Shore Tel [®]	✓ 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

Overview	4
Broadvox Overview and Contact	2
Ingate Overview & Contact	2
Architecture Overview	3
Requirements, Certification and Limitati	ons 5
Broadvox Validation Test Results	6
Table 1-1: Initialization and Basic Calls	6
Table 1-2: Media and DTMF Support	7
Table 1-3: Performance & Quality of Service	7
Table 1-4: Enhanced Services and Features	9
Configuration Overview	11
ShoreTel Unsupported Features	11
ShoreTel Configuration	11
Ingate Configuration	24
Web Admin	24
Connecting the Ingate Firewall/SIParator	25
Connecting the nighter new and on article	
Using the Startup Tool	26
Using the Startup Tool Configure the Unit for the First Time	26 26
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration	26 26 30
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology	26 26 30 33
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology IP-PBX.	26 30 33 44
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology IP-PBX Internet Service provider (ITSP)	26 26 30 33 44 46
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology IP-PBX. Internet Service provider (ITSP) Upload Configuration	26 26 30 33 44 46 47
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology IP-PBX. Internet Service provider (ITSP) Upload Configuration Ingate – Additional Conjguration Parameters .	26 30 33 44 46 47 50
Using the Startup Tool Configure the Unit for the First Time Change or Update Configuration Network Topology IP-PBX. Internet Service provider (ITSP) Upload Configuration Ingate – Additional Coniguration Parameters . OPTIONS Configuration Internet service provider (ITSP)	26 30 33 44 46 47 50 51

Configuration Troubleshooting	53
Startup Tool Troubleshooting	53
Status Bar	53
Configure Unit for the First Time	53
Change or Update Configuration	54
Network Topology	55
IP-PBX	56
Internet service provider (ITSP)	56
Apply Configuration	56
Ingate Web GUI Configuration	57
Network – Network & Computers	58
Basic Configuration – SIParator Type	58
SIP Service – Basic	59
SIP Service – Interoperability	59
SIP Traffic – Filtering	60
SIP Traffic – Dial Plan	61
SIP Traffic – SIP Trunk	62
Ingate Basic Call Troubleshooting	63
Troubleshooting Outbound Calls	63
Troubleshooting Inbound calls	66
Broadvox Configuration & Support	69
Document & Software Copyrights	69
Trademarks	69
Disclaimer	69
Company Information	69
	2.

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: <u>techsupport@Broadvox.com</u> 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 <u>Steve@ingate.com</u> 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



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHDRE Fax +1.408.331.3333 www.ShoreTel.com

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.





Headquarters Office

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	5.0.1
SIParator version	
ShoreTel 13.x	✓

Broadvox network equipment: Broadvox Fusion Version 1.0

Broadvox Validation Test Results

Basic test plan:

TABLE 1-1	: INITIALIZ	ATION AND	BASIC	CALLS
-----------	-------------	-----------	-------	-------

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

TABLE 1-2: MEDIA AND DTMF SUPPORT

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

TABLE 1-3: PERFORMANCE & QUALITY OF SERVICE

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

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.



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

ID	Name	Description	Notes
3.2	Capacity Test	Verify the service provider interface can sustain services through period of	Pass
		heavy outbound and inbound load.	
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



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

TABLE 1-4: ENHANCED SERVICES AND FEATURES

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 3^{rd} party SIP endpoints.



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

ID	Name	Description	Notes
4.14	Inbound call to a	Verify that calls route to the proper	Pass
	Workgroup	Workgroup and are answered	
		successfully by an available	
		workgroup agent with audio in both	
		directions using G.729 and G.711	
		codecs.	_
4.15	Inbound call to	Verify that inbound calls to a user, via	Pass
	DNIS / DID and	DID / DNIS, routes to the proper user	
	leave a voice	mailbox and a message can be left	
4.16	Call Earnard	With proper audio.	Daga
4.10	Call Forward –	forwarded to a user's "Find Me"	Pass
	Findivie	destination	
4.17	Call Forward	Verify that inbound calls are	Dass
4.17		immediately automatically forwarded	1 455
	1 Hways	to a user's external destination	
4.18	Inbound /	Verify that inbound / outbound fax	Pass
	Outbound Fax	calls complete successfully.	
	calls	I I I I I I I I I I I I I I I I I I I	
4.19	ShoreTel	Verify that inbound calls are properly	Not Tested
	Converged	forwarded to the ShoreTel Converged	
	Conferencing	Conferencing Server and it properly	
	Server	accepts the access code and you're	
		able to participate in the conference	
		bridge.	
4.20	Inbound call to	Verify that inbound calls properly	Pass
	Bridged Call	presented to all of the phones that	
	Appearance	have BCA configured and that the call	
	(BCA) extension	can be answered, placed on-hold and	
1 21	Inhound call to a	Verify that inbound calls properly	Dass
4.21	Group Pickup	presented to all of the phones that	1 455
	extension	have Group Pickup configured and	
	extension	that the call can be answered placed	
		on-hold and then transferred.	
4.22	Office Anywhere	Verify that inbound calls are properly	Pass
	External	presented to the Office Anywhere	
		External PSTN destination.	
4.23	Simul Ring	Verify that inbound calls are properly	Pass
		presented to the desired extension and	
		the "Additional Phones" destinations.	
4.24	MakeMe	Verify that an inbound call can be	Pass
	Conference	conferenced with three (or more)	
		additional parties	~
4.25	Park / Unpark	Verify that an inbound call can be	Pass
1.2.5		parked and unparked	P
4.26	Call Recording	Verify that external calls can be	Pass
		recorded via the SIP Irunk using	
		Shore Let Communicator	

ShoreTel 960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

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

Table 1-5: Security

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

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).



Call Control Options	Save	Reset	<u>Help</u>
Edit			
Edit this record	Refresh this page	<u>je</u>	
General:			
Use Distributed Routing Service for call rout	ing.		
Enable Monitor / Record Warning Tone.			
Enable Silent Coach Warning Tone.			
Generate an event when a trunk is in-use for	240 minut	es.	
Park Timeout (1-100000) after 60 s	econds.		
Hang up Make Me Conference after 20	minutes of sile	ence.	
Delay before sending DTMF to Fax Server:	2000	msec	
DTMF Payload Type (96 - 127):	102		
SIP:			
Realm:	ShoreTel		
✓ Enable SIP Session Timer.	_		
Session Interval (90 - 3600):	3600	sec 🚽	
Refresher:	Caller (UAC) 🔻		
Voice Encoding and Quality of Service:			
Maximum Inter-Site Jitter Buffer (20 - 400):	300	msec	
DiffServ / ToS Byte (0-255):	184	(DSCP = 0x2e)	
Media Encryption:	None	•	
Admission control algorithm assumes RTP h	eader compression	n is being used.	
Always Use Port 5004 for RTP (This option i	is unavailable beca	use your system utilizes SIP	Servers,
SIP Trunks or SIP Extensions. This feature is in	compatible with SI	P devices.)	
Call Control Quality of Service:			
DiffServ / ToS Byte (0-255):	104	(DSCP = 0x1a)	
Video Quality of Service:			
DiffServ / ToS Byte (0-255):	136	(DSCP = 0x22)	
Trunk-to-Trunk Transfer and Tandem Trunks	E.		
Hang up after 60 minutes of silence	9.		
Hang up after 480 minutes.			

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



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

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).

ShoreTel 960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.8DSHDRE Fax +1.408.331.3333 www.ShoreTel.com

Figure 7 – Site Bandwidth settings

Bandwidth:		
Admission Control Bandwidth:	2046 kbps	
Intra-Site Calls:	Very High Bandwidth Codecs	*
Inter-Site Calls:	Very Low Bandwidth Codecs	*
FAX and Modem Calls:	Fax Codecs - High Bandwidth	~

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





960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

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

STATU	
TF	P-50V-VMB
Port	Port Type
1	5 SIP Trunks 🛛 😽
2	5 IP Phones 😽
3	Conference 😽
4	Conference 😽
11 Edit	Extension 😪
12	Available 😽

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

ShoreTel [®]	
Director	
Build 18.41.4902.0	
Logoff Administrator	
Administration	
Users	
Trunks	
 Individual Trunks 	
• Trunk Groups	
SIP Profiles JEDN Profiles	
 ISON Profiles Local Profixor 	
• ID Dhones	
Platform Hardware	
Call Control	
Voice Mail	
Auto-Attendant Menus	
 Workgroups 	
Schedules	
Communicator	
 System Directory 	
 Application Servers 	
SIP Servers	
Sites	
System Parameters	
Preferences	

Administration Trunk Groups

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

Figure 11 - Trunk Groups Settings

Trunk Groups						He
Add new trunk grou	p at site: Headquarters	of type: SIP		• <u>G</u>	0	
Name	Туре	Site	Trunks	DID	Destination	Access Code
Analog Loop Start	Analog Loop Start	Headquarters	0	No	1700	9
Digital Loop Start	Digital Loop Start	Headquarters	0	No	1700	9
Digital Wink Start	Digital Wink Start	Headquarters	0	No	1700	9

From the pull down menus on the "Trunk Groups" screen, select the site desired and select the **"SIP"** trunk type to configure. 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

Trunk Groups Edit SIP Trunk Group	New Copy Save Delete Reset
Edit this record	Refresh this page
Name:	Broadvox
Site:	Headquarters
Language:	English(US) -
Enable SIP Info for G.711 DTMF Signaling	
Profile:	Default ITSP
Digest Authentication:	<none></none>
Username:	
Password:	

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

Inbound:		
Number of Digits from CO:	10	←
DNIS	Edit DNIS Map	
	Edit DID Range	
Extension		
Translation Table:	<none> 😽</none>	
O Prepend Dial In Prefit	x:	
O Use Site Extension F	Prefix	
🗹 Tandem Trunking 🛛 🗲		
User Group:	Executives	~
Prepend Dial In Prefix:		
Destination:	700 : Default	Search



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

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:

V	Outbound:	
	Network Call Routing:	
	Access Code:	9
	Local Area Code:	408
	Additional Local Area Codes:	Edit
	Nearby Area Codes:	Edit
	Billing Telephone Number:	+1 (408) 470-3067 (e.g. +1 (408) 331-3300)
	Trunk Services:	
	V Local	
	✓ Long Distance	
	✓ International	
	Enable Original Caller Information	
	☑ n11 (e.g. 411, 611, except 911 which is specified below)	
	Emergency (e.g. 911)	
	Easily Recognizable Codes (ERC) (e.g. 800, 888, 900)	
	Explicit Carrier Selection (e.g. 1010xxx)	
	☑ Operator Assisted (e.g. 0+)	
	Caller ID not blocked by default	
	Enable Caller ID (Please confirm with the Carrier(s) or the S	ervice Provider(s) on how the end-to-end caller name is delivered)
	When Site Name is used for the Caller ID, overwrite it with:	
	Trunk Digit Manipulation:	
	Remove leading 1 from 1+10D	
	Hint: Required for some long distance service providers.	
	Remove leading 1 for Local Area Codes (for all prefixes unless	ss a specific local prefix list is provided below)
	Hint: Required for some local service providers with overlay are	a codes.
	Dial 7 digits for Local Area Code (for all prefixes unless a sp	ecific local prefix list is provided below)
	Hint: Local prefixes required for some local service providers w	ith mixed 7D and 1+10D in the same home area.
	Dial in E.164 Format	
	Local Prefixes:	None Go to Local Prefixes List
	Prepend Dial Out Prefix:	
	Off System Extensions:	Edit
	Translation Table:	<none> 💌</none>

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:

Trunk Digit Manipulation:				
Remove leading 1 from 1+10D				
Hint: Required for some long distance	service providers.			
Remove leading 1 for Local Area Co	des (for all prefixes unless a specific local prefix list is provided below)			
Hint: Required for some local service p	providers with overlay area codes.			
Dial 7 digits for Local Area Code (fo	r all prefixes unless a specific local prefix list is provided below)			
Hint: Local prefixes required for some	local service providers with mixed 7D and 1+10D in the same home area.			
Dial in E.164 Format				
Local Prefixes:	None Co to Local Prefixes List			
Prepend Dial Out Prefix:				
Off System Extensions:	Edit			
Translation Table:	<none> ▼</none>			

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.

<u>U</u> sername:	admin	
1		

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.)



Trunk Group Dialing Rules:	
Generated:	View
Custom:	Edit
Trunk Groups Dialing Rules Webpage Dialo	g <u>23</u>
;10E	*
Sava Cancel	Ŧ
Save	

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:

Trunks by Group)							Help
Add new trunk a	at site: Headqua	rters 🔻 in tr	unk group:	Broadvox	▼ <u>Go</u>		-	
Records 25	 per page 							
Delete								
Name	Group	Туре	Site	Switch		Port/Channel	SIP IP Address	

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

Trunks Edit Trunk	New Copy Save Delete Reset		<u>Help</u>
Edit this record	Defeash this page	* modified	
Luit uns record	<u>Reliesh this page</u>		
Site:	Headquarters		
Trunk Group:	Broadvox		
Name:	Broadvox		
Switch:	HQ-SG90 🔻		
IP Address:	192.168.1.1		
Number of Trunks (1 - 220):	5		

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 <u>http://www.ingate.com/startuptool.php</u>. 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.

inGa	te Firewall		Broa	dvox 5.0.2		
Administratio	on Basic Configuration Network	k Rules and SIP Relays Services	SIP SIP Traffic Trunks Fai	ilover Virtual Private Networks	Quality of Logging Service and Tools Abo	out
You were no	ot logged on.					
Local pass	word					
Username:	admin					
Password:	•••••					
Log in						
inC	ate Page ger Ingate F	nerated 2013-08-21 19:19 Firewall 5.0.2. Copyr	:13 -0400. ight © 2013 Ingate	Systems AB.		
·I	0					

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.
- 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.

🕞 Select Product Type 📃 🗖	×
Welcome to the Ingate Startup tool TG - this tool will assist you in setting up your new Ingate unit	
Setup	
LAN	
Connect your computer to your Ingate unit like this.	
Please Select model	

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



Ingate Startup Tool TC Version	Help	
You are running the latest version of this tool	nep	
		Help
First select what you would like to do:	Assign IP address and pass	word, establish contact
Configure the unit for the first time	Inside (Interface Eth0)	
Change or update configuration of the unit	IP Address:	192 . 168 . 1 . 1
Check SIP configuration and logs	MAC Address:	01 29 f0 11 de ed
Register this unit with Ingate	The Address	91-20-10-11-02-80
Upgrade this unit	Select a password	
✓ Enable SIP module	Password:	•••••
Configure Remote SIP Connectivity		
Configure SIP trunking	Confirm Password:	
Backup the created configuration	Interface of your PC	
Create a config without connecting to a unit	Interface of your PC	
This tool remembers passwords		•
		🛞 Contact
Status		
Ingate Startup Tool TG Version 1.0.7 Startup tool version available on the Ingate web: 1.0. You are running the latest version of the Startup tool. More information is available here: http://www.ingate	.7 .com/startuptool.php	*

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

First select what you would like to do:
 Configure the unit for the first time
Change or update configuration of the unit
Check SIP configuration and logs
Register this unit with Ingate
🔲 Upgrade this unit
Enable SIP module
Configure Remote SIP Connectivity
🔽 Configure SIP trunking
Backup the created configuration
Create a config without connecting to a unit
This tool remembers passwords

- 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.

Inside (Interface Eth0)		
IP Address:	192 . 168 . 1 . 1	
MAC Address:	91-28-f0-11-de-ad	

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

Select a password	
Password:	•••••
Confirm Password:	•••••

- 7. Choose the PC interface used to connect to the unit..
 - Interface of your PC



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.



Assign IP address and passy	vord, establish contact
IP Address:	192 . 168 . 1 . 1
MAC Address:	91-28-f0-11-de-ad
Select a password	
Password:	•••••
Confirm Password:	•••••
Interface of your PC	
Local Area Conne	ection 2 🔹
	Contact

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.



GSelect Proc	duct Type
Welcome to t	the Ingate Startup tool TG - this tool will assist you in setting up your new Ingate unit —
-Setup -	
	LAN LAN
	Connect your computer to your Ingate unit like this.
Please	Select model

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

ingate Startup Tool TG Version	Help	
rou are running the latest version of this tool.		Help
First select what you would like to do:	Establish contact	
Configure the unit for the first time	Inside (Interface Etho)
Change or update configuration of the unit	IP Address:	192 . 168 . 1 . 1
Check SIP configuration and logs		
Pegister this unit with Ingate		
Upgrade this unit	Enter the password	
✓ Enable SIP module	Password:	
Configure Remote SIP Connectivity		
Backup the created configuration		
Create a config without connecting to a unit		
This tool remembers passwords		
		Contact
Status		
Jacoba Startup Teol TC Version 1.0.7		
Startup tool version available on the Ingate web: 1.0	0.7	^ ^
You are running the latest version of the Startup too). re. com/startuntool.nbn	
nore into mator is available nere: http://www.iligat	ercompter tup toonphp	
		Ψ.



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

First select what you would like to do:
\odot Configure the unit for the first time
Change or update configuration of the unit
C Check SIP configuration and logs
 Register this unit with Ingate Upgrade this unit Enable SIP module Configure Remote SIP Connectivity
Configure SIP trunking
Backup the created configuration
Create a config without connecting to a unit
This tool remembers passwords

- 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.

Es	tablish contact								
	Inside (Interface Eth0)								
	IP Address:	192	•	168	•	1	•	1	

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

Enter the password	
Password:	•••••



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

Establish contact Inside (Interface Eth0) IP Address:	192 . 168 . 1 . 1
Enter the password Password:	•••••
	Contact

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.

Product Type:	DMZ-LAN SIParator 🔹	
-Inside (Interface E	Firewall	-
ID address:	Standalone SIParator	
IF duuress;	DMZ-LAN SIParator	
	DMZ SIParator	
Netmask:	LAN SIParator	
	WAN 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" . Product Type: 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.



Inside (Interface Ef	th0) —							
IP address:	10	•	40	•	12	•	2	
Netmask:	255	•	255	•	255	•	0	

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

Outside (Interface I	Eth 1)						
Use DHCP to obtain IP							
IP Address:	10 . 40 . 251 . 10						
Netmask:	255 . 255 . 255 . 0						
Allow https access to web interface from Internet							

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).

Gateway:	10	40	251	1

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

DNS server							
Primary:	4	•	2	•	2	•	2
Secondary: (Optional)	8	•	8	•	8	•	8

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.

	-PBX ITSP Upload Configuration	1	
Product Type:	Standalone SIParator		
IP address:	10 . 40 . 12 . 2	Internet	
Netmask:	255 . 255 . 255 . 0		
Outside (Interfa	ce Eth1) obtain IP	Ingate SIParator	firewall
Netmask:	255 . 255 . 255 . 0		
Allow https a	ccess to web interface from Internet	2-0	
Gateway:	10 . 40 . 251 . 1		
		DNG annual	
		Primary: 4 . 2 . 2 . 2	
		Secondary: 8 . 8 . 8 . 8 (Optional)	
Status Ingate Startup	Tool TG Version 1.0.7, connected to:	Ingate Firewall 1210, IG-094-213-5062-1	
VPN	rity zed) SIP Traversal Licenses		•
Enhanced Secu 50 (+55 unutili: Unlimited SIP U Software Versi Your unit's soft	ser Registration Licenses on: 5.0.1 ware is newer than the Startup Tool,	consider using a newer version.	*

Configuration Steps:

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

Product Type:	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.

•

Inside (Interface E	th0) —						
IP address:	10	•	40	•	12	•	2
Netmask:	255	•	255	•	255	•	0



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

Outside (Interface	Eth1)						
Use DHCP to obtain IP							
IP Address:	10 . 40 . 251 . 10						
Netmask:	255 . 255 . 255 . 0						
Allow https access to web interface from Internet							

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

Gateway:	10	•	40	•	251		1	
----------	----	---	----	---	-----	--	---	--

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

DNS server							
Primary:	4	•	2	•	2	•	2
Secondary: (Optional)	8	•	8	•	8	•	8

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.



Product Type:	DMZ SIParator	
DMZ (Interface I	Eth0)	Internet
IP address:	10 . 40 . 12 . 2	
Netmask:	255 . 255 . 255 . 0	
LAN IP address i	range	DMZ
Low IP:	10 . 40 . 251 . 10	Ingate SIParator
High IP:	255 . 255 . 255 . 0	LAN
-		
Gateway:	10 . 40 . 251 . 1	IC DRY
🔽 Use NATing f	îrewall	
Firewall extern I	P: 66 . 162 . 145 . 11]
		DNS server
		Primary: 4 . 2 . 2 . 2
		Secondary: 8 . 8 . 8 . 8 (Optional)
Status Ingate Startup	Tool TG Version 1.0.7, connected	to: Ingate Firewall 1210, IG-094-213-5062-1
VPN		
Enhanced Secu	rity	
50 (+55 unutili: Unlimited STP U	zed) SIP Traversal Licenses Iser Registration Licenses	
Software Versi Your unit's soft	on: 5.0.1 ware is newer than the Startup T	ool, consider using a newer version.

Configuration Steps:

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

Product Type:	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.

Inside (Interface Et	h0) —						
IP address:	10	•	40	•	12	•	2
Netmask:	255	•	255	•	255	•	0

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



-LAN IP address	range
Low IP:	10 . 40 . 251 . 10
High IP:	255 . 255 . 255 . 0

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

Gateway:	10	•	40	•	251	·	1	

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

Vse NATing firewall									
Firewall extern IP:	66	•	162		145		11		

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

DNS server							
Primary:	4	•	2	•	2	÷	2
Secondary: (Optional)	8	•	8	•	8	•	8

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.

Product Type:

DMZ-LAN SIParator

Ŧ



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.

Inside (Interface E	h0)	
IP address:	10 . 40 . 12 . 2	!
Netmask:	255 . 255 . 255 . 0	

- 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.

DMZ (Interface Eth	1)					
Use DHCP to ob	tain IP					
IP Address:	10 . 40 . 251 . 1					
Netmask:	255 . 255 . 255 . 0					
Allow https access to web interface from Internet						

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.

Use NATing firewall									
Firewall extern IP:	66		162		145		11		

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

DNS server							
Primary:	4	÷	2	•	2	•	2
Secondary: (Optional)	8	•	8	•	8	•	8

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.

ork Topology IP-F	PBX ITSP Upload Configuration	1		
Product Type:	LAN SIParator		\sim	
-LAN (Interface Et	h0)			
IP address:	10 . 40 . 12 . 2		Internet	
Netmask:	255 . 255 . 255 . 0			
		F _		
			Existing firewa	0
			`	
		LAN		
Gateway:	10 . 40 . 251 . 11		IP-PBX Ingate SIParato	or
🔽 Use NATing fin	ewall			
✓ Use NATing fin Firewall extern IP	ewall			
☑ Use NATing fir Firewall extern IP	ewall : 66 . 162 . 145 . 11	DNS server		
✓ Use NATing fir Firewall extern IP	ewall : 66 . 162 . 145 . 11	DNS server Primary:	4 . 2 . 2 . 2	
☑ Use NATing fir Firewall extern IP	ewall	DNS server Primary: Secondary: (Optional)	4 . 2 . 2 8 . 8 . 8	
Use NATing fir Firewall extern IP	ewall	DNS server Primary: Secondary: (Optional)	4 . 2 . 2 8 . 8 . 8	
Use NATing fir Firewall extern IP Status Ingate Startup To	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to	DNS server Primary: Secondary: (Optional)	4 . 2 . 2 . 2 8 . 8 . 8 . 8 G-094-213-5062-1	
Use NATing fir Firewall extern IP Status Ingate Startup To VPN OoS	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, IG	4 . 2 . 2 . 2 8 . 8 . 8 . 8 G-094-213-5062-1	•
Use NATing fir Firewall extern IP Status Ingate Startup To VPN QoS Enhanced Securi	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, IG	4 . 2 . 2 . 2 8 . 8 . 8 . 8 G-094-213-5062-1	•
Use NATing fir Firewall extern IP Status Ingate Startup Tr VPN QoS Enhanced Securi S0 (+55 unutilize Unlimited SIP Us)	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to ity ed) SIP Traversal Licenses er Registration Licenses	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, IG	4 . 2 . 2 . 2 8 . 8 . 8 . 8 G-094-213-5062-1	•
Use NATing fir Firewall extern IP Status Ingate Startup Tr VPN QoS Enhanced Securit S0 (+55 unutilize Unlimited SIP Use S0 (-55 unutilize)	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to ity ed) SIP Traversal Licenses er Registration Licenses	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, IG	4 . 2 . 2 . 2 8 . 8 . 8 . 8 G-094-213-5062-1	•
Use NATing fir Firewall extern IP Status Ingate Startup To VPN QoS Enhanced Securi 50 (+55 unutilize Unlimited SIP Us Software Versior Your unit's softw	ewall Gef . 162 . 145 . 11 ool TG Version 1.0.7, connected to ity ed) SIP Traversal Licenses er Registration Licenses n: 5.0.1 are is newer than the Startup Tool	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, Id	4 . 2 . 2 8 . 8 . 8 G-094-213-5062-1	4 III
Use NATing fir Firewall extern IP Status Ingate Startup To VPN QoS Enhanced Securi 50 (+55 unutilize Unlimited SIP Us Software Versior Your unit's softw	ewall Geb . 162 . 145 . 11 Geb . 162 . 145 . 11 Geb . 162 . 145 . 11 Geb . 10.7, connected to ity ed) SIP Traversal Licenses er Registration Licenses h: 5.0.1 ware is newer than the Startup Tool	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, Id	4 . 2 . 2 8 . 8 . 8 G-094-213-5062-1	• III •
Use NATing fir Firewall extern IP Status Ingate Startup Tr VPN QoS Enhanced Securi 50 (+55 unutilize Unlimited SIP Usi Software Versior Your unit's softw	ewall 66 . 162 . 145 . 11 ool TG Version 1.0.7, connected to ity ed) SIP Traversal Licenses er Registration Licenses n: 5.0.1 vare is newer than the Startup Tool	DNS server Primary: Secondary: (Optional) : Ingate Firewall 1210, Id	4 . 2 . 2 8 . 8 . 8 G-094-213-5062-1 . . .	• III •

Configuration Steps:

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



Product Type:	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.

Inside (Interface E	h0)	
IP address:	10 . 40 . 12	. 2
Netmask:	255 . 255 . 255	. 0

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

Gateway:	10		40		251		11	
----------	----	--	----	--	-----	--	----	--

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.

1	Use	NATing	firewall	
---	-----	--------	----------	--

Firewall extern IP:	66		162		145		11
---------------------	----	--	-----	--	-----	--	----

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

DNS server							
Primary:	4	•	2	•	2	•	2
Secondary: (Optional)	8	•	8	•	8	•	8

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.

G Ingate Startup Tool TG
Network Topology IP-PBX ITSP Upload Configuration
IP-PBX (should be located on the LAN) Type: ShoreTel ShoreGear IP Address: 10 40 12 31 ID Use domain name SIP Domain: SIP Domain: SIP Domain:
Ingate Startup Tool TG Version 1.0.7, connected to: Ingate Firewall 1210, IG-094-213-5062-1 QoS Enhanced Security 50 (+fst.unutilized) SIP Traversal Licenses Unlimited SIP User Registration Licenses
Software Version: 5.0.1 Your unit's software is newer than the Startup Tool, consider using a newer version. Warning: Normally when using a private IP address on the external interface the "Use NATing firewall" should be en:
Нер

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.

IP-PBX (should be located on the LAN)					
Type:	ShoreTel ShoreGear	•			

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.

IP Address:	10	40	12	31	



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.

Names	DID (start of same)
Name: Generic (no register)	(user name):
	DID range size:
	PBX local numbers (start of range):
Provider address	(same as DID if empty)
IP Address: 64 . 86 . 96 . 135	Account authentication
	Authentication
Use domain name	(same as DID if empty)
	Increment authentication name for ranges
< Advanced	Password:
Prefix to match and remove from incoming calls	
Prefix:	
Prefix to add to outgoing calls	
Prefix:	
Status	
	-

Configuration Steps:

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



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.

Provider address		
IP Address:	64 . 86 . 96 . 135	
🔲 Use domain nan	ne	

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.



Ingate Startup Tool TG	
twork Topology IP-PBX ITSP_1 Upload Configuration	
Disclaimer Please note that this tool generates basic settings for the Ingate product. Further configuration of the Ingate product and the PBX may be required in order to ensure interoperability and security in a specific installation. For technical assistance reparding end-to-end	Verbose Logging (SIP debug)
interoperability issues, please contact support@ingate.com.	Final step Logon to web GUI and apply settings Apply settings directly using serial interface Backup the configuration
Status Ingate Startup Tool TG Version 1.0.7, connected to: Ingate	Upload
QoS Enhanced Security 50 (+55 unutilized) SIP Traversal Licenses Unlimited SIP User Registration Licenses	
Your unit's software is newer than the Startup Tool, consid	der using a newer version.
	Help

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.

in©ate Firewall	Config	ured by	' Inga	te SUT TG		Log Out
Administration Basic Configuration Network	Rules and SIP Relays Servi	SIP ces Traffic	SIP Trunks	Failover Virtual Pr Networ	ivate Quality of rks Service	Logging and Tools About
Changes have been made to the p	reliminary conf	iguration, b	ut have r	not been applied.		
Save/Load Show User Configuration Configuration Administration	on Upgrade Loc	ole Date and ok Time	Restart	Change Language		
Test Run and Apply Conf	(Help) S	Show Mes	sage A	bout Unappli	ed Changes	
Duration of limited test mode:	0	On every	page			
30 seconds Apply configuration	C	On the Sa Never	we/Load	1 Configuration pa	ıge	
Backup (Help)						
The permanent configuration is not a	fected.					
Save to local file Load from loo	al file Local f	file: Brows	e_ No	file selected.		
Save/Load CLI Command	File (Help)					
The permanent configuration might b	e affected by lo	ading a CL	I file.			
Save config to CLI file Load CL	I file Local file	e: Browse.	. No fi	le selected.		
Abort All Edits (Help)	F	Reload Fa	ctory	Configuration	(<u>Help)</u>	
The permanent configuration is not a	fected. Th	e permanen	t configu	tration is not affect	ted.	
Abort all edits	L	oad factory	configu	ration		
incoate Page genera	ted for 'admin' 20 wall 5.0.1-rc1.	13-07-08 10:52 Copyright	2:54 -0400 © 2013). Ingate Systems A	B.	

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





Configured by Ingate SUT TG



1 other administrator(s) currently logged in.



You are currently testing the preliminary configuration. You must press either the **Save configuration** or the **Continue testing** button within 30 seconds, or the firewall will revert to the normal permanent configuration.

Save configuration Continue testing Revert

ingate Firewall 5.0.2. Copyright © 2013 Ingate Systems AB.

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".

in©ate Firewall	Broadvox 5.0.2	Log Out
Administration Basic Network Rules and SIA Configuration Network Relays Servi	P SIP SIP Failover Virtual Private ices Traffic Trunks Failover Networks	e Quality of Logging Service and Tools About
SIP Trunks		
View trunk: SIP Trunk 2: Broadvox;ShoreTel 💌	Goto SIP Trunk page	
Save Undo		

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:



in©ate Firewall	Broadvox 5.0.2	Log Out
Administration Basic Configuration Network Rules and SI Relays Serv	P SIP SIP ices Traffic Trunks Failover Virtual Prive Networks	nte Quality of Logging Service and Tools About
View trunk: SIP Trunk 2: Broadvox, Shore Tel 💌	Goto SIP Trunk page	
SIP Trunk 2 (Help)		
Inable SIP Trunk		
Disable SIP Trunk		
SIP Trunking Service (Help)		
O Use parameters from other SIP trunk		
Define SIP trunk parameters		
Service name:	Broadvox	(Descriptive name)
Service Provider Domain:	dl01-03.fs.broadvox.net	(FQDN or IP address)
Restrict to calls from:	Broadvox -	('-' = No restriction)

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.

Name	Use This					Or This	Dalata Dam
Ivame	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Kow
Emergency		911	nothing -		192.168.1.1		
OPTIONS-Ping			nothing -		192.168.1.1		
Operator		0	nothing -		192.168.1.1		
Outbound	1		any character 🔻		192.168.1.1		

Matching Request-URI (Help)

Add new rows 1 rows.

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



Forward To (H	elp)							
Namo	Subno	Use This	Or	This		Or This	Or This	Delete Rem
Таше	Subio.	Account	Replacement Domain	Port	Transport	Reg Expr	Trunk	Delete Kow
+ Broadvox	1						SIP Trunk 2: Broadvox;ShoreTel 🔻	
+ Broadvox OPTI	1		dl01-03.fs.broad	5060	UDP 👻		- •	
· · · · · · · · · · · · · · · · · · ·								

Add new rows 1 groups with 1 rows per group.

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.

Dial Plan	(<u>Help)</u>									
N	From	Desmark UDI	A	E-mail T-	Add I	Prefix	ENUM D	Time	C	Delete
140.	Header	Kequest-UKI	Action	Forward 10	Forward	ENUM	ENUM ROOI	Class	Comment	Row
1	ShoreTel -	Outbound -	Forward -	Broadvox -			- •	- •		
2	ShoreTel -	Emergency -	Forward -	Broadvox -			- •	- •		
3	ShoreTel -	Operator -	Forward -	Broadvox -			- •	- •		
4	ShoreTel 🔻	OPTIONS-Ping -	Forward 👻	Broadvox OPTIONS 🔻			- •	- •		
5	WAN 👻	-	Reject 🗸	- •			- •	- •		
Add new ro	ws 1 ro	ows.								

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,



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHDRE Fax +1.408.331.3333 www.ShoreTel.com

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.

Ingate Startup Tool TG Version 1.0.7 Startup tool version available on the Ingate web: 1.0.7 You are running the latest version of the Startup tool. More information is available here: http://www.ingate.com/startuptool.php	*
	Ŧ

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	It is possible that an IP Address or Password have
been assigned to the Ingate Unit	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.



Ingate Startup Tool Version 2.4.0 Startup tool version available on the Ingate web: 2.4.0 You are running the latest version of the Startup tool. More information is available here: http://www.ingate.com/startuptool.php Failed to contact the unit, check settings and cabling	3

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	 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. If the Browser also does not have access it 						
	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.

Status	
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-	D
Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses	<u>~</u>
Software Version: 4.6.2 Error: Primary DNS not setup. Error: Default gateway is not reachable. Error: Settings for eth1 is not correct.	
	~

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.



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHDRE Fax +1.408.331.3333 www.ShoreTel.com

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.

AN.
LAN.
AN.

Possible Problems & Resolutions

Possible Problems	Possible Resolution					
Error: The IP PBX IP does not seem to be on	The IP Address of the IP-PBX must be on the same					
the LAN.	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 Domain or IP Address used for Remote SIP					
enter a SIP domain. Alternatively you may	Connectivity. Note: must be a Domain when used					
configure a static IP address on eth1 under	with SIP Trunking module.					
Network Topology						

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	Verify the IP address of the PC with the Startup
from the IP address of the PC.	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.

in © at	e Fire	wall					Br	oad	lvox 5	.0.2			L	og Out	
Administration	Basic Configura	tion Netw	ork	Rules a Relay	nd s	SIP Service	S S Tra	IP iffic 1	SIP Trunks Fai	ilover	Virtual Priva Networks	ite Quality of Service	Logging and Tools	About	
Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	EthO	Eth 1	Eth2	Eth3	Interface Status	PPPoE	Topology				
Networks and Computers															
						Low	er Li	mit			Up _] (for	per Limit IP ranges)			

Name Subgrou		Subarrown	Lower	Limit	(for IP 1	ranges)	Interface (VI AN	Dele		
	me	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAN	Roy		
+ Broad	vox	- •	208.93.224.224	208.93.224.224	208.93.224.239	208.93.224.239		-		
	[- •	208.93.226.208	208.93.226.208	208.93.226.223	208.93.226.223	- ,	•		
		- •	208.93.227.208	208.93.227.208	208.93.227.223	208.93.227.223	-	•		
+ LAN		- 🔻	192.168.1.0	192.168.1.0	192.168.1.255	192.168.1.255	inside (eth0 untagged)	•		
+ Shore	Tel	- •	192.168.1.40	192.168.1.40			-	•		
+ WAN		- 🔻	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	•		
Add new rows 1 groups with 1 rows per group.										
Save	Jndo L	ook up all IP a	ddresses again							



Inget Firewall 5.0.2. Copyright © 2013 Ingate Systems AB.

BASIC CONFIGURATION - SIPARATOR TYPE

Use the appropriate SIParator configuration for your deployment.



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

in©ate Firewal	I	Broa	dvox	5.0.2			Log Out
Administration Basic Configuration	Network Rules and Si Relays Serv	IP SIP vices Traffic	SIP Trunks	Failover Virt	tual Private Networks	Quality of Service	Logging and Tools About
Signaling Media Basic Encryption Encryption	Interoperability Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Surviva Status			
SIP Module (Help) © Enable SIP module © Disable SIP module	>						
SIP Signaling Acc	ess Control (Help)		SIP	Logging	(Help)		
Specify the networks an firewall accepts SIP Sig	d computers from which naling.	the	Log cl signalir	ass for SIP 1g:	Lo pa	g class for S ckets:	IP
- •			Loca		L	ocal	•
Additional SIP Si	gnaling Ports (Help)	Log cl license	ass for SIP messages:	Lo err	g class for S ors:	IP
Port Transport Com	ment Delete Row		Loca	- -	L	ocal	•
Add new rows 1	rows.	Log cl messa	ass for SIP r ges:	g class for S bug message	IP es:		
SIP Media Port R	ange (Help)		Loca	· ▼	L	ocal	•
Ports: 58024 - 60	0999		SIP	Servers To	o Monito	or <u>(Help)</u>	
Public IP Address	for NATed firewall	(Help)	:	Server	Port	Transport	Delete Row
configuration.	ted for the Standalone		192.	168.1.40	5060	UDP 👻	
DNS Name or IP Address	Address		dl01 Add	-03.fs.broad	5060 1 row	UDP 🔻	
Save Undo Lool	k up all IP addresses agai	in					

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.

Gate Fir	ewall		Broadvox 5.	.0.2			Log C	Dut	
inistration Configu	ic ration Network	Rules and SIP Relays Services	SIP Traffic Trunks Fai	lover Virtu N	ual Private etworks S	ality of Log ervice and	ging Tools Al	pout	
IP Li hods Filtering Reg	ocal Authentico istrar and Accourt	tion SIP Dial nting Accounts Plan	Routing Status IDS/	IDS/IP IPS Status	S SIP SIF Test Test St	atus			
Use Dial Plan On Off Fallback	(<u>Help</u>)	Emergency Nur	nber <u>(Help)</u>						
Matching Fro	m Header	<u>Help)</u>]	
Name	Username	Domain	Or This Reg Expr	·	Transport	Netwo	ork	Delete Row	
ShoreTel	*	*		U	DP 👻	ShoreTel	•		
	*	*		Ar	ıy 👻	WAN	•		
WAN	I								
WAN Add new rows Matching Rec	1 rows. quest-URI (<u>Help)</u>	Use This				(Or This	D.L.C. D
WAN Add new rows Matching Red Name	1 rows. quest-URI (Prefix	Help) Head	Use This Tail	Min. T	ail Do	main	(Re	Or This g Expr	Delete Ro
WAN Add new rows Matching Rec Name Emergency	1 rows.	Help) Head 911	Use This Tail nothing	Min. T	'ail Do	main 3.1.1	(Re	Or This og Expr	Delete R
WAN Add new rows Matching Red Name Emergency OPTIONS-Ping	1 rows. quest-URI (Prefix	Help) Head 911	Use This Tail nothing • nothing •	Min. T	ail D a 192.16	main 3.1.1	(Re	Dr This 9g Expr	Delete Ro
WAN Add new rows Matching Red Name Emergency OPTIONS-Ping Operator	1 rows. puest-URI (Prefix	Help) Head 911 0	Use This Tail nothing • nothing •	Min. T	ail Do 192.16 192.16 192.16	main 3.1.1 3.1.1 3.1.1 5	(Re	Or This •g Expr	Delete R



Forward To (Help)

Namo	Subno	Use This	Or This			Or This	Or This	Delete Per
Ivame	Subno.	Account	Replacement Domain	Port	Transport	Reg Expr	Trunk	Delete Kow
+ Broadvox	1						SIP Trunk 2: Broadvox;ShoreTel 🔻	
+ Broadvox OPTI	1		dl01-03.fs.broad	5060	UDP 👻		- •	

Add new rows 1 groups with 1 rows per group.

Dial Plan (Help)

N	From	Barnart UDI	A	E-marked T-	Add l	Prefix	ENUM De et	Time	C	Delete
110.	Header	Kequest-UKI	Action	Forward 10	Forward	ENUM	ENUM KOOL	Class	Comment	Row
1	ShoreTel -	Outbound -	Forward -	Broadvox -			- •	- •		
2	ShoreTel -	Emergency -	Forward -	Broadvox -			- •	- •		
3	ShoreTel -	Operator -	Forward -	Broadvox -			- •	- •		
4	ShoreTel -	OPTIONS-Ping -	Forward -	Broadvox OPTIONS -			- •	- •		
5	WAN -	- •	Reject -	- •			· •	- •		

Add new rows 1 rows.

SIP TRAFFIC - SIP TRUNK

Configure the Dial Plan according to the picture below.





lain Trunk Line (H	<u>elp)</u>								
No. Dec		Outgoin	g Calls		Authe	ntication	Incomin	g Calls	
No. Keg		Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to	
No 🔻			4084703067		4084703067	Change Password	(*)	\$1	
BX Lines (Help)									
Ja Bag		Outgoi	ng Calls		Aut	hentication	Inco	oming Calls	Del
From PB2	K Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Mat	ch Forward to PBX Account	at
No - anonymou	IS		anonymous@anonym			Change Password	1		
No 🔻 (.*)			4084703067		4084703067	Change Password	1 (408470306[7-8]{1})	\$1	
dd new rows 1 row	vs.								
	Outgoin	or Calls	Authentic	ation	Incoming Cal	ls]		
o. Reg From SIP Num	ber/User Displa	ay Name User Nan	ne Identity User ID Pa	ssword Incoming Tru	ink Match Forwa	ard to SIP Account	Delete Row		
 Define PBX settir PBX Name: Use alias IP address 	gs ShoreTel	(Desci	riptive name) es this source address fr	om our side)					
		Authe	entication	PBX IP A	Address				
PBX Registration	SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain N	Name -		
			Change Password	192.168.1.40	192.168.1.40				
(At least one of PBX I	Registration, IP	address or Domain	Name is required to loc	ate the PBX)					
PBX Network:		ShoreTel	-						
Signaling transport:		- 🔻		('-' = Automa	atic)				
Port number:									
Match From Numbe	r/User in field:	From URI	•						
To header field:		 Same Copy Initial as enter 	as Request-URI from Trunk Request-URI ered:						
Remote Trunk Group	Parameters u	sage: -		✓ ('-' = Don't u	ise TGP)				
Level Treels Correct)			- (1 - Doutt)	TCD)				

Ingate Basic Call Troubleshooting

TROUBLESHOOTING OUTBOUND CALLS

Save Undo Look up all IP addresses again

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.



Packet Display Logging Log Capture Load Configuration Classes Sending			
acket selection: only those packets that meet the search criteria in the three c_{1}	Show newest at top		
ickets as selected choice.	Time Limits		
Protect Type Colection	Show log from: (clear)		
all active type belection	date (YYYY- time		
Ан раскета	MINI-DD) (HH:MINI:55)		
IP Address Selection (Help)	Show log until: (clear)		
inot this address	date (YYYY- time		
not this address	MM-DD) (HH:MM:SS)		
$A \operatorname{src} \cap A \operatorname{dst} \circ A \operatorname{anv}$			
A to B \bigcirc B to A \bigcirc Between A&B \square not this combination	Show This		
Protocol/Port Selection	□ IP packets as selected		
	Configuration server logins		
All IF protocols	Administration and configuration		
○ TCP ○ All ports	Manual reconfigurations and		
○ UDP	reboots		
A: not this port	Time changes		
B: not this port	DHCP/PPPoE client		
○ A src ○ A dst ⊙ A any	RADIUS errors		
○ A to B ○ B to A ○ Between A&B	SNMP problems		
○ICMP Select type/code: (Help)	Hardware errors		
Type: 🗌 not	Mail errors		
Code: not	🔲 Negotiated IPsec tunnels		
,	🔲 IPsec key negotiations		
○ ESP	🔲 IPsec user authentication		
OProtocol number: (Help)	PPTP negotiations		
	SIP errors		
	SIP signaling		
SIP Packet Selection (Help)	SIP packets		
all-ID: 🗌 Show internal SIP signaling	SIP license messages		

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.



play Packet Display Logging Log Log og Capture Load Configuration Classes Sending			
Packet selection: only those packets that meet the search criteria in the three sections below will be selected. This selection will only have effect on the ${f IP}$	Show newest at top		
packets as selected choice.	Time Limits		
Packet Type Selection	Show log from: (<u>clear</u>) date (YYYY- time MM-DD) (HH:MM:SS)		
IP Address Selection (Help)	Show log until: (clear)		
A: not this address B: not this address O A src O A dst O A any not this combination	date (YYYY- time MM-DD) (HH:MM:SS)		
○ A to B ○ B to A ○ Between A&B □ not this combination	Show This		
All IP protocols	Configuration server logins		
 TCP ○ All ports UDP ③ Selected ports: (Help) A: □ not this port B: □ not this port ○ A src ○ A dst ○ A any ○ A to B ○ B to A ○ Between A&B □ not this combination 	 Administration and computation Manual reconfigurations and reboots Time changes DHCP/PPPoE client RADIUS errors SIMMP problems 		
○ ICMP Select type/code: (Help) Type: □ not Code: □ not	 Hardware errors Mail errors Negotiated Psec tunnels Psec key negotiations 		
○ ESP	IPsec user authentication		
O Protocol number: (Help)	 PPTP negotiations SP errors 		
SIP Packet Selection (Help)	■ IP signaling IP packets		
Call-ID: Spow internal SIP signaling	SIP license messages		

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:



960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

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

Copyright © 2013 by ShoreTel, Inc., Sunnyvale, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of ShoreTel Communications, Inc. ShoreTel, Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to typographical, arithmetic or listing errors.

Trademarks

The ShoreTel logo, ShoreTel, ShoreCare, ShoreGear, ShoreWare and ControlPoint are registered trademarks of ShoreTel, Inc. in the United States and/or other countries. ShorePhone are trademarks of ShoreTel, Inc. in the United States and/or other coupyrights and trademarks herein are the property of their respective owners.

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

