the ShoreGear SIP trunk switch will be receiving from Broadvox SIP Trunking Gateway. Enable (check) the **"DNIS"** or **"DID"** parameters as needed. It is no longer needed to enable the **"Extension"** parameter. We recommend that the **"Tandem Trunking"** parameter be enabled (checked) otherwise transfers to external telephone numbers will fail via SIP trunks. Finally, be sure to specify the proper **"User Group:"** that has access to the correct trunks. For additional information on these parameters please refer to the *ShoreTel Administration Guide*.

Note: The following section is configured no different than any normal Trunk Group

Figure 14 – Outbound and Trunk Services:



If outbound call service is required, enable (check) the **"Outbound"** parameter and define a Trunk **"Access Code"** and **"Local Area Code"** as appropriate. In addition you should also define the **"Billing Telephone Number"** with the appropriate main number provided by Broadvox SIP Trunking service.

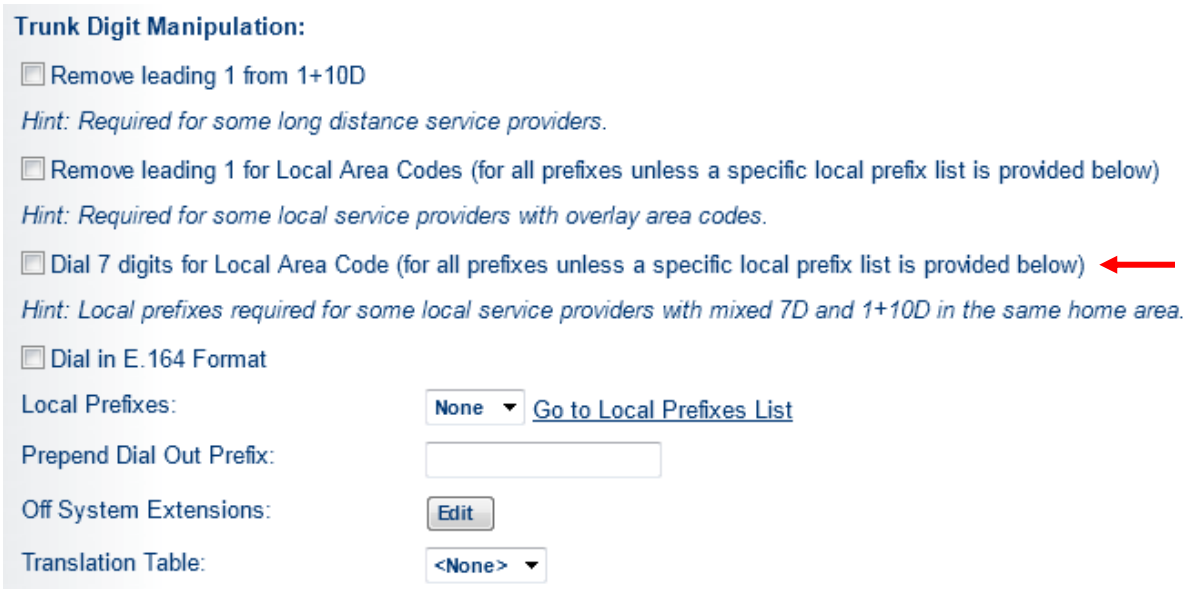
In the **"Trunk Services:"** area, make sure the appropriate services are enabled or disabled based on what Broadvox supports and what features are needed from this Trunk Group.

The parameter **"Caller ID not blocked by default"** determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID will impact how information is passed out to the SIP Trunk group.

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

The next parameter for configuration in the Trunk Group is **"Trunk Digit Manipulation"** (**Figure 15**):

Figure 15 – Trunk Digit Manipulation:

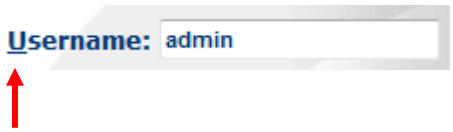


The only parameters that require adjustment (from default) to interface with Broadvox are: "Dial 7 digits for Local Area Code", and **"Prepend Dial Out Prefix"** Disable (uncheck) the "Dial 7 digits for Local Area Code" parameter. In the "Prepend Dial Out Prefix" , type the string that this trunk group prepends to outbound numbers if needed.

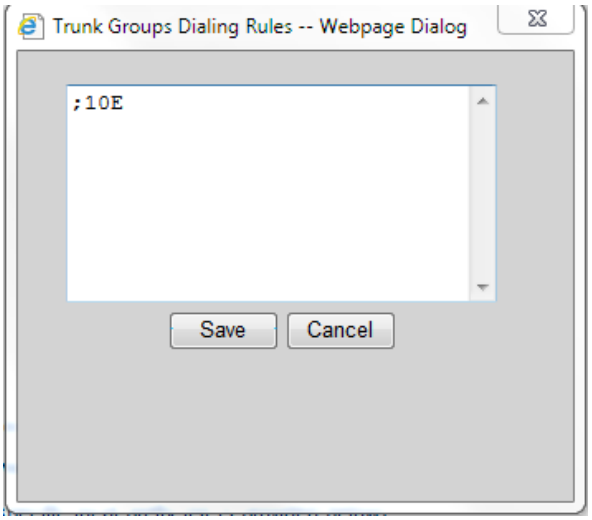
After these settings are made to the "Edit SIP Trunk Group" screen, click the "**Save**" button to input the changes.

The final parameter setting for the Trunk Group will remove the leading "+" sign from dialed numbers within all SIP headers. This parameter can only be changed by logging into ShoreTel Director in the "Support Entry" mode.

Log into ShoreTel Director using the "Support Entry" mode (hold down the CTRL + Shift keys and click on the **"U"** of the Username), then log in normally.



Then go to the SIP trunk group you're using and scroll to the bottom of the page, to the right of the "Custom" entry click on Edit and enter the parameter ;10E (note: the "E" is case sensitive and must be capitalized.)



Click the **"Save"** button to input the changes.. This will remove the "+" and the country code, for US and Canada, we just send 10 digits.

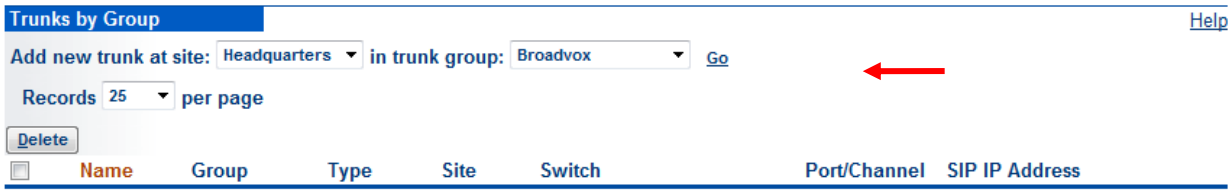
System Settings – Individual Trunks

This section covers the configuration of the individual trunks. Select **"Administration"**, then **"Trunks"** followed by **"Individual Trunks"** to configure the individual trunks (**Figure 19**).

Figure 19 – Individual Trunks

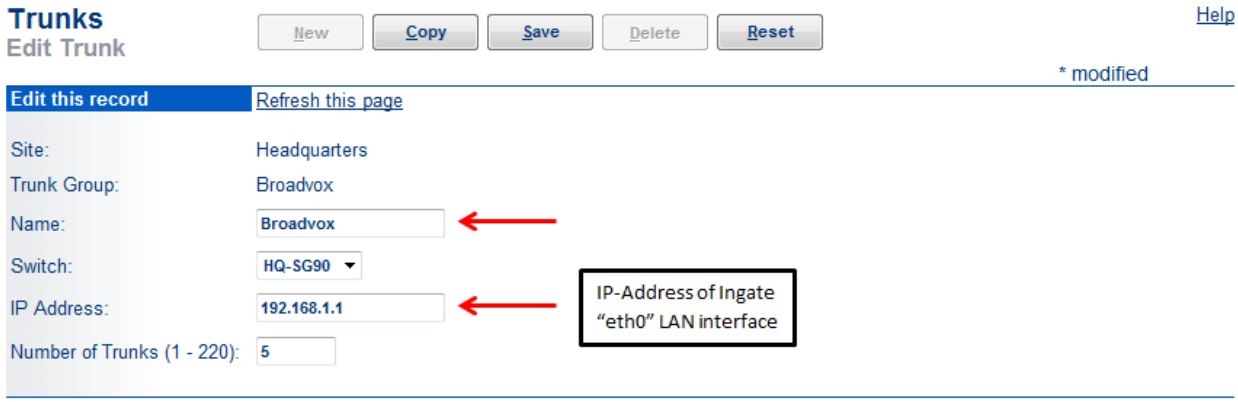
The **"Trunks by Group**" screen that is used to change the individual trunks settings then appears (**Figure 20**).

Figure 20 – 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 "Broadvox", as created above, see **Figure 12.** Click on the "**Go**" button to bring up the "Edit Trunk" screen (**Figure 21**).

Figure 21 - Edit Trunks Screen for Individual Trunks



From the individual trunks "Edit Trunk" screen, input a **"Name:"** for the individual trunks, then select the appropriate **"Switch".** 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 trunks will be created. For the parameter **"IP Address"**, define the IP address of the Ingate SIParator product. The last step is to select the number of individual trunks desired **"Number of Trunks (1 – 220)"** (each one supports "one" audio path – example if 10 is configured, then 10 audio paths can be up at one time). Once these changes are complete, select the **"Save"** button to commit 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.

Ingate Configuration

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 addresses of the enterprise, and the private IP addresses which are only known on the inside LAN. These private IP addresses are created and assigned to devices on the enterprise LAN, and provide one of the security layers of the enterprise network. In addition, the Ingate products provide routing rules that assign a SIP traffic flow that ensures only allowed SIP traffic will pass.

Ingate Startup Tool

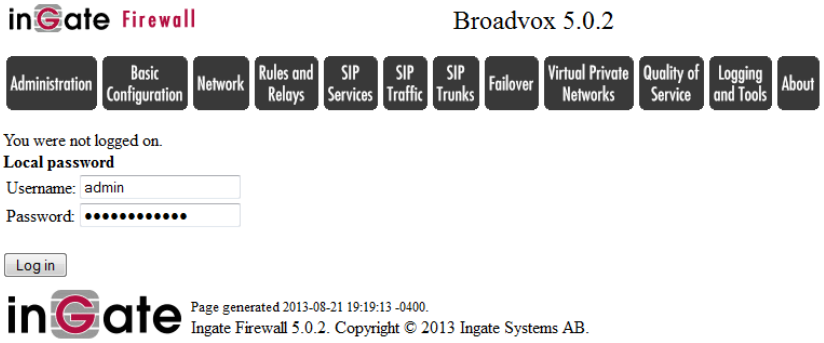
The Ingate Startup Tool is an installation tool for Ingate Firewall® and Ingate SIParator® products, and facilitates the "out of the box" set up of SIP Trunking solutions with ShoreTel and various Internet Telephony Service Providers. Designed to simplify SIP trunk deployments, the tool will automatically 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 the Internet Telephony Service Provider (ITSP) they use; 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.

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.



CONNECTING THE INGATE FIREWALL/SIPARATOR

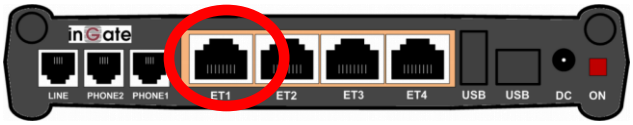
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

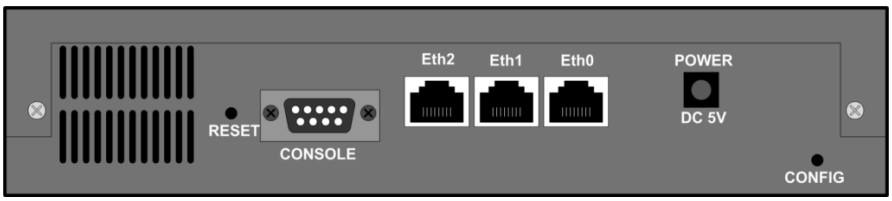
Configuration Steps:

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".

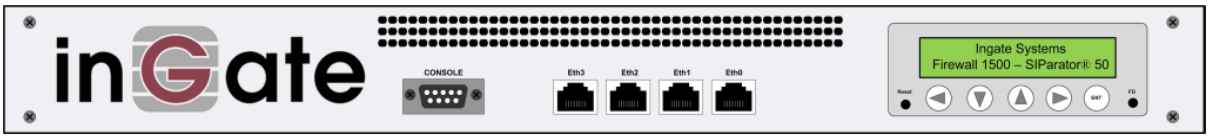
Ingate SIParator SBE (Back)



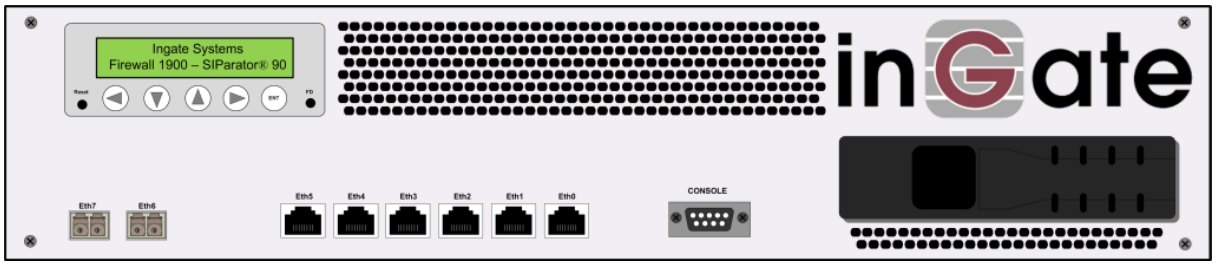
Ingate 1190 Firewall & SIParator 19 (Back)



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

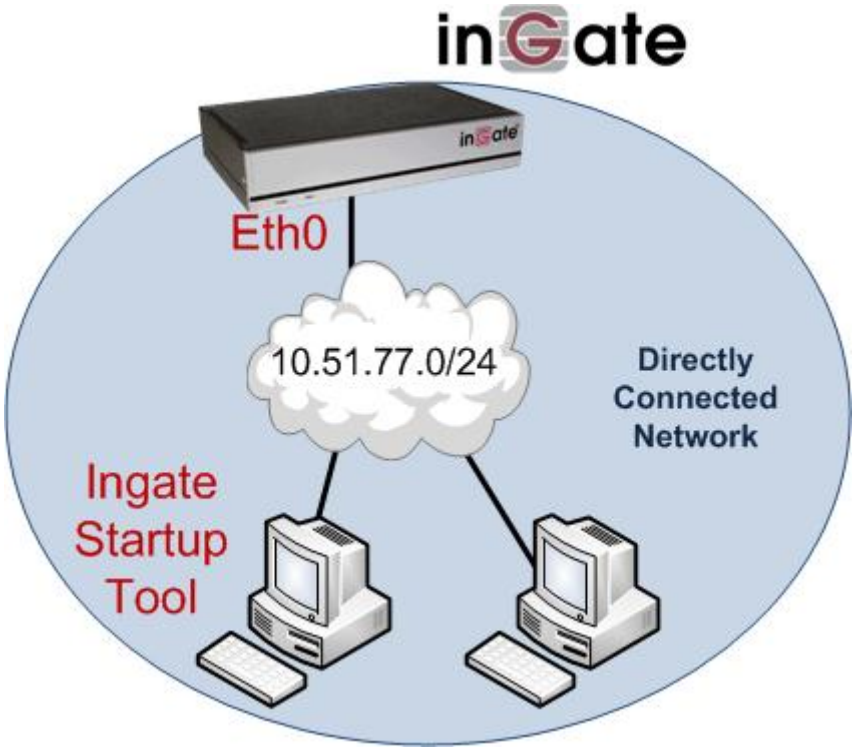


Ingate 1900 Firewall & SIParator 90



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.

USING THE STARTUP TOOL

There are three main reasons for using the Ingate Startup Tool. First, the "Out of the Box " configuring of 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.

CONFIGURE THE UNIT FOR THE FIRST TIME

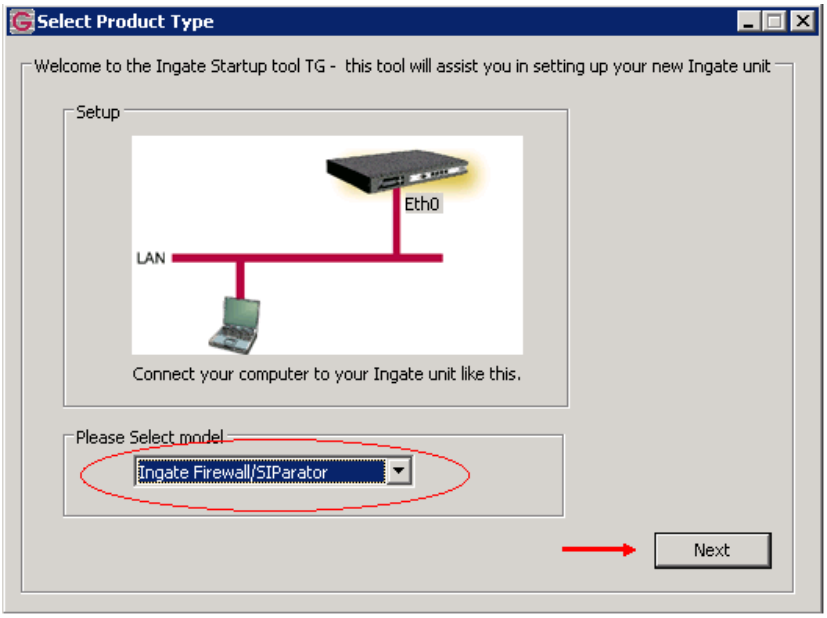
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

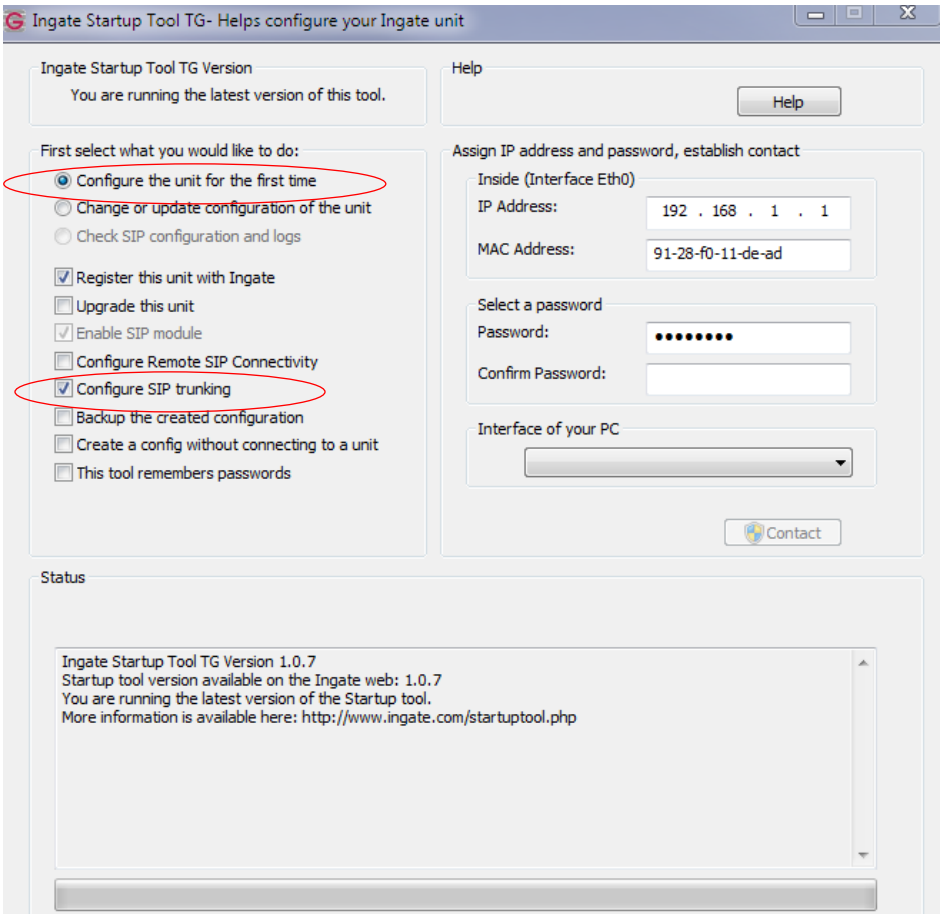
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 4.2: "Change or Update Configuration".

Configuration Steps:

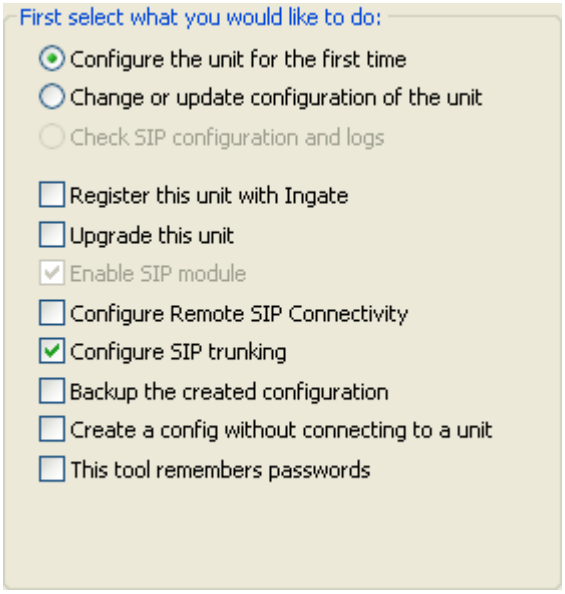
1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.



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



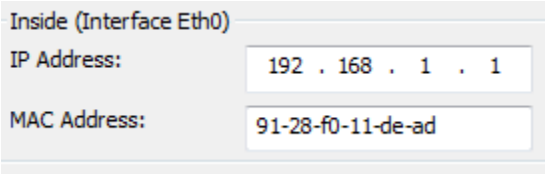
4. Other Options in the "Select first what you would like to do",



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

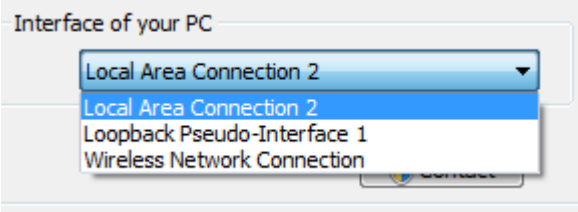
c. Select "Register this unit with Ingate" if you want the tool to connect with www.ingate.com to register the unit. If selected, see Section 4.3: Licenses and Upgrades.
d. Select "Upgrade this unit" if you want the tool to connect with www.ingate.com to download the latest software release and upgrade 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.

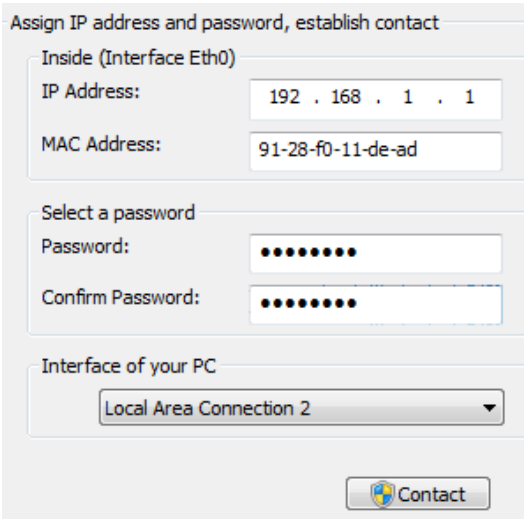


6. In the "Select a Password", enter the Password to be assigned to the Ingate unit.

7. Choose the PC interface used to connect to the unit..



8. 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.



9. Proceed to Section 3.3.3: Network Topology.

CHANGE OR UPDATE CONFIGURATION

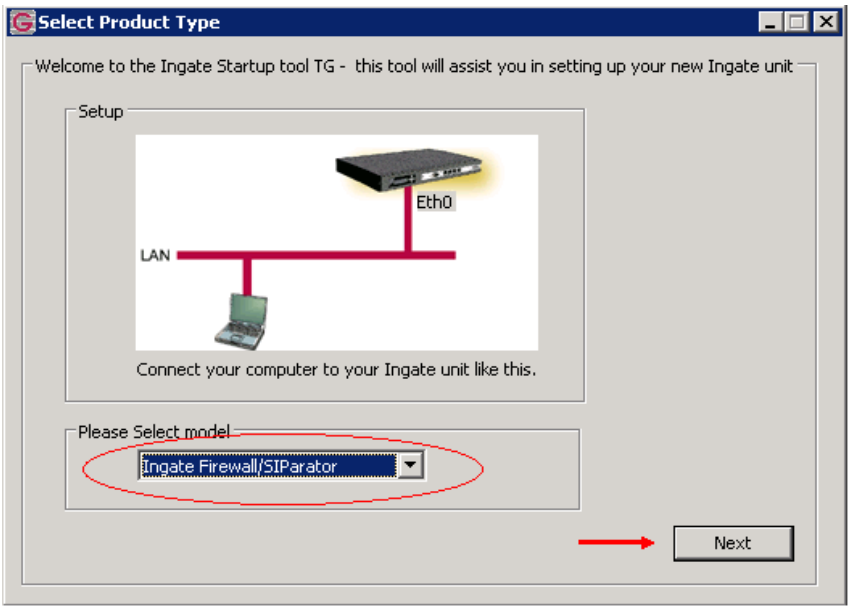
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool - "Configure the unit for the first time" or via the Console port.

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.

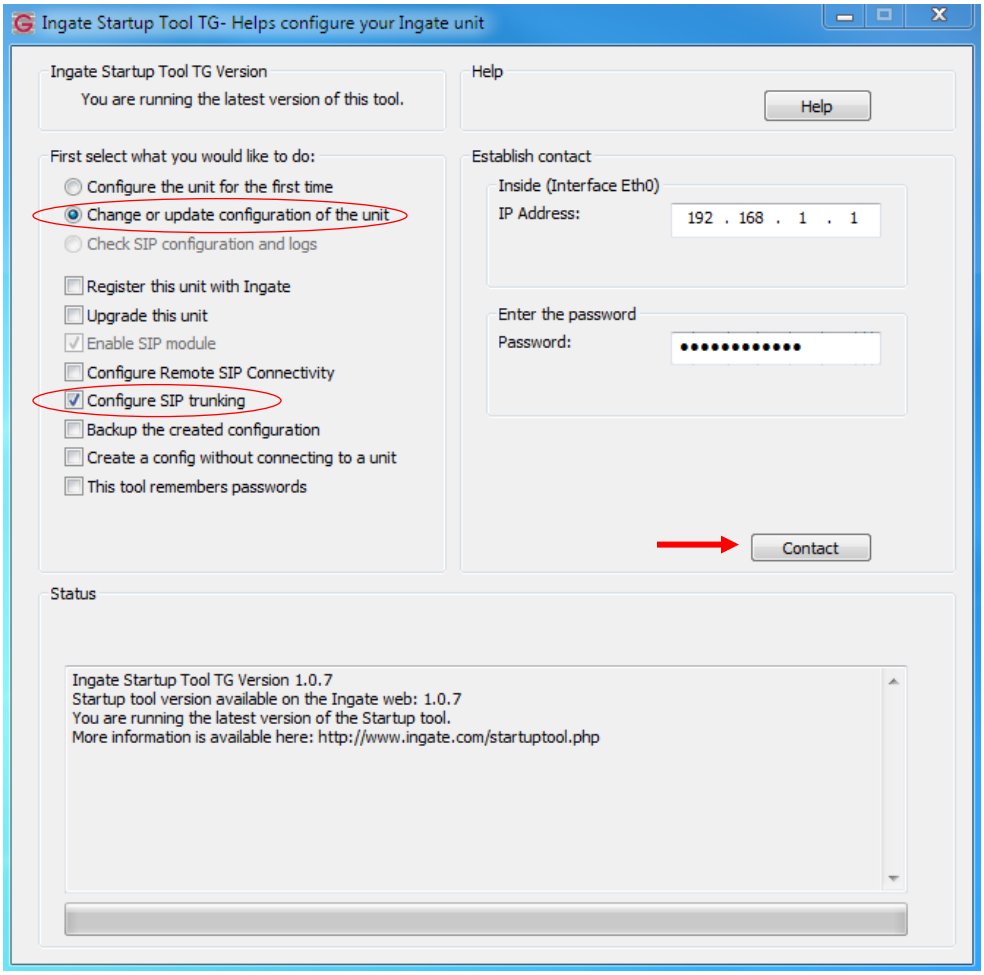
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 4.1: "Configure the Unit for the First Time".

Configuration Steps:

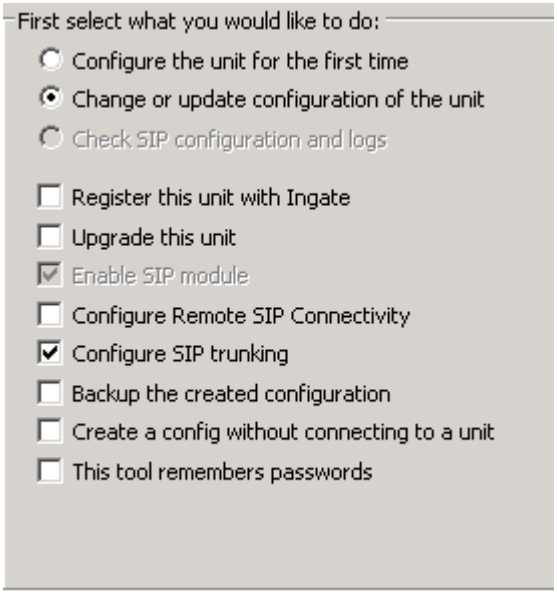
1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.



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

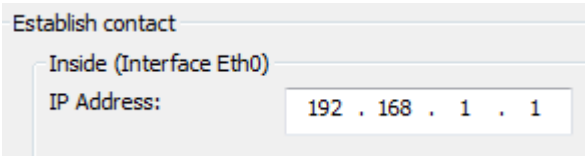


4. Other Options in the “Select first what you would like to do”,

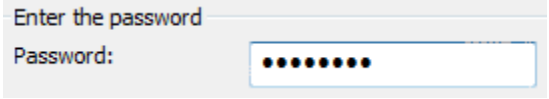


   a. Select “Configure SIP Trunking” if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
   b. Select “Configure Remote SIP Connectivity” if you want the tool to configure Remote Phone access to an IP-PBX
   c. Select “Register this unit with Ingate” if you want the tool to connect 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.

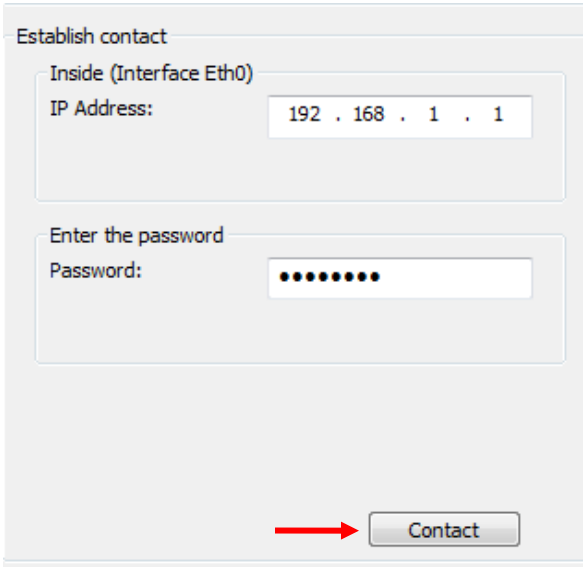
5. In the “Inside (Interface Eth0)”,
   a. Enter the IP Address of the Ingate Unit.



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



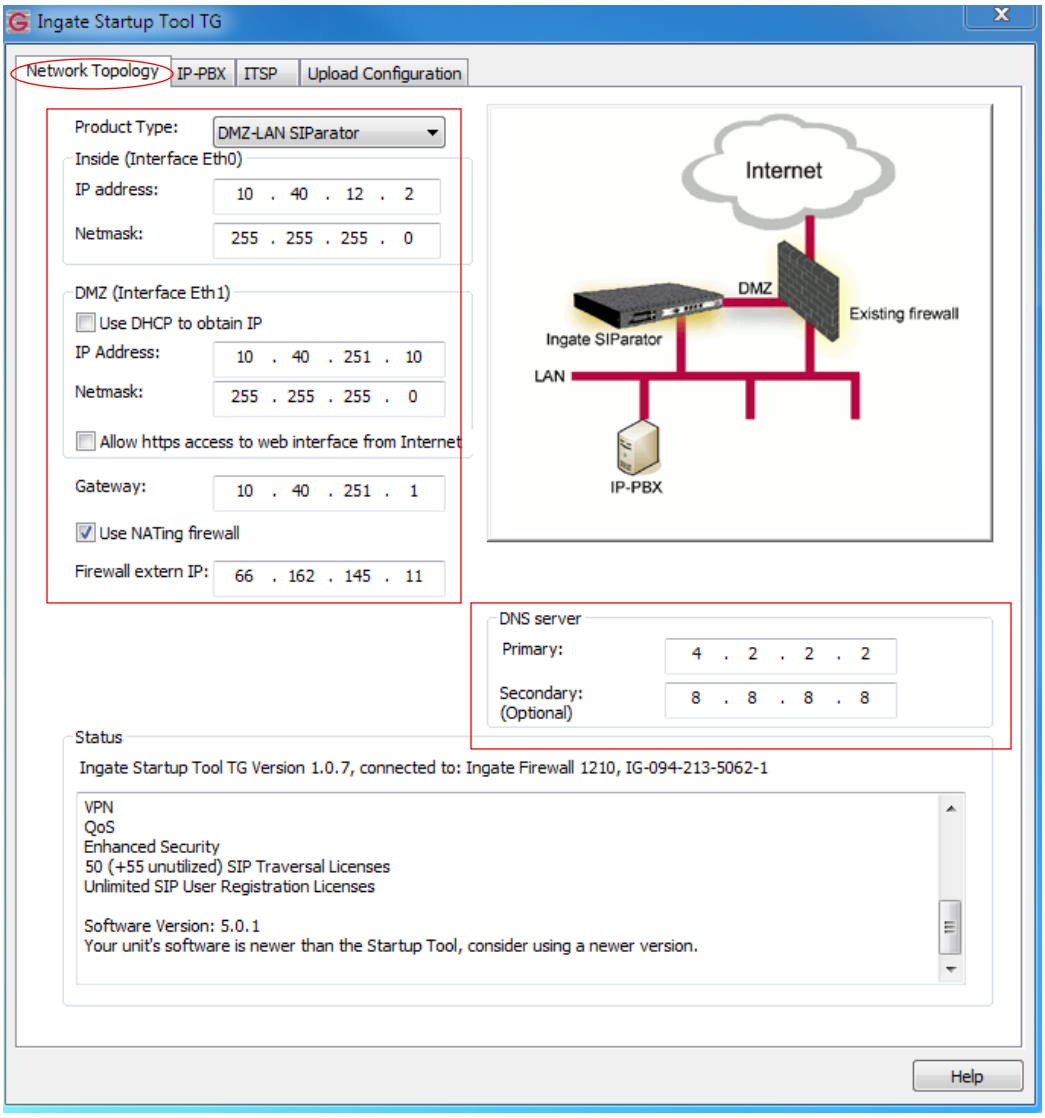
7. Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.



8. Proceed to Section 3.3.3: Network Topology.

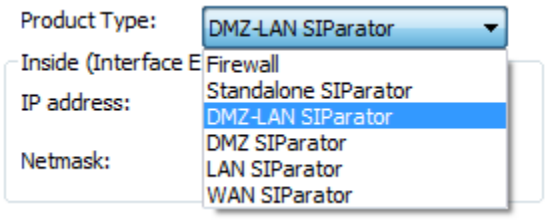
NETWORK TOPOLOGY

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.

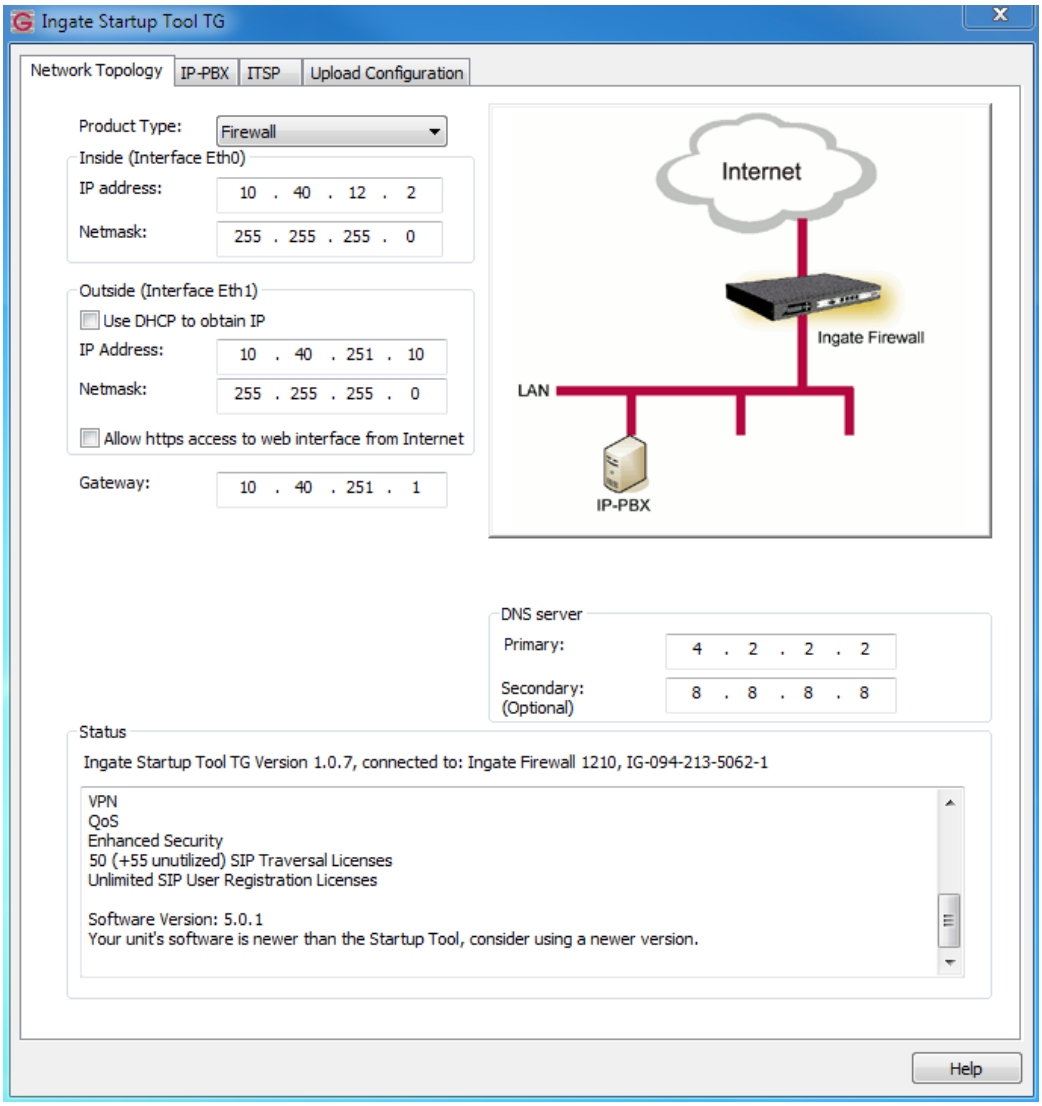


Hint: Match the picture to the network deployment.

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

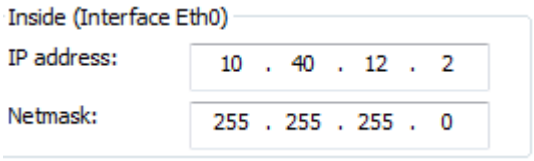
When deploying an Ingate Firewall, there is only one way the Firewall can be installed. The Firewall must be the Default Gateway for the LAN; it is the primary edge device for all data and voice traffic out of the LAN to the Internet.



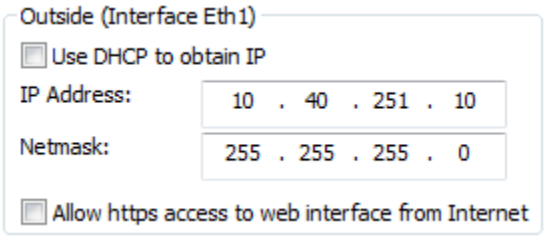
Configuration Steps:

1. In Product Type, select "Firewall".

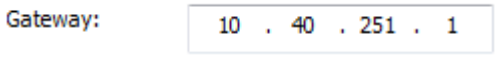
2. Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.



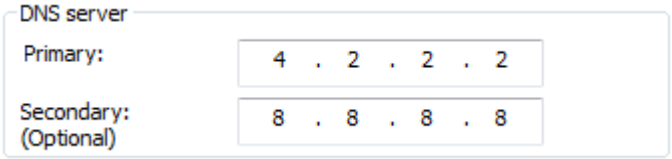
3. Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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

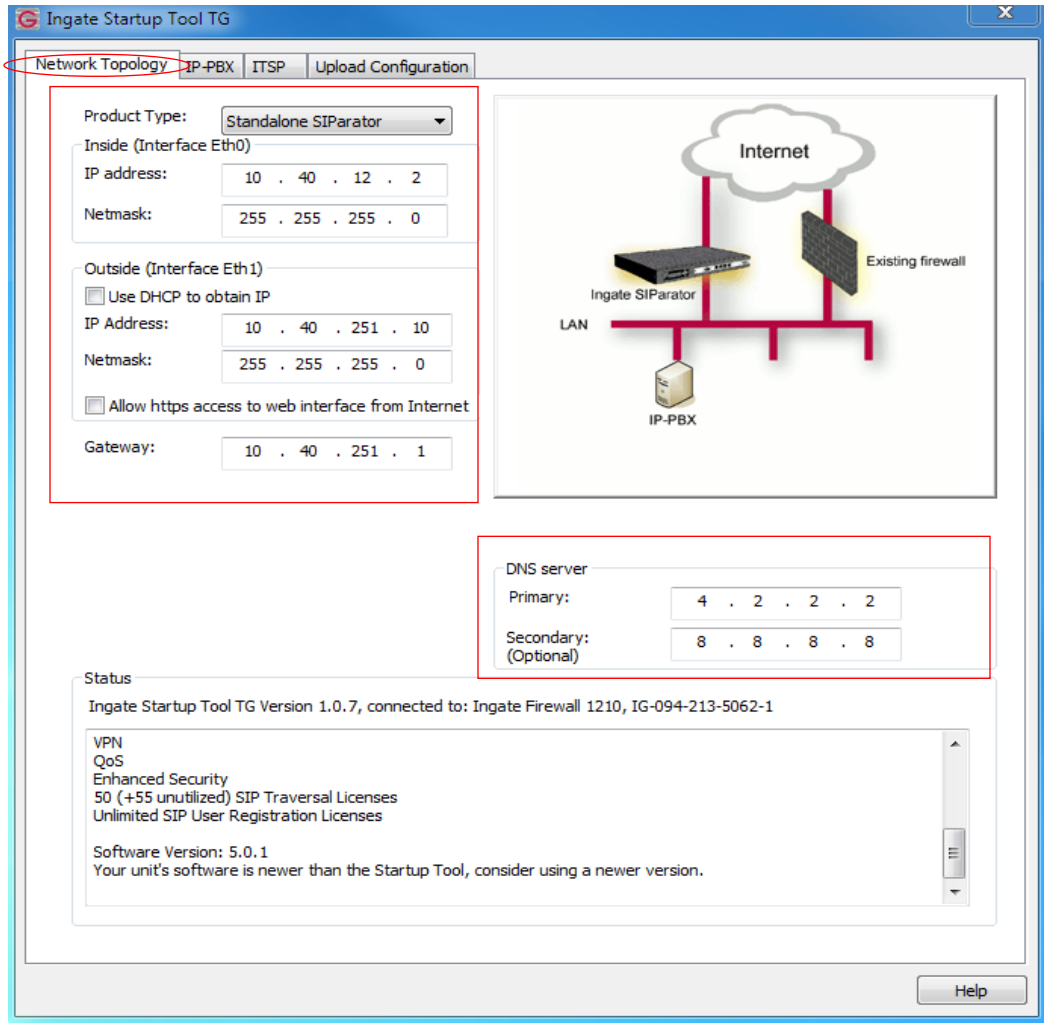


5. Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.



Product Type: Standalone

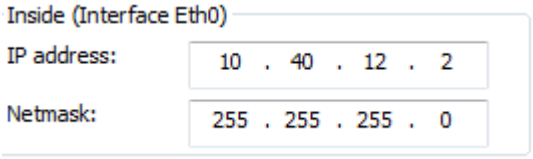
When deploying an Ingate SIParator in a Standalone configuration, the SIParator resides on a LAN network and on the WAN/Internet network. The Default Gateway for SIParator resides on the WAN/Internet network. The existing Firewall is in parallel and independent of the SIParator. Firewall is the primary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



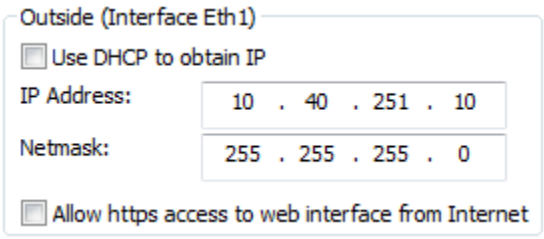
Configuration Steps:

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

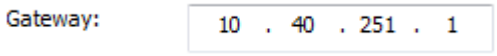
2. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



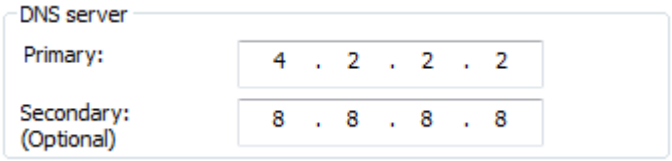
3. Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
    a. A Static IP Address and Netmask can be entered
    b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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

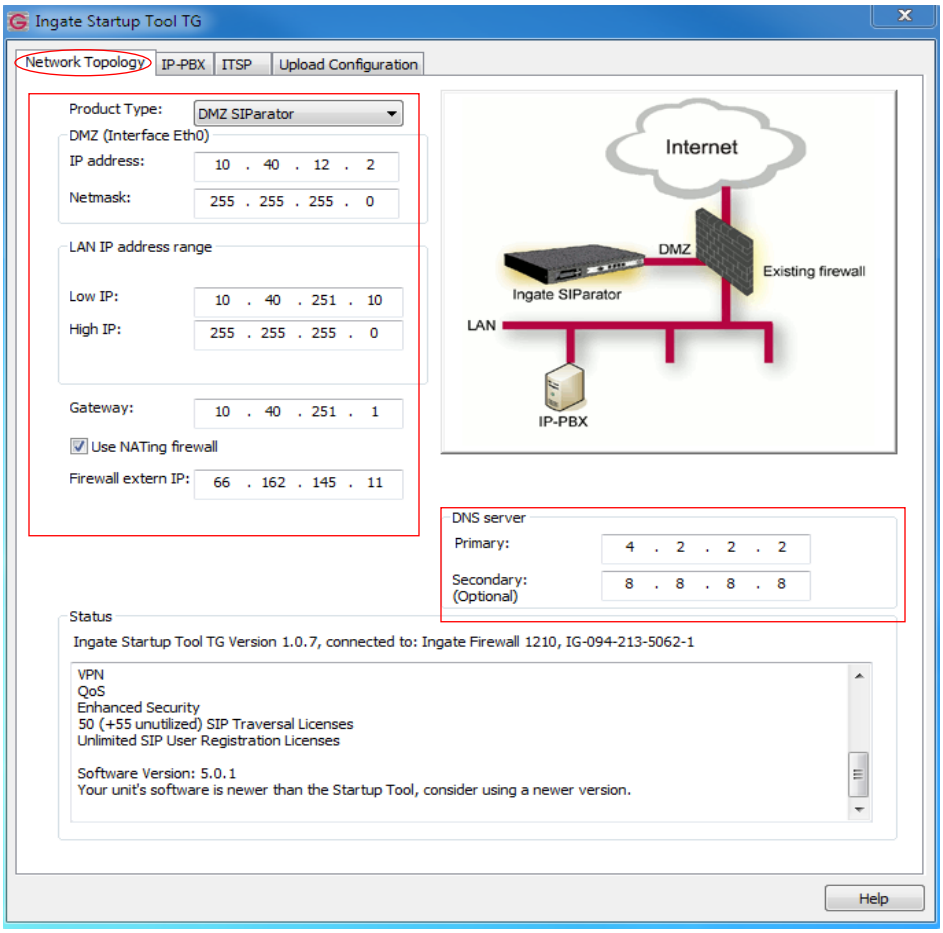


5. Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.



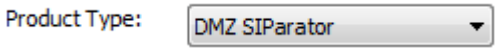
Product Type: DMZ SIParator

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.

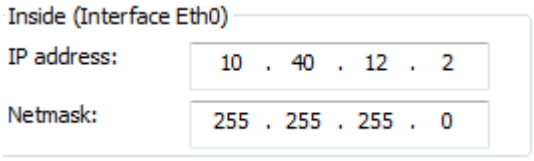


Configuration Steps:

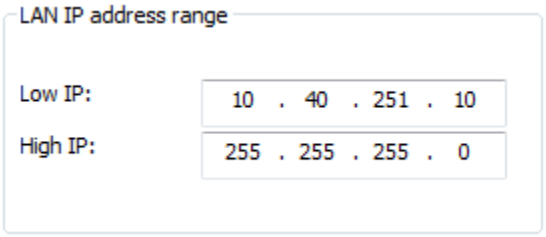
1. In Product Type, select "DMZ SIParator".



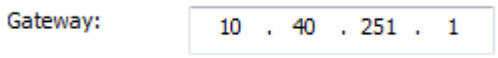
2. Define the IP Address and Netmask of the DMZ (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.



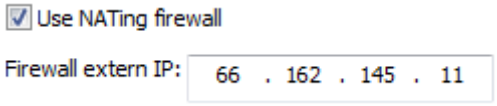
3. Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.



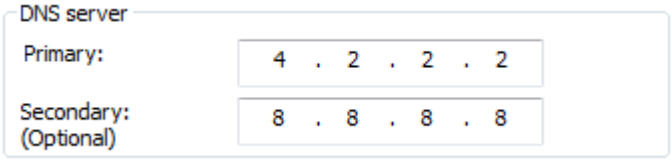
4. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.



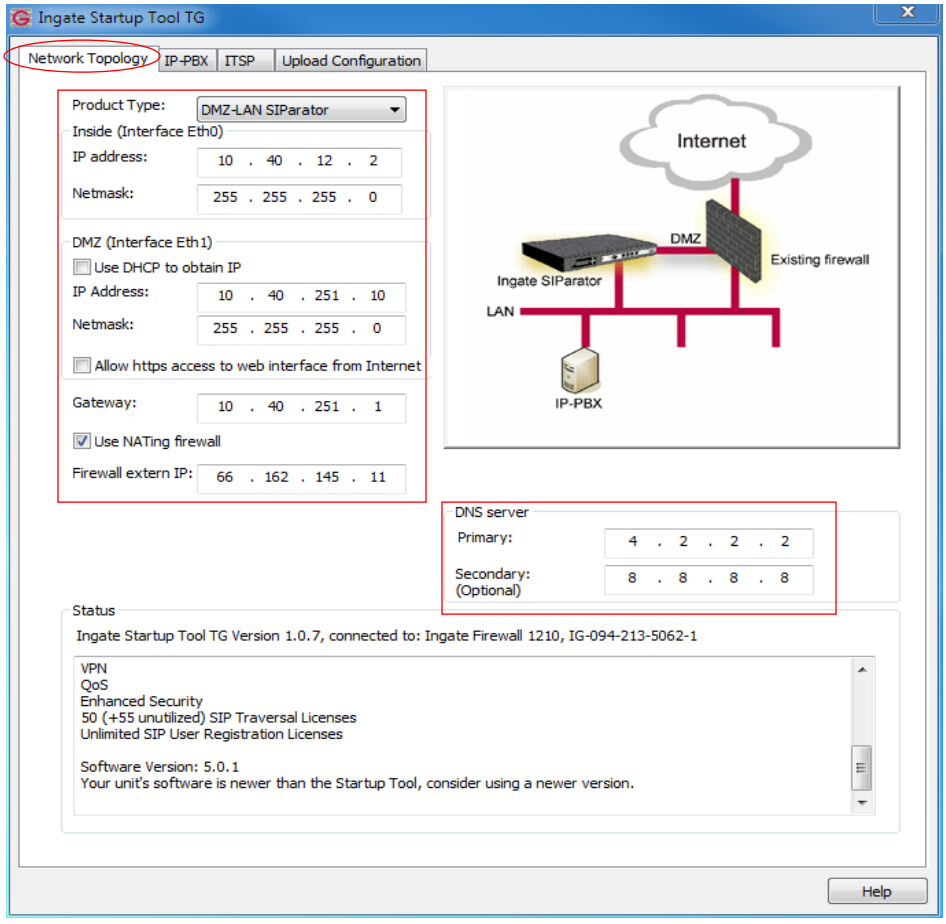
7. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   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 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.

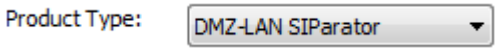
Product Type: DMZ-LAN SIParator

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.

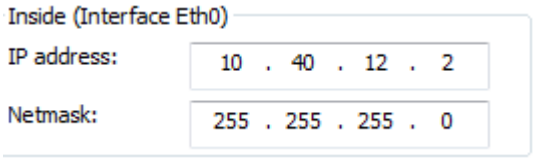


Configuration Steps:

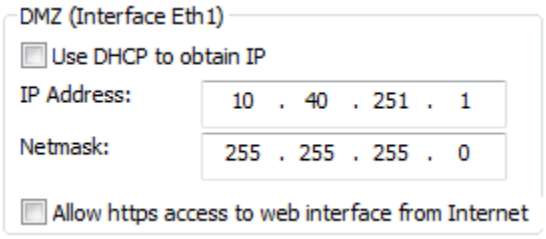
1. In Product Type, select "DMZ-LAN SIParator".
2.



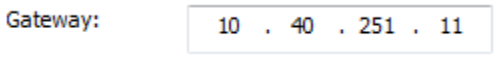
3. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



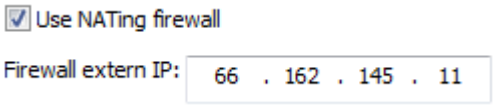
4. Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate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



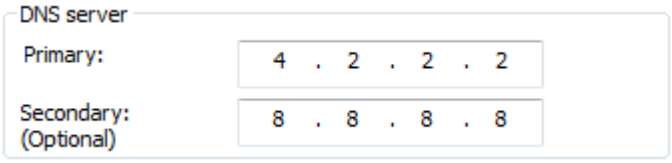
5. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



6. Enter the 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.



7. 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.



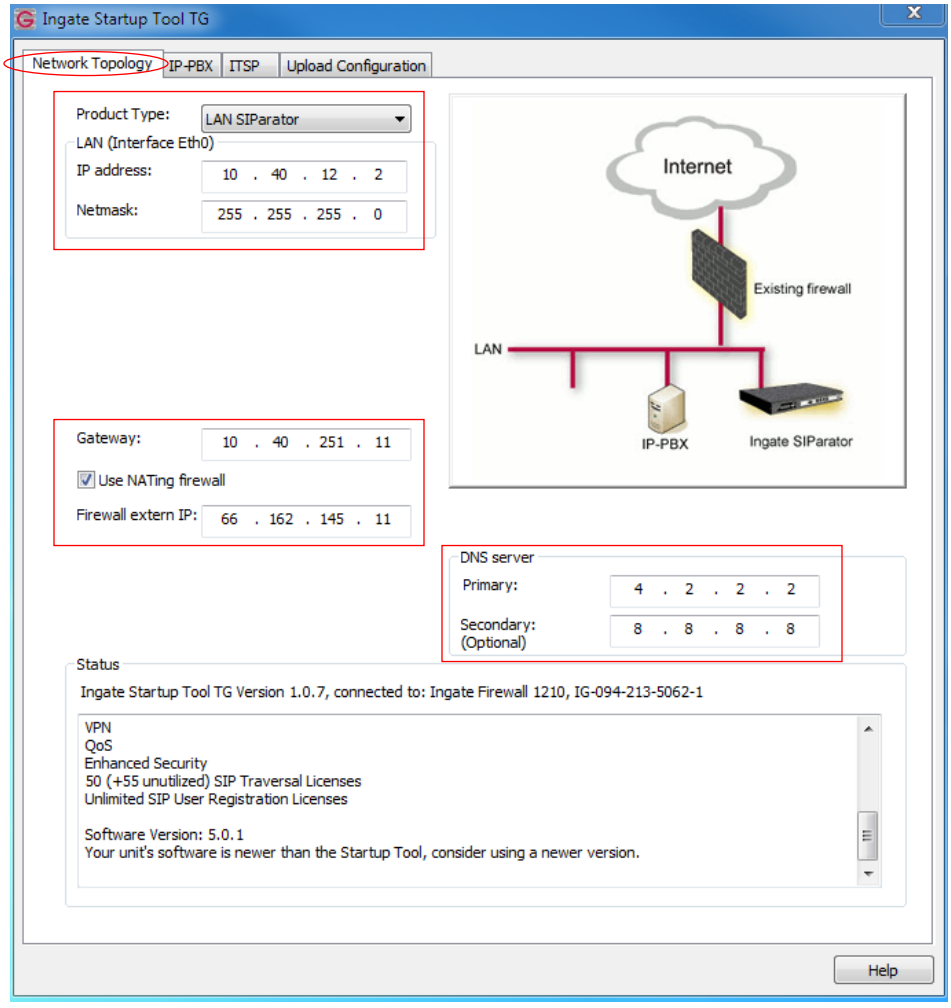
8. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   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

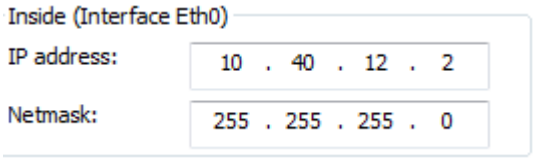
When deploying an Ingate SIParator in a LAN configuration, the Ingate resides on a LAN network with all of the other network devices. The existing Firewall must be the Default Gateway for the LAN network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN to 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.



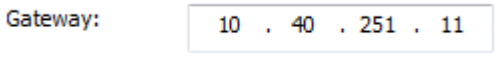
Configuration Steps:

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

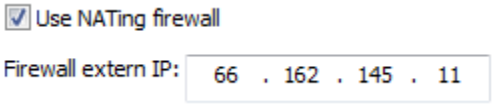
2. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



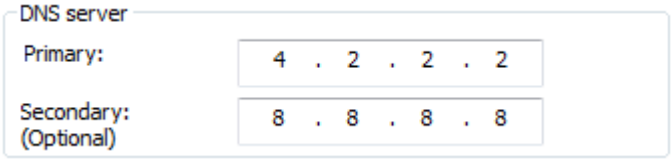
3. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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.

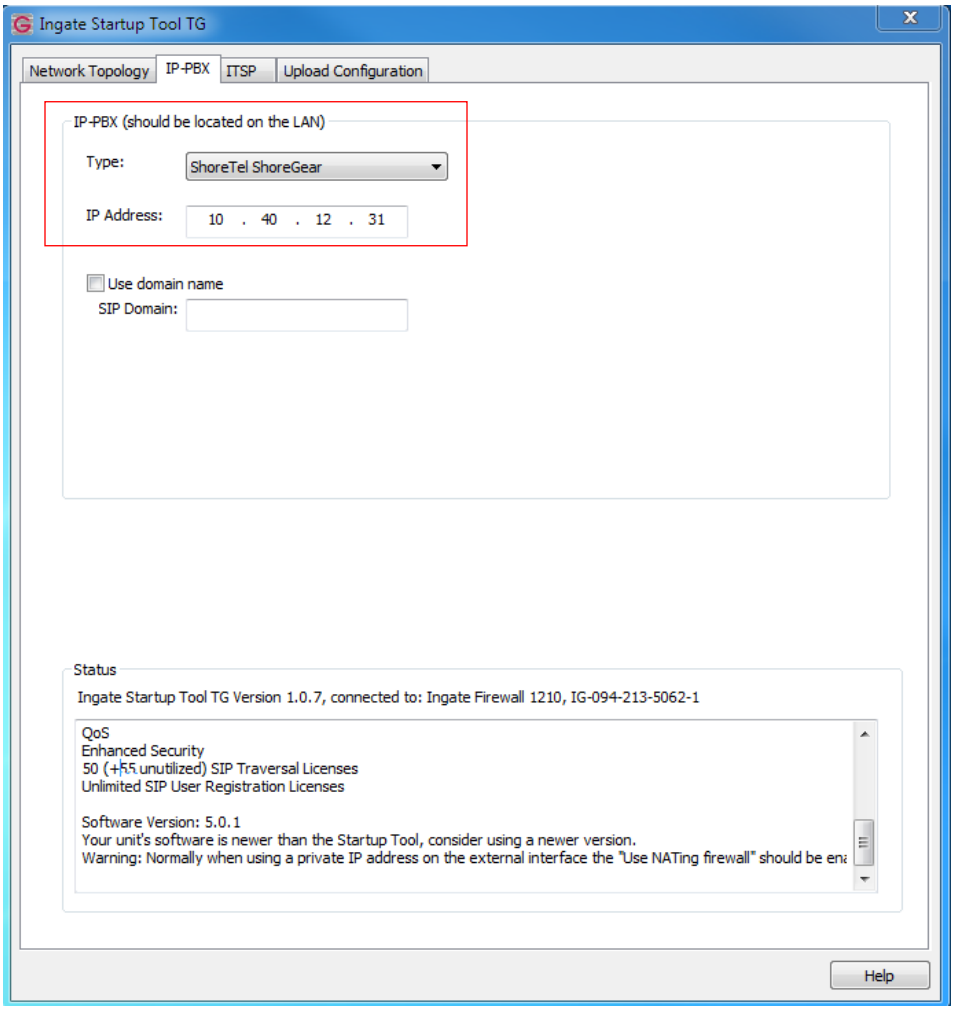


6. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   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

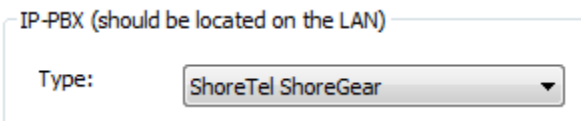
IP-PBX

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 with several of the leading IP-PBX vendors.



Configuration Steps:

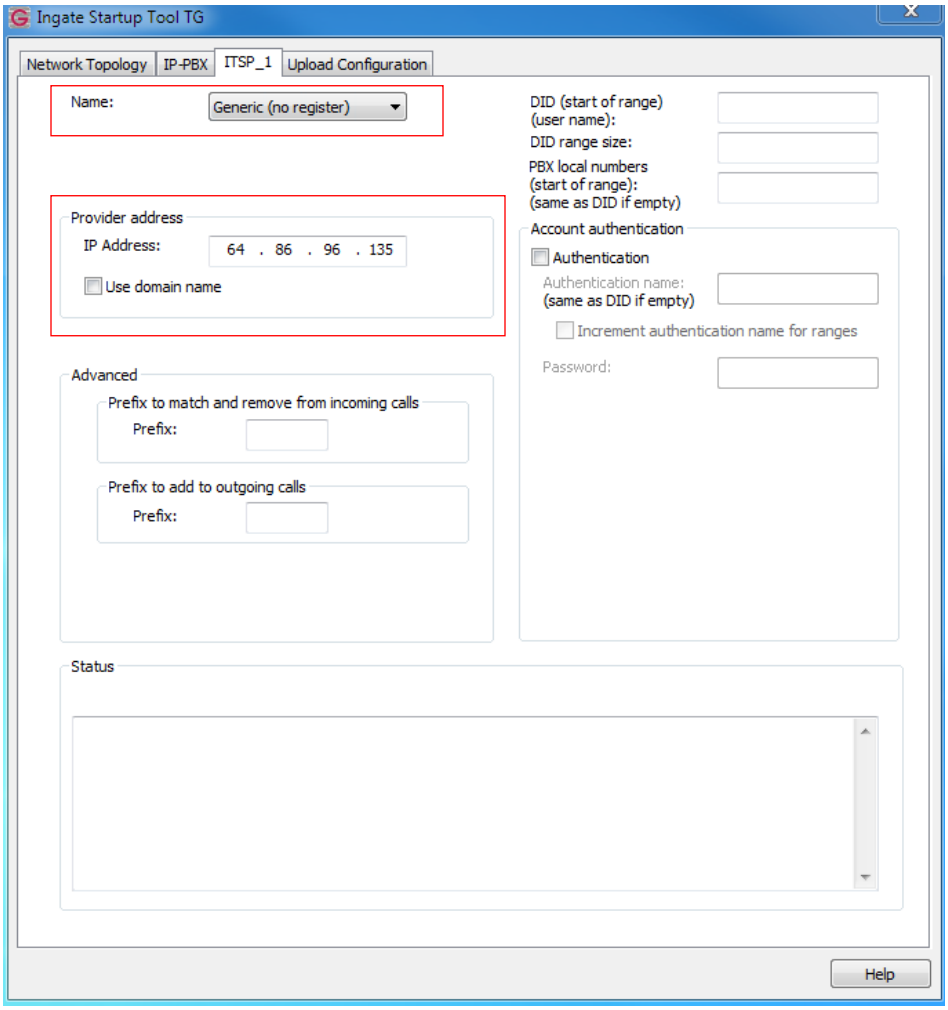
1. In the IP-PBX Type drop down list, select "ShoreTel ShoreGear". Ingate has confirmed interoperability with ShoreTel, the unique requirements of the vendor testing are contained in the Startup Tool.



2. Enter the IP Address of the ShoreTel ShoreGear SIP Trunk switch. The IP Address should be on the same LAN subnet as the Ingate unit.

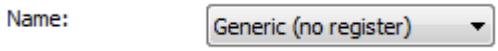
INTERNET SERVICE PROVIDER (ITSP)

The ITSP section is where all of the attributes of the Broadvox SIP Trunking service 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. Note only Innovation Network validated ITSPs are supported by ShoreTel. Click here for a current list of ShoreTel Innovation Network validated ITSPs: http://www.shoretel.com/partners/technology/certified_partners.html.



Configuration Steps:

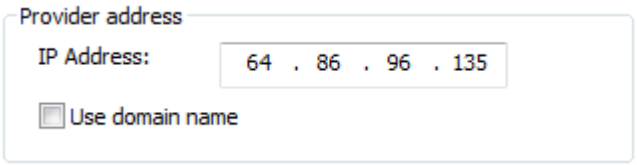
1. In the ITSP drop down list, select "Generic (no register)".



Ingate has confirmed interoperability with several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool. Note only Innovation Network validated ITSPs are supported by ShoreTel. Click here for a current list of ShoreTel Innovation Network validated ITSPs: http://www.shoretel.com/partners/technology/certified_partners.html

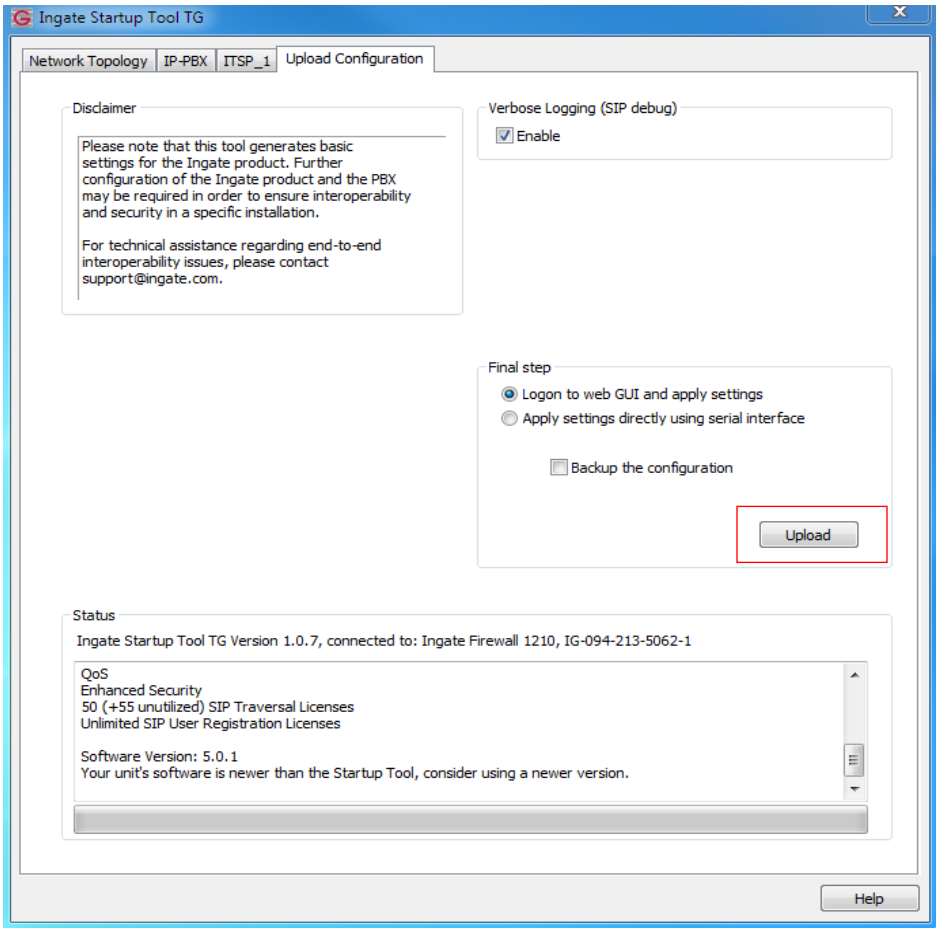
When you select a specific ITSP vendor, the Startup Tool will have the individual connection requirements predefined for that ITSP, the only additional entries may be the specific site requirements.

2. For the "Provider address"enter the IP Address provided by Broadvox.



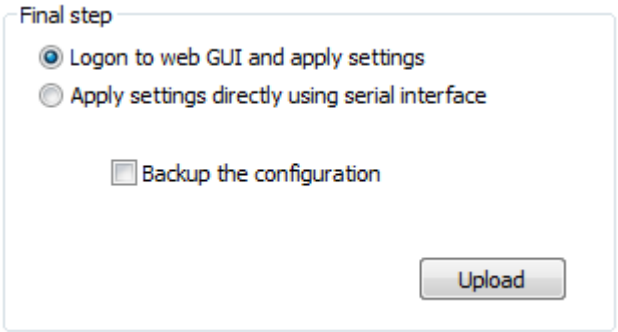
UPLOAD CONFIGURATION

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.

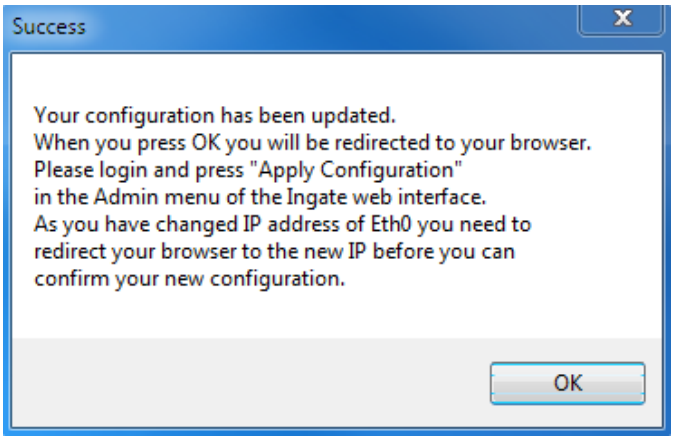


Configuration Steps:

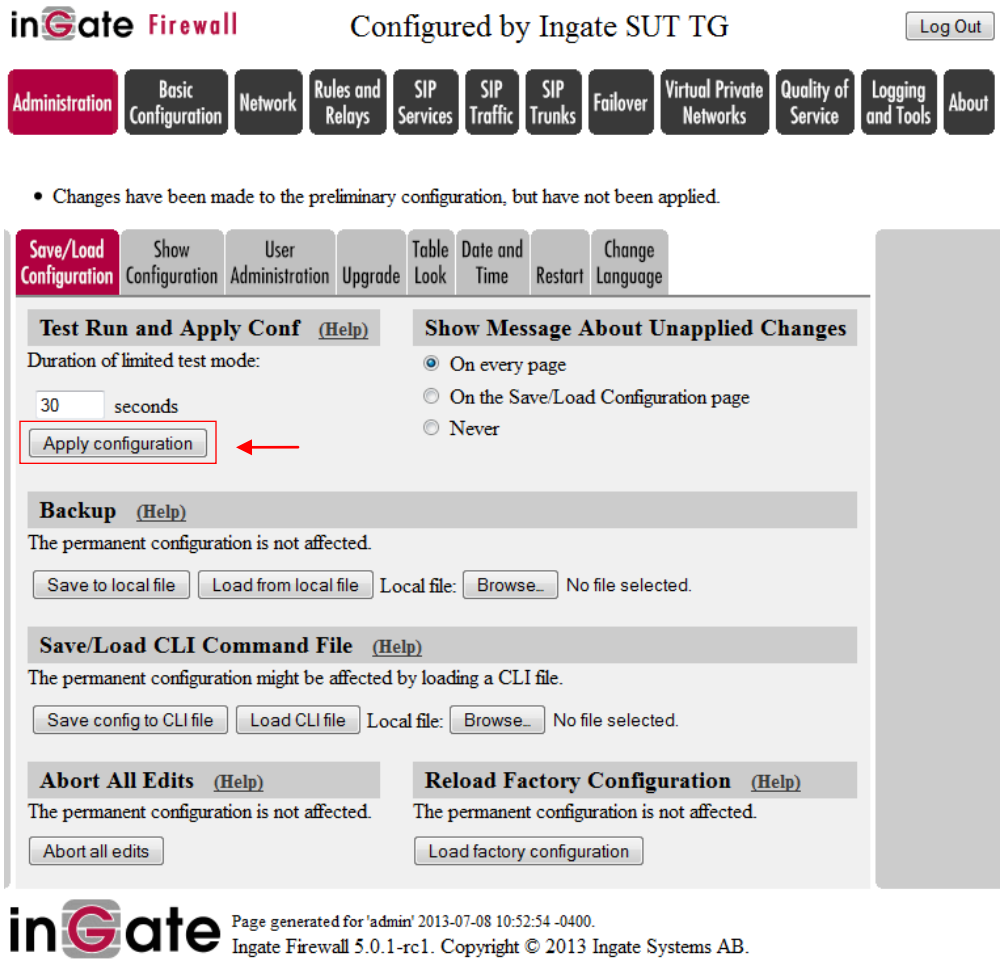
1. Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



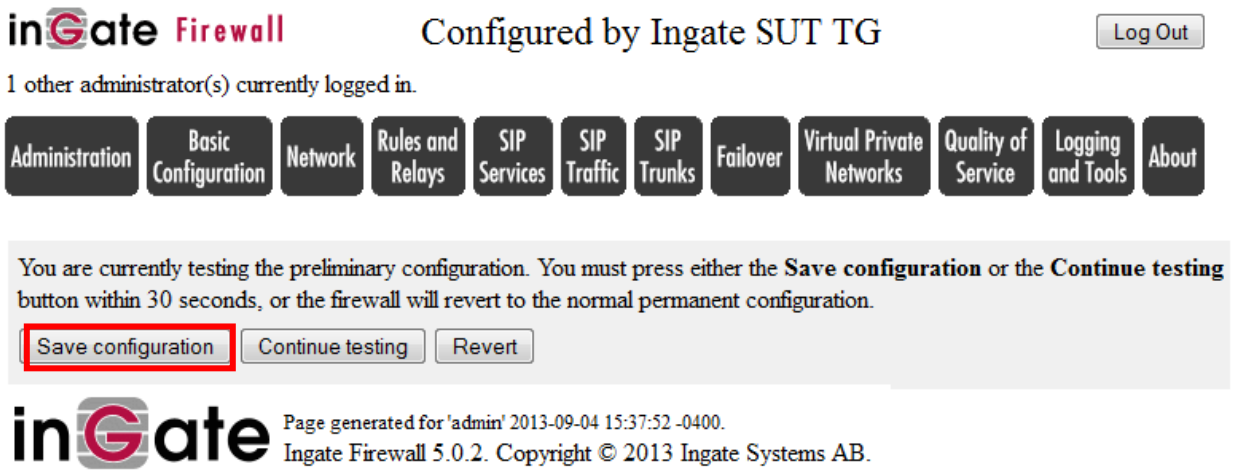
2. When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



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.

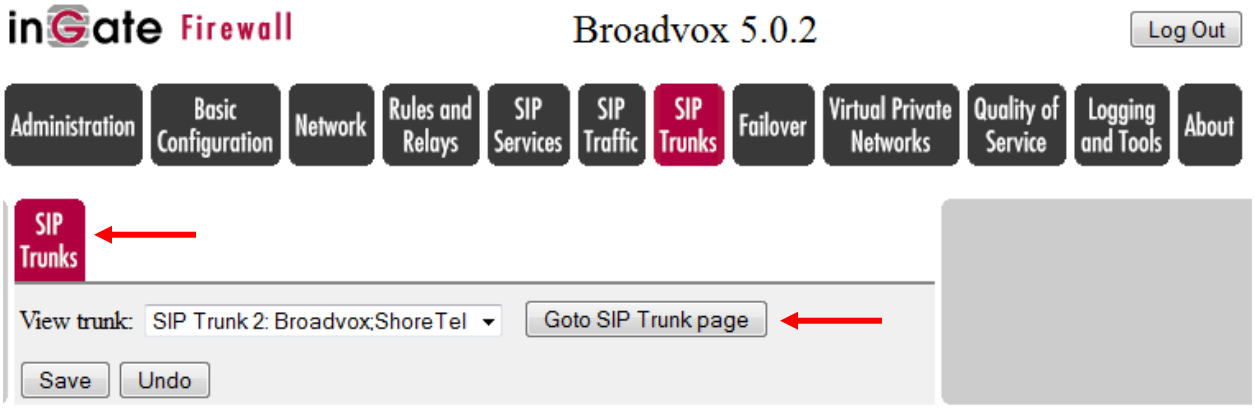


4. A new page will appear after the previous step requesting to save the configuration. Press "Save Configuration" to complete the saving process.

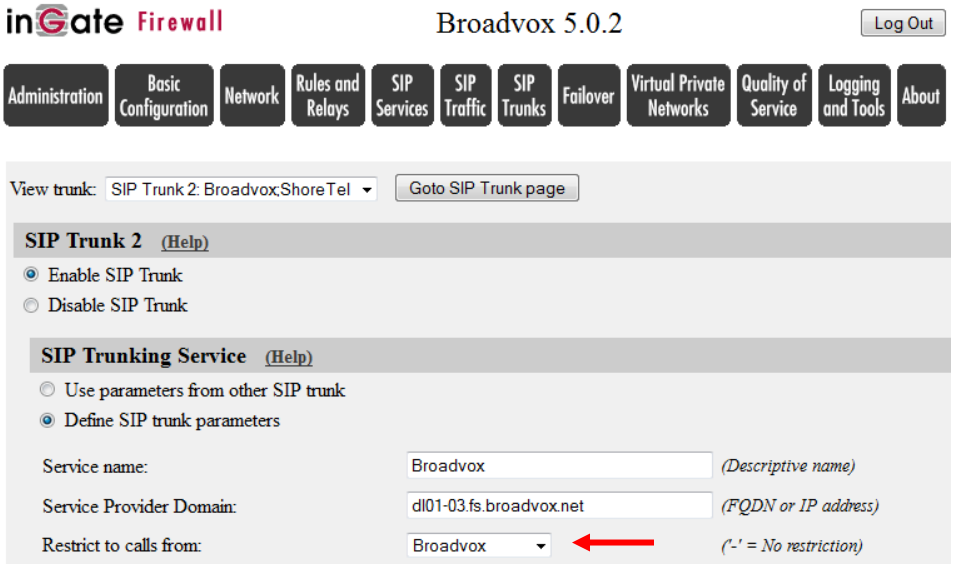


INGATE – ADDITIONAL CONIGURATION PARAMETERS

The Startup Tool addresses the majority of the configuration on the Ingate SIParator, the remaining configuration steps are required to interface with Broadvox. Log into the Ingate Web UI, then go to "SIP Trunks".



Select the appropriate SIP Trunk by selecting the "Goto SIP Trunk page" button or the "Trunk 1" tab. Once in the actual Trunk Group page, scroll down to the "SIP Trunking Service" parameter section:



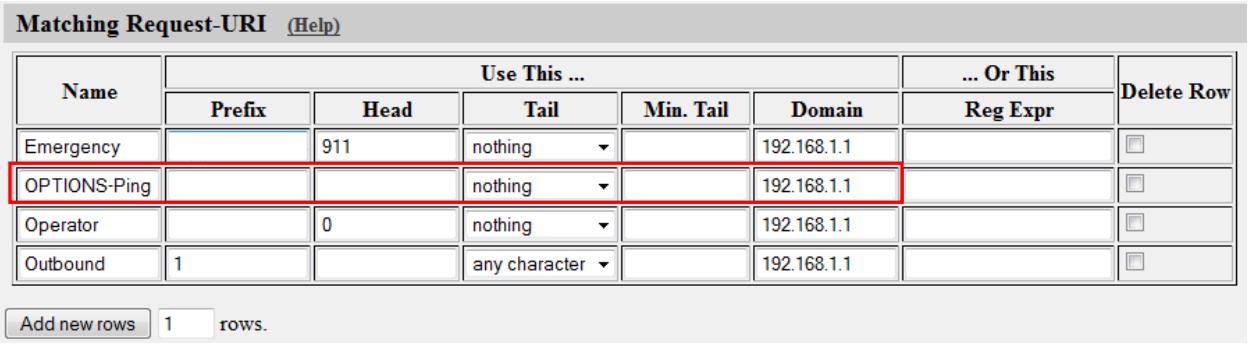
Configure the "Restrict to calls from:"parameter, using the drop down link to "Generic (no register)" or to "Broadvox" if this was selected in the Startup Tool, or just leave this blank (no selection). Be sure to apply and save the configuration change, as noted at the end of the Startup Tool section above.

OPTIONS CONFIGURATION

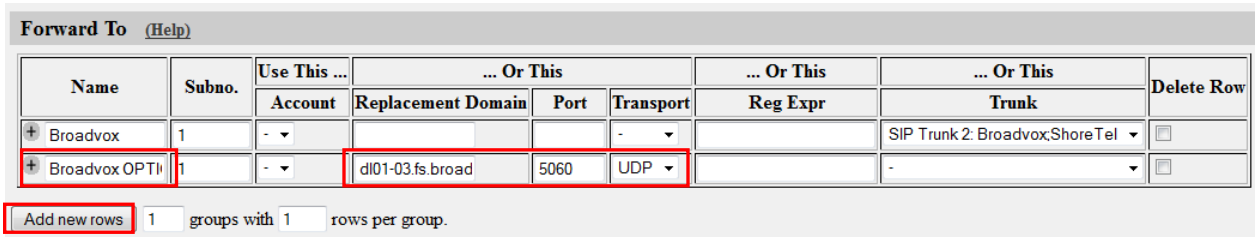
ShoreTel 13 adds the ability to determine whether the SIP trunks are in service or not, it does so via the SIP OPTIONS message. By default Ingate responds to the OPTIONS message, which should be sufficient, but is not optimal since Ingate will be operational for the most part. Instead we recommend that you configure Ingate to pass the OPTIONS message onto Broadvox, this way if there's a connectivity issue between Ingate and Broadvox, ShoreTel can properly take the SIP trunks out of service.

Log into the Ingate Web GUI, select the "SIP Traffic" tab, followed by the "Dial Plan" page. Scroll down to the "Matching Request–URI" section and click on the "Add new rows" button.

In the "Name" field define a name, we chose "OPTIONS-Ping" for clarity, then in the "Tail" field, use the drop down arrow and select "nothing", finally in the "Domain" field enter Ingate's LAN interface IP address, which will be the IP address defined for ShoreTel's individual SIP Trunks.

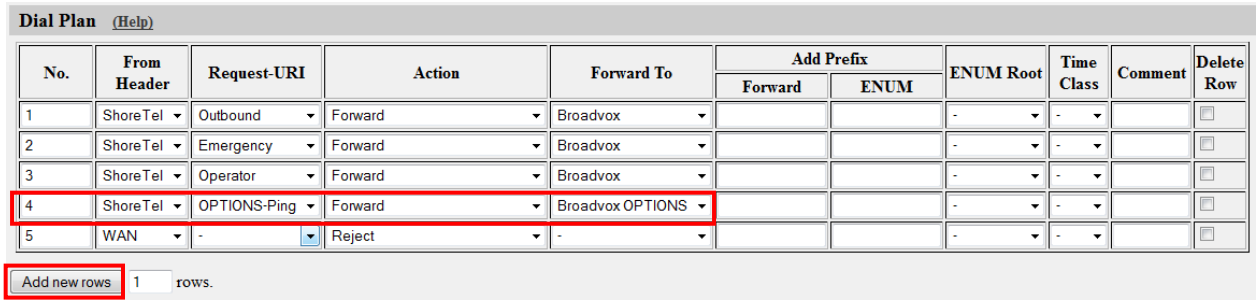


Locate the "Forward To" section and click on the "Add new rows" button.



In the "Name" field define a name, we chose "Broadvox Options", then in the "Replacement Domain" field enter the TCP/IP address provided by Broadvox, and in the "Port" field enter "5060", finally in the "Transport" field enter "UDP". Scroll down to the bottom of the page and click on the "Save" button.

Locate the "Dial Plan" section and click on the "Add new rows" button.



The "No." field will automatically increment, modify the number to be one above the entry that contains "WAN", in our example we changed the number to 2. In the "From Header" field, use the drop down to select "ShoreTel ShoreGear", then in the "Request-URI" field, use the drop down to select the Request-URI created earlier (in our example it is "OPTIONS-Ping"), then in the "Action" field use the drop down to select "Forward". Finally in the "Forward To" field, use the drop down to select Forward To selection created earlier (in our example it is "Broadvox Options"). Scroll down to the bottom of the page and click on the "Save" button.

Be sure to apply and save the configuration change, as noted at the end of the Startup Tool section above.

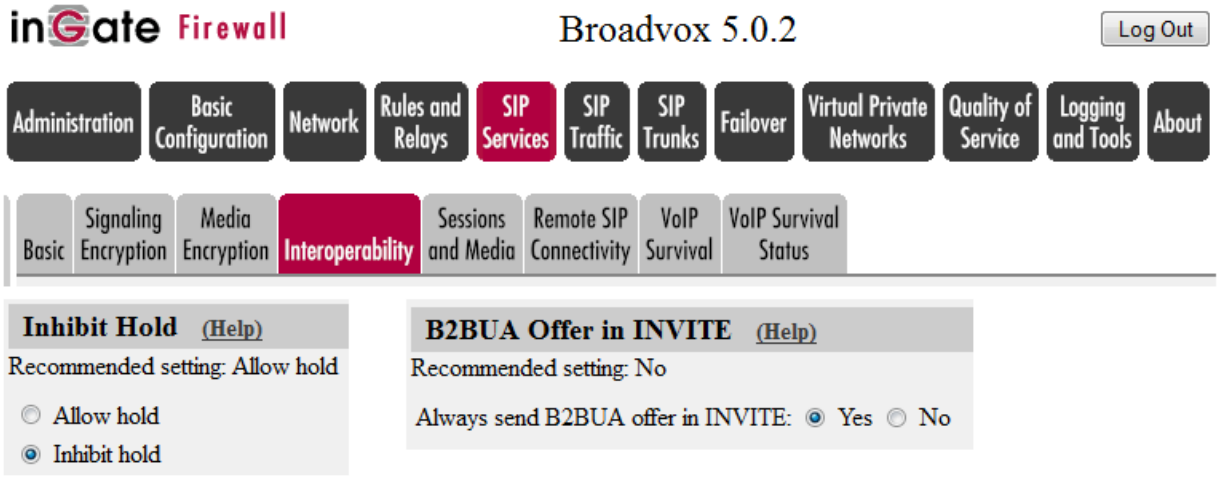
INTEROPERABILITY PARAMETERS

Interoperability testing was performed using a ShoreTel 13.2 IPPBX with the Ingate in Firewall mode and trunks connected directly through the internet to Broadvox's trunking gateway. Two interoperability parameters were changed from their default values in order to get basic inbound calls and some call transfers to work properly. Enable these settings only if your SIP Trunking configuration is having problems with call transfers. NOTE: The success of using these parameters may be connected to the use of Music on Hold. It is highly recommended to enable file based MoH when using the settings below.

B2BUA Offer in INVITE – Some call transfer scenarios might result in the ShoreTel sending an INVITE without the SDP offer resulting in possible call problems for the transfer. Enable this setting to always send B2BUA offer in INVITE, by translating a re-INVITE without SDP offer to a re-INVITE with a SDP offer. Do not confuse this setting with the similar but different "SDP Offer in re-INVITE".

Inhibit Hold - This setting controls if the firewall should remove requests for on-hold from SDP offers before forwarding them. When "inhibit hold" is used, the stream(s) in SDP offers will be converted from sendonly,

recvonly or inactive to sendrecv before being forwarded by the firewall. Forwarded SDP answers will only reflect the stream mode (sendonly, recvonly etc.) requested in the offer, and will not depend on the received SDP answer.

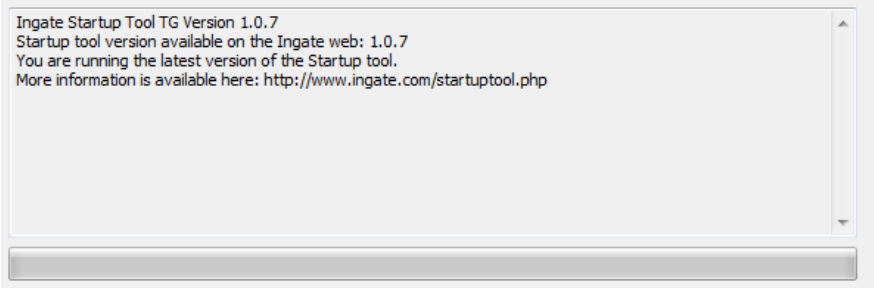


Configuration Troubleshooting

STARTUP TOOL TROUBLESHOOTING

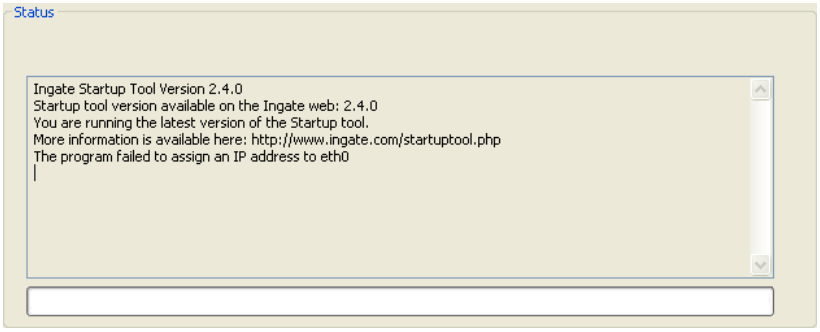
STATUS BAR

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.



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".

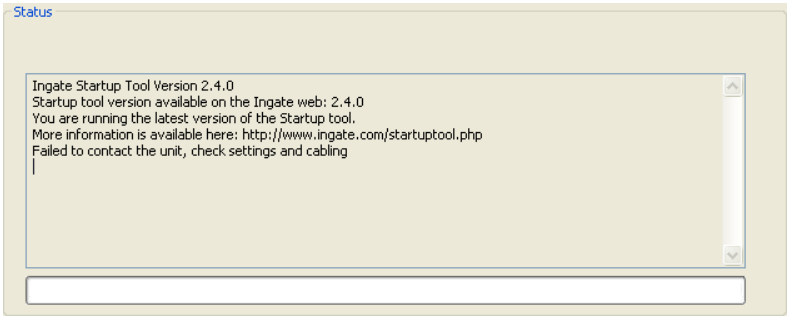


Possible Problems & Resolutions

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.

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.

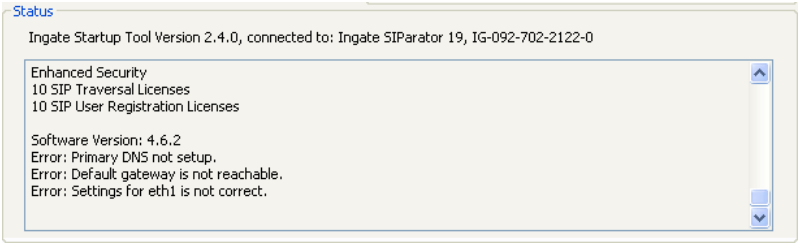


Possible Problems & Resolutions

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".

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.



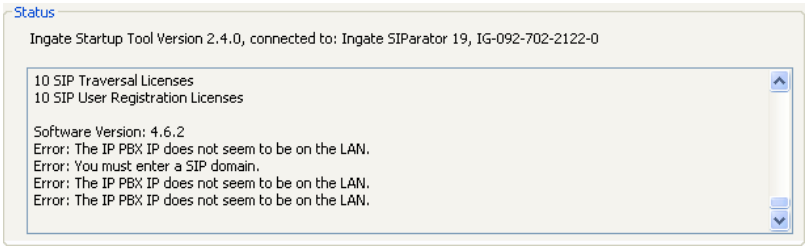
Possible Problems & Resolutions

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

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.

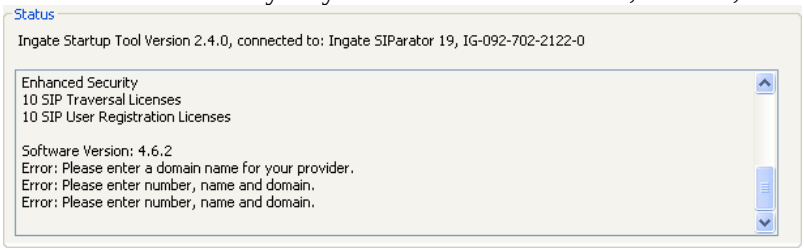


Possible Problems & Resolutions

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.

INTERNET SERVICE PROVIDER (ITSP)

The errors here are fairly easy to resolve. The IP address, Domain, and DID of Broadvox must be entered



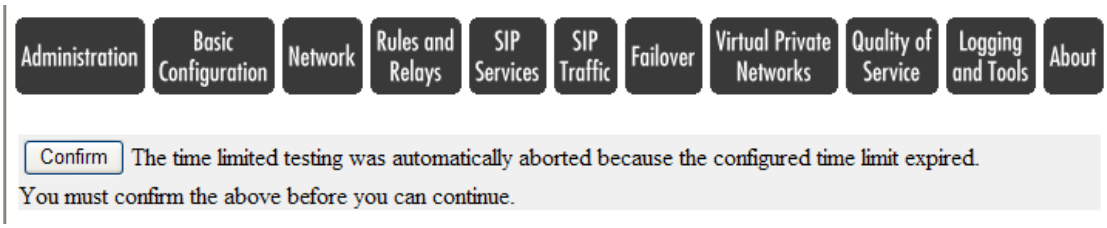
Possible Problems & Resolutions

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"

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 & 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.

Ingate Web GUI Configuration

The following example shows basic configuration parameters for the Ingate device in Firewall mode using the Web GUI. The IP-Addresses and DID's are used as an example only. Actual values will depend on what Broadvox assigns for your solution. Note: The Ingate Firewall screen shots in the following pages may vary from other Ingate modes of operation.

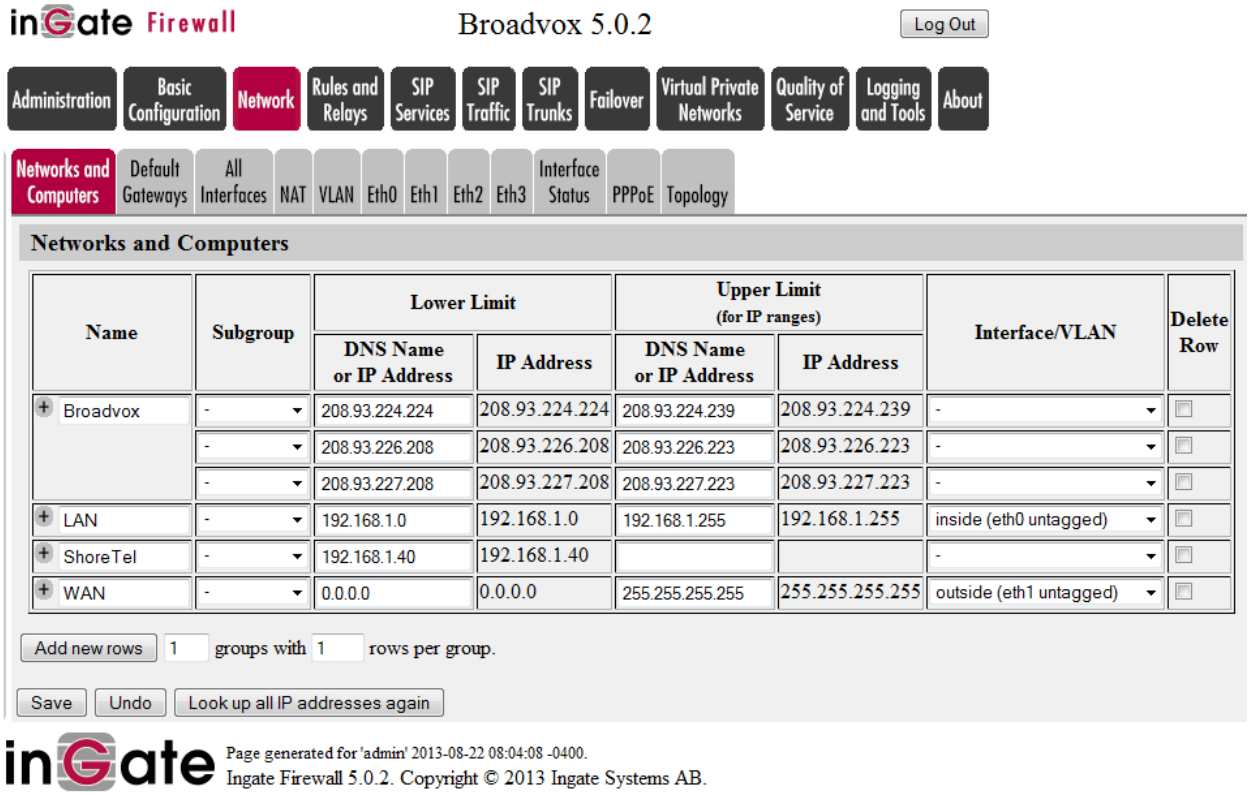
Configure your Ingate Firewall or Ingate SIParator to get basic network connectivity on all applicable interfaces. Please refer to the Reference Guide and other documentation as needed.
Remember to configure the following:

- 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 then 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.

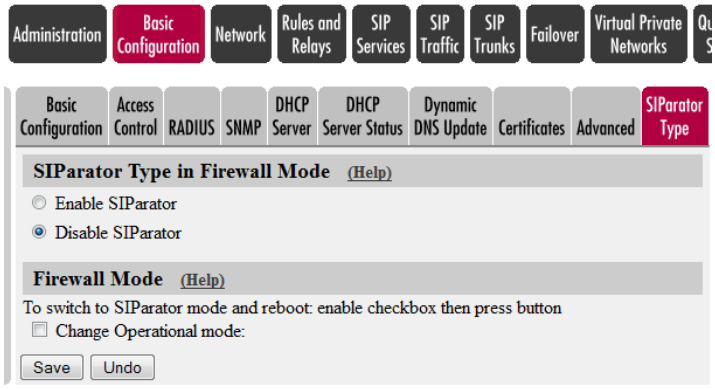
NETWORK – NETWORK & COMPUTERS

- Add a network for the Service Provider (Broadvox). 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 IP for ShoreTel IP-PBX switch.
- Add a network for the LAN (inside IP range) and WAN (outside IP Range) and assign to respective interface.



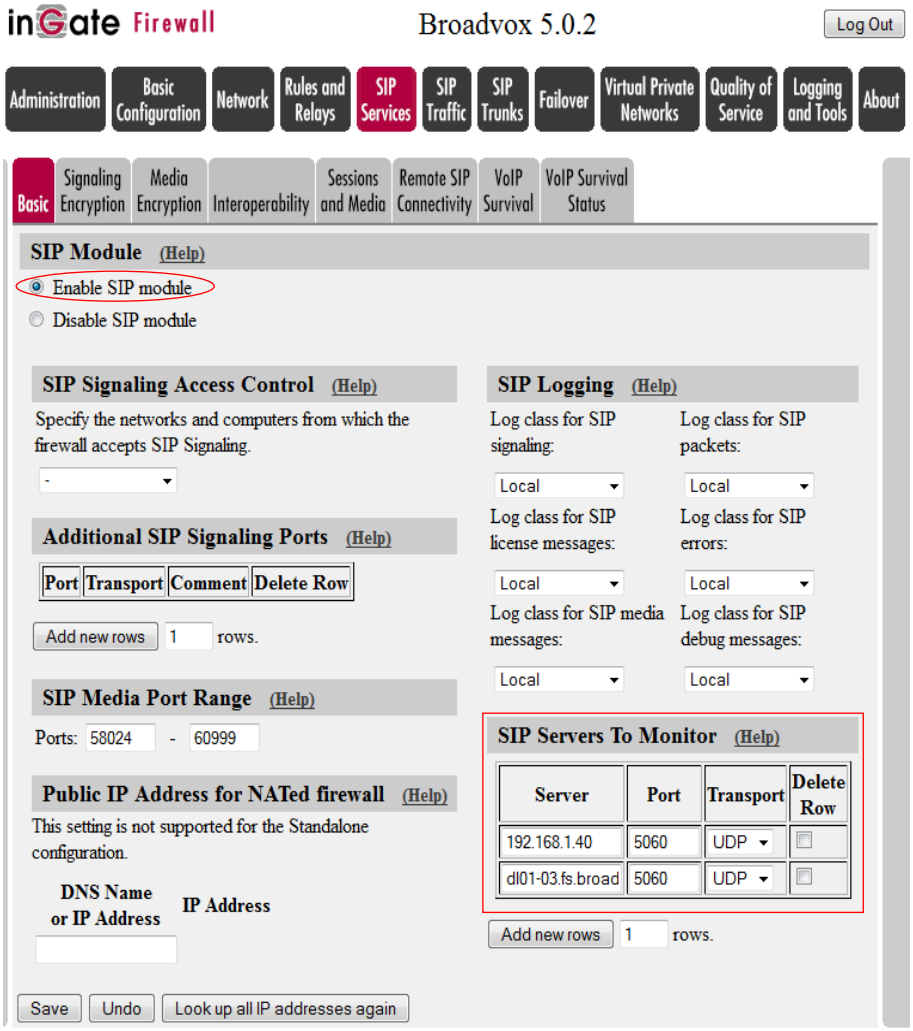
BASIC CONFIGURATION – SIPARATOR TYPE

Use the appropriate SIParator configuration for your deployment.



SIP SERVICE – BASIC

- SIP Module: On.
- SIP Servers To Monitor (ShoreTel Director, Broadvox Gateway for sent traffic (dl01-03.fs.broadvox.net)



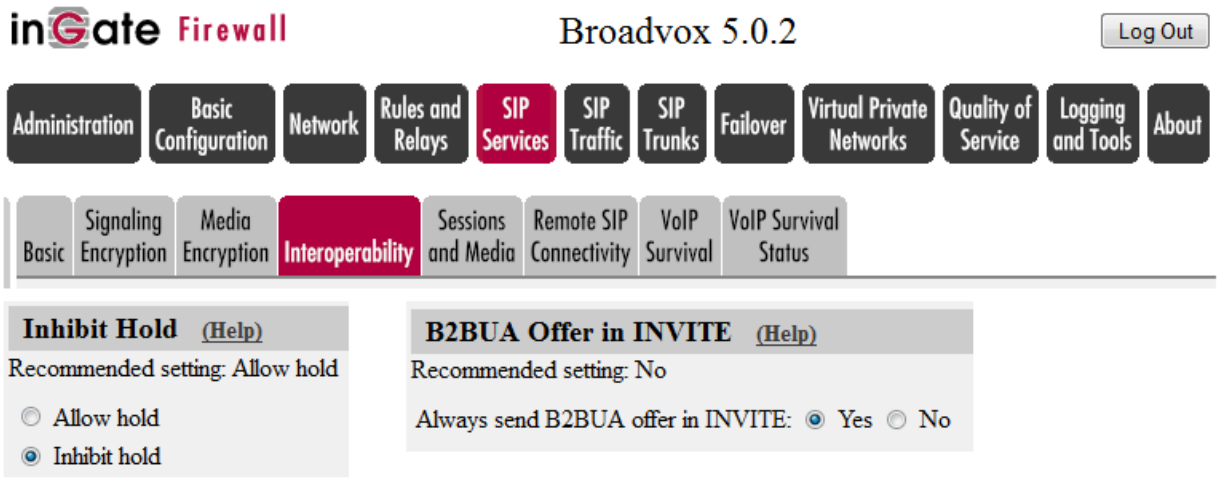
SIP SERVICE – INTEROPERABILITY

Interoperability testing was performed using a ShoreTel 13.2 IPPBX with the Ingate in Firewall mode and trunks connected directly through the internet to Broadvox's trunking gateway. Two interoperability parameters were changed from their default values in order to get basic inbound calls and some call transfers to work properly. Enable these settings only if your SIP Trunking configuration is having problems with call transfers. NOTE: The success of using these parameters may be connected to the use of Music on Hold. It is highly recommended to enable file based MoH when using the settings below.

B2BUA Offer in INVITE – Some call transfer scenarios might result in the ShoreTel sending an INVITE without the SDP offer resulting in possible call problems for the transfer. Enable this setting to always send B2BUA offer in INVITE, by translating a re-INVITE without SDP offer to a re-INVITE with a SDP offer. Do not confuse this setting with the similar but different "SDP Offer in re-INVITE".

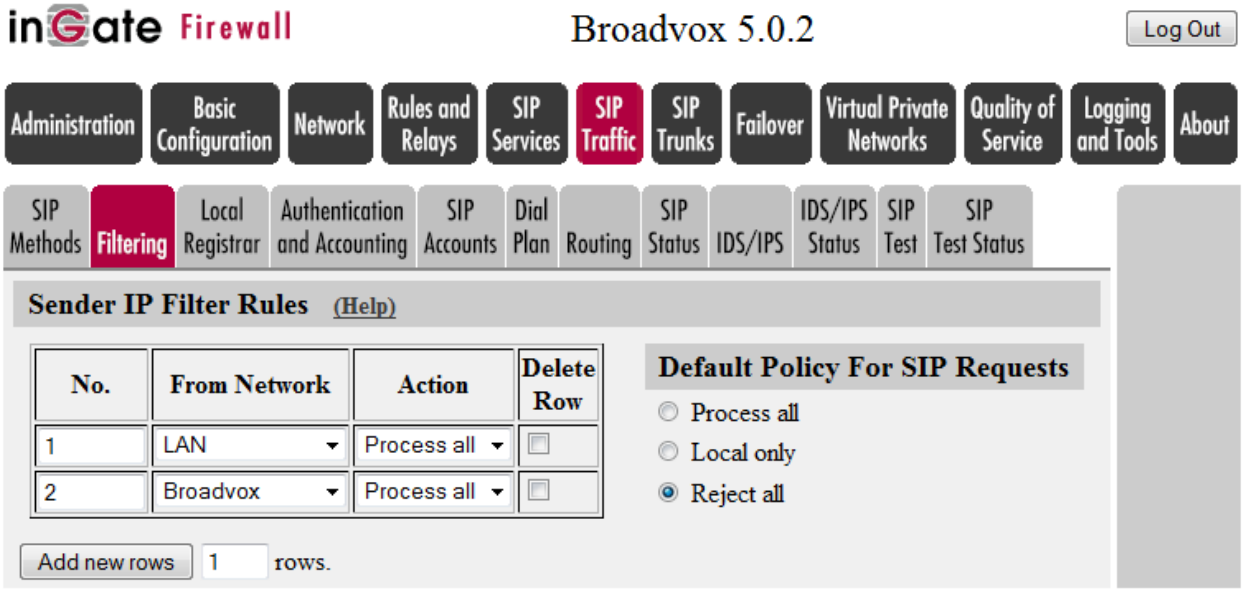
Inhibit Hold - This setting controls if the firewall should remove requests for on-hold from SDP offers before forwarding them. When "inhibit hold" is used, the stream(s) in SDP offers will be converted from sendonly,

1. Inhibit Hold
2. Always send B2BUA offer in INVITE



SIP TRAFFIC – FILTERING

1. Under Proxy Rules, change the Default Policy for SIP Requests to "Reject All". NOTE: From a security perspective start by trusting no one (reject all) and then build in your security by adding entries into "Sender IP Filter Rules" (taken from "Networks and Computers") and use these as a starting point for further processing in a Dial Plan and Call Flow Policy.
2. Content Type: Add */* and Allow – Yes

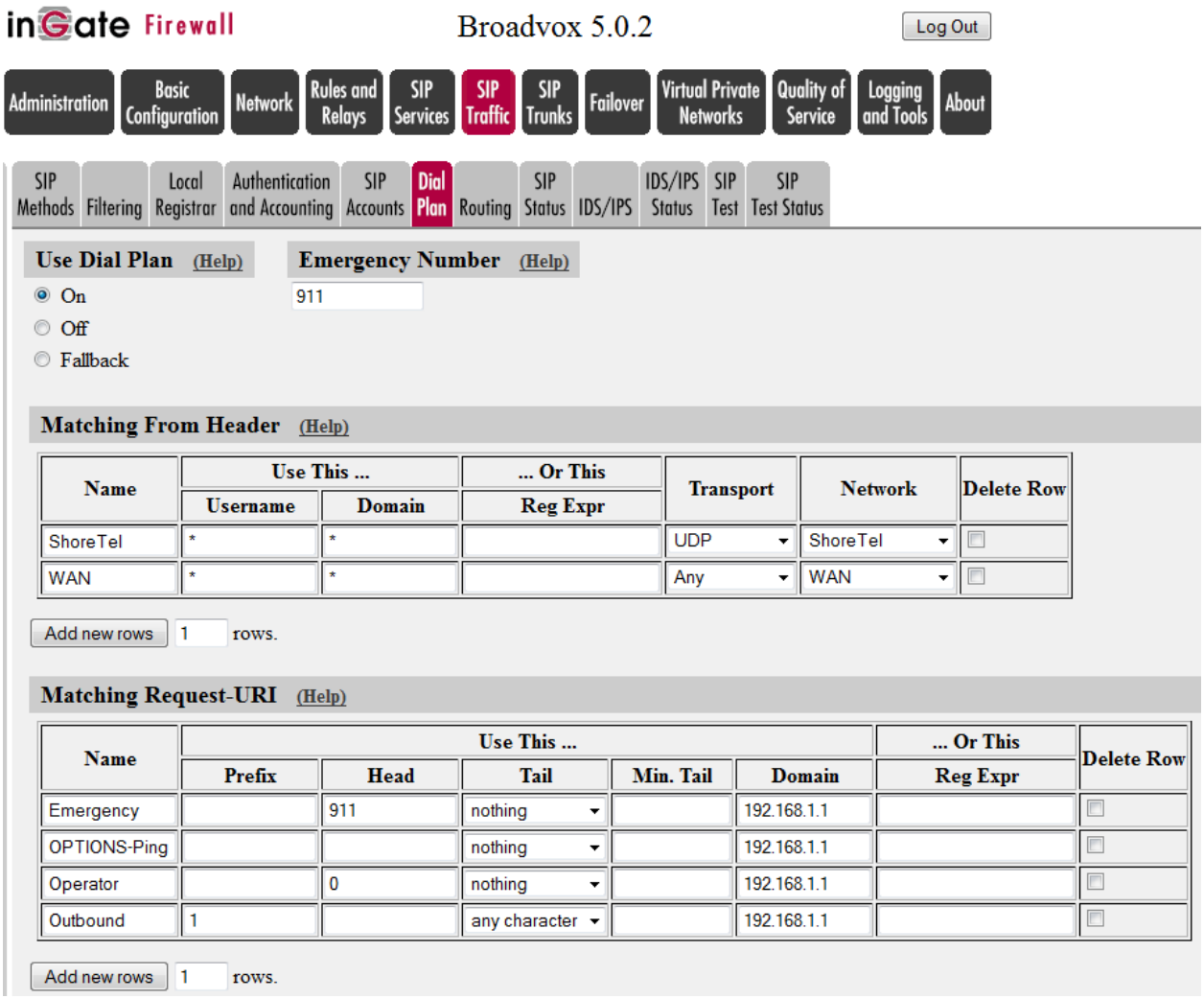


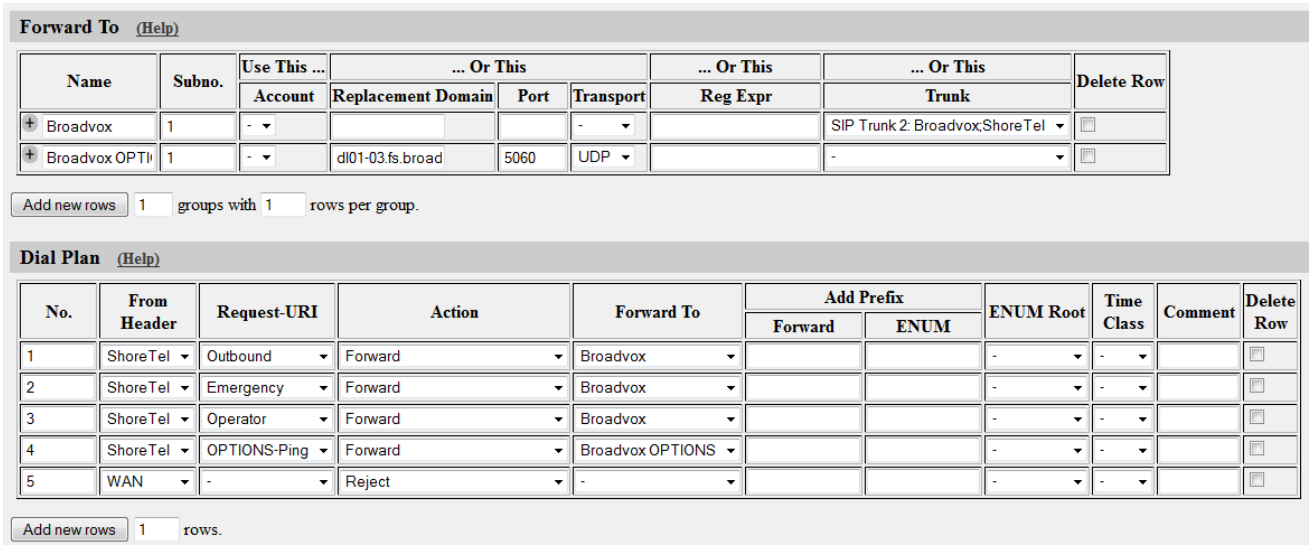
Content Type Filter Rules (Help)

Content Type	Allowed	Delete Row
/	Yes	

SIP TRAFFIC – DIAL PLAN

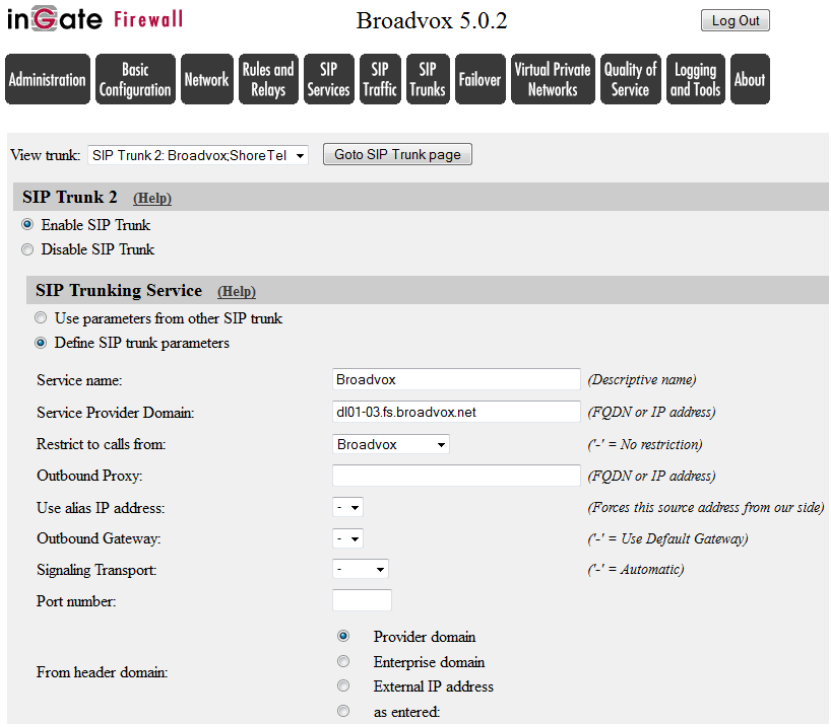
Configure the Dial Plan according to the picture below.

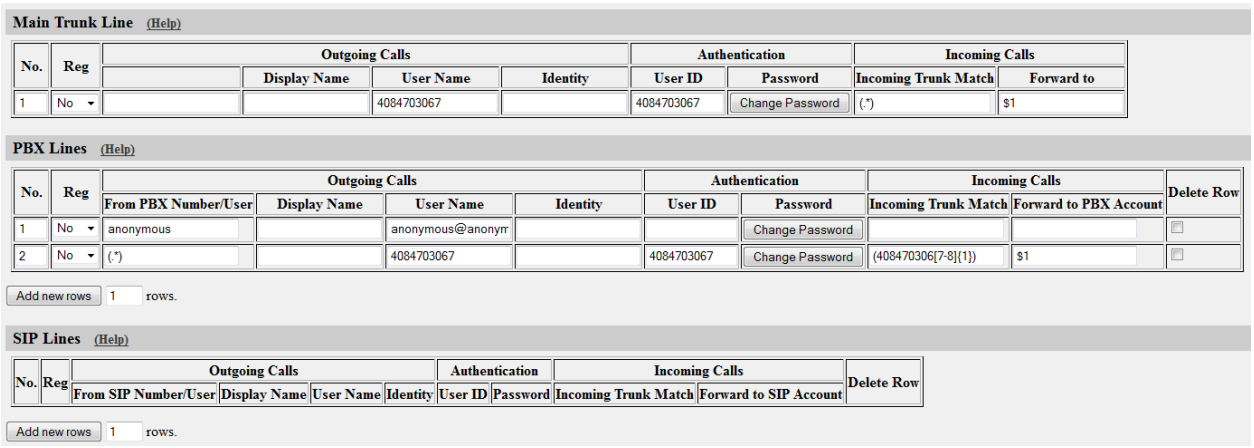


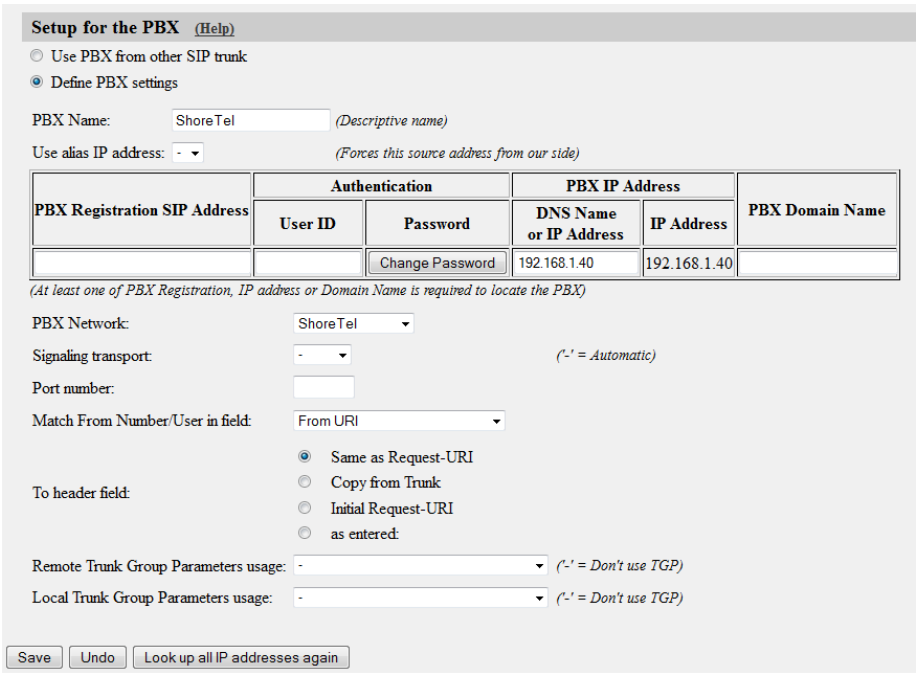


SIP TRAFFIC – SIP TRUNK

Configure the Dial Plan according to the picture below.





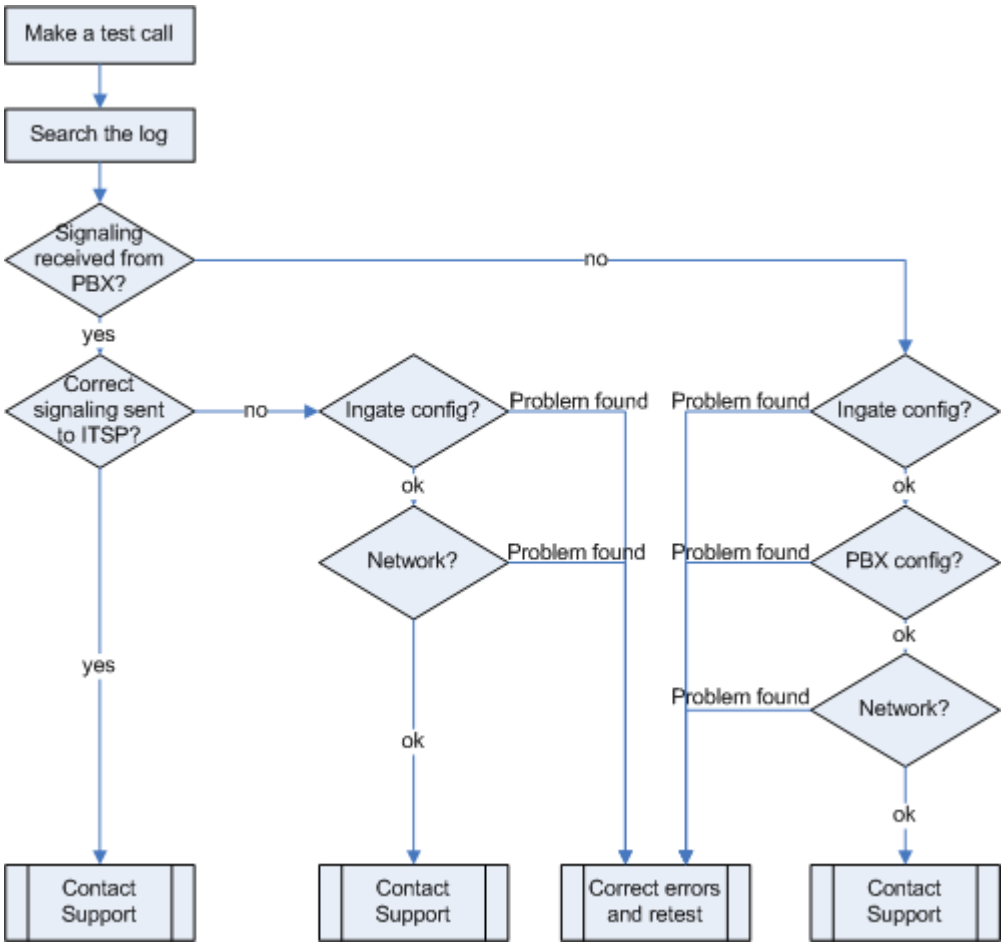


Ingate Basic Call Troubleshooting

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.

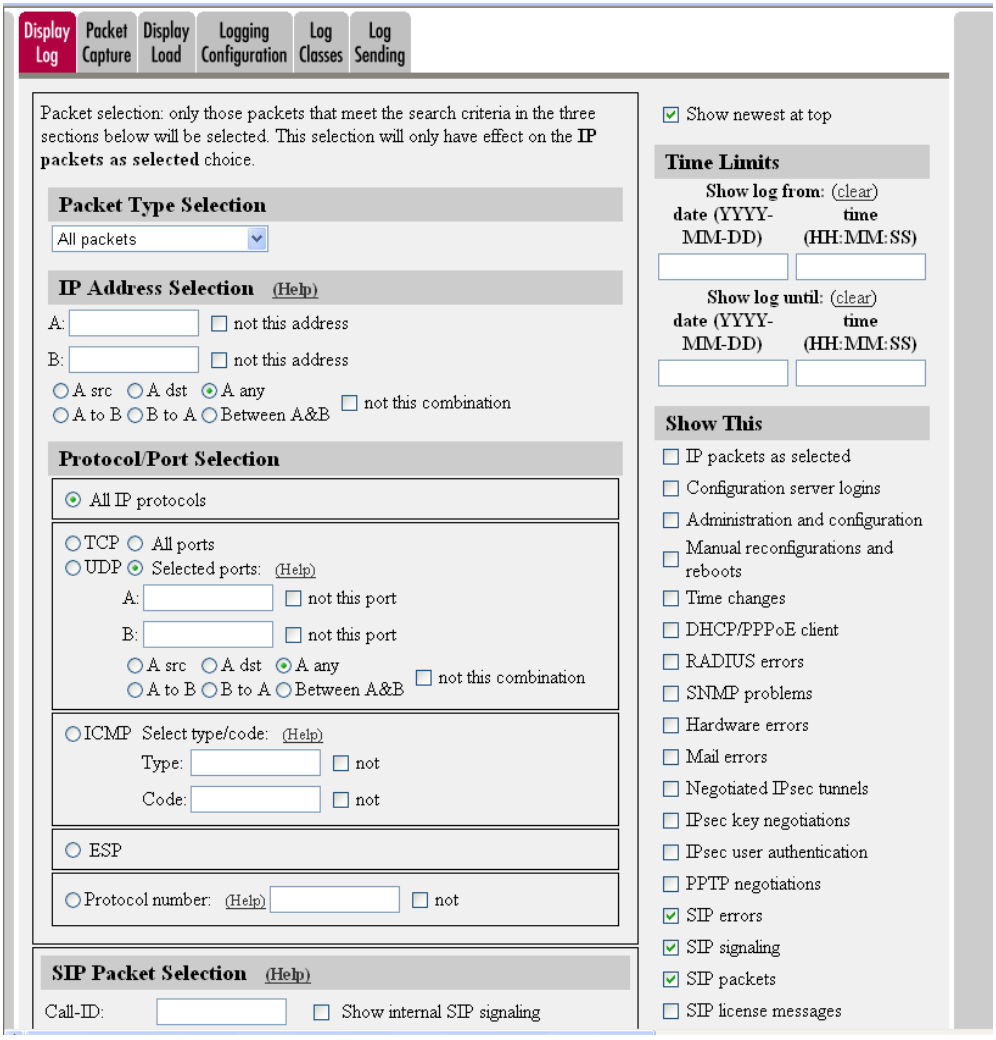


Outbound traffic troubleshooting overview

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 Broadvox 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:

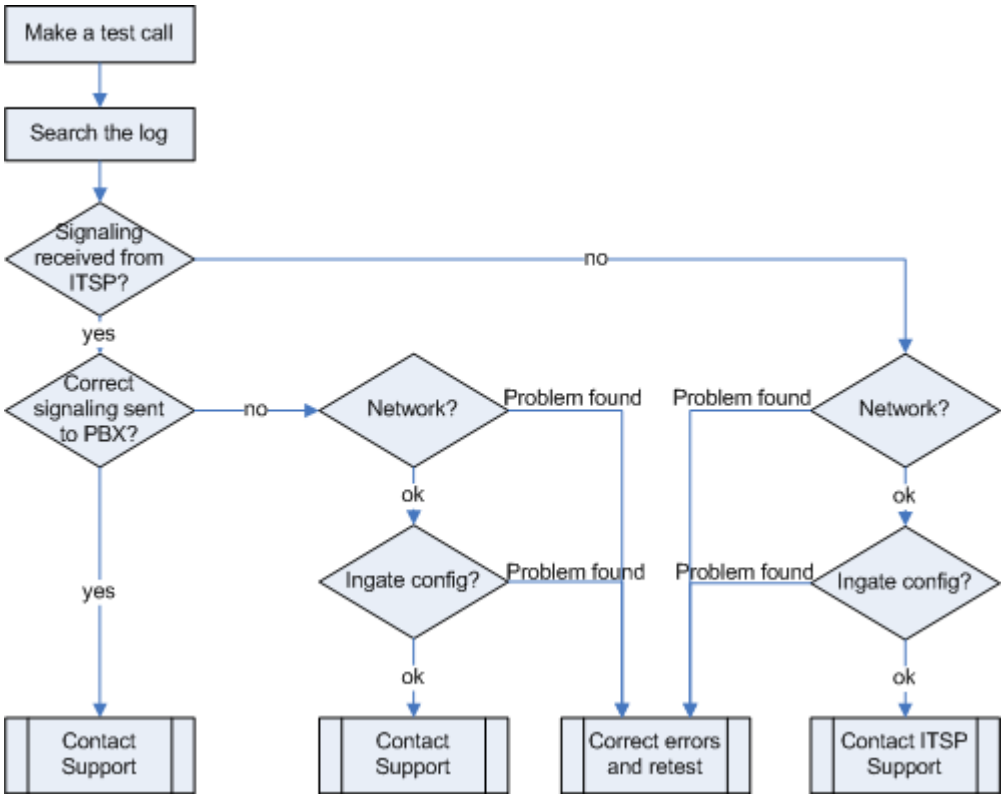
1. Make sure that the Ingate is configured correctly.
2. Make sure the IP connectivity between the Ingate and Broadvox is working. Contact your network administrator for assistance if needed.

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

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

TROUBLESHOOTING INBOUND CALLS

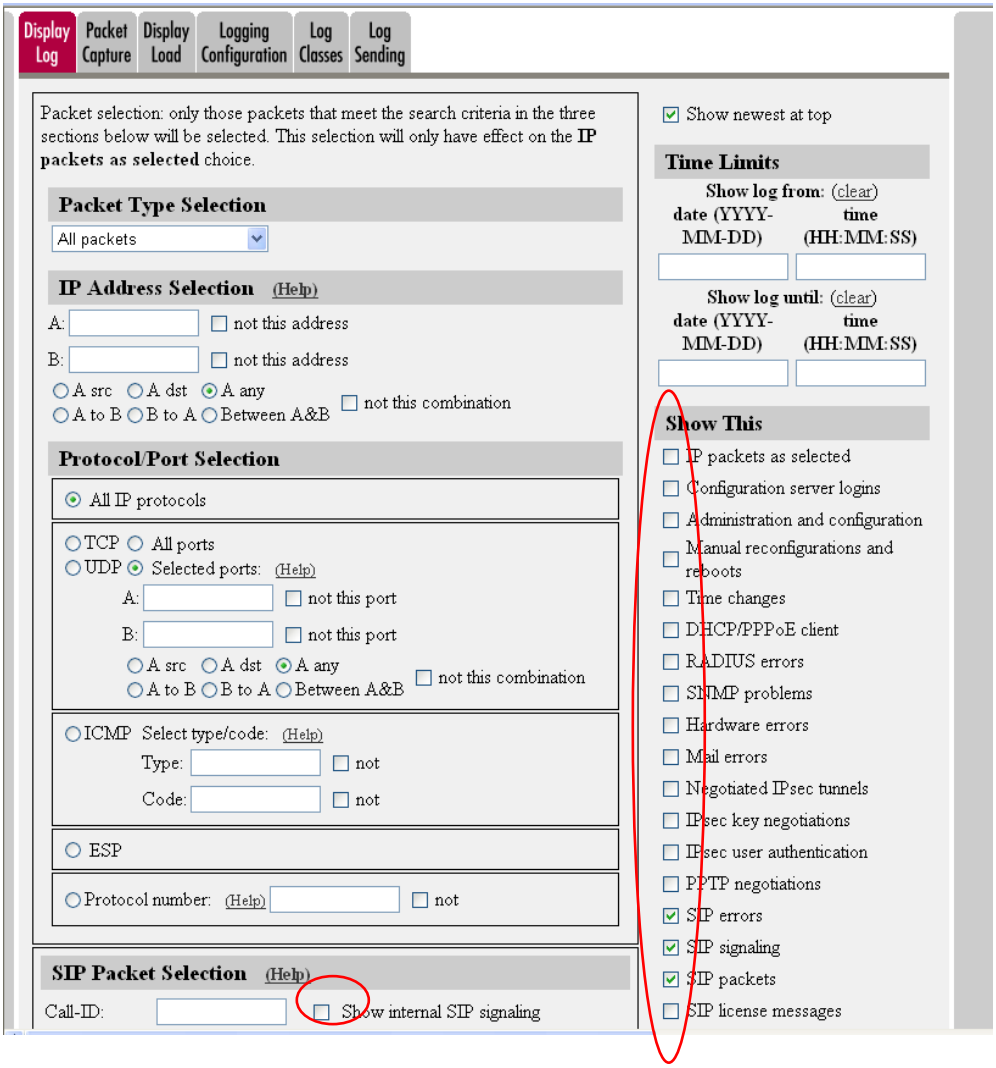
Symptom: When trying to make an inbound call to a ShoreTel phone via the SIP Trunk there is no ringing signal on the ShoreTel phone.
Note: If you get a ringing signal on the ShoreTel phone, these troubleshooting steps will not help you to find the problem. Please contact your sales representative for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

Localize the call initiation from the Trunking provider by searching for "invite sip" in your browser. (use Ctrl-F). You should look for the first packet coming from Broadvox 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 Broadvox to the Ingate. Follow these steps:

1. Make sure you have IP connectivity between the Ingate and Broadvox. 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 Broadvox 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.

Broadvox Configuration & Support

For General Inquiries: 888-849-9608

For Support: techsupport@Broadvox.com

Document & Software Copyrights

Trademarks

Disclaimer

ShoreTel tests and validates the interoperability of the Member's solution with ShoreTel's published software interfaces. ShoreTel does not test, nor vouch for the Member's development and/or quality assurance process, nor the overall feature functionality of the Member's solution(s). ShoreTel does not test the Member's solution under load or assess the scalability of the Member's solution. It is the responsibility of the Member to ensure their solution is current with ShoreTel's published interfaces.

The ShoreTel Technical Support organization will provide Customers with support of ShoreTel's published software interfaces. This does not imply any support for the Member's solution directly. Customers or reseller partners will need to work directly with the Member to obtain support for their solution.

Company Information

ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085 USA

+1.408.331.3300
+1.408.331.3333 fax