

# **Application Note**

# **Microsoft OCS 2007 Configuration Guide**

15 October 2009

Microsoft OCS 2007 Configuration Guide

# Table of Contents

1	MICROSOFT OCS 2007 AND INGATE	1
	1.1 SIP TRUNKING SUPPORT	2
2	INGATE STARTUP TOOL	3
3	USING THE STARTUP TOOL	4
	3.1 CONNECTING THE INGATE FIREWALL/SIPARATOR	4
	3.2 CONFIGURE THE UNIT FOR THE FIRST TIME	
	3.3 CHANGE OR UPDATE CONFIGURATION	
	3.4 NETWORK TOPOLOGY	
	3.4.1 Product Type: Firewall	13
	3.4.2 Product Type: Standalone	15
	3.4.3 Product Type: DMZ SIParator	
	3.4.4 Product Type: DMZ-LAN SIParator	
	3.4.5 Product Type: LAN SIParator	
	3.5 IP-PBX	
	3.6 ITSP	
	3.7 UPLOAD CONFIGURATION	
4	MICROSOFT OCS 2007 CONFIGURATION	29
	4.1 CONFIGURATION OF STD ED OR ENT ED FRONT END SERVER	
	4.1.1 Global Properties	
	4.1.2 Voice Properties	
	4.2 STANDARD EDITION SERVERS – FRONT END PROPERTIES	
	4.3 CONFIGURATION OF MEDIATION SERVER	
5	TROUBLESHOOTING	44
	5.1 CALL FLOW EXAMPLES	44
	5.1.1 Incoming Call	
	5.1.2 Outgoing Call	
	5.2 Startup Tool	
	5.2.1 Status Bar	
	5.2.2 Configure Unit for the First Time	
	5.2.3 Change or Update Configuration	
	5.2.4 Network Topology	
	5.2.5 IP-PBX	
	5.2.6 ITSP	
	5.2.7 Apply Configuration	
	5.3 INGATE EXAMPLE CONFIGURATION 5.3.1 Network and Computers	
	5.3.1 Network and Computers 5.3.2 Interoperability	
	5.3.3 Dial Plan	
	5.4 INGATE TROUBLESHOOTING TOOLS	
	5.4.1 Display Logs	
	5.4.2 Packet Capture	
	5.4.3 Check Network	

# Tested versions:Ingate Firewall and SIParator version 4.7.1Startup Tool version 2.6.1Office Communications Server 2007 (3.0.6362.0)

#### Revision History:

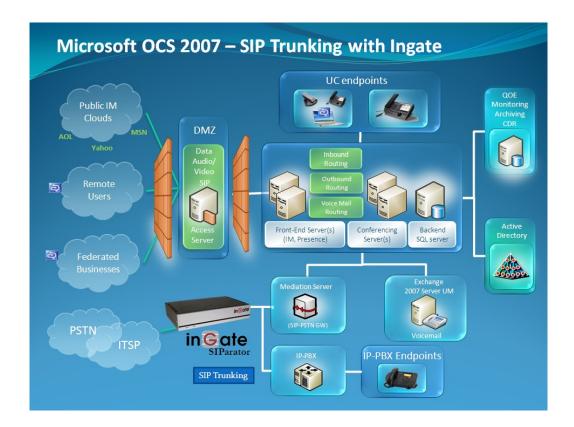
Revision	Date	Author	Comments
	2009-10-15	Scott Beer	First Draft

# 1 Microsoft OCS 2007 and Ingate

Microsoft Office Communications Server 2007, OCS 2007, is an enterprise real-time communications server, providing the infrastructure for enterprise instant messaging, presence, file transfer, Peer to peer and multiparty Voice and Video calling, ad hoc and structured conferences (audio, video and web) and PSTN connectivity. These features are available within an organization, between organizations, and with external users on the public internet, or standard phones, on the PSTN as well as SIP Trunking.

Office Communications Server 2007 R2 allows an enterprise to connect its softwarepowered VoIP network directly to IP service providers that offer PSTN origination and termination. This capability allows VoIP calls to be transmitted to the PSTN in packet format without requiring conversion to a traditional circuit format using an IP PSTN gateway. The Office Communications Server 2007 R2 SIP Trunking capability allows enterprise voice users to make local and long-distance calls to E.164 compliant numbers terminated on the PSTN as a service of the corresponding service provider, and to contact an enterprise user inside or outside the corporate firewall by dialing a Direct Inward Dialing (DID) number associated with that user.

Ingate offers SIParators and Firewalls, an Enterprise level SIP Session Border Controller (E-SBC) and SIP Security device. A powerful tool that offers enterprises a controlled and secured migration to VoIP (Voice over IP) and other live communications, based on Session Initiation Protocol (SIP). With the SIParator and Firewall, even the largest of businesses, with branch offices around the world and remote workers, can easily harness the productivity and cost-saving benefits of VoIP and other IP-based communications while maintaining current investments in security technology.



# 1.1 SIP Trunking Support

In this application, the Office Communications Server 2007 solution is an enterprise realtime communications server, providing the infrastructure for enterprise Peer to peer and multiparty Voice and Video calling, like an IP-PBX. The OCS Mediation Server is the conversion point between SIP Trunking and the call control server processing the phone features and IP-PBX functionality of the OCS 2007 Server required for an enterprise. It resides on the private LAN segment of enterprise, away from the Internet and protected by the Ingate from any attacks.

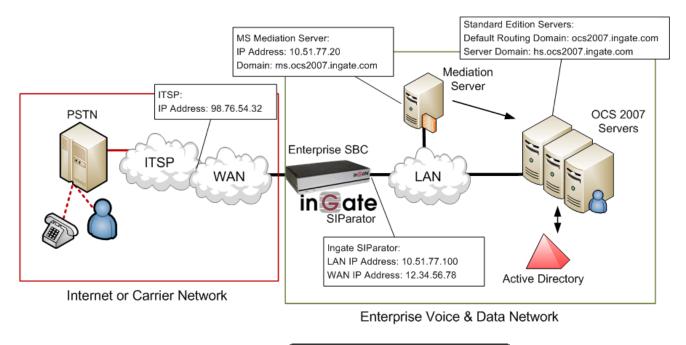
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

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

#### **Requirements:**

- 1) The Microsoft OCS 2007 solution must have a Mediation Server connected to the LAN and will direct calls to the OCS 2007 Server.
- The Ingate must have the SIP Trunking Module to provide Routing Rules, basic Security Policies, Client/Server Registrar, B2BUA capabilities, SIP Protocol 'Normalization' and more.

#### **Application Diagram**



Microsoft。 Office Communications Server

to focus your

attention to specific OCS setup instructions. These instructions are specific to the Ingate & OCS deployment with SIP Trunking.

Look for the Microsoft OCS Icon

# 2 Ingate Startup Tool

The Ingate Startup Tool is an installation tool for Ingate Firewall® and Ingate SIParator® products using the Ingate SIP Trunking module or the Remote SIP Connectivity module, which facilitates the setup of complete SIP Trunking solutions or remote user solutions.

The Startup Tool is designed to simplify the initial "out of the box" commissioning and programming of the Network Topology, SIP Trunk deployments and Remote User deployments. The tool will automatically configure a user's Ingate Firewall or SIParator to work with the IP-PBX, SIP Trunking service provider of their choice, and sets up all the routing needed to enable remote users to access and use the enterprise IP-PBX. Thanks to detailed interoperability testing, Ingate has been able to create this tool with pre-configured set ups for several of the leading IP-PBX vendors and ITSPs.

Download Free of Charge: The Startup Tool is free of charge for all Ingate Firewalls and SIParators. Get the latest version of the Startup Tool at http://www.ingate.com/Startup\_Tool.php

For more detailed programming instructions consult the Startup Tool – Getting Started Guide, available here: http://www.ingate.com/appnotes/Ingate Startup Tool Getting Started Guide.pdf

Make sure that you always have the latest version of the configuration tool as Ingate continuously adds new vendors once interoperability testing is complete. If you don't find your IP-PBX vendor or ITSP in the lists, please contact Ingate for further information.

The Startup Tool will install and run on any Windows 2000, Windows XP, Windows Vista, and Wine on Linux operating systems.

Keep in mind, this Ingate Startup Tool is a commissioning tool, not an alternate administration tool. This tool is meant to get an "out of the box" Ingate started with a pre-configured setup, enough to make your first call from IP-PBX to an ITSP. Additional programming and administration of this Ingate unit should be done through the Web Administration.

# **3 Using the Startup Tool**

There are three main reasons for using the Ingate Startup Tool. First, the "Out of the Box" configuring the Ingate Unit for the first time. Second, is to change or update an existing configuration. Third, is to register the unit, install a License Key, and upgrade the unit to the latest software.

# 3.1 Connecting the Ingate Firewall/SIParator

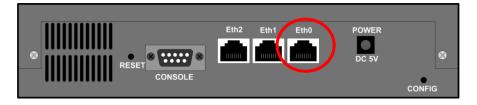
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

#### Ingate 1190 Firewall and SIParator 19 (Back)



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

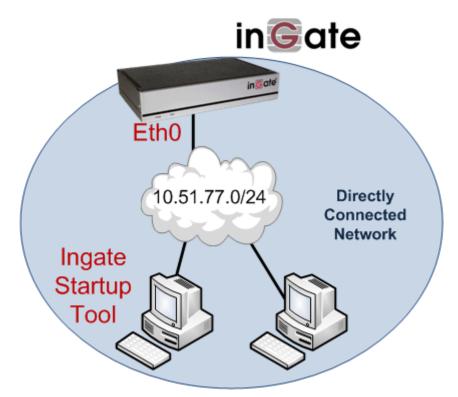


#### Ingate 2950 Firewall and SIParator 95



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 3.2: Using the Startup Tool for instructions on using the Startup Tool.

# 3.2 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 Address and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 3.2: "Change or Update Configuration".

#### **Configuration Steps:**

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

G Select Pr	oduct Type
Welcome to t	the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit
- Setup -	
	LAN
	Connect your computer to your Ingate unit like this.
Ingate	model - Please Select model
	Ingate Firewall/SIParator SIParator SBE

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

Ingate Startup Tool Version	Help
You are running the latest version of this tool.	Help
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	Assign IP address and password, establish contact Inside (Interface Eth0) IP Address: 10 , 51 , 77 , 100 MAC Address: 00-d0-c9-a2-44-55 Select a password Password: Confirm Password: ••••••
Status Ingate Startup Tool Version 2.4.0 Startup tool version available on the Ingate web: 2. You are running the latest version of the Startup to More information is available here: http://www.inga	pol.

4) Other Options in the "First select what you would like to do",

Microsoft。 Office Communications Server

- a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between the Microsoft OCS and an ITSP.
- b. For any other option please consult the Startup Tool Getting Started Guide

- 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:	10 . 51 . 77 . 100
MAC Address:	00-D0-C9-A2-44-55

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

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

7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool find the Ingate unit on the network, assign the IP Address and Password.

Inside (Interface Eth0 IP Address:	)
MAC Address:	00-D0-C9-A2-44-55
Select a password	
Password:	••••
Confirm Password:	•••••

8) Proceed to Section 3.4: Network Topology.

# 3.3 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 Address and Password assigned to it, proceed directly to Section 3.1: "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.

🕼 Select Product Type
Welcome to the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit
Setup
LAN EthO
Connect your computer to your Ingate unit like this.
Ingate model - Please Select model Ingate Firewall/SIParator Ingate Firewall/SIParator SIParator SBE Next

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

ngate Startup Tool Version	Help	
You are running the latest version of this tool.		Help
rst select what you would like to do:	Establish contact	
Configure the unit for the first time	-Inside (Interface Eth0)	
Change or update configuration of the unit     Check SIP configuration and logs	IP Address:	10 . 51 . 77 . 100
Register this unit with Ingate		
Upgrade this unit	Enter the password	
✓ Enable SIP module	Password:	•••••
Configure Remote SIP Connectivity		
Configure SIP trunking		
Backup the created configuration		
Create a config without connecting to a unit		
This tool remembers passwords		
		Contact
tatus		
Ingate Startup Tool Version 2.4.0		
Startup tool version available on the Ingate web: 2 You are running the latest version of the Startup to More information is available here: http://www.ing.	ool.	

4) Other Options in the "First select what you would like to do",

First select what you would like to do:
Configure the unit for the first time
<ul> <li>Change or update configuration of the unit</li> </ul>
$\bigcirc$ 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

Microsofta Office Communications Server

- a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
- b. For any other option please consult the Startup Tool Getting Started Guide

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

-Inside (Interface Eth0)-				
IP Address:	10	. 51	. 77	. 100

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

Enter the password		
Password:	••••	

 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:	10 .	51	. 77	. 100	]
Enter the password Password:	•••••				
			Conta	act	

8) Proceed to Section 3.4: Network Topology.

# 3.4 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.

es and Upgrades	Network Topology	IP-PBX ITSP	_1 Upload Configuration		
Product Type: Inside (Interface	Standalone SIPara	ator 🔽		$\sim$	
				Internet	
IP address:	10 . 51 . 7	77 . 100		T	
Netmask:	255 . 255 . 2	55 . 0			
Outside (Interfac	e Eth1)				Existing firewall
Use DHCP to a	obtain IP		Ingate SIPa		
IP Address:	172 . 51 . 1	77 . 100	LAN		
Netmask:	255 . 255 . 2	FF 0			
			1		
Allow https ac	cess to web interfac	e from Internet	IP-	PBX	
Gateway:	172 . 51 . 1	77 1			
	172 . 51				
			DNS server		
			DNS server Primary:	4 . 2 . 2 .	2
				4 . 2 . 2 . 0 . 0 .	
Status	Tool Version 2.4.0	connected to: I	Primary: Secondary: (Optional)	0.0.0.	
Ingate Startup	Tool Version 2.4.0,	connected to: Ir	Primary: Secondary:	0.0.0.	0
	Tool Version 2.4.0,	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	
Ingate Startup VoIP Survival VPN QoS		connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers	urity sal Licenses	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers	urity	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers	urity sal Licenses egistration Licenses	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re	urity sal Licenses egistration Licenses	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re	urity sal Licenses egistration Licenses	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0
Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re	urity sal Licenses egistration Licenses	connected to: Ir	Primary: Secondary: (Optional)	0.0.0.	0

#### **Configuration Steps:**

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

Hint: Match the picture to the network deployment.

2) When selecting the Product Type, the rest of the page will change based on the type selected. Go to the Sections below to configure the options based on your choice.

## 3.4.1 Product Type: Firewall

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

gate Startup Tool	
icenses and Upgrades Network Topology IP-PBX ITSP	Upload Configuration
Product Type: Firewall  Inside (Interface Etho) IP address: 10 . 51 . 77 . 1 Netmask: 255 . 255 . 0	Internet
Netmask:       255 , 255 , 255 , 0         Outside (Interface Eth1)         Use DHCP to obtain IP         IP Address:       12 , 23 , 34 , 45         Netmask:       255 , 255 , 0         Allow https access to web interface from Internet         Gateway:       12 , 23 , 34 , 1	LAN Igate Firewall
⊂ Status	ONS server           Primary:         4 . 2 . 2 . 1           Secondary:         4 . 2 . 2 . 2           (Optional)         4 . 2 . 2 . 2
Ingate Startup Tool Version 2.4.0, connected to: In Remote SIP Connectivity VPN QoS Enhanced Security 15 SIP Traversal Licenses 20 SIP User Registration Licenses Software Version: 4.6.2	ngate Firewall 1190, IG-092-719-5012-4
	Неір

#### **Configuration Steps:**

1) In Product Type, select "Firewall".

Product Type: 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 E	th0)
IP address:	10 . 51 . 77 . 1
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 ob	otain IP
IP Address:	12 . 23 . 34 . 45
Netmask:	255 . 255 . 255 . 248
Allow https acce	ess 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:	12	23	•	34	•	41	]

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

DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

### 3.4.2 Product Type: Standalone

When deploying an Ingate SIParator in a Standalone configuration, the SIParator resides on a LAN network and on the WAN/Internet network. The Default Gateway for SIParator resides on the WAN/Internet network. The existing Firewall is in parallel and independent of the SIParator. Firewall is the primary edge device for all data traffic out of the LAN to the Internet. The SIParator is the primary edge device for all voice traffic out of the LAN to the Internet.

Product Type: Standalone SIParator  Inside (Interface Etho) IP address: 10 . 51 . 77 . 100 Netmask: 255 . 255 . 0 Outside (Interface Eth1) Use DHCP to obtain IP IP Address: 12 . 23 . 34 . 45 Netmask: 255 . 255 . 255 . 248 Allow https access to web interface from Internet Gateway: 12 . 23 . 34 . 41 DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 Status Ingate SIParator 19, IG-092-702-2122-0 Nature SIParator 19, IG-092-702-2122-0 VoIP Survival VeN QooS Enhanced Security 10 3D Varses Software Version: 4.6.2	rk Topology IP-	PBX ITSP	Upload Configuration		
Inside (Interface Eth0)         IP address:       10 . 51 . 77 . 100         Netmask:       255 . 255 . 255 . 0         Outside (Interface Eth1)       Ise DHCP to obtain IP         IP Address:       12 . 23 . 34 . 45         Netmask:       255 . 255 . 255 . 248         Allow https access to web interface from Internet         Gateway:       12 . 23 . 34 . 41         DNS server         Primary:       4 . 2 . 2 . 1         Secondary:       (Optional)         Ingate Statup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VeN       VeN         VPS       Status         Ingate Statup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VeN       VeN         VeN       VeN         QoS       Enhanced Security         10 SIP Traversal Licenses         10 SIP User Registration Licenses	Product Type:	Standalone	SIParator 🗸	$\frown$	
IP address:       10 . 51 . 77 . 100         Netmask:       255 . 255 . 255 . 0         Outside (Interface Eth1)       Use DHCP to obtain IP         IP Address:       12 . 23 . 34 . 45         Allow https access to web interface from Internet       Imade SiParator         Gateway:       12 . 23 . 34 . 41         DNS server       Primary:         4 . 2 . 2 . 1         Secondary:       12 . 2 . 2 . 1         Secondary:       4 . 2 . 2 . 2         Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VPI Survival VPR       VPN VPN         QoS Enhanced Security 10 SIP Traversal Licenses         ID SIP User Registration Licenses	Inside (Interface			Internet	
Outside (Interface Eth1)         Use DHCP to obtain IP         IP Address:       12 . 23 . 34 . 45         Allow https access to web interface from Internet         Gateway:       12 . 23 . 34 . 41         DNS server         Primary:       4 . 2 . 2 . 1         Secondary:       (optional)         Ingate StParator       1         Status       Ingate StParator         Ingate Statup Tool Version 2.4.0, connected to: Ingate StParator 19, IG-092-702-2122-0         VPI Survival VPN QOS Enhanced Security 10 StP Traversal Licenses         ID StP User Registration Licenses	IP address:	10 . 51	l . 77 . 100	internet	
□ Use DHCP to obtain IP         IP Address:       12       23       34       45         Netmask:       255       255       255       248         Allow https access to web interface from Internet.       Impate SiParator       Impate SiParator         Gateway:       12       23       34       41         DNS server       Primary:       4       2       2         Primary:       4       2       2       2         Status       Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0       Impate Superson 19, IG-092-702-2122-0         Vol P Survival Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0       Impate SiParator 19, IG-092-702-2122-0	Netmask:	255 . 25	5.255.0		
IP Address:       I2 · 23 · 34 · 45         Netmask:       255 · 255 · 255 · 248         Allow https access to web interface from Internet         Gateway:       I2 · 23 · 34 · 41         DNS server         Primary:       4 · 2 · 2 · 1         Secondary:       (Optional)         (Optional)       4 · 2 · 2 · 2         Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VolP Survival VPN Qos Enhanced Security ID SIP User Registration Licenses	Outside (Interfa	ce Eth1)		Existing	firewall
Netmask:       255 · 255 · 255 · 248         Allow https access to web interface from Internet         Gateway:       12 · 23 · 34 · 41         DNS server         Primary:       4 · 2 · 2 · 1         Secondary:       (Optional)         (Optional)       4 · 2 · 2 · 2         Status         Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses         10 SIP User Registration Licenses	Use DHCP to	obtain IP		Ingate SIParator	
Allow https access to web interface from Internet Gateway: 12 . 23 . 34 . 41  DNS server Primary: 4 . 2 . 2 . 1 Secondary: (Optional)  Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0  VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses	IP Address:	12 . 23	3.34.45	LAN	
Gateway: 12 . 23 . 34 . 41 DNS server Primary: 4 . 2 . 2 . 1 Secondary: 4 . 2 . 2 . 2 Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0 VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses	Netmask:	255 . 25	5 . 255 . 248		
Gateway:       12 , 23 , 34 , 41         DNS server         Primary:       4 , 2 , 2 , 1         Secondary:       4 , 2 , 2 , 2         (Optional)       4 , 2 , 2 , 2         Status         Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0         VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses	Allow https a	ccess to web in	terface from Internet	IP-PBX	
DNS server       Primary:       4       Secondary:       (Optional)       4       VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses	Gateway:	10 00	2 24 41		
(Optional) Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0 VoIP Survival VPN Qo5 Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses					
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0 VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses				Primary: 4 . 2 . 2 . 1	
VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses				Primary:         4         2         2         1           Secondary:         4         2         2         2         2	
10 SIP User Registration Licenses	Ingate Startup		2.4.0, connected to: I	Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	
Software Version: 4.6.2	Ingate Startup VoIP Survival VPN QoS Enhanced Sec	urity	2.4.0, connected to: I	Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	
	Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver	urity sal Licenses		Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	
	Ingate Startup VoIP Survival VPN Qo5 Enhanced Sec 10 SIP Traver 10 SIP User R	curity sal Licenses egistration Lice		Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	
	Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R	curity sal Licenses egistration Lice		Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	
	Ingate Startup VoIP Survival VPN QoS Enhanced Sec 10 SIP Traver 10 SIP User R	curity sal Licenses egistration Lice		Primary:         4         .         2         .         1           Secondary: (Optional)         4         .         2         .         2	

#### **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 . 51 . 77 . 100
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	·	
IP Address:	12 . 23 . 34 . 45	
Netmask:	255 . 255 . 255 . 248	
Allow https acce	ess to web interface from Interne	t

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



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

### 3.4.3 Product Type: DMZ SIParator

When deploying an Ingate SIParator in a DMZ configuration, the Ingate resides on a DMZ network connected to an existing Firewall. The Ingate needs to know what the Public IP Address of the Firewall. This existing Firewall must be the Default Gateway for the DMZ network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN and DMZ to the Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, both from the Internet to the SIParator and from the DMZ to the LAN.

e Startup Tool			
nses and Upgrades	Network Topology	IP-PBX ITSP_1	Upload Configuration
Product Type:	DMZ SIParator	*	
IP address:	10 . 51 . 77	. 100	Internet
Netmask:	255 . 255 . 255	. 0	
-LAN IP address ra	ange		DMZ Existing firewall
Low IP:	192 . 168 . 1	. 1	Ingate SIParator
High IP:	192 . 168 . 1	. 255	
Gateway:	10 . 51 . 77	. 1	IP-PBX
Firewall extern IP	12 . 23 . 34	. 45	
			DNS server
			Primary: 4 . 2 . 2 . 2
			Secondary: 4 . 2 . 2 . 1 (Optional)
Status Ingate Startup	Tool Version 2.4.0, co	nnected to: Inga	ate SIParator 19, IG-092-702-2122-0
VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re			<u>~</u>
Software Versi	-		
			Hel

#### **Configuration Steps:**

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

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

-DMZ (Interface Eth	0)
IP address:	192 . 168 . 100 . 100
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 ran	ige						
Low IP:	10	•	10	•	10	•	1
High IP:	10		10		10		255

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:	192	. 186	. 100	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.

Firewall extern IP: 98 . 87 . 76 . 65	Firewall extern IP: 98 . 87 . 76 . 65							
		Firewall extern IP:	98	•	87	76	65	]

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

-DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

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

On the existing Firewall:

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

### 3.4.4 Product Type: DMZ-LAN SIParator

When deploying an Ingate SIParator in a DMZ-LAN configuration, the Ingate resides on a DMZ network connected to an existing Firewall and also on the LAN network. The Ingate needs to know what the Public IP Address of the Firewall. This existing Firewall must be the Default Gateway for the DMZ network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN and DMZ to the Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

Product Type:       DM2-LAN SIParator         Inside (Interface Ethi)       IP address:       10 . 51 . 77 . 100         Netmask:       255 . 255 . 255 . 0         DM2 (Interface Ethi)       IP address:       192 . 168 . 100 . 100         IP Address:       192 . 168 . 100 . 100       IP address:         IP Address:       192 . 168 . 100 . 100       IP address:         IP Address:       192 . 186 . 100 . 1       IP address:         IP Address:       192 . 186 . 100 . 1       IP address:         IP Address:       192 . 186 . 100 . 1       IP address:         IF rewall extern IP:       98 . 67 . 76 . 65       DNS server         Primary:       4 . 2 . 2 . 1       Secondary: (optional)         Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0       Vol         VPIP Survival VP Survival VPIP Survival ID SIP Traversal Licenses       ID SIP User Registration Licenses         10 SIP User Registration Licenses       Software Version: 4.6.2       V	e Startup Tool vork Topology IP-P	PBX ITSP Upload Configuration		
Status     DNS server       Primary:     4       Secondary:     4       4     2       Status       Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0       VoIP Survival       VPN       QoS       Enhanced Security       10 SIP Uraversal Licenses       10 SIP Uraversal Licenses       Software Version: 4.6.2	Inside (Interface IP address: Netmask: DM2 (Interface EI Use DHCP to o IP Address: Netmask: V Allow https ac Gateway:	10       51       77       100         255       255       255       0         h1)       bbain IP       192       168       100       100         255       255       255       0       cstate       cstate       cstate         192       168       100       100       cstate       cstat	Ingate SIParator	Existing firewall
Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0 VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses Software Version: 4.6.2	THOWAI EXCENTIF	98 . 87 . 76 . 65	Primary: Secondary:	
	Ingate Startup VoIP Survival VPN QoS Enhanced Sect 10 SIP Travers 10 SIP User Re	irity al Licenses gistration Licenses	gate SIParator 19, IG-092	

#### **Configuration Steps:**

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

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

-Inside (Interface El	:h0)	
IP address:	10 . 51 . 77 . 100	
Netmask:	255 . 255 . 255 . 0	

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

-DMZ (Interface Eth	1								
IP Address:	192 . 168 . 100 . 100								
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.

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



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

DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

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

On the existing Firewall:

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

### 3.4.5 Product Type: LAN SIParator

When deploying an Ingate SIParator in a LAN configuration, the Ingate resides on a LAN network with all of the other network devices. The existing Firewall must be the Default Gateway for the LAN network; the existing Firewall is the primary edge device for all data and voice traffic out of the LAN to the WAN/Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, from the Internet to the SIParator. The voice traffic from the LAN is directed to the SIParator then to the existing Firewall.

te Startup Tool		
work Topology IP-	-PBX ITSP Upload Configuration	
Product Type:	LAN SIParator	$\frown$
		Internet
IP address:	10 . 51 . 77 . 100	internet
Netmask:	255 . 255 . 255 . 0	
		Existing frewall
Gateway:	10 . 51 . 77 . 1	IP-PBX Ingate SIParator
Firewall extern I	P: 98 . 87 . 76 . 65	
		ONS server
		Primary: 4 . 2 . 2 . 1
		Secondary: 4 . 2 . 2 . 2 (Optional)
- Status		(optional)
Ingate Startu	o Tool Version 2.4.0, connected to: In	ngate SIParator 19, IG-092-702-2122-0
VoIP Survival VPN		
QoS Ephanced Sec	a with a	
Enhanced Sec 10 SIP Traver	sal Licenses	
Enhanced Sec 10 SIP Traver		
Enhanced Sec 10 SIP Traver	sal Licenses legistration Licenses	
Enhanced Sec 10 SIP Traver 10 SIP User R	sal Licenses legistration Licenses	
Enhanced Sec 10 SIP Traver 10 SIP User R	sal Licenses legistration Licenses	
Enhanced Sec 10 SIP Traver 10 SIP User R	sal Licenses legistration Licenses	M Help

#### **Configuration Steps:**

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

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

LAN (Interface Eth	0)
IP address:	10 . 51 . 77 . 100
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 . 51 . 77 . 1								_
	Gateway:	10	•	51	•	77	1	

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.

				 	 	_	
Firewall extern IP:	98	•	87	76	65		
						-	

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

-DNS server							
Primary:	4	•	2	•	2	•	1
Secondary: (Optional)	4	•	2	•	2	•	2

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

On the existing Firewall:

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

# 3.5 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 Microsoft OCS 2007 Mediation Server as to direct SIP traffic for the use with SIP Trunking. The IP Address of the Microsoft OCS Mediation Server must be on the same network subnet as the IP Address of the inside interface of the Ingate unit.



#### **Configuration Steps:**

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

~

2) Enter the IP Address of the Microsoft OCS Mediation Server. The IP Address should be on the same LAN subnet as the Ingate unit.

IP Address:	10	51	77	,	20	7	

# 3.6 ITSP

The ITSP section is where all of the attributes of the SIP Trunking Service Provider are programmed. Details like the IP Addresses or Domain, DIDs, Authentication Account information, Prefixes, and PBX local number. The configuration of the ITSP will allow for the Ingate unit to know the location of the ITSP as to direct SIP traffic for the use with SIP Trunking. Ingate has confirmed interoperability many of the leading ITSP vendors.

	Ingate Startup Tool
	Network Topology IP-PBX ITSP_1 Upload Configuration
	Name: Generic ITSP DID (start of range) (user name): DID range size: 1
25	Provider address       Account information:         IP Address:       0       0         Use domain name       Authentication name:         (same as DID if blank)       Increment authentication name for range
	Prefix to match and remove from inbound calls Domain: Prefix: Prefix: Password: Use user account on incoming call
	Prefix to add to outbound calls       PBX local numbers (advanced)         Prefix:       Local number(start of range, use same as DID if local numbers are not used):         Forward 3xx messages       PBX local numbers (advanced)         ✓ Enable       Password (only used if PBX registers at the Ingate):
	Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SIParator 19, IG-092-702-2122-0 VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses
Help	Software Version: 4.6.2
	VoIP Survival VPN QoS Enhanced Security 10 SIP Traversal Licenses 10 SIP User Registration Licenses

#### **Configuration Steps:**

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



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

- 2) Service Providers come in one of two flavors, either they have a trusted IP deployment or they require a Registration account.
  - a. In the case where the Service Provider uses a Trusted IP deployment, all that is required is to enter the IP Address or Domain of the Service Providers SIP Server or SBC. Enter the IP Address here, or select "Use domain name" and enter the FQDN of the Service Provider.

Provider address IP Address:		0	0	0	]
Provider address Domain: Vise domain nam	ie				]

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

Account information:	
🗹 Use account	
Authentication name:	
(same as DID if blank)	· · · · · · · · · · · · · · · · · · ·
Increment authenticati	on name for ranges
Domain:	
Password:	
🗹 Use user account o	n incoming call

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

DID (start of range) (user name): DID range size:	1

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

Account information:	
🔽 Use account	
Authentication name: (same as DID if blank)	
Increment authentica	tion name for ranges
	contraine for ranges
Domain:	
Password:	
Use user account	on incoming call

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

Prefix:	
-Prefix to add to	o outbound calls
Prefix:	
-Forward 3xx m	essages
🗹 Enable	

# 3.7 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.

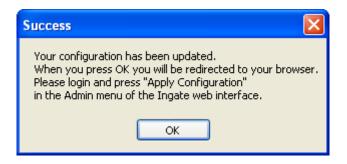
e Startup Tool	•
ork Topology IP-PBX ITSP_1 Upload Configuration	
Disclaimer and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical assistance regarding end-to-end interoperability issues, please contact support@inqate.com.	-Verbose Logging (SIP debug) I Enable
	Final step         • Logon to web GUI and apply settings         • Apply settings directly using serial interface         Backup the configuration
- Status Ingate Startup Tool Version 2.4.0, connected to: Ingate S 10 SIP Traversal Licenses 10 SIP User Registration Licenses Software Version: 4.6.2	Upload
Error: Please enter number, name and domain. Error: Please enter number, name and domain.	

#### **Configuration Steps:**

 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.

Administration	Basic Configuration	Network	Rules and Relays	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
Save/Load Configuration	Show Configuration	User Administratio	on Upgrade		Date and Time	Restart	Change Language			
Test Ru	n and App	ly Conf	(Help)	Sh	ow Mes	ssage A	About Unap	plied Ch	anges	
Duration of	limited test m	ode:		) ۞	On every	page				
30	seconds			00	On the Sa	ave/Load	d Configuration	page		
Apply o	onfiguration			01	Never					
Backup	(Help)									
The permar	ient configura	tion is not at	ffected.							
Save to	local file	Load fro	m local file	Lo	ocal file:			Browse		
Save/Lo	ad CLI Co	ommand	File (He	<u>lp)</u>						
The permar	ent configura	tion might b	e affected i	by load	ing a CL	I file.				
Save	config to CLI fil	e Lo	oad CLI file	Loc	al file:			Browse		
Abort A	ll Edits (	Help)		Re	load Fa	ictory	Configurati	on <u>(Help</u>	0	
The permar	ent configura	tion is not at	ffected.	The p	ermaner	nt configu	uration is not af	fected.		
Abort all	edits				Load fac	tory con	figuration			

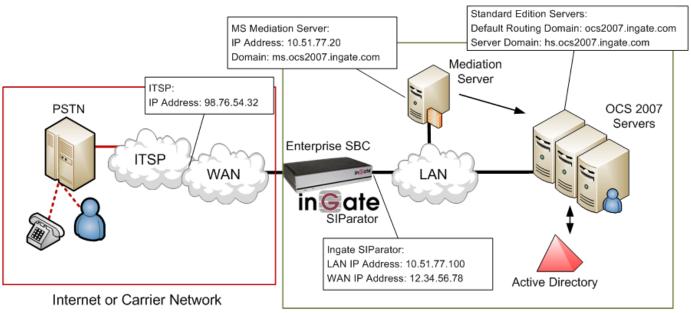
4) A new page will appear after the previous step requesting to save the configuration. Press "Save Configuration" to complete the saving process.



# 4 Microsoft OCS 2007 Configuration

#### Microsoft. Office Communications Server

The picture below describes the typical network configuration. The LAN networks will typically be NATed private networks. There are a variety of SIP Trunking Service Providers offering different connectivity to the PSTN, the Ingate unit must have a routable IP address on the WAN Network, the Ingate will perform NAT and none of the internal private IP addresses will be displayed outside the Ingate. Note that some Carriers extend their own private network to the Enterprise as well.



Enterprise Voice & Data Network

The Ingate can be a Firewall or a SIParator as described in previous sections, but the principal network setup looks the same. There cannot be a NATing device between the Ingate and the Internet or Carrier Network. If there is a firewall between Internet and the Ingate it must allow traffic to and from the Ingate on UDP port 5060 and configured media ports.

The OCS 2007 Mediation Server is the destination to send SIP Trunking. The internal edge of a Mediation Server should be configured to correspond to a unique static route that is described by an IP address and a port number. The default port is 5061.

The OCS Standard Edition or Enterprise Edition Front End Server is ultimately responsible for SIP communications between client and servers. Providing IM, presence, Peer-to-peer Voice, Conferencing but has No PSTN, No External Access, and is Not Highly Available.

# 4.1 Configuration of Std Ed or Ent Ed Front End Server

Please configure the Standard Edition Server or Enterprise Edition Front End Server according to Microsoft documentation.

The following is an example display of OCS 2007 settings and parameters.

### 4.1.1 Global Properties

Here is a display of the Forest Global properties.



Here is where the Default Routing SIP Domain and other SIP Domains are programmed.

Office Commu	nications Ser	ver Global Pi	roperties		x
Federatio General	on   Search	Archiving User	Call D Meetings	etail Records Edge Servers	
state of the second sec	Diffice Communications Server Global Settings				
	IP domains sup s the default ro		organization. Cl	neck one domain	
Domains	17.ingate.com				
000000	r.ingate.com				
			A <u>d</u> d	<u>R</u> emove	
	OK	Cancel	Apply	Help	

Here is the Forest - Status page showing the Default Routing Domain.

Microsoft Office Communications Serve	r 2007	- <b>D</b> ×
Eile <u>W</u> indow <u>H</u> elp		_ <b>B</b> ×
Office Communications Server 2007     Forest - ocs2007.ingate.com     Enterprise pools	Office Communications Server 2007	
Standard Edition Servers     📴 60 hs	Status Voice	Voice Task Flow Resources
Users 	🗉 General Settings	
Applications	Forest:	Information not available in this view
Archiving and CDR Servers	Schema version:	Information not available in this view
Unassigned users	Prep state:	Information not available in this view
Mediation Servers ms.ocs2007.ingate.com	∃ Supported <u>D</u> omains:	
Live Communications Server 2005	l	
	Default Routing Domain:	ocs2007.ingate.com
	<u>     M</u> eeting Settings	
	Eederation Settings	
	Archiving Settings	
	<u> </u>	
	•	

# 4.1.2 Voice Properties

Here is a display of the Forest Voice properties.

Microsoft Office Co	mmunications Server	2007	
📴 File <u>W</u> indow <u>H</u> ei	lp		
Forest - openanication			nications
Enter Pro	operties 🔸	<u>G</u> lobal Properties Voice Properties	
E Stand New	w <u>W</u> indow from Here	voice Properties	
	fresh		
	lp		
Archiving and	d CDR Servers		
🖳 🛄 Unassigned u	users		
📄 📄 Mediation Sei	rvers		
🔤 ms.ocs20	007.ingate.com		
Live Commun	nications Server 2005		

## **Location Profiles**

Here are the location profiles that define how number are to be translated when dialed from a defined location.

Office Communications S	ierver Voice Properties		
Location Profiles Phone L	Usages Policy Routes		
Location profiles define how numbers are to be translated when dialed from a defined location. Each profile has a set of normalization rules.			
Location Profiles:			
Name	Description		
Inbound	Test		
[	Add Edit <u>H</u> emove		
OK	Cancel <u>A</u> pply Help		

Within the Location Profile are a set of list of Normalization Rules.

Location Profile					
Name:	Inbo	ound			
Description:					
Test					A 7
Normalization Rules	are processed ir	n list order; p	lease use th	e buttons o	n the
	e order.				
Allt_till_test1	e order.			-	
	e order.				Цр
All <u>t</u> til_test1	e order.				<u>U</u> р D <u>o</u> wn
Allt_till_test1		<u>E</u> dit	<u>R</u> emove		

The Normalization Rules are defined within the Translations:

- Phone pattern regular expression: This consists of designators and variables that represent specific sets of numbers. For example, the phone pattern regular expression of ^9(\d{7})\$ describes phone numbers that consist of the number 9 followed by any seven digits.
- Translation pattern regular expression: This consists of the + symbol, numbers, and the \$ symbol. The \$ symbol captures the items of the phone pattern regular expression that are included inside the parenthesis. The number following the \$ symbol must be less than or equal to the total number of captures specified by the phone pattern regular expression.

For example, the translation pattern regular expression of +1425\$1 describes a translation that adds a prefix of +1425 to the captures (the phone pattern items in parenthesis). If the phone pattern regular express is

^9(\d{3})(\d{4})\$ (containing two captures), the number following the \$ sign can only be 1 or 2.

Office Communications Server Voice Properties
Edit Location Profile
Edit Phone Number Normalization Rule
Name: All_till_test1
Click to copy an existing rule.
Description:
×
Translation
Phone pattern regular expression:
sip:(.*)
Iranslation pattern regular expression:
7322162717
Valid translation characters are +, numbers, and \$. Example: +1425\$1.
Click Helper for assistance in creating common phone number Helper
Test translation
To test the translation, enter a sample dialed number. If it matches the phone pattern, the translation will be shown.
Sample dialed number:
T <u>r</u> anslated number:
OK Cancel Help

# Routes

A Route requires a target phone number regular expression, one or more gateways, and one or more phone usages. Here is where we add the route.

Dffice Communications Server Voice Properties					
Location Profiles Phone U	Usages Policy Routes				
Please use the buttons below to modify, add, view, or remove a route. To see the entire routing table, please see the Status Pane.					
Routes:					
Name	Description				
To_Ingate	Sends all calls to the Mediation server				
	Add Edit <u>R</u> emove				
ОК	Cancel <u>A</u> pply Help				

Here is where we define the Route:

- 1) Target Phone Numbers: The number pattern that will use this Route.
- 2) Gateways: The advanced media gateway or Mediation Server that calls matching this Route will be sent to.
- 3) Phone Usage: The list contains the phone usage records that are required to call a number using this route. For a user to be able to call numbers matching the target phone-number regular expression specified for this route, the caller's user policy must contain at least one usage record that matches a usage record for the route.

Office Communications	Server Voice	Properties		X
Location Profiles Phon	e Usages   Polic	<sub>cy</sub> Routes		
Edit Route			×	
Name:	To_Ingate			
Description:				
Sends all calls to the Me	ediation server		▲ ▼	
A route requires a target gateways, and one or mo	ore phone usage		i, one or more	
Target regular expressi				
× .				
,			<u>H</u> elper	
<u>G</u> ateways				
Address ms.ocs2007.ingate.c	E0C1			
nis.ocs2007.ingate.c	011.5061			
		<u>A</u> dd	<u>R</u> emove	H
Phone usages				
Default Usage				
			<u>C</u> onfigure	
	OK	Cancel	Help	

Here is the Forest - Voice page showing the voice settings.

🗖 Microsoft Office Communications Server 2007 📃 🖸 🛛						
📴 Eile <u>W</u> indow <u>H</u> elp				_ 8 ×		
Office Communications Server 2007     Forest - ocs2007.ingate.com     Enterprise pools	Office Comm Server 2007	unications				
E-E Standard Edition Servers	Status	Voice	Voice Task Flow	Resources		
Users	∃ Global Policy					
Applications	Policy name:		Default Policy			
Archiving and CDR Servers	Allow simultaneous	ringing of phones:	1			
Unassigned users	Phone Route Usages:		Default Usage			
ms.ocs2007.ingate.com						
Live Communications Server 2005	<u>N</u> ormalization Rules					
	Location Profiles					
	B Routes					
	🖃 To_Ingate		Sends all calls to the	Mediation server		
	Phone Number Pat	tern:				
	Phone Usage:					
	🗄 Default Usage					
	Gateways: ms.ocs2007.in/	nate.com:5061				
		gacorconnooor				
	•					

# 4.2 Standard Edition Servers – Front End Properties

🔯 Microsoft Office Communications Serve	r 2007
📴 File <u>W</u> indow <u>H</u> elp	
Forest - ocs2007.ingate.com	Office Communications Server 2007
Standard Edition Servers      Standard Edition Servers      Users	Front End Web Conferencing
hstocs2007.ii Validation	General Settings
Applicatic Valuation	service: Runn ncing service: Runn
Mediation Servers     Start     Stop     Live Communications	Conferencing service: Runn     settings
Properties	Eront End Properties ×pir
<u>V</u> iew New <u>W</u> indo	w from Here
Refresh	ess: Port:
Help	5061
	IN LIVE Conferencing IP address: Port:

Here is where the Front End Server handles inbound connections.

Here is where the Front End Server handles inbound connections.

Front End Server Properties	×
General IM Conferencing Telephony Conferencing Certificate	
Office Communications Server, Front End	
EQDN:	
hs.ocs2007.ingate.com	
Connections Specify how this server handles inbound connections:	
Address Port Transport	
All 5061 MTLS	
Add <u>E</u> dit <u>R</u> emove	
OK Cancel Apply Help	

Here is the Front End – Status page.

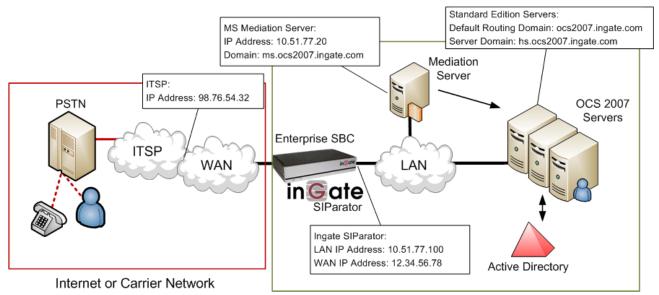
<u>File W</u> indow <u>H</u> elp					
Office Communications Server 2007 Forest - ocs2007.ingate.com Enterprise pools	Office Comr Server 2007	nunications			
Standard Edition Servers	Front End	Web Conferencing	A/V Conferencing	Web Components	Event Log
Users	🖃 General Settings				
Applications	Windows services	;			
Archiving and CDR Servers	Front End service	:	Running		
🛅 Unassigned users	IM Conferencing	service:	Running		
🖃 🧰 Mediation Servers	Telephony Confe	rencing service:	Running		
	🗐 🖸 Certificate setting	js			
	Name:		Expiration Date:		
	OCS-CA		2011-09-08		
	🗉 Eront End Server				
	SIP IP address:		Port: 1	Transport:	
	All		5061 M	4TLS	
	IM Conferencing	IP address:	Port:		
	All		5062		
	Telephony Confe	rencing IP address:	SIP Port:		
	All		5064		

# 4.3 Configuration of Mediation Server

The OCS 2007 Mediation Server is the destination to send SIP Trunking. The "internal" edge Mediation Server should be configured to correspond to a unique static route that is described by an IP address and a port number. The default port is 5061. The "external" edge Mediation Server can be configured to have the same IP address as the "Internal" edge but use port is 5060. In the deployment example the FQDN of the Mediation server is ms.ocs2007.ingate.com and the same IP address are used for both communication with the gateway and the OCS Front End.

When configuring Mediation Server, you are advised to accept the default media port gateway range of 60,000 to 64,000. The default range media port range enables the server to handle up to 1,000 simultaneous voice calls. Reducing the port range greatly reduces server capacity and should be undertaken only for specific reasons by an administrator who is knowledgeable about media port requirements and scenarios. For this reasons, altering the default port range is not recommended.

Ingate recommends a setup where the Mediation Server only requires One IP Address, rather than the two Interface setup typically seen with the Mediation Server, with its "Internal" and "External" setup.



Enterprise Voice & Data Network

#### **Configuration Steps:**

1) Go to the Mediation Server Properties.



2) The same IP Address can be used for the Communication Server Listening ("Internal") as the Gateway Listening ("External"). Ingate recommends a setup where the Mediation Server only requires One IP Address, rather than the two Interface setup.

ms.ocs2007.ingate.com Properties
General Next Hop Connections Certificate
Mediation Server
EQDN: ms.ocs2007.ingate.com
Communications Server listening IP address:
10.100.0.151
Gateway listening IP address:
10.100.0.151
A/V Edge Server:
(None)
Default location profile:
Inbound View
Media port range: 60000 to 64000
OK Cancel Apply Help

a) Under "Next Hop Connections", enter the IP Address and port 5060 of the Ingate SIParator in the "PSTN Gateway next hop" IP address.b) Under "Next Hop Connections", select the SIP Domain of the Front End Server and port 5061.

ms.ocs2007.ingate.com Properties
General Next Hop Connections Certificate
Office Communications Server next hop
Specify the Office Communications Server used for routing inbound PSTN calls.
EQDN:
hs.ocs2007.ingate.com
Port: 5061
PSTN Gateway next hop
Specify the PSTN gateway connected to this server.
IP address: 10 . 51 . 77 . 100
Port: 5060
OK Cancel Apply Help

- 4) Start Mediation service, first on the FE-server and verify that the service is running on the Mediation server.
- 5) Configure Phone usage under Forrest Properties Voice Properties.



6) Phone usage records are identified as 'classes of calls' (for example, local, longdistance, or international). Phone usage records are assigned to both routes and users for the purposes of specifying call authorization. Policies are named sets of phone usage records. Policies are used to assign call privileges to users.

Office Communications S	erver Voice Properties 🗙
Location Profiles Phone I	Usages Policy Routes
Use the Add, Edit, and R records.	emove buttons to manage the phone usage
Phone usage records:	
Name	Description
Default Usage Test 0523	Sample phone usage Jannes test
168(_0020	Janines (est
	Add Edit <u>R</u> emove
	Cancel Apply Help
	Cancel <u>Apply</u> Help

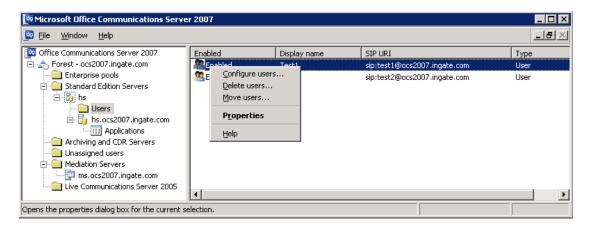
7) Add a Route that sends outbound calls to the Mediation Server. A Route requires a target phone number regular expression, one or more gateways, and one or more phone usages. Here is where we add the route.

Office Communications S	erver Voice Properties	<
	Usages Policy Routes elow to modify, add, view, or remove a route. To le, please see the Status Pane.	
Routes: Name To_Ingate	Description Sends all calls to the Mediation server	
[	Add Edit <u>R</u> emove	
OK	Cancel <u>Apply</u> Help	

- 8) Here is where we define the Route:
  - a. Target Phone Numbers: The number pattern that will use this Route.
  - b. Gateways: The advanced media gateway or Mediation Server that calls matching this Route will be sent to.
  - c. Phone Usage: The list contains the phone usage records that are required to call a number using this route. For a user to be able to call numbers matching the target phone-number regular expression specified for this route, the caller's user policy must contain at least one usage record that matches a usage record for the route.

It Route         Iteme:       To_Ingate         Itescription:       Itescription:         Sends all calls to the Mediation server       Image: Tescher the server	ation Profiles   Phone		y Routes	
Pescription:  Sends all calls to the Mediation server  route requires a target phone number regular expression, one or more rateways, and one or more phone usages.  Target phone numbers:  Target regular expression  *  Gateways  Address  Ms.ocs2007.ingate.com:5061  Phone usages  Default Usage	oute			
Sends all calls to the Mediation server         In route requires a target phone number regular expression, one or more lateways, and one or more phone usages.         Target phone numbers:        arget regular expression         [*        aleways        Address        ms.ocs2007.ingate.com:5061	ne:	o_Ingate		
A route requires a target phone number regular expression, one or more phone usages.         Target phone numbers:        arget regular expression         .*        ddeways        Address        ms.ocs2007,ingate.com;5061	cription:			
ateways, and one or more phone usages.         Target phone numbers:        arget regular expression         *	nds all calls to the Med	diation server		*
ateways, and one or more phone usages.         Target phone numbers:        arget regular expression         *				<b>v</b>
Iarget regular expression         *				n, one or more
*     Helper       Gateways     Address       Ms. ocs2007.ingate.com:5061     Remove   Phone usages       Phone usages   Default Usage	arget phone numbers:			
Helper       Gateways       Address       ms.ocs2007.ingate.com:5061       Add       Add       Remove   Phone usages       Default Usage		on		
Gateways Address ms.ocs2007.ingate.com:5061 Add Phone usages Default Usage				
Address ms.ocs2007.ingate.com.5061 Add Phone usages Default Usage				Helper
Address ms.ocs2007.ingate.com.5061 Add Phone usages Default Usage				
ms.ocs2007.ingate.com:5061	-			
Phone usages Default Usage		m:5061		
Phone usages Default Usage				
Phone usages Default Usage				
Default Usage			<u>A</u> dd	<u>R</u> emove
Configure	ione usages			
Configure				

9) To enable voice for users, go to the Standard Edition Servers, in the User folder, here we enable Enterprise Voice for each user under User Properties.



User Test1 Properties	×			
Communications				
Enable user for Office Communications Server				
Sign-in name:				
sip:test1 @ ocs2007.ingate.com 💌				
Server or pool:				
hs.ocs2007.ingate.com				
Allow anonymous participants				
Policy: Default Policy				
<u>View</u> Note: Meeting settings cannot be changed unless the global setting allows per user configuration.				
Additional options: Configure				
OK Cancel Apply Help				

10) In the Additional Options, it is recommended to use full E.164 (+<country code><full number>) number format when communicating between the Ingate and the Mediation Server.

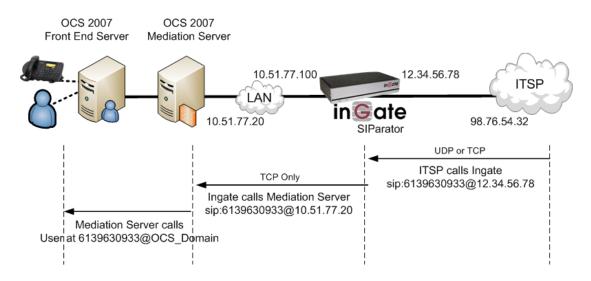
Us	er Test1 Properties			×			
Us	er Options			2	×		
	Telephony Select a telephony option. These settings affect only those calls that are routed through IP-PSTN or remote call control gateways.						
	C Enable <u>P</u> C-to-PC com	munication only					
	C Enable <u>R</u> emote call c	ontrol					
	Enable Enterprise Voi						
	🔲 Enable PBX integ	ation					
	Note: To enable both Server URI below.	remote call control and PBX integration,	, you mus	st specify a			
	P <u>o</u> licy:	Default Policy	-	⊻iew			
	<u>S</u> erver URI:	sip:					
	Line URI:	tel:+17322162717					
	Federation						
	Enable federation						
	Enable remote user access						
	Enable public IM connectivity						
Γ	Archiving						
-	C Archive internal IM conversations						
	C Archive federated IM conversations						
	Note: Archiving settings cannot be changed unless the global setting allows per user configuration.						
	Enable enhanged presence Note: Enhanced presence cannot be changed once it has been set.						
		ОКС	ancel	Help			

# 5 Troubleshooting

## 5.1 Call Flow Examples

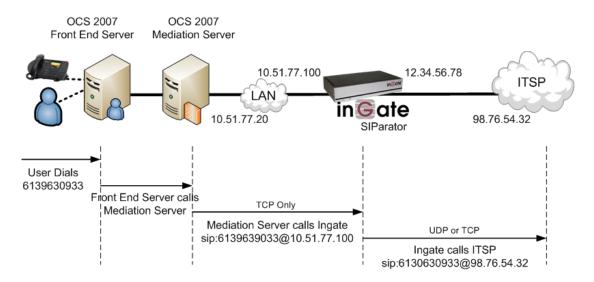
## 5.1.1 Incoming Call

Incoming calls will always originate from the Service Provider and be addressed directly to the Ingate SIParator IP Address. The Ingate in turn will route the call to the Mediation Server. Many times the Ingate will have to convert UDP to TCP, this is done in the Dial Plan or other places in the Ingate.



## 5.1.2 Outgoing Call

Outgoing calls will always originate from the OCS 2007 and be addressed within the SIP Protocol directly to the Ingate IP address. The Ingate in turn will route the call to the ITSP. Many times the Ingate will have to convert TCP to UDP, this is done in the Dial Plan or other places in the Ingate.



# 5.2 Startup Tool

### 5.2.1 Status Bar

Located on every page of the Startup Tool is the Status Bar. This is a display and recording of all of the activity of the Startup Tool, displaying Ingate unit information, software versions, Startup Tool events, errors and connection information. Please refer to the Status Bar to acquire the current status and activity of the Startup Tool.

- St	atus	
	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	

## 5.2.2 Configure Unit for the First Time

Right "Out of the Box", sometimes connecting and assigning an IP Address and Password to the Ingate Unit can be a challenge. Typically, the Startup Tool cannot program the Ingate Unit. The Status Bar will display **"The program failed to assign an IP address to eth0"**.

ou are running the	Version 2.4.0 available on the Ingate web: 2.4.0 latest version of the Startup tool. available here: http://www.ingate.com/startuptool.php o assign an IP address to eth0	
		~

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 must always be used with the
Eth0.	Startup Tool.
Incorrect MAC Address	Check the MAC address on the Unit
	itself. MAC Address of Eth0.

Possible Problems	Possible Resolution
An IP Address and/or Password have	It is possible that an IP Address or
already been assigned to the Ingate	Password have been already been
Unit	assigned to the unit via the Startup
	Tool or Console
Ingate Unit on a different Subnet or	The Startup Tool uses an application
Network	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.

## 5.2.3 Change or Update Configuration

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

You are running th	n available on the Ingate v e latest version of the Star	tup tool.		<u>~</u>
	s available here: http://ww he unit, check settings and		hp	

#### **Possible Problems and Resolutions**

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power
Incorrect IP Address	Check the IP Address using a Web Browser.
Incorrect Password	Check the Password.
Despite your best efforts	<ol> <li>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.</li> <li>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".</li> </ol>

### 5.2.4 Network Topology

There are several possible error possibilities here, mainly with the definition of the network. Things like IP Addresses, Gateways, NetMasks and so on.



Possible Problems	Possible Resolution
Error: Default gateway is not	The Default Gateway is always the way
reachable.	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	IP Address of Netmask is in an Invalid
correct.	format.
Error: Please provide a correct	Netmask is in an Invalid format.
netmask for eth0/1	
Error: Primary DNS not setup.	Enter a DNS Server IP address

## 5.2.5 IP-PBX

The errors here are fairly simple to resolve. The IP address of the IP-PBX must be on the same LAN segment/subnet as the Eth0 IP Address/Mask.



**Possible Problems and Resolutions** 

Possible Problems	Possible Resolution
Error: The IP PBX IP does not	The IP Address of the IP-PBX must be
seem to be on the LAN.	on the same subnet as the inside
	interface of the Ingate Eth0.
Error: You must enter a SIP	Enter a Domain, or de-select "Use
domain.	Domain"
Error: As you intend to use RSC	Enter a Domain or IP Address used for
you must enter a SIP domain.	Remote SIP Connectivity. Note: must
Alternatively you may configure a	be a Domain when used with SIP
static IP address on eth1 under	Trunking module.
Network Topology	

### 5.2.6 ITSP

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



Possible Problems	Possible Resolution
Error: Please enter a domain name	Enter a Domain, or de-select "Use
for your provider	Domain"
Error: Please enter number, name	Enter a DID and Domain, or de-select
and domain.	"Use Account"

## 5.2.7 Apply Configuration

At this point the Startup Tool has pushed a database to the Ingate Unit, you have Pressed "Apply Configuration" in Step 3) of Section 4.7 Upload Configuration, but the "Save Configuration" is never presented. Instead after a period of time the following webpage is presented. This page is an indication that there was a change in the database significant enough that the PC could no longer web to the Ingate unit.



Possible Problems	Possible Resolution
Eth0 Interface IP Address has	Increase the duration of the test mode,
changed	press "Apply Configuration" and start a
	new browser to the new IP address, then
	press "Save Configuration"
Access Control does not allow	Verify the IP address of the PC with the
administration from the IP address	Startup Tool. Go to "Basic
of the PC.	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.

# 5.3 Ingate Example Configuration

Here are some highlights and explanation of an example configuration of the Ingate SIParator.

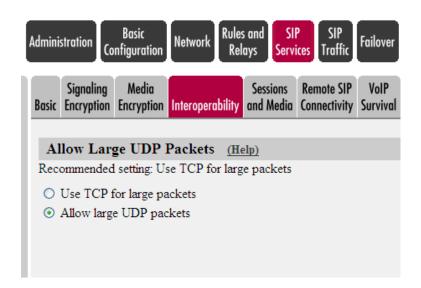
## 5.3.1 Network and Computers

This is an example of the Network – Networks and Computers page with an Ingate SIParator in a Stand-alone configuration. The Networks and Computer page is a IP Table List or Route List, providing the Ingate knowledge of its surrounding networks and what interface they are connected too. Also, the table provides identification of specific IP Addresses for later use in providing filter and identification of source IP addresses in the Dial Plan and other locations.

ninistration Basic Configura	tion Network SIP	SIP Traffic Failover	'irtual Private Networks	Quality of Logging Service and Tools	About		
tworks and Default computers Gateways	All Interfaces VLAN Eth	0 Eth1 Eth2 Status	PPPoE Topolo	ay			
Networks and C	Computers						
N	6-1	Lower Li	mit	Upper (for IP r		Interferen All AN	
Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAN	
• ITSP_IP	- •	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	
+ LAN	- 🗸	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	
Microsoft OCS	- 🗸	10.51.77.20	10.51.77.20			-	
+ WAN	- V	0.0.0.0	0.0.0.0	255,255,255,255	255,255,255,255	outside (eth1 untagged)	i

## 5.3.2 Interoperability

Microsoft OCS 2007 requires the use of TCP transport, many Service Providers support only UDP transport. In this case, where the Service Provider can only support UDP we need to allow large UDP packets. This will ensure all TCP packets are converted to UDP, even when they are over the UDP packet size limit.



## 5.3.3 Dial Plan

This is an example of the SIP Traffic - Dial Plan on the Ingate SIParator. There are three main parameters that need to be defined to create the Dial Plan. Matching From Header, Matching Request URI and Forward To are parameters that when combined together form the Dial Plan.

The key difference in the MS OCS 2007 integration is the use of TCP as the transport, thus the Forward To section Regular Expression has sip:\$1@10.51.77.20;transport=tcp

If the Service Provider does not support TCP, be sure to define the ITSP for use with the UDP transport, with a Regular Expression sip:\$1@98.76.54.32;transport=udp

SIP thods Filtering	Local Registrar	Authentica and Accour		Dial Plan Rout	Time SIP ting Classes Status						
Use Dial P	lan <u>(He</u>		Emergency	Numbe	er <u>(Help)</u>						
) On ) Off		9	11								
) Fallback											
Matching	From H	leader (	( <u>Help)</u>								
Name		U	se This		Or This	Tran	mort	Net	work	Delete Row	
Ivame	1	Username	e Dom	ain	Reg Expr	Iran	sport	Ine	work	Delete Kow	
Generic ITSF	*		*			UDP	*	ITSP_IF	*		
LAN	*		*			TCP	~	LAN	*		
Microsoft OC	S *		*			TCP	*	Microso	ft OCS 🔽		
WAN	*		*			Any	*	WAN	*		
		Profix	Hes	hd		Min	Tail	D	main		— Dele
Name					Use This					Or This	Delet
		Prefix	Hea	ıd	Tail	Min	. Tail	De	main	Reg Expr	— Dele
Inbound		Prefix	Hez	ıd			. Tail	De	main		
		Prefix	Hez	ıd	Tail		. Tail		omain	Reg Expr	56 🗆
Inbound		rows.	Hez	ıd	Tail - 🗸		. Tail		omain	Reg Expr sip:(.*)@12.34.	56 🗆
Inbound Outbound Add new rows	`o <u>(Help</u>	rows.	Use This		Tail	his			Or Thi	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.	56
Inbound Outbound Add new rows Forward T Name	`O <u>(Help</u> e	rows.	Use This Account		Tail - 💌		Trans	port	Or Thi Reg Exp	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           sip:(.*)@10.61.           sip:(.*)@10.61.	56
Inbound Outbound Add new rows Forward T Nam. * Generic II	°o <u>(Help</u> e	] rows. )) Subno. 1	Use This Account		Tail	his	Trans	sport sig	Or Thi Reg Exp p:\$1@98.76	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           sip:(.*)@10.51.           sip:(.*)@10.51.           sip:(.*)@10.51.	56
Inbound Outbound Add new rows Forward T Name	°o <u>(Help</u> e	rows.	Use This Account		Tail	his	Trans	sport sig	Or Thi Reg Exp	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           sip:(.*)@10.51.           sip:(.*)@10.51.           sip:(.*)@10.51.	56
Inbound Outbound Add new rows Forward T Nam. * Generic II	o (Help e rsp ocs	] rows. )) Subno. 1	Use This Account		Tail - • • • • • • • • • • • • • • • • • • •	his	Trans	sport sig	Or Thi Reg Exp p:\$1@98.76	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           sip:           b.54.           1.77.	56
Inbound Outbound Add new rows Forward T Nam Generic II Microsoft Add new rows	o (Help e rsp ocs	rows.	Use This Account	Replace	Tail - • • • • • • • • • • • • • • • • • • •	his	Trans	sport v sip	Or Thi Reg Exp 9:\$1@98.76 9:\$1@10.57	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           s           Delete R.           5.54.           1.77.	56
Inbound Outbound Add new rows Forward T Name Generic II Microsoft Add new rows Dial Plan No.	o (Help) From H	rows. )) Subno. 1 groups wi Ieader	Use This Account	Replace	Tail	his Port	Trans -	sport sip sip	Or Thi Reg Exp 0.\$1@98.7( 0.\$1@10.51	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           s           Delete R.           5.54.           1.77.	56
Inbound Outbound Add new rows Forward T Nam. Ceneric II Microsoft Add new rows Dial Plan	°o (Help)	rows. 20 Subno. 1 1 groups with Ieader OCS V	Use This Account - • - • ith 1 row Request URI Outbound • 1	Replace	Tail	his Port	Trans	sport sip sip	Or Thi Reg Exp 0:\$1@90.7( 0:\$1@10.5*	Reg Expr           sip:(.*)@12.34.           sip:(.*)@10.51.           s           Delete R.           5.54.           1.77.	56

# 5.4 Ingate Troubleshooting Tools

## 5.4.1 Display Logs

Here is the internal logging of the Ingate. The Display Logs show all SIP Signaling and also TLS (SSH) certificate exchange and setup.

Administration Basic Network SIP SIP Failover Virtual Private Quality Services Traffic	
Display Log Capture Network Configuration Classes Sending	
Search the Log (Help)         Display log         Display log         Periodice         Press "Display Log"         to See internal logs         Packet selection         As selected choice.         Packet Type Selection         All packets         IP Address Selection (Help)         A:	Support Report (Help)         Include configuration database:         Yes () No         Make sure the Log class for SIP         debug messages is set to Local if         you have a SIP-related problem.         Export support report         Time Limits         Show log from: (clear)         date (YYY'- time         MM-DD)         (HH:MM:SS)         Show log until: (clear)         date (YYY'- time         MM-DD)         (HH:MM:SS)
B: ☐ not this address ○ A src ○ A dst ⊙ A any ○ A to B ○ B to A ○ Between A&B ☐ not this combination	Show newest at top Show This Select All, None, SIP.
Protocol/Port Selection	✓ IP packets as selected
○ TCP         ○ UDP           ○ ICMP         ○ ICMP           ○ ESP         ○	Configuration server logins Administration and configuration Manual reconfigurations and reboots Time changes DHCP/PPPoE client RADIUS errors
○ Protocol number:(Help) □ not	□ SNMP problems
SIP Packet Selection (Help)         Call-ID:       Show internal SIP signaling         SIP Methods:       Filter on SIP         IP addresses:       Filter on SIP         From Header:       Filter on SIP         To Header:       Specific fields	<ul> <li>Hardware errors</li> <li>Mail errors</li> <li>Negotiated IPsec tunnels</li> <li>IPsec key negotiations</li> <li>IPsec key negotiation debug messages</li> <li>IPsec user authentication</li> <li>PPTP negotiations</li> <li>SIP errors</li> <li>SIP signaling</li> <li>SIP packets</li> <li>Filter on SIP traffic only</li> <li>SIP debug messages</li> </ul>
Export the Log (Help) Export log TAB-separated file 20 MB max	Clear form

## 5.4.2 Packet Capture

The Packet Capture capability of the Ingate allows for the capture and export of all traffic on any one or ALL interfaces simultaneously. Then export to your PC where it can be viewed in Wireshark or Ethereal.

Administration Basic Configuration Network SIP SIP Failover Virtual Private Quality of Services Traffic Failover Virtual Private Quality of Service and Tools
Display Packet Check Logging Log Capture Network Configuration Classes Sending
Capture status: Inactive
Captured data size: 7 kB
Captured when: 2009-04-28 12:52:21
Ingate SIParator has a built-in packet capture function which produces pcap trace files. You can select to capture traffic on one specific interface or on all interfaces.
For contacts with the Ingate Support Team, a packet capture is not what is usually expected (sometimes it is even not useful). For these purposes, please always send a <u>Support Report</u> .
Network Interface Selection
All interfaces
Select "All Interfaces" to
You can also select the type of IP pactors cook multiple captures
trom multiple interfaces
IP Address Selection (Help) into one PCAP
A: not this address
$\land$ A src $\land$ A dst $\odot$ A any $\land$ A to B $\bigcirc$ B to A $\bigcirc$ Between A&B $\Box$ not this combination
Protocol/Port Selection
All IP protocols
O TCP
O UDP Filter on Port,
Transport and
O ICM₽ other criteria
O ESP
Download PCAP File
○Protocol number:(Help) □ not
Start capture Download captured data
Start capture     Download captured data       Stop capture     Delete captured data
Stop capture Delete captured data
Stop capture Delete captured data Start Capture,
Stop capture Delete captured data
Stop capture     Delete captured data       Start Capture,     reproduce the
Stop capture         Delete captured data           Start Capture, reproduce the problem, then         Image: Capture data

## 5.4.3 Check Network

Standard PING and Trace Route feature for simple network checks.

