Application Note

Microsoft OCS 2007 Configuration Guide

15 October 2009

Table of Contents

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

Revision History:

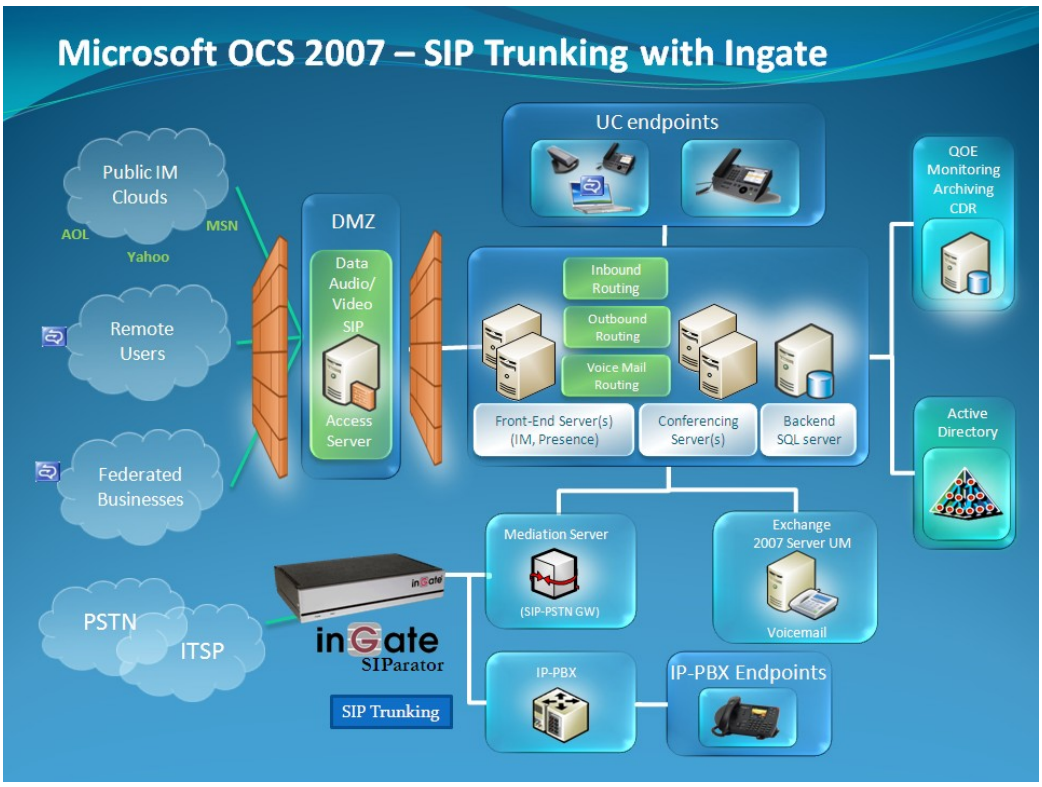
Revision	Date	Author	Comments
	2009-10-15	Scott Beer	First Draft

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 software-powered 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 real-time 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.

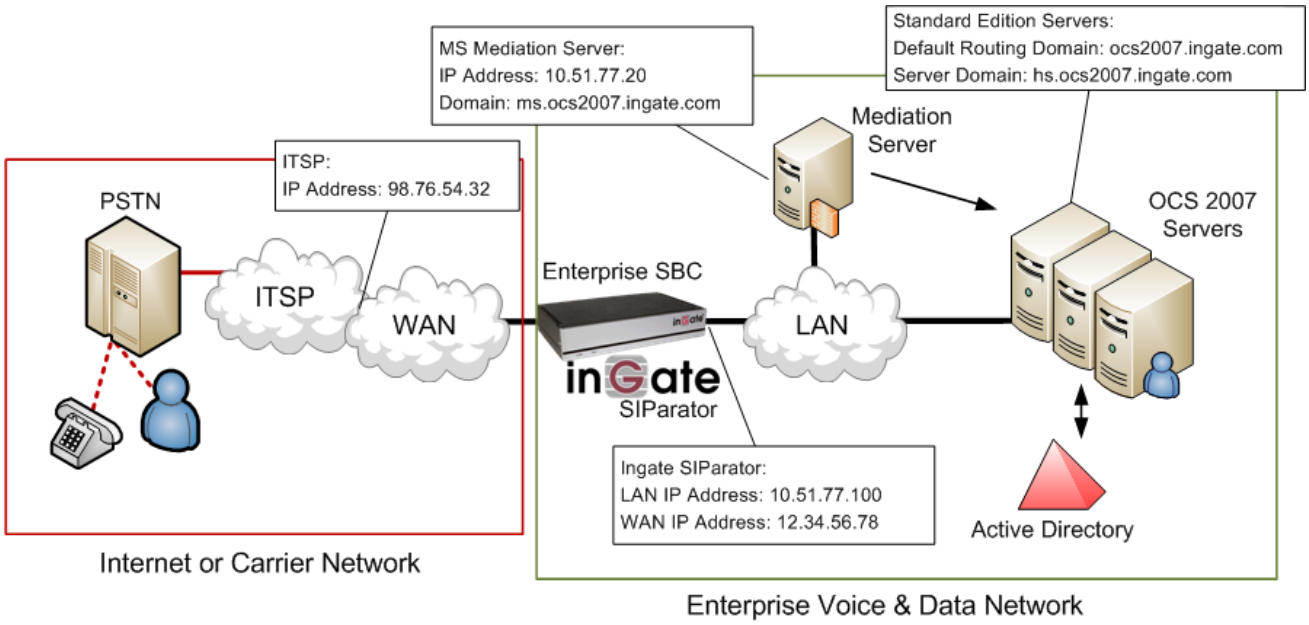
The Ingate SIParator or Firewall sits on the Enterprise network edge, providing a security solution for data and SIP communications with E-SBC functionality. It is responsible for all SIP communications security by providing Policy and Routing Rules to allow specific SIP traffic intended for the Enterprise.

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.
2) 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



Look for the Microsoft OCS Icon 

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

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

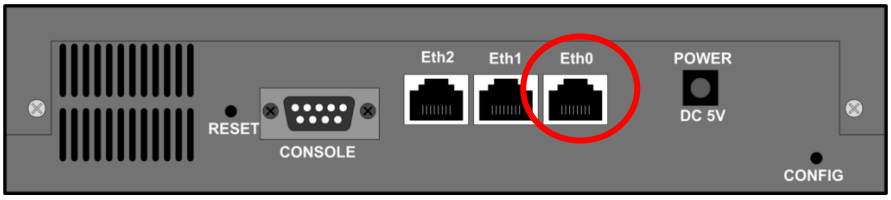
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

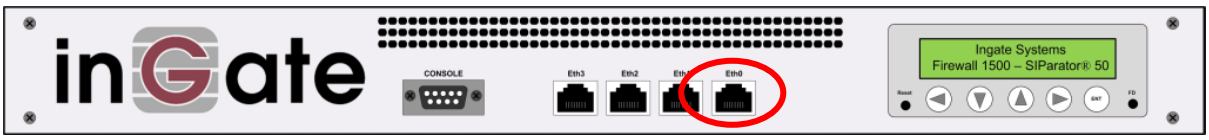
Configuration Steps:

1) Connect Power to the Unit.
2) Connect an Ethernet cable to "Eth0". This Ethernet cable should connect to a LAN network. Below are some illustrations of where "Eth0" are located on each of the Ingate Model types.

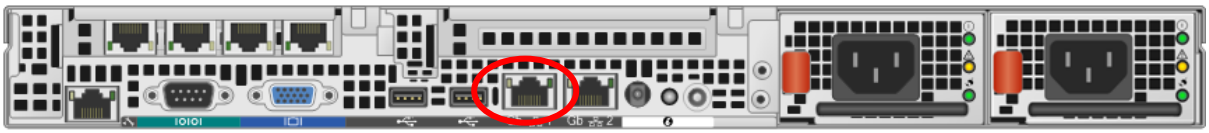
Ingate 1190 Firewall and SIParator 19 (Back)



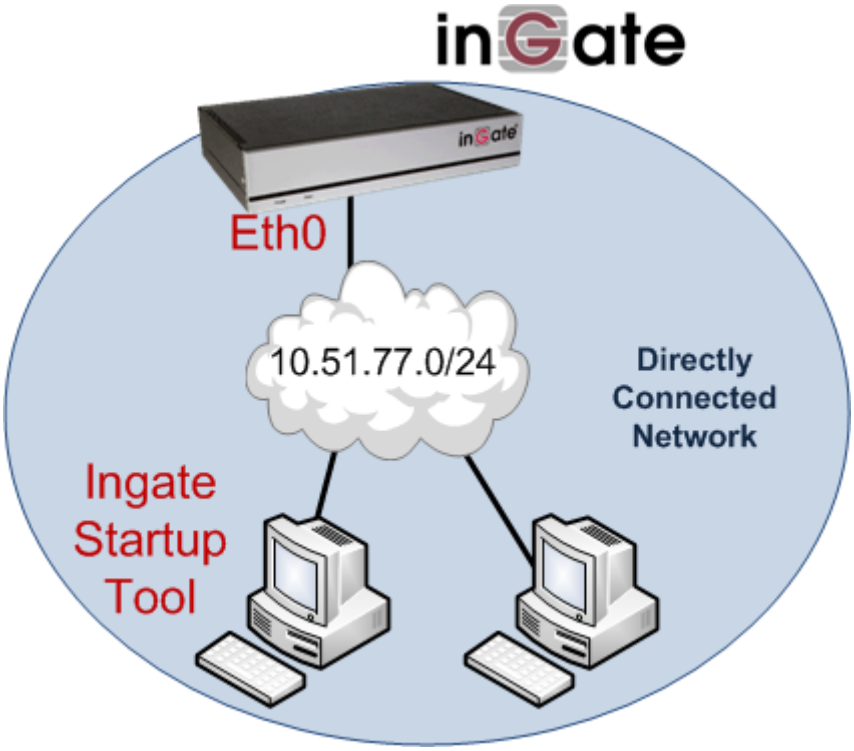
Ingate 1500/1550/1650 Firewall and SIParator 50/55/65



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

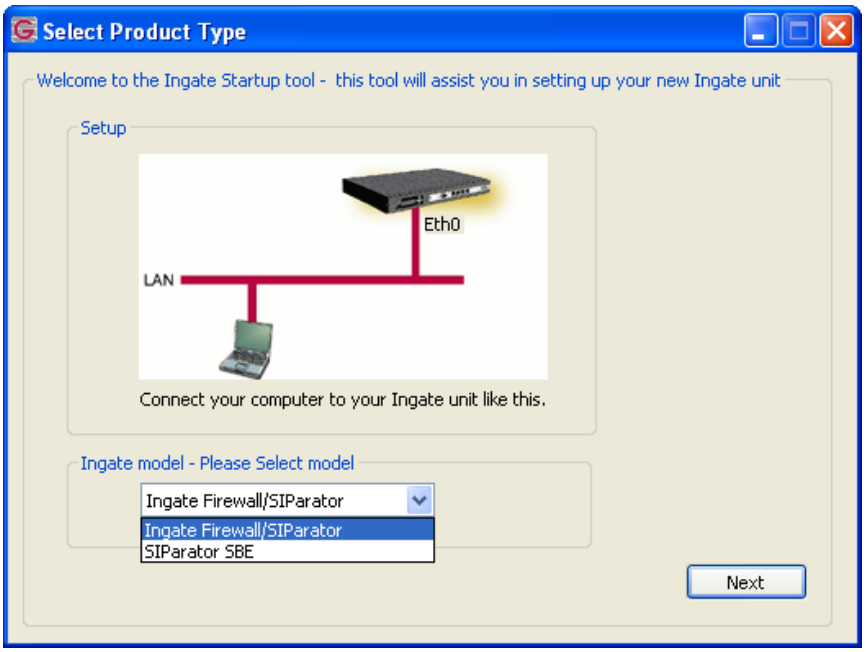
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

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.

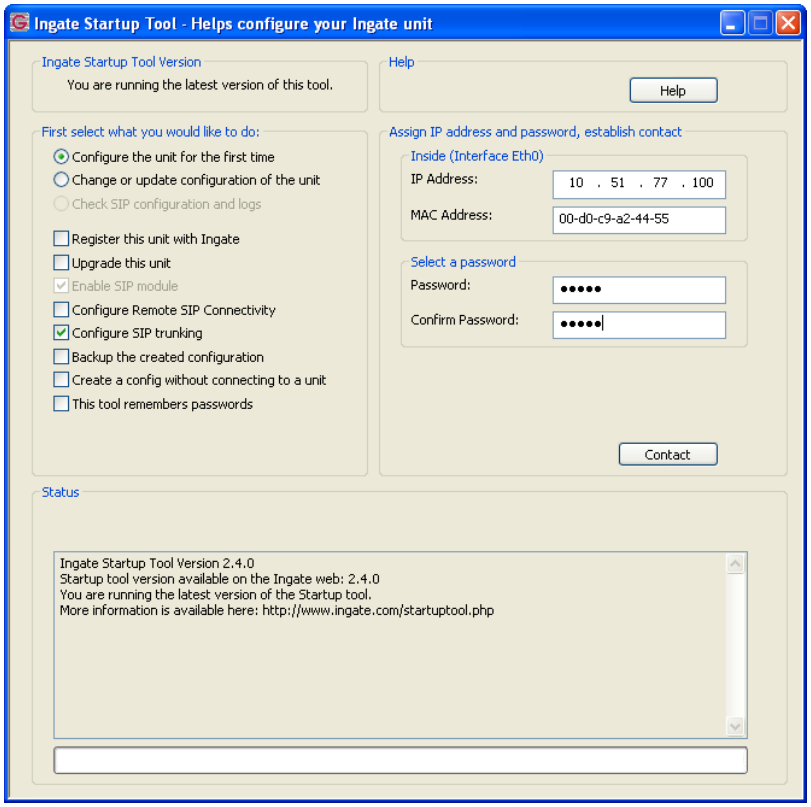
Note: If the Ingate Unit already has an IP Address and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 3.2: "Change or Update Configuration".

Configuration Steps:

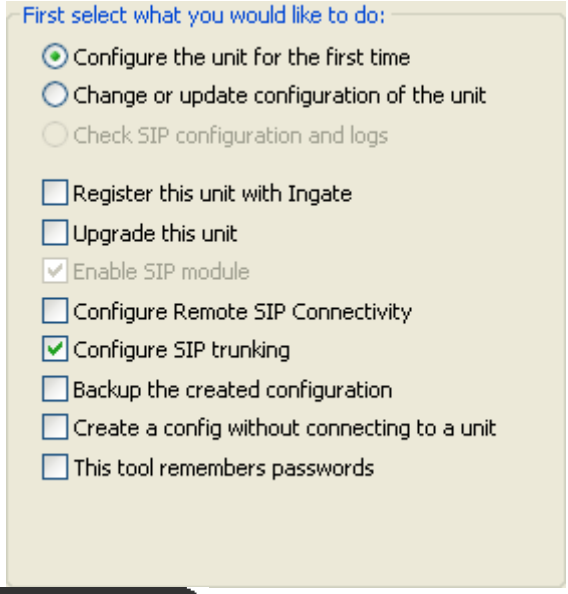
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



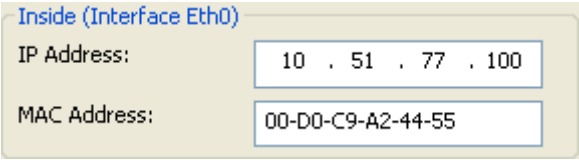
4) Other Options in the "First select what you would like to do",



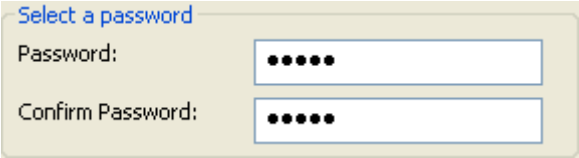
Microsoft
Office Communications Server

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

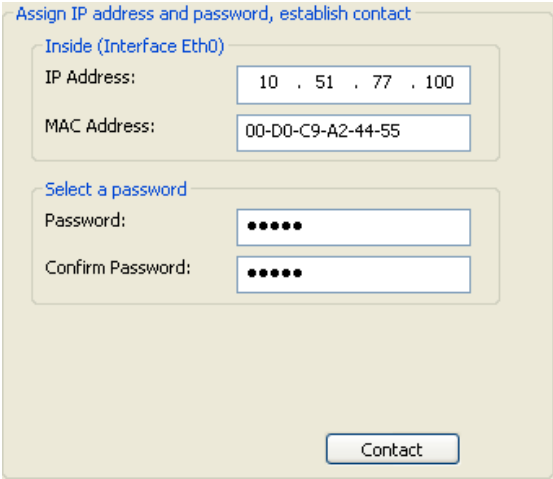
5) In the "Inside (Interface Eth0)",
   a. Enter the IP Address to be assigned to the Ingate Unit.
   b. Enter the MAC Address of the Ingate Unit, this MAC Address will be used to find the unit on the network. The MAC Address can be found on a sticker attached to the unit.



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



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



8) Proceed to Section 3.4: Network Topology.

3.3 Change or Update Configuration

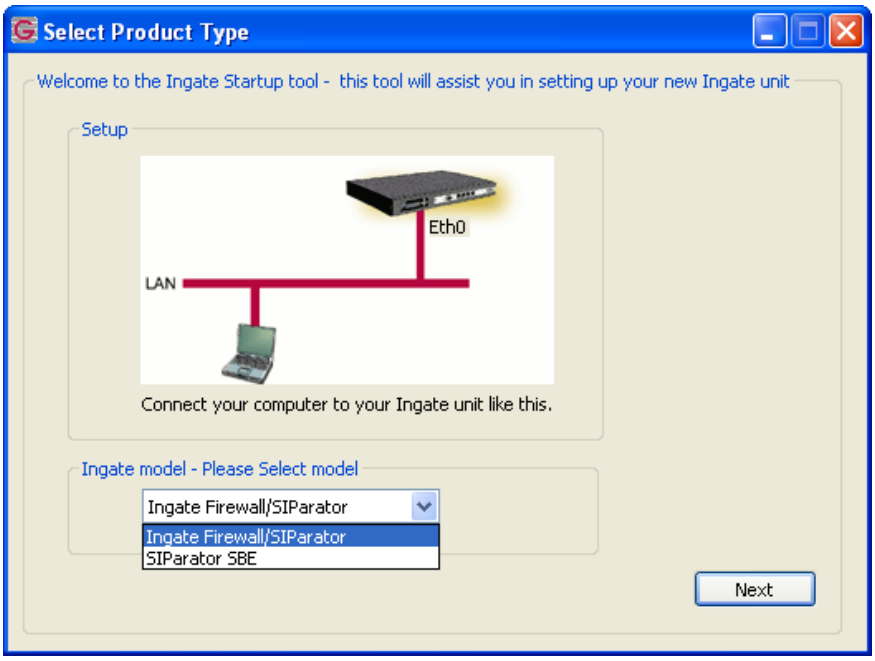
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

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.

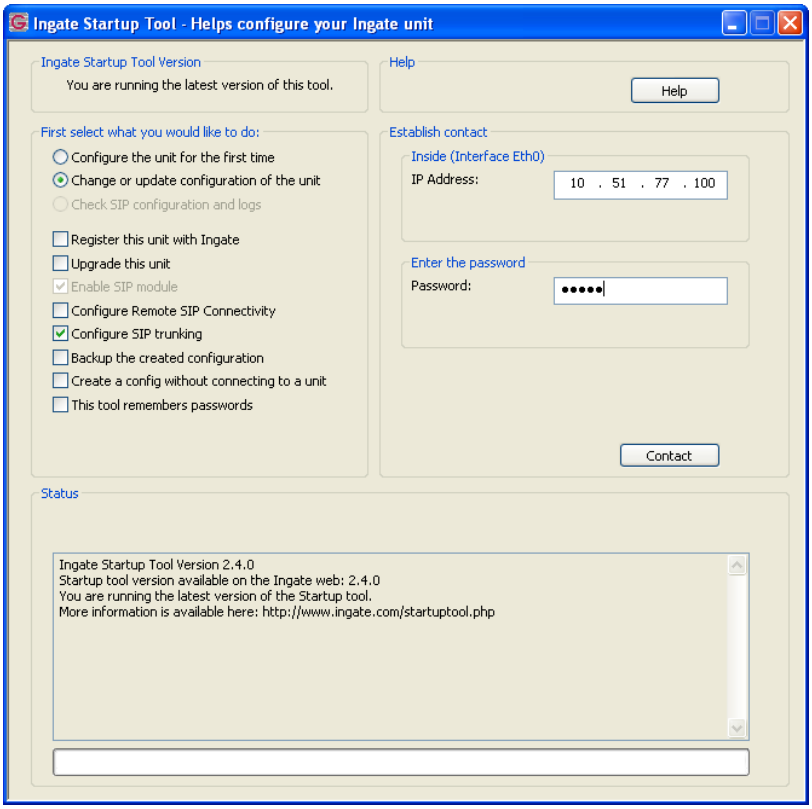
Note: If the Ingate Unit does not have an IP Address and Password assigned to it, proceed directly to Section 3.1: "Configure the Unit for the First Time".

Configuration Steps:

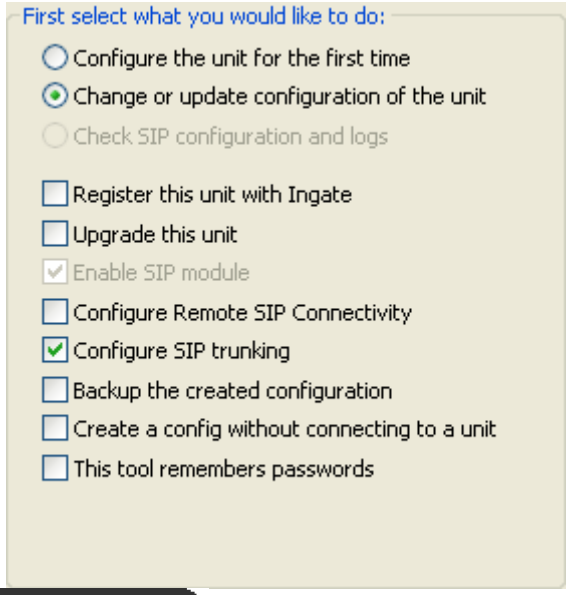
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



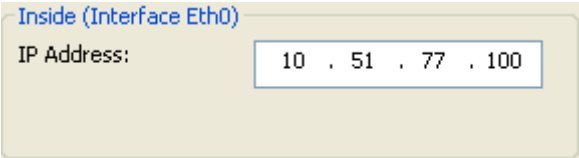
4) Other Options in the "First select what you would like to do",



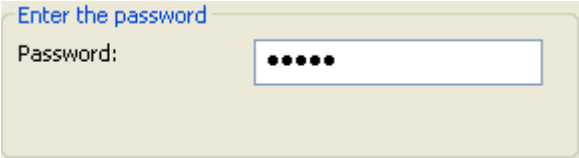
Microsoft
Office Communications Server

a. Select "Configure SIP Trunking" if you want the tool to configure SIP Trunking between 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.



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

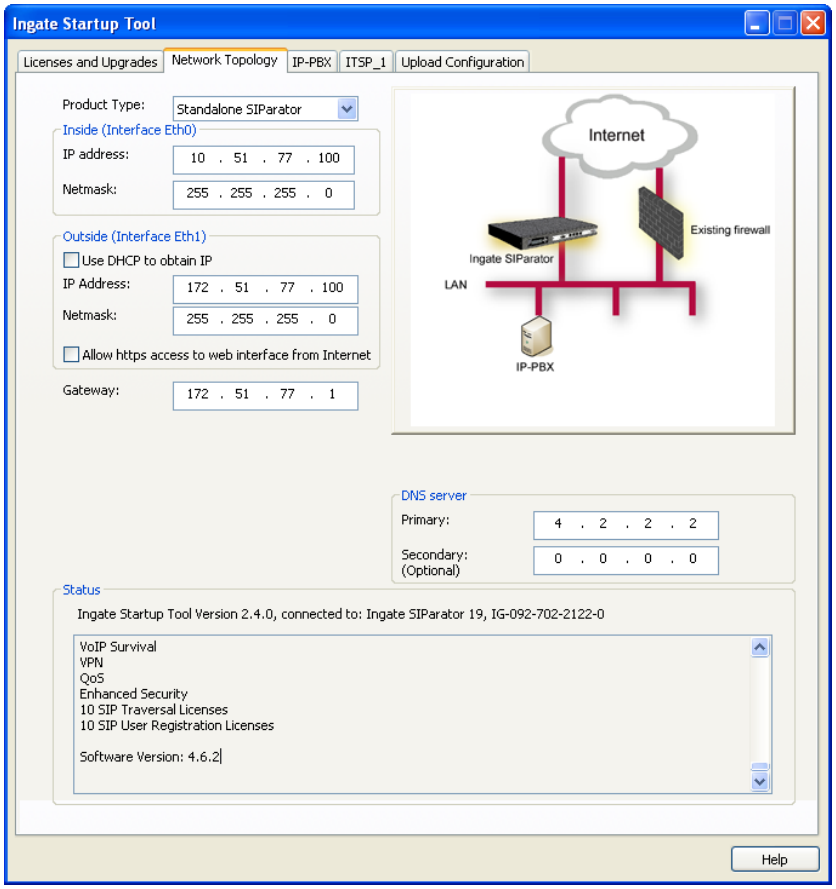


7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.

8) Proceed to Section 3.4: Network Topology.

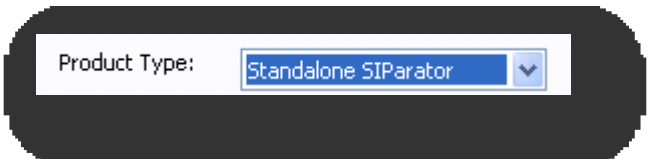
3.4 Network Topology

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.



Configuration Steps:

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

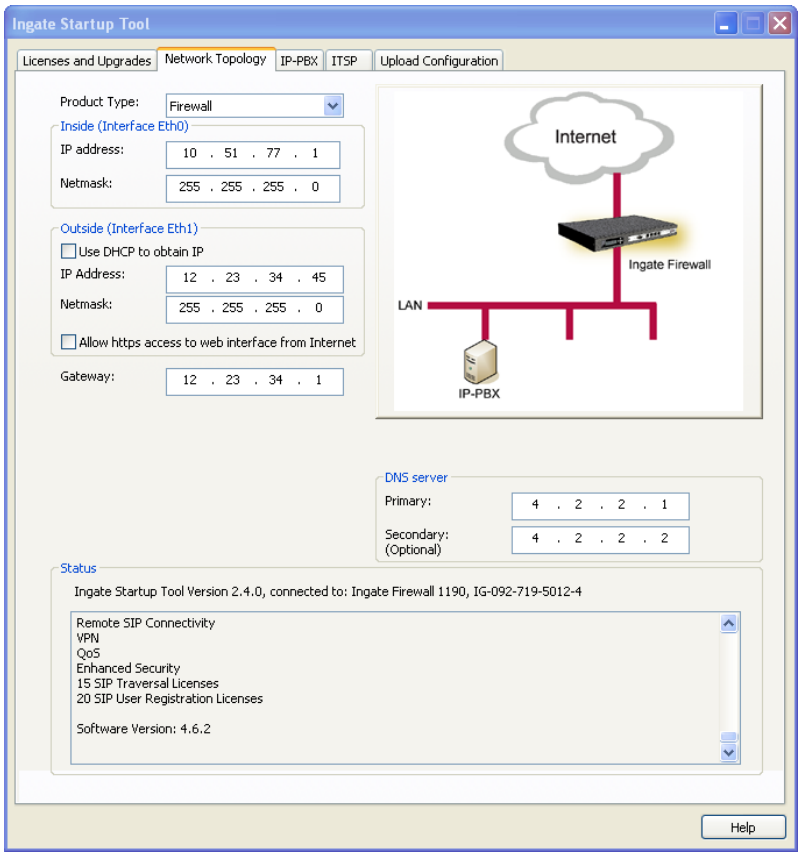


Hint: Match the picture to the network deployment.

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.

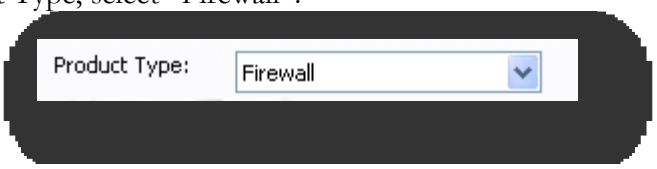
3.4.1 Product Type: Firewall

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.

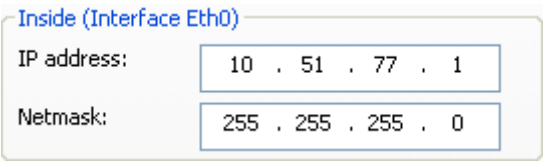


Configuration Steps:

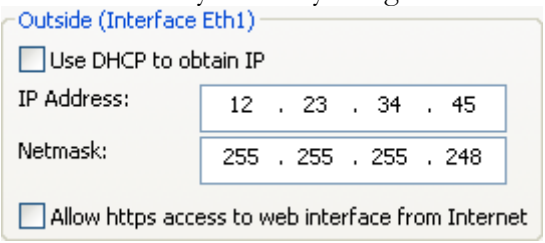
1) In Product Type, select "Firewall".



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

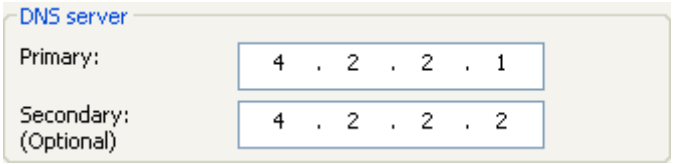


3) Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
   a. A Static IP Address and Netmask can be entered
   b. Or select "Use DHCP to obtain IP", if you want the Ingate Unit to acquire an IP address dynamically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



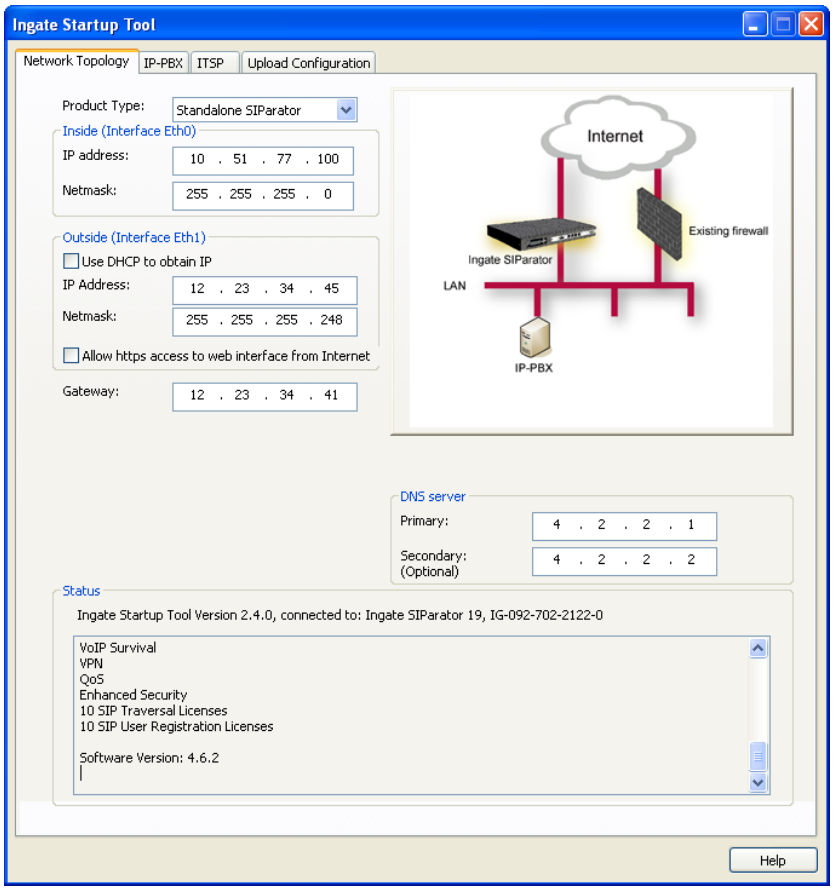
4) Enter the Default Gateway for the Ingate Firewall. The Default Gateway for the Ingate Firewall will always be an IP Address of the Gateway within the network of the outside interface (Eth1).

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



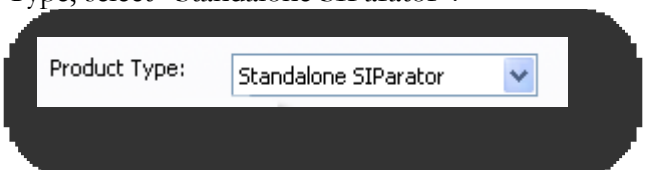
3.4.2 Product Type: Standalone

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.

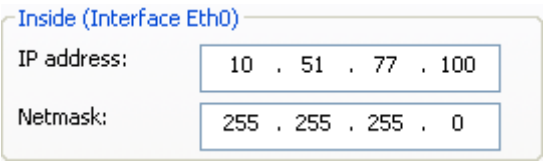


Configuration Steps:

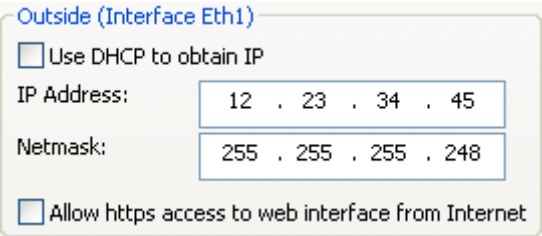
1) In Product Type, select "Standalone SIParator".



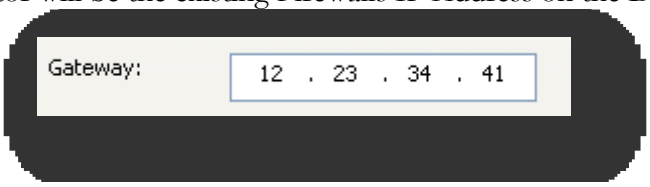
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



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



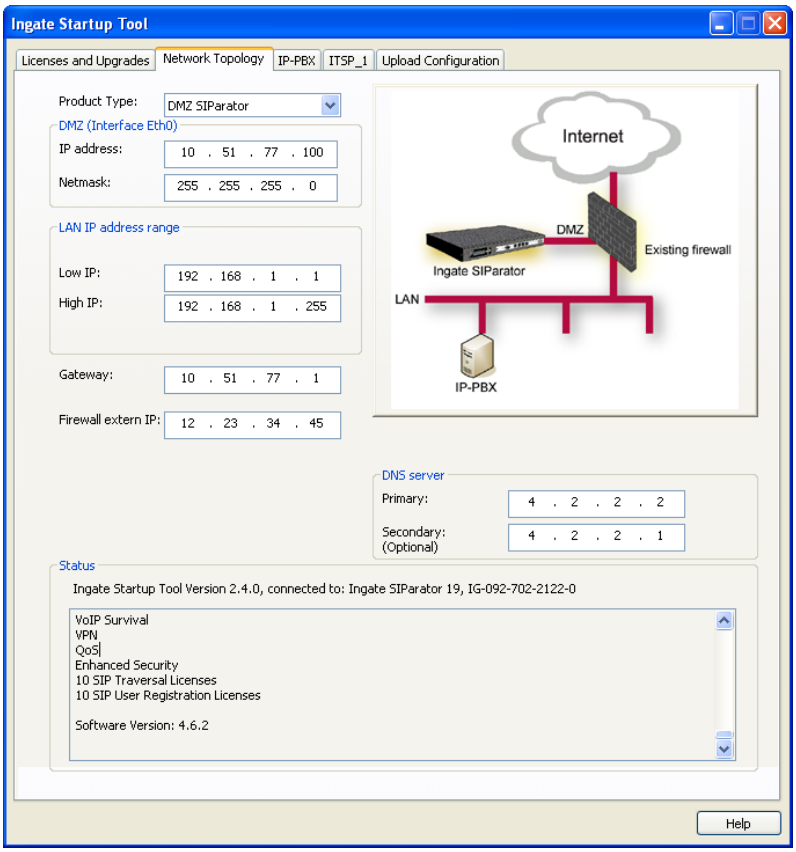
4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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

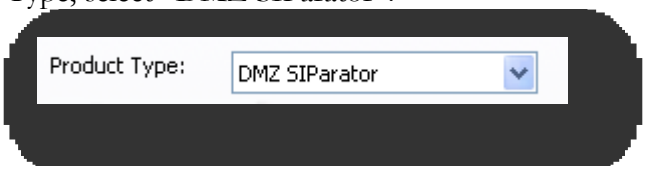
3.4.3 Product Type: DMZ SIParator

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.

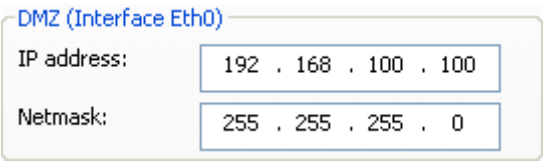


Configuration Steps:

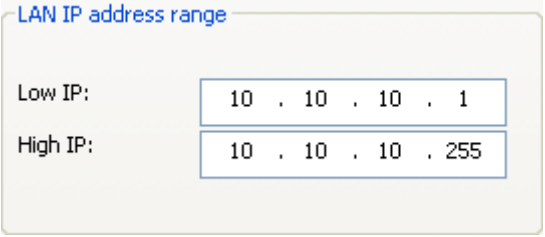
1) In Product Type, select "DMZ SIParator".



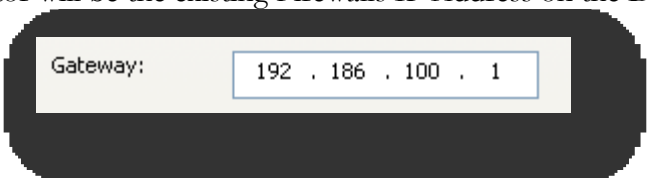
2) Define the IP Address and Netmask of the DMZ (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.



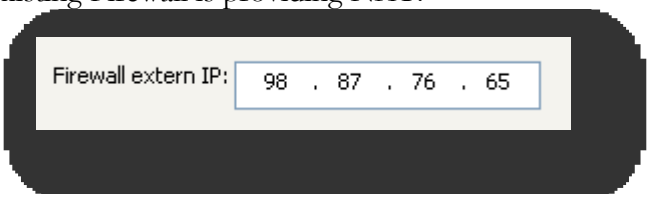
3) Define the LAN IP Address Range, the lower and upper limit of the network addresses located on the LAN. This is the scope of IP Addresses contained on the LAN side of the existing Firewall.



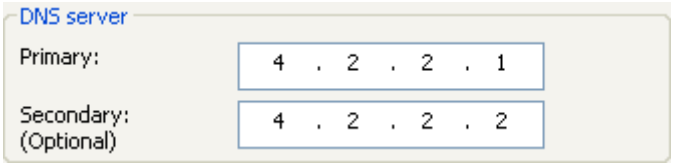
4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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



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



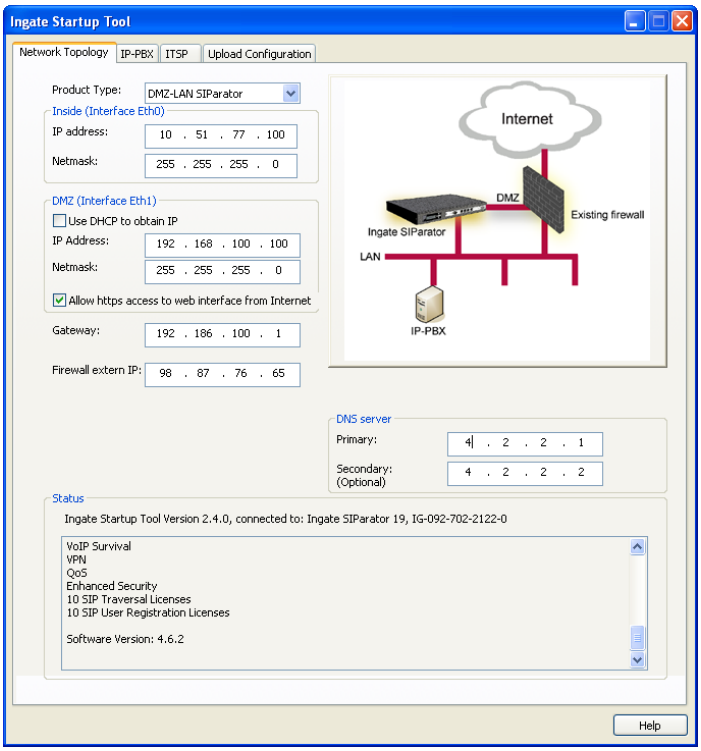
7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

   On the existing Firewall:

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

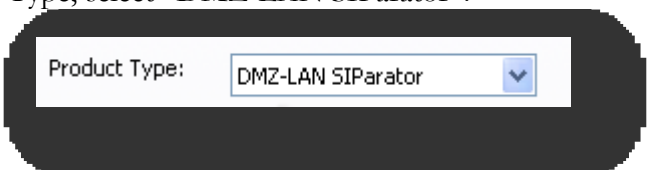
3.4.4 Product Type: DMZ-LAN SIParator

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.

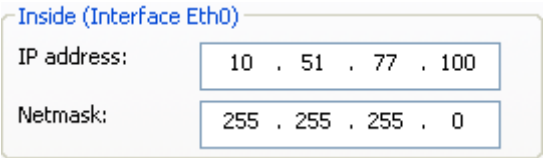


Configuration Steps:

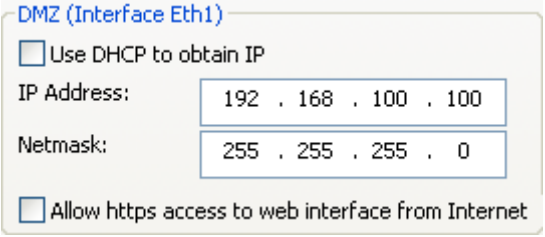
1) In Product Type, select "DMZ-LAN SIParator".



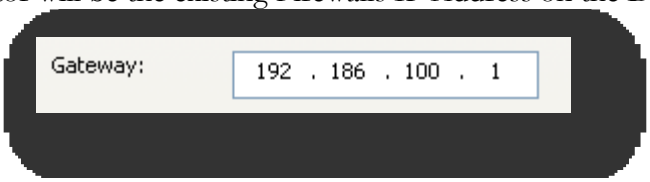
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



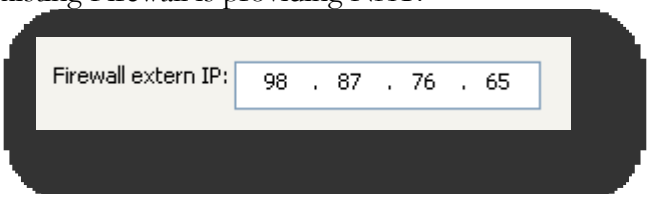
3) Define the IP Address and Netmask of the DMZ (Interface Eth1). This is the IP Address that will be used on the Ingate unit to connect to the DMZ network side on the existing Firewall.
    a. A Static IP Address and Netmask can be entered
    b. Or select "Use DHCP to obtain IP", if you want the Ingate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



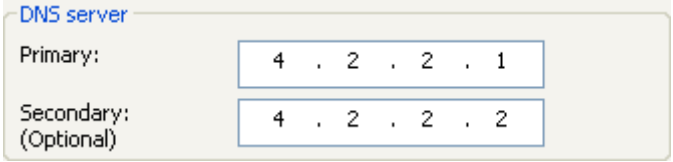
4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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



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

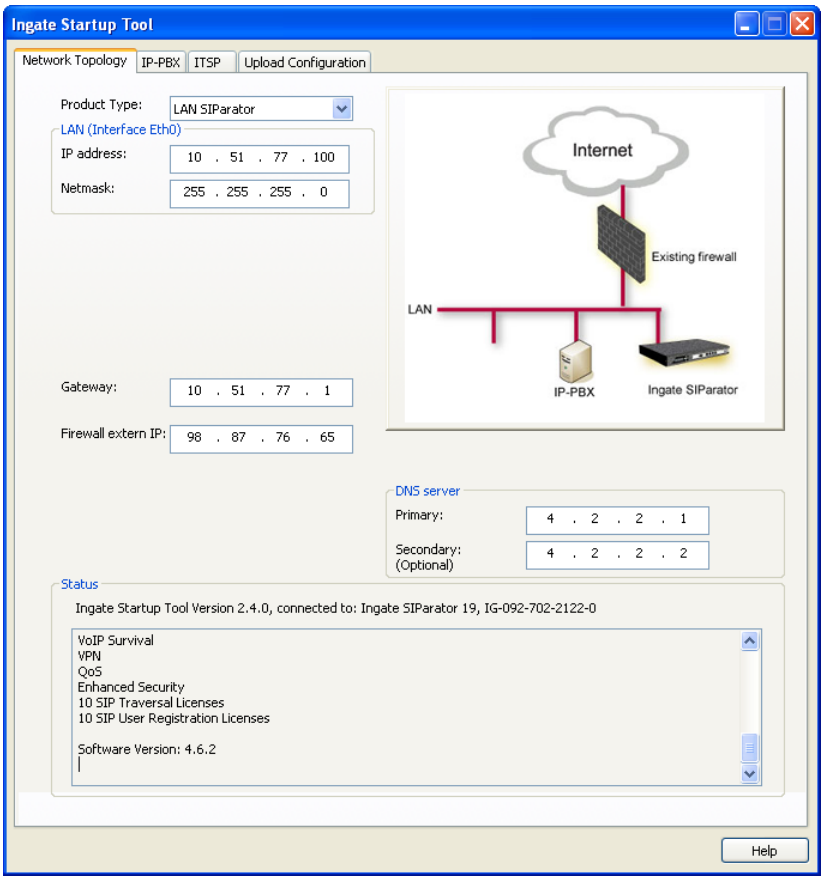


7) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

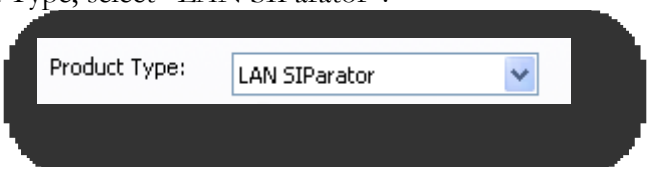
3.4.5 Product Type: LAN SIParator

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.

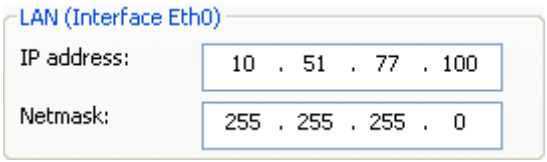


Configuration Steps:

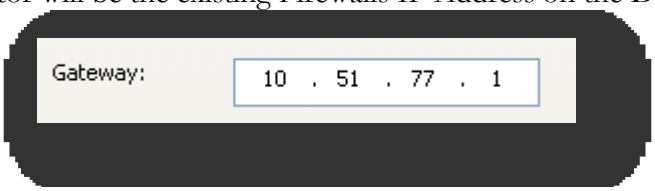
1) In Product Type, select "LAN SIParator".



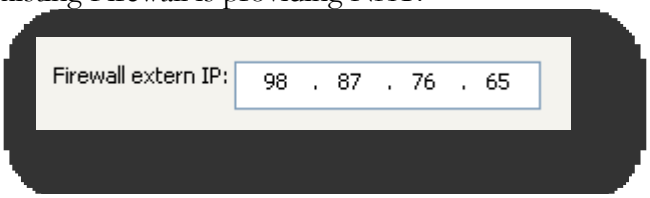
2) Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



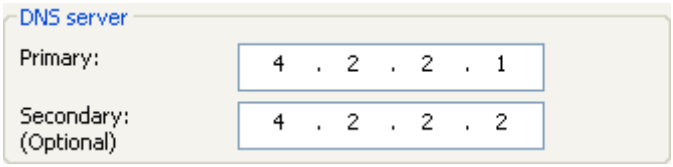
3) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.



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



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

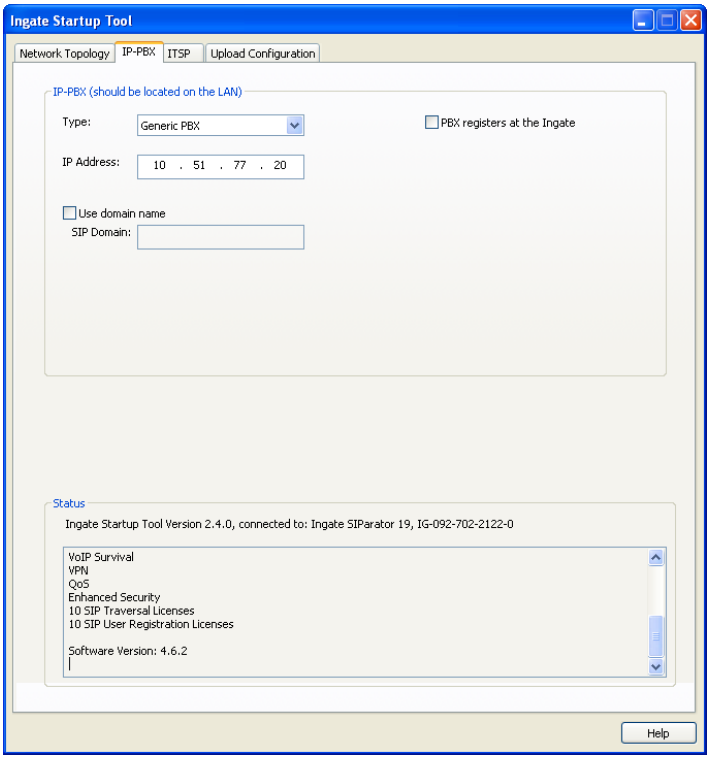


6) On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

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

3.5 IP-PBX

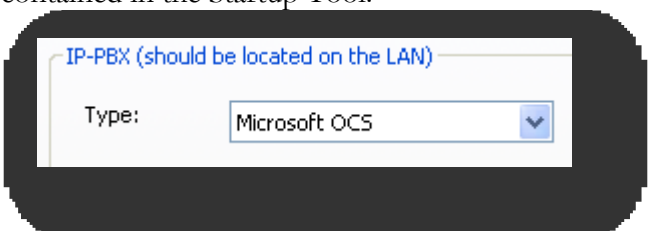
The IP-PBX section is where the IP Addresses and Domain location are provided to the Ingate unit. The configuration of the IP-PBX will allow for the Ingate unit to know the location of the Microsoft OCS 2007 Mediation Server as to direct SIP traffic for the use with SIP Trunking. The IP Address of the Microsoft OCS Mediation Server must be on the same network subnet as the IP Address of the inside interface of the Ingate unit.



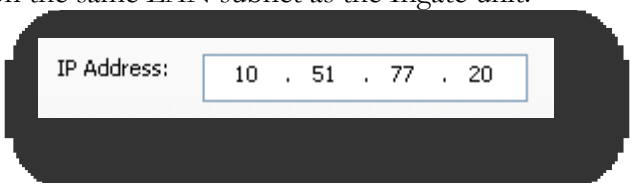
Microsoft
Office Communications Server

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.

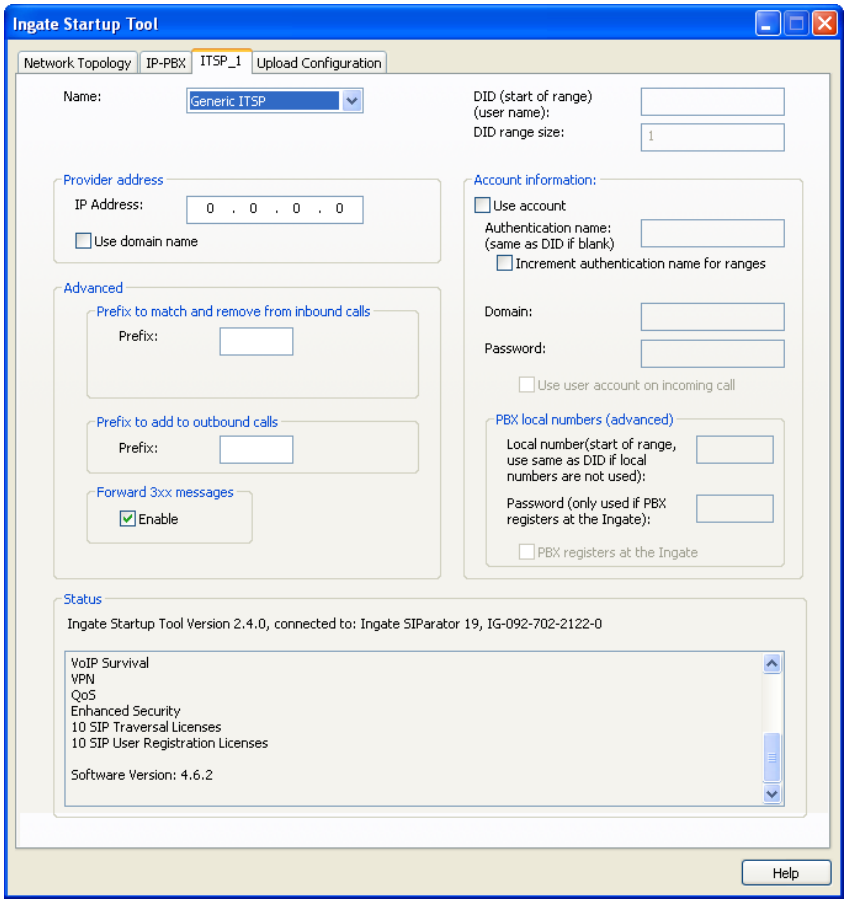


2) Enter the IP Address of the Microsoft OCS Mediation Server. The IP Address should be on the same LAN subnet as the Ingate unit.



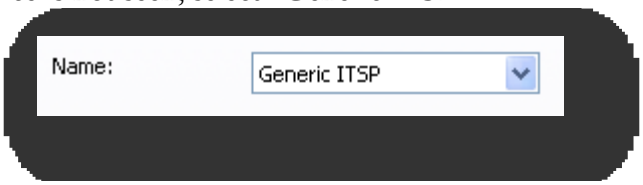
3.6 ITSP

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.



Configuration Steps:

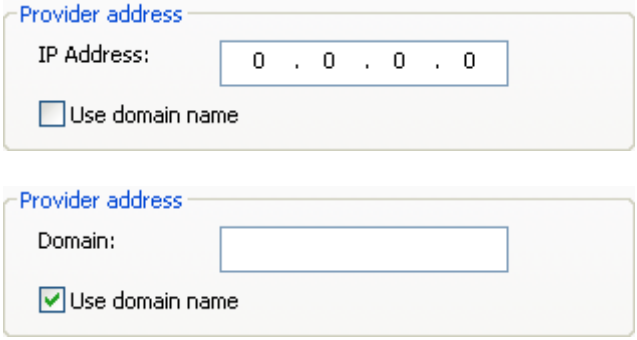
1) In the ITSP drop down list, select the appropriate ITSP vendor. Ingate has confirmed interoperability several of the leading ITSP vendors, the unique requirements of the vendor testing are contained in the Startup Tool. If the vendor choice is not seen, select "Generic ITSP".



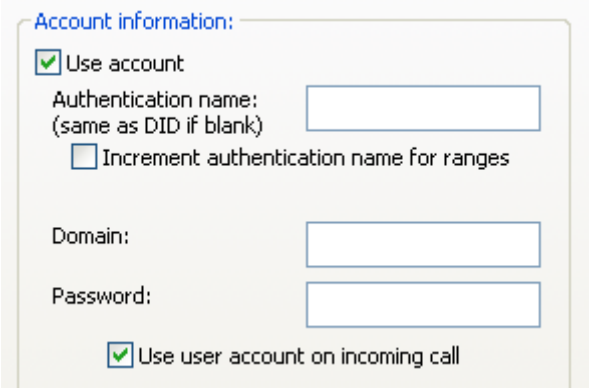
When you select a specific ITSP vendor, the Startup Tool will have the individual connection requirements predefined for that ITSP, the only additional entries may be the specific site requirements.

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.

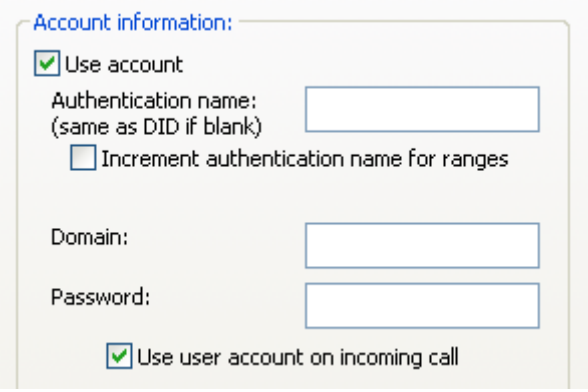


   b. In the case where the Service Provider requires the Ingate to Register with the Service Providers SIP Server or SBC, select "Use Account". When "Use Account" is selected, the Registration Account information from the Service Provider is required. Information such as Username/DID, Service Providers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

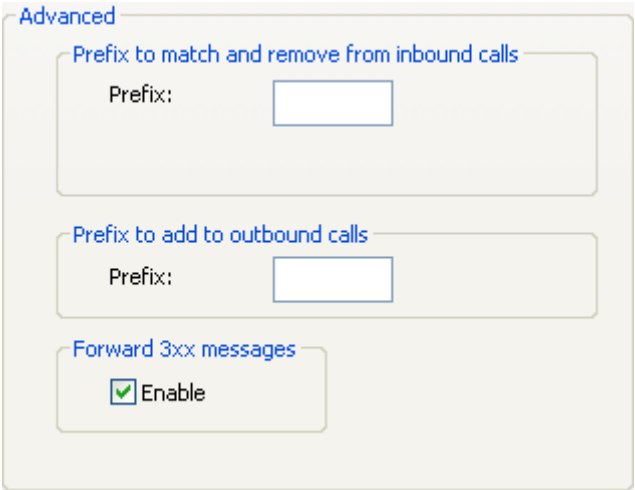


      i. Enter a DID (Username) in which the Ingate will register with the Service Provider. The Startup Tool also has the ability to program a sequential range of DIDs.

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

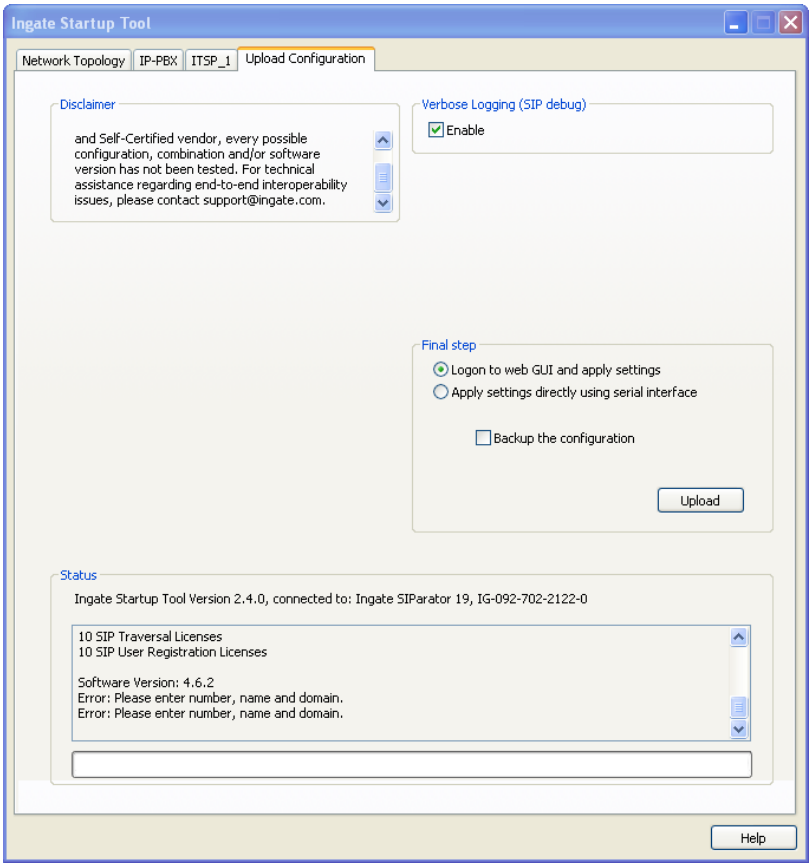


3) The Ingate has the ability to add/remove digits and characters from the Request URI Header. A typical scenario is the addition/removal of ENUM character "+". Many IP-PBX and ITSPs either need to add or remove this character prior to sending or receiving SIP requests. Here you can enter values to Match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



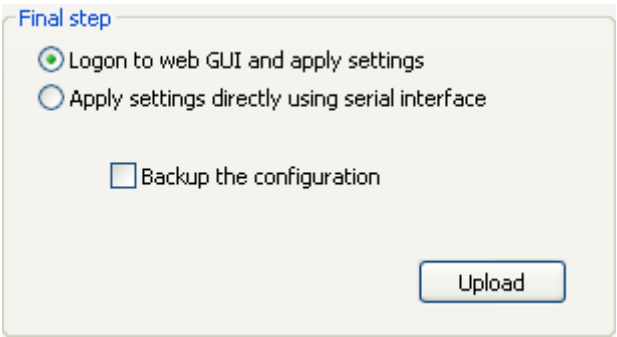
3.7 Upload Configuration

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.

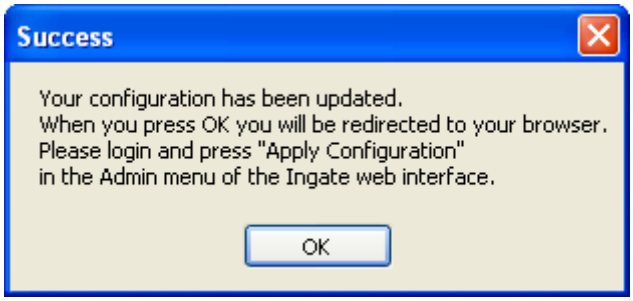


Configuration Steps:

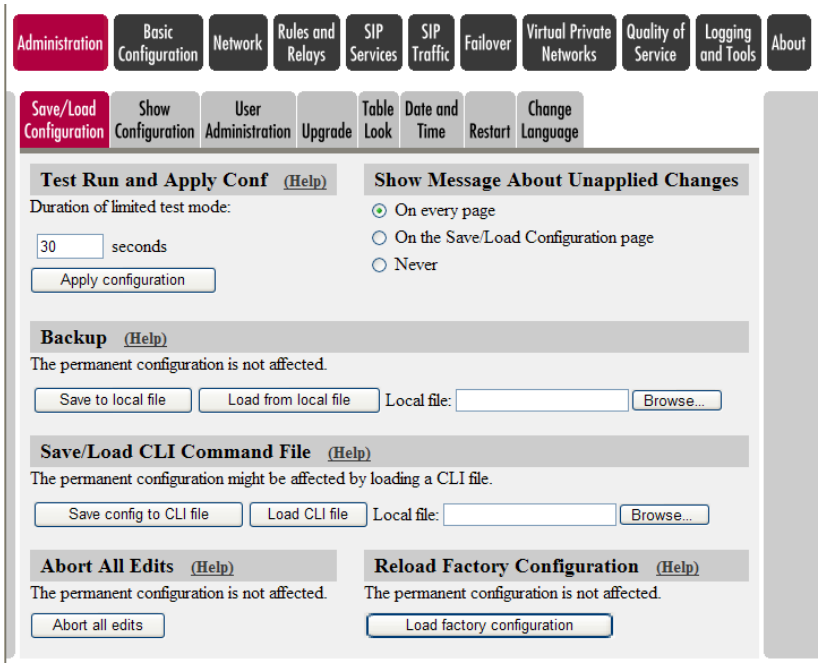
1) Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



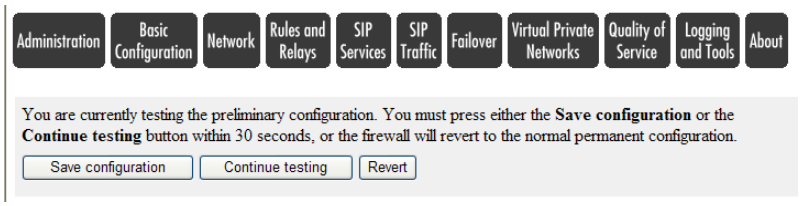
2) When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



3) Although the Startup Tool has pushed a database into the Ingate unit, the changes have not been applied to the unit. Press "Apply Configuration" to apply the changes to the Ingate unit.

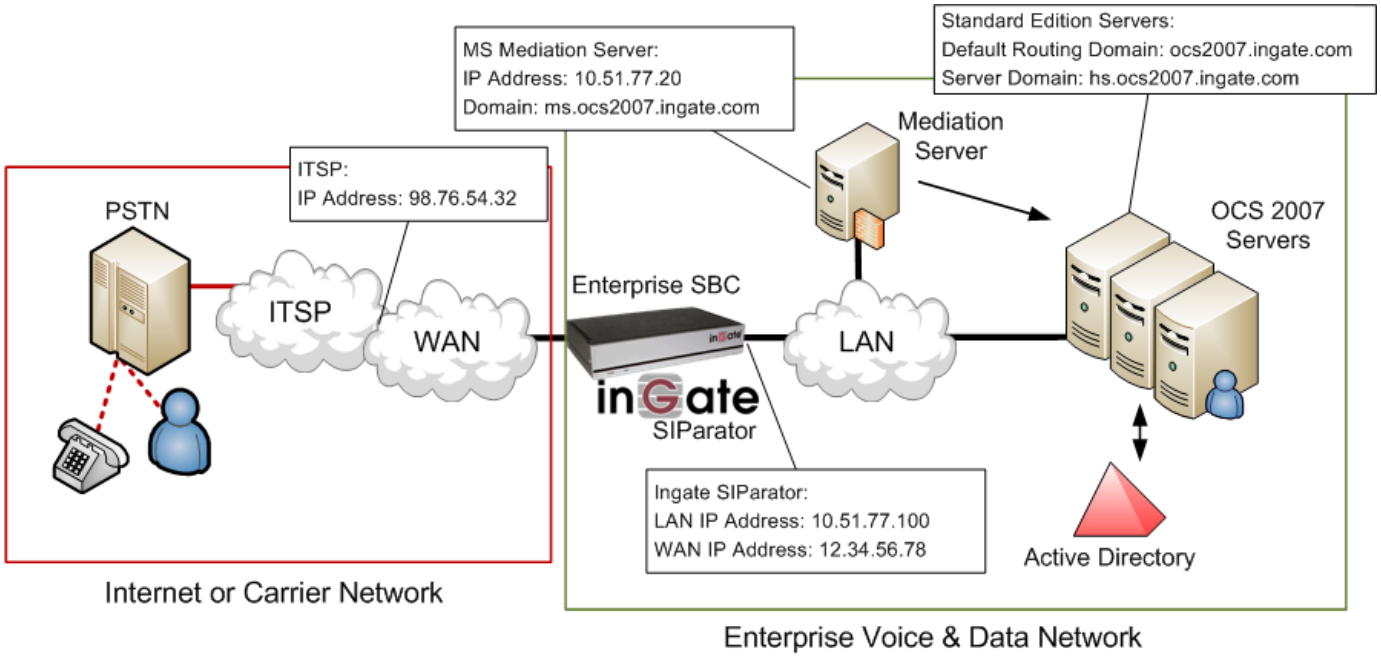


4) A new page will appear after the previous step requesting to save the configuration. Press "Save Configuration" to complete the saving process.



4 Microsoft OCS 2007 Configuration

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.



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.

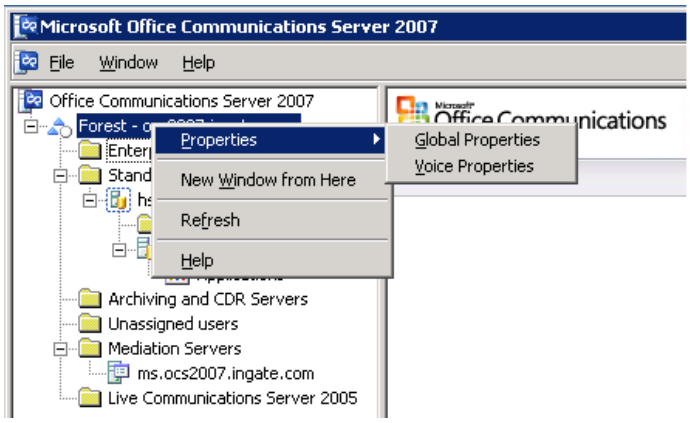
4.1 Configuration of Std Ed or Ent Ed Front End Server

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

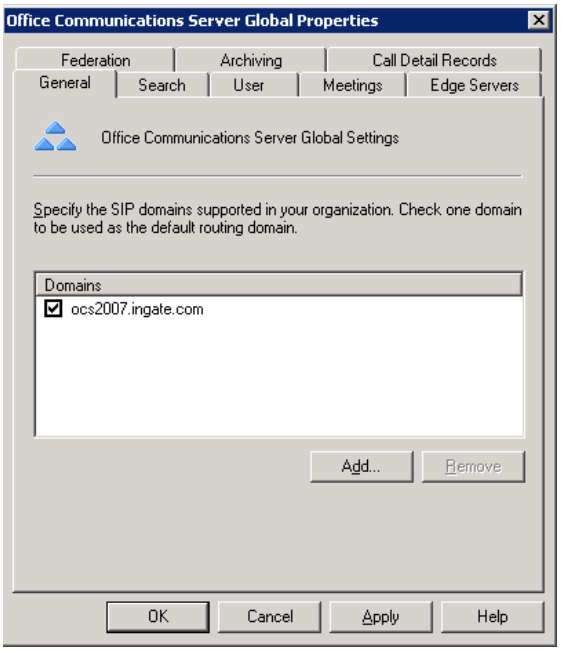
The following is an example display of OCS 2007 settings and parameters.

4.1.1 Global Properties

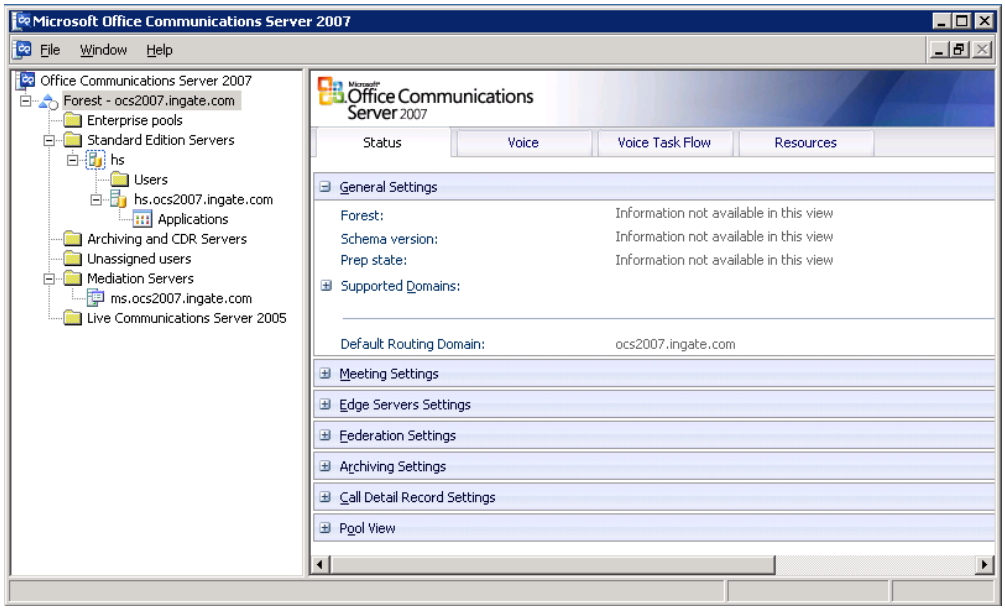
Here is a display of the Forest Global properties.



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



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

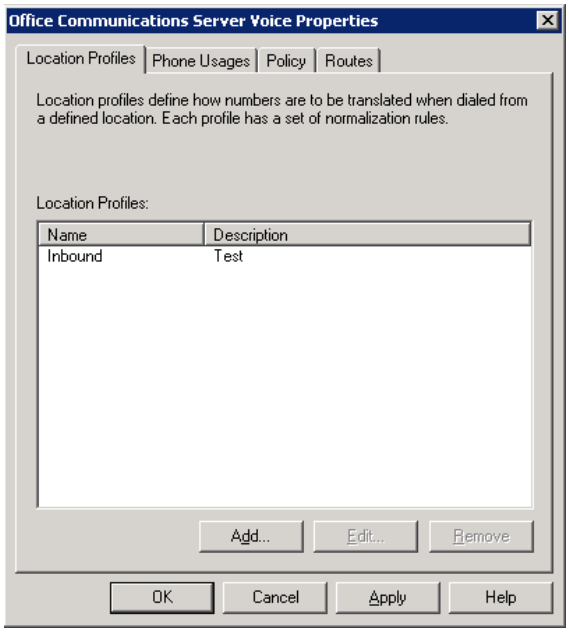


4.1.2 Voice Properties

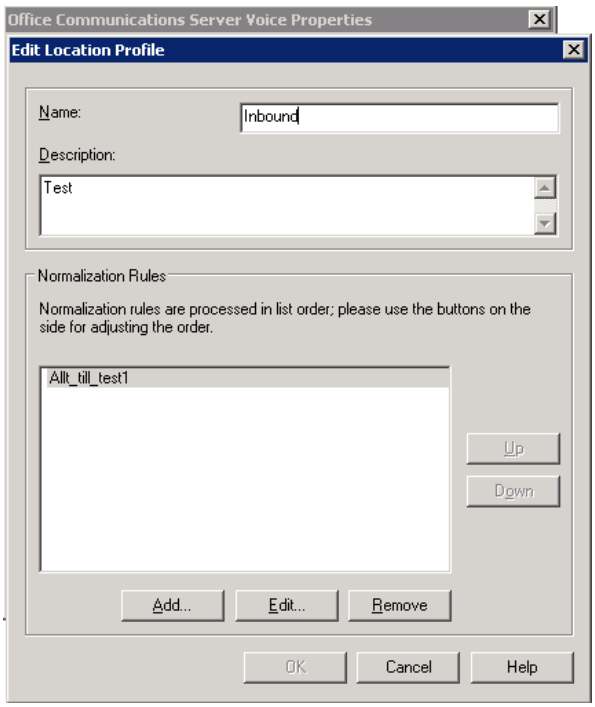
Here is a display of the Forest Voice properties.

Location Profiles

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



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

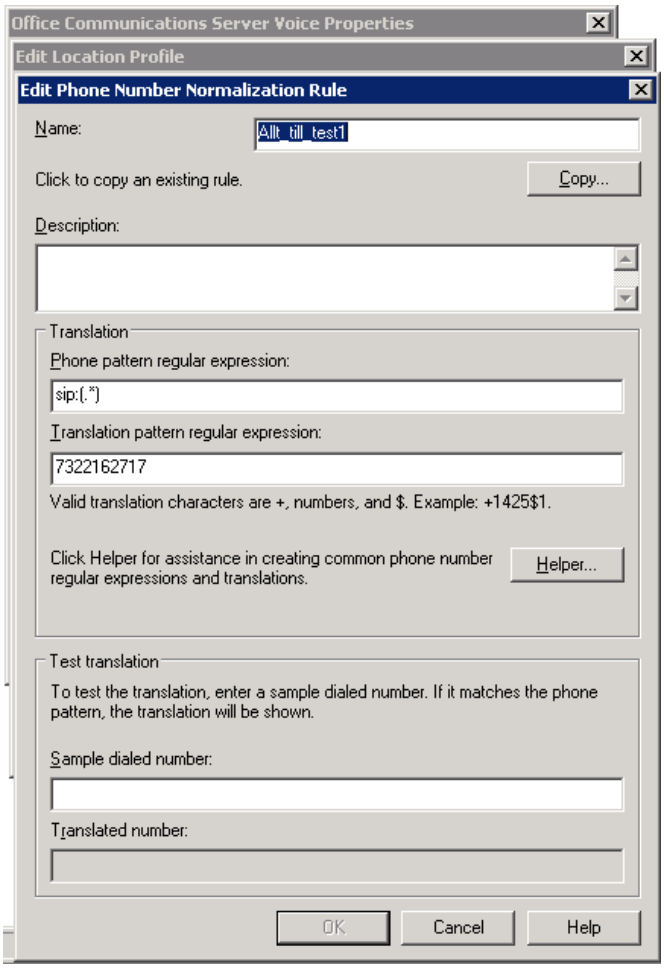


The Normalization Rules are defined within the Translations:

1) 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.

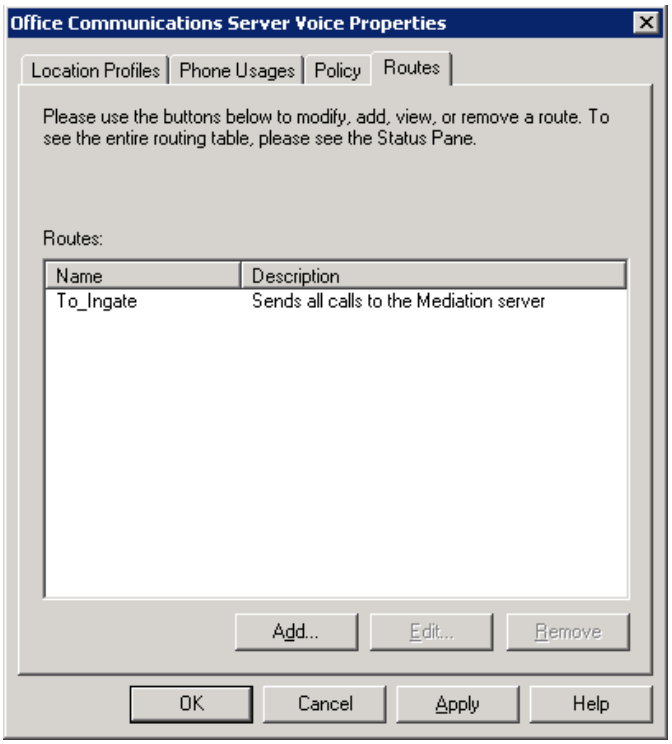
2) Translation pattern regular expression: This consists of the + symbol, numbers, and the $ symbol. The $ symbol captures the items of the phone pattern regular expression that are included inside the parenthesis. The number following the $ symbol must be less than or equal to the total number of captures 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.



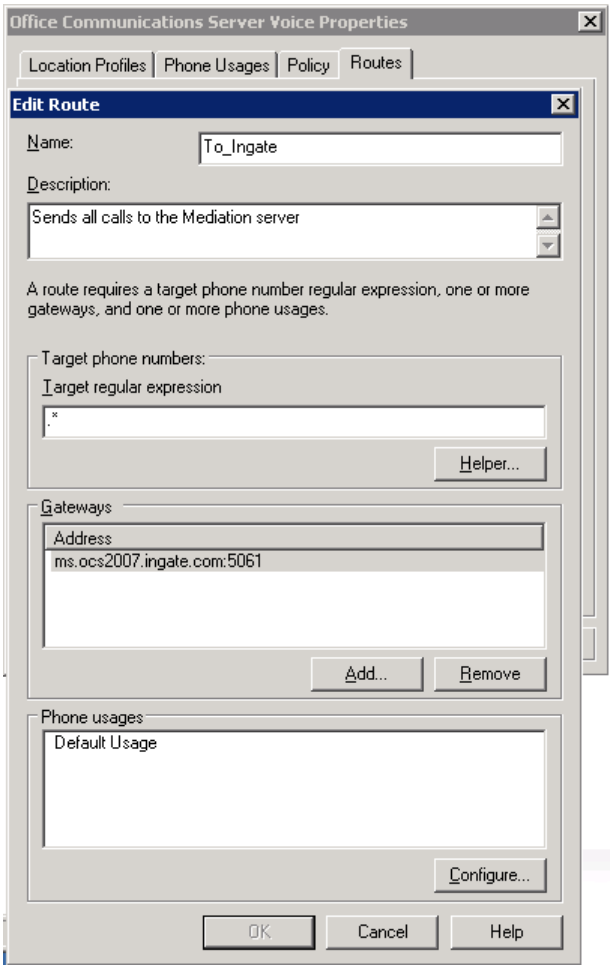
Routes

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.

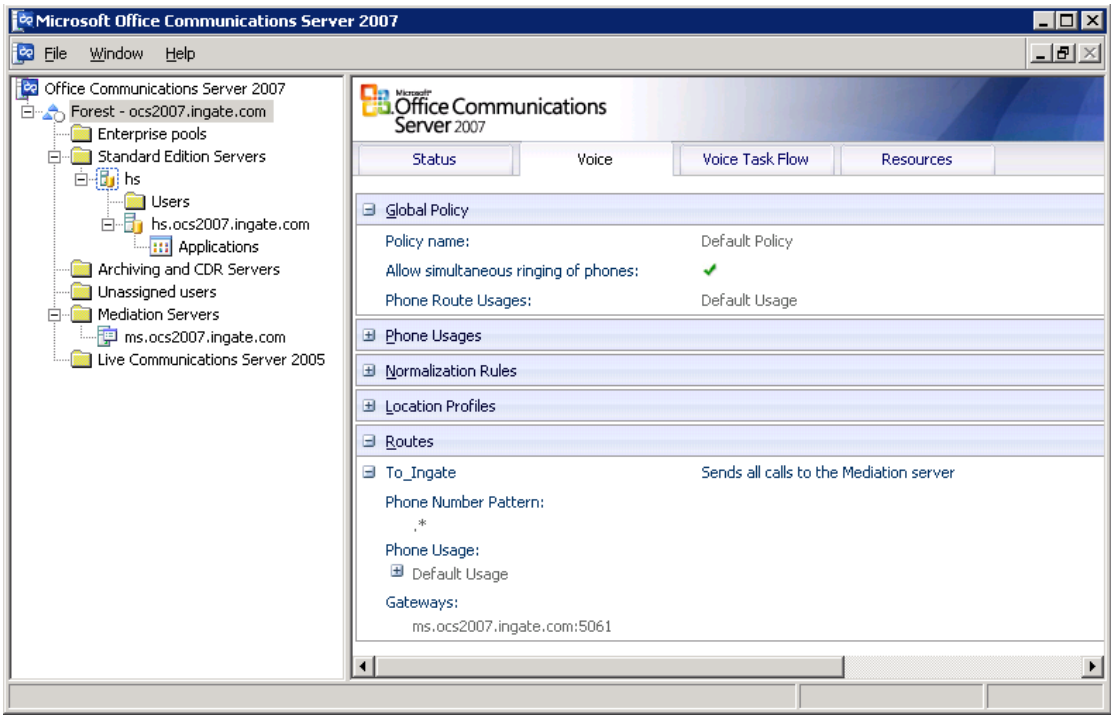


Here is where we define the Route:

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.



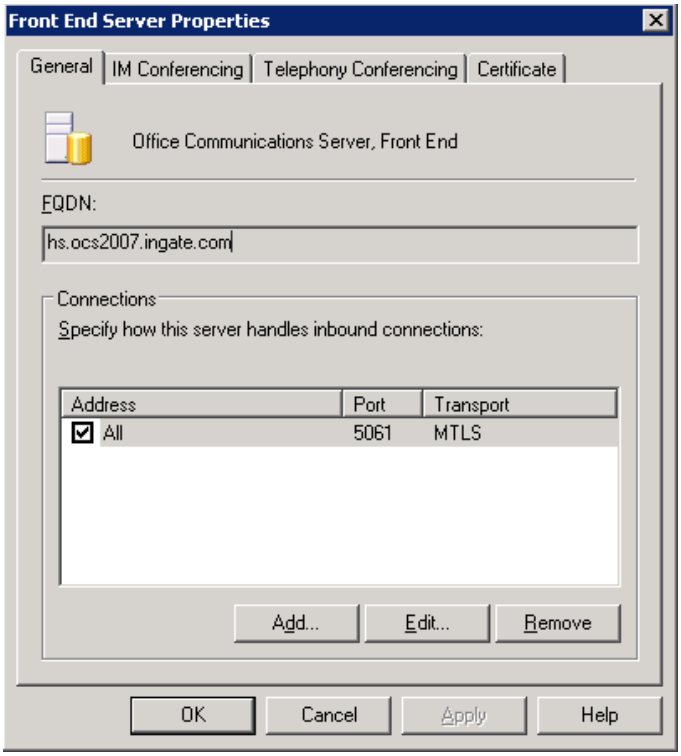
Here is the Forest – Voice page showing the voice settings.



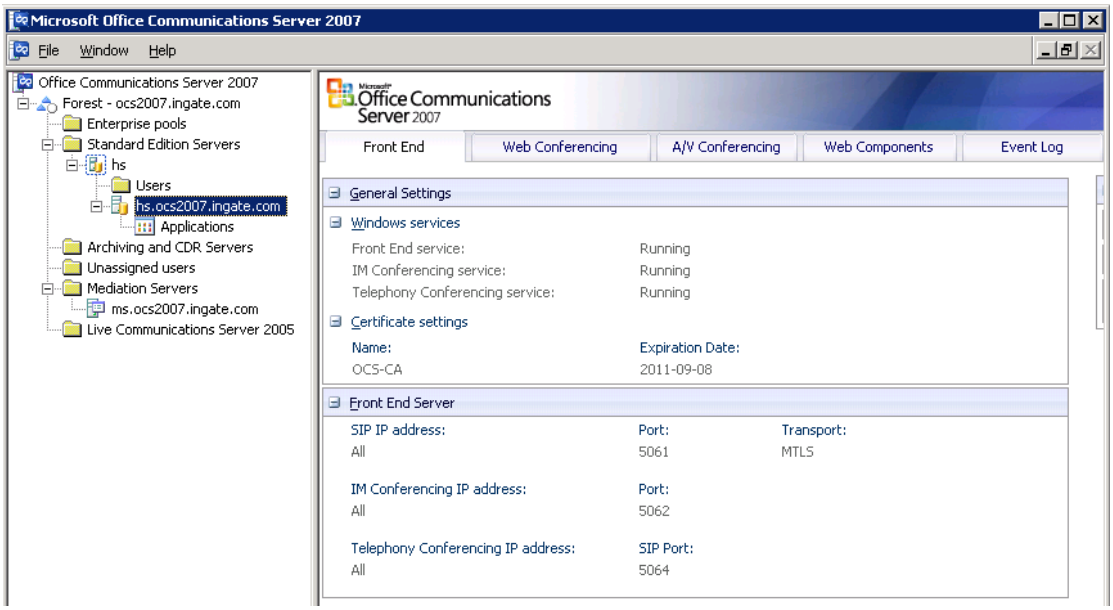
4.2 Standard Edition Servers – Front End Properties

Here is where the Front End Server handles inbound connections.

Here is where the Front End Server handles inbound connections.



Here is the Front End – Status page.

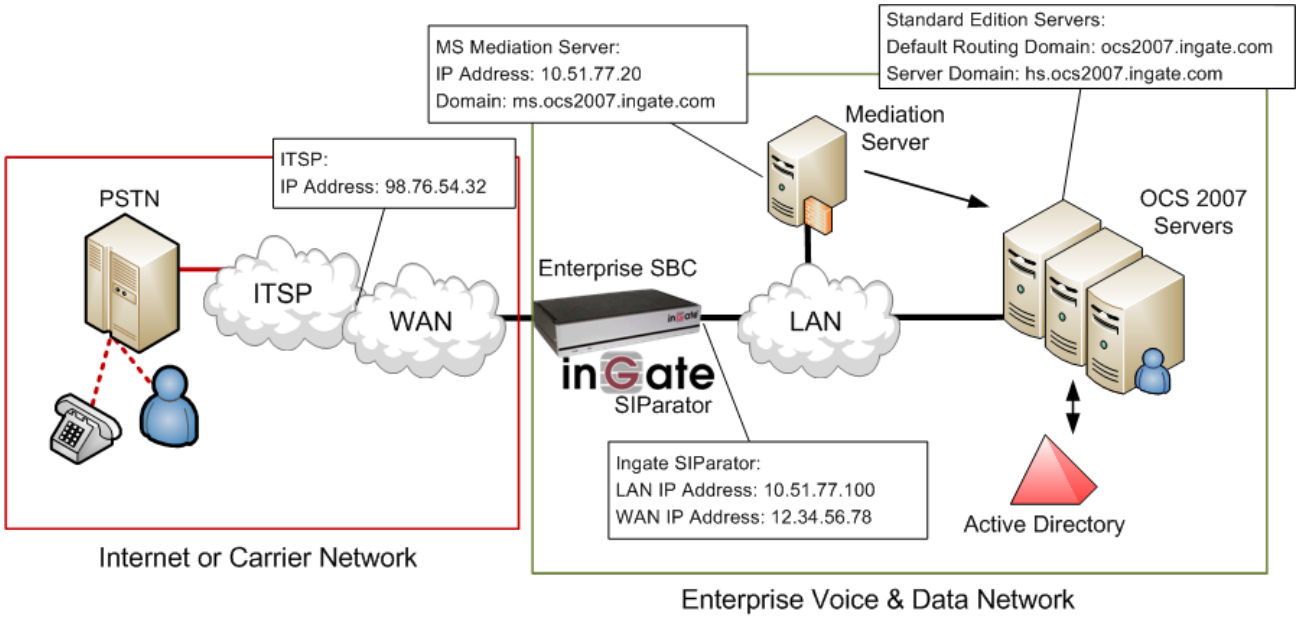


4.3 Configuration of Mediation Server

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.

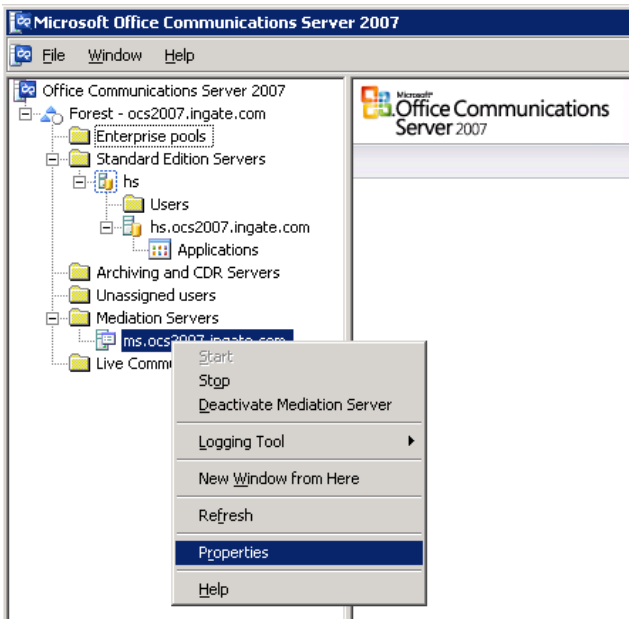
When configuring Mediation Server, you are advised to accept the default media port gateway range of 60,000 to 64,000. The default range media port range enables the server to handle up to 1,000 simultaneous voice calls. Reducing the port range greatly reduces server capacity and should be undertaken 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.

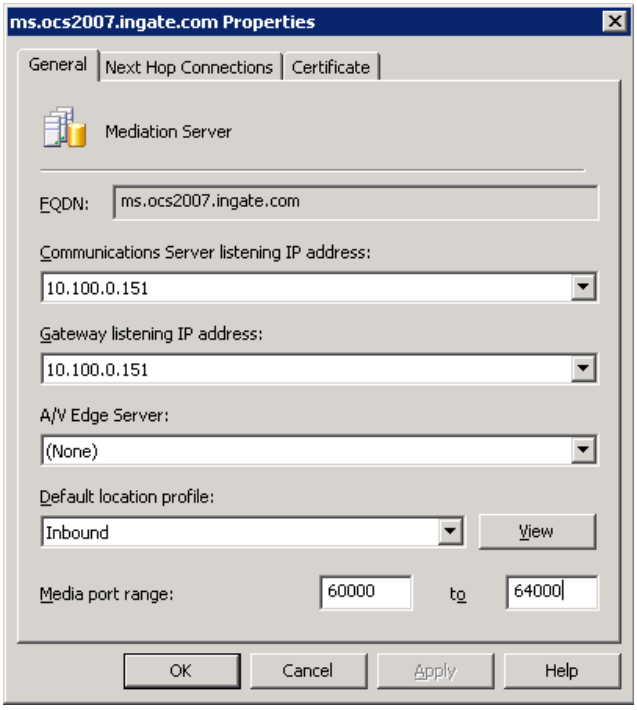


Configuration Steps:

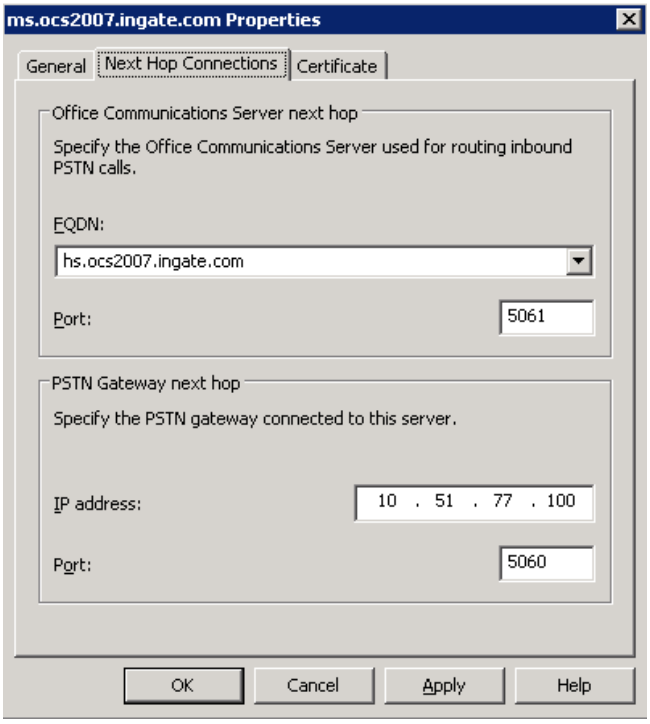
1) Go to the Mediation Server Properties.



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.



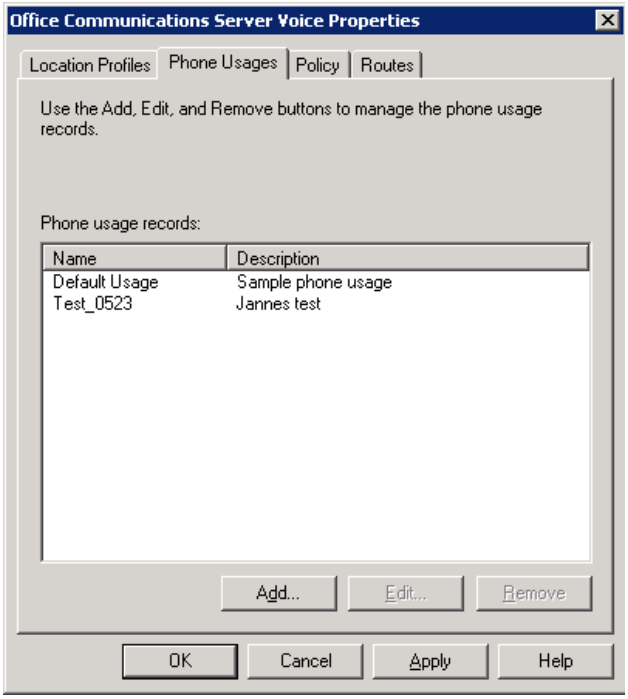
3) a) Under "Next Hop Connections", enter the IP Address and port 5060 of the Ingate SIParator in the "PSTN Gateway next hop" IP address.
b) Under "Next Hop Connections", select the SIP Domain of the Front End Server and port 5061.



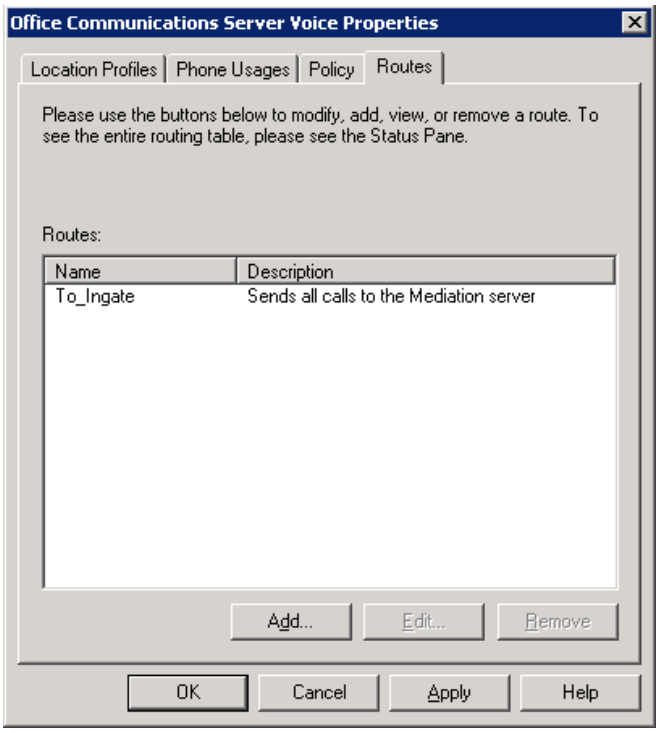
4) Start Mediation service, first on the FE-server and verify that the service is running on the Mediation server.

5) Configure Phone usage under Forrest Properties – Voice Properties.

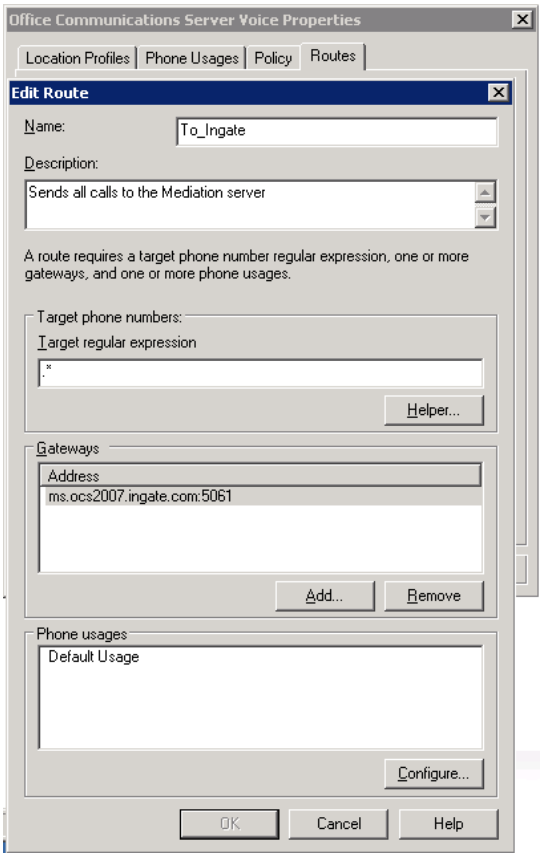
6) Phone usage records are identified as 'classes of calls' (for example, local, long-distance, or international). Phone usage records are assigned to both routes and users for the purposes of specifying call authorization. Policies are named sets of phone usage records. Policies are used to assign call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



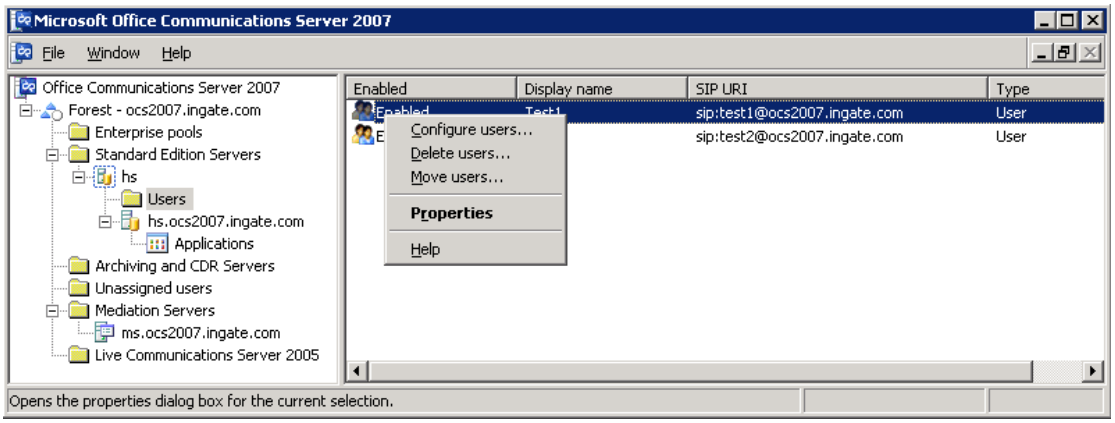
7) Add a Route that sends outbound calls to the Mediation Server. A Route requires a target phone number regular expression, one or more gateways, and one or more phone usages. Here is where we add the route.

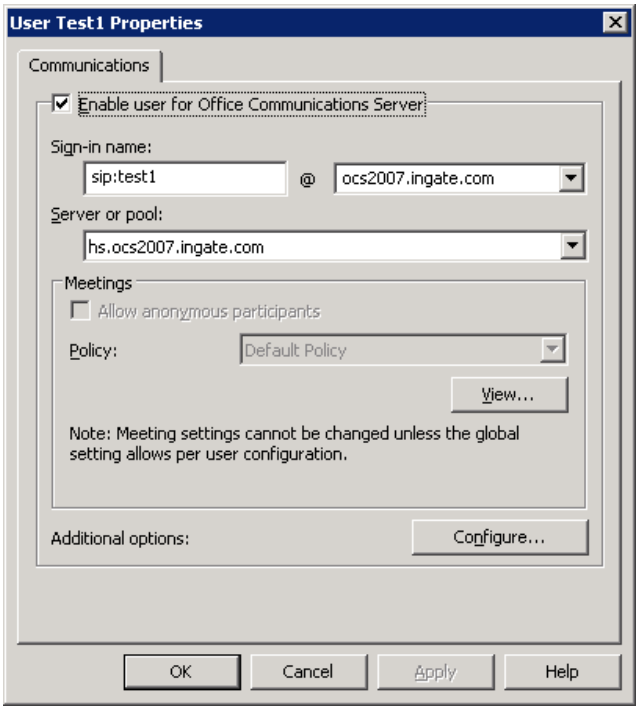


8) Here is where we define the Route:
   a. Target Phone Numbers: The number pattern that will use this Route.
   b. Gateways: The advanced media gateway or Mediation Server that calls matching this Route will be sent to.
   c. Phone Usage: The list contains the phone usage records that are required 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.

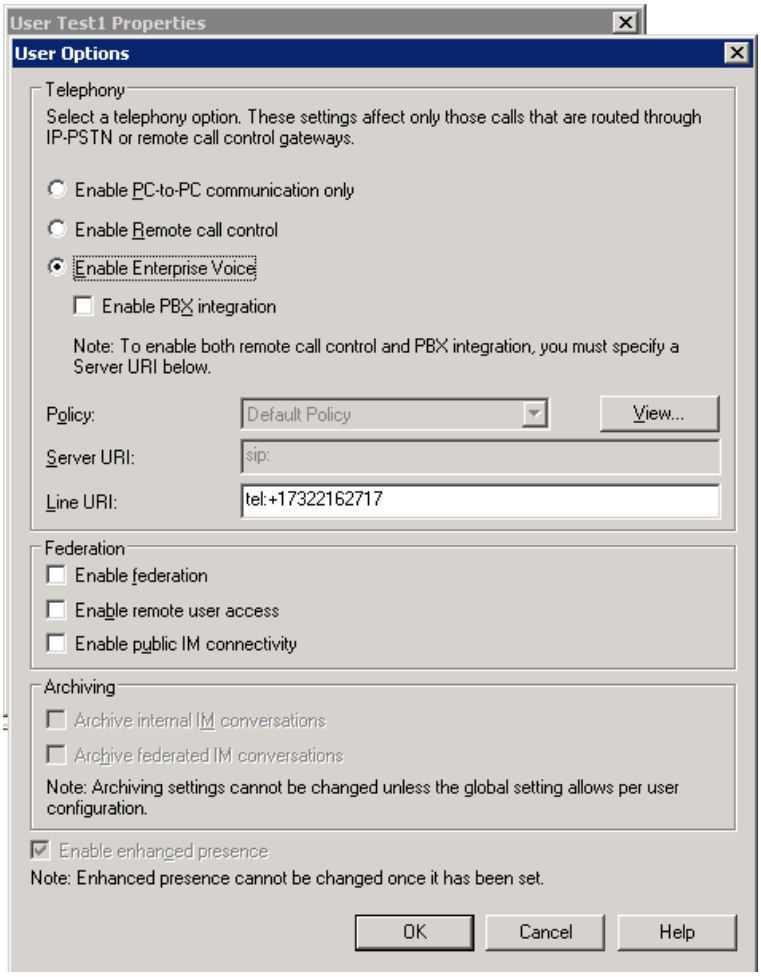


9) To enable voice for users, go to the Standard Edition Servers, in the User folder, here we enable Enterprise Voice for each user under User Properties.





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.

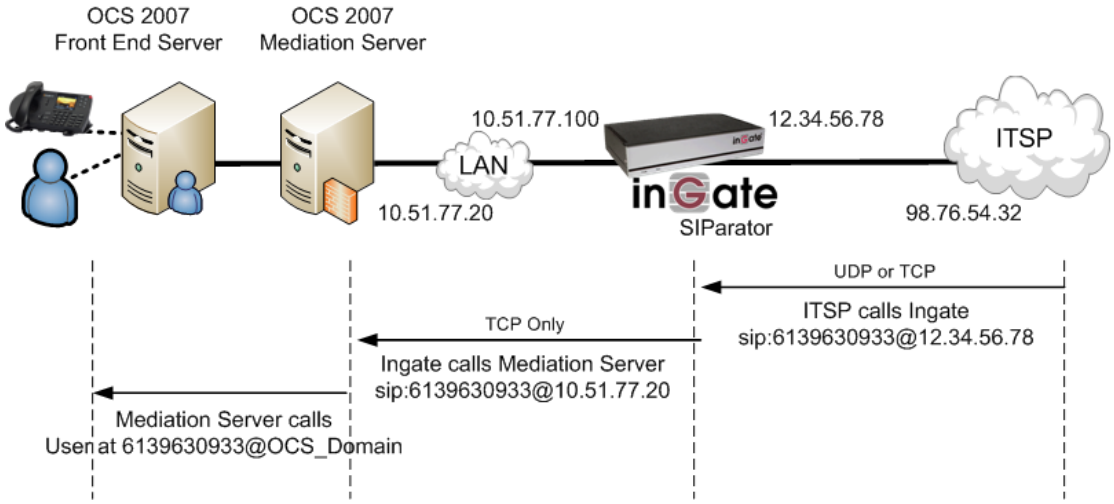


5 Troubleshooting

5.1 Call Flow Examples

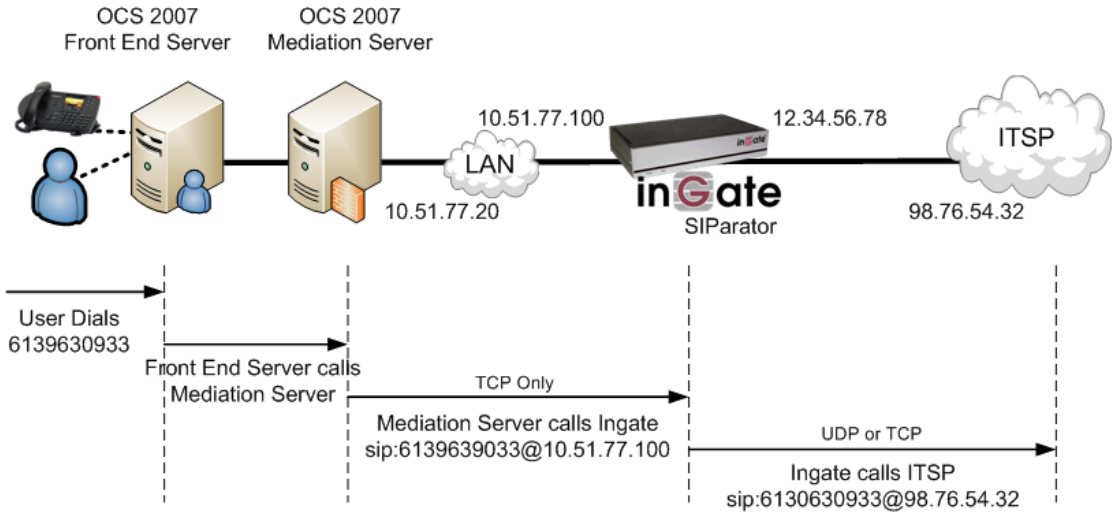
5.1.1 Incoming Call

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.



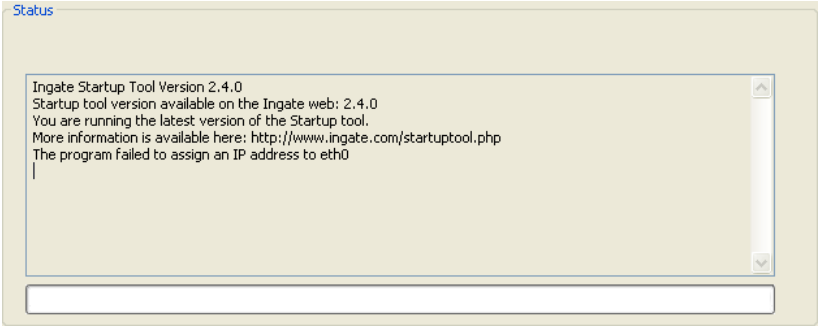
5.2 Startup Tool

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.

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"**.



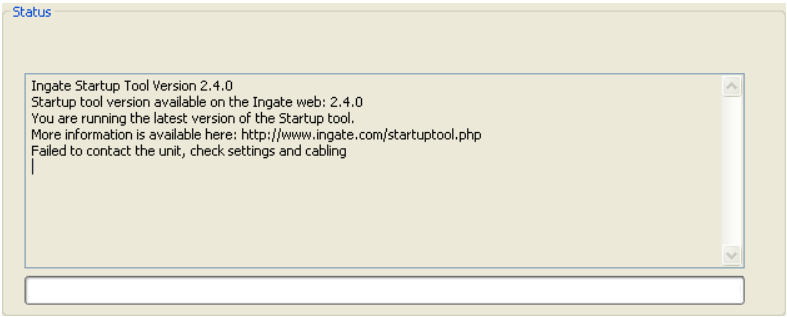
Possible Problems and Resolutions

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power (Trust me, I've been there)
Ethernet cable is not connected to Eth0.	Eth0 must always be used with the Startup Tool.
Incorrect MAC Address	Check the MAC address on the Unit itself. MAC Address of Eth0.

Possible Problems	Possible Resolution
An IP Address and/or Password have already been assigned to the Ingate Unit	It is possible that an IP Address or Password have been already been assigned to the unit via the Startup Tool or Console
Ingate Unit on a different Subnet or Network	The Startup Tool uses an application called "Magic PING" to assign the IP Address to the Unit. It is heavily reliant on ARP, if the PC with the Startup Tool is located across Routers, Gateways and VPN Tunnels, it is possible that MAC addresses cannot be found. It is the intension of the Startup Tool when configuring the unit for the first time to keep the network simple. See Section 3.
Despite your best efforts…	1) Use the Console Port, please refer to the Reference Guide, section "Installation with a serial cable", and step through the "Basic Configuration". Then you can use the Startup Tool, this time select "Change or Update the Configuration" 2) Factory Default the Database, then try again.

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.

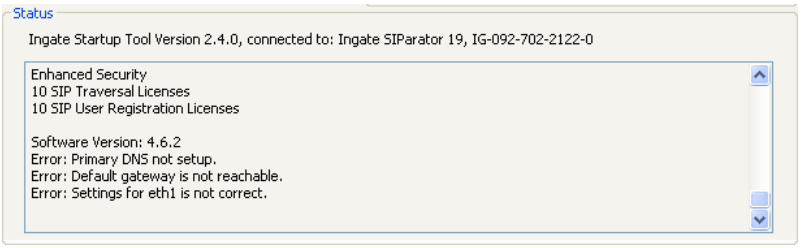


Possible Problems and Resolutions

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power
Incorrect IP Address	Check the IP Address using a Web Browser.
Incorrect Password	Check the Password.
Despite your best efforts…	1) Since this process uses the Web (http) to access the Ingate Unit, it should seem that any web browser should also have access to the Ingate Unit. If the Web Browser works, then the Startup Tool should work. 2) If the Browser also does not have access, it might be possible the PC's IP Address does not have connection privileges in "Access Control" within the Ingate. Try from a PC that have access to the Ingate Unit, or add the PC's IP Address into "Access Control".

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.

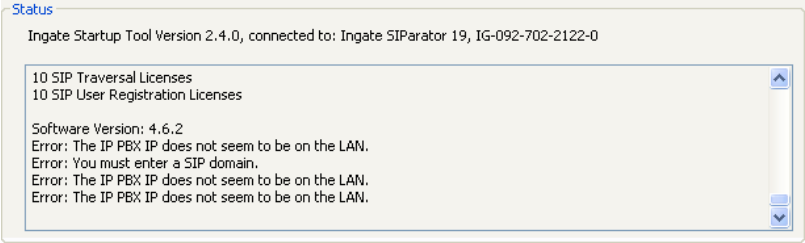


Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: Default gateway is not reachable.	The Default Gateway is always the way to the Internet, in the Standalone or Firewall it will be the Public Default Gateway, on the others it will be a Gateway address on the local network.
Error: Settings for eth0/1 is not correct.	IP Address of Netmask is in an Invalid format.
Error: Please provide a correct netmask for eth0/1	Netmask is in an Invalid format.
Error: Primary DNS not setup.	Enter a DNS Server IP address

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.

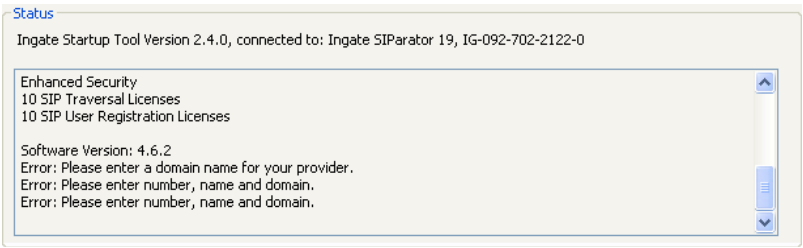


Possible Problems and Resolutions

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

5.2.6 ITSP

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

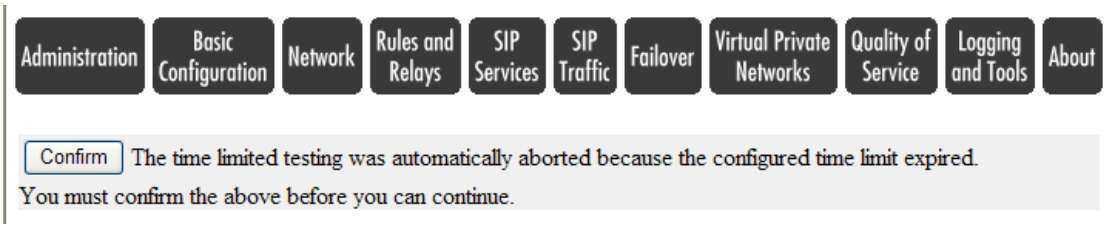


Possible Problems and Resolutions

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

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 and Resolutions

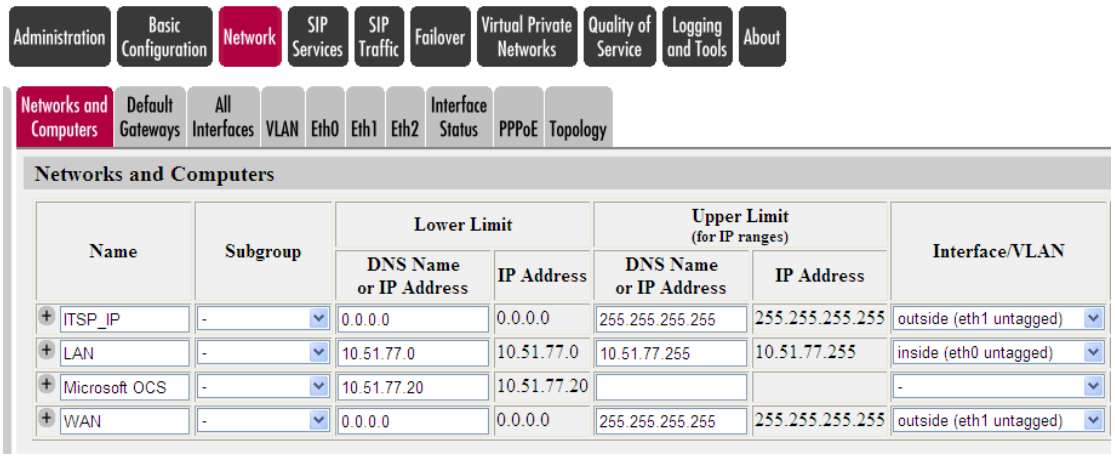
Possible Problems	Possible Resolution
Eth0 Interface IP Address has changed	Increase the duration of the test mode, press "Apply Configuration" and start a new browser to the new IP address, then press "Save Configuration"
Access Control does not allow administration from the IP address of the PC.	Verify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

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

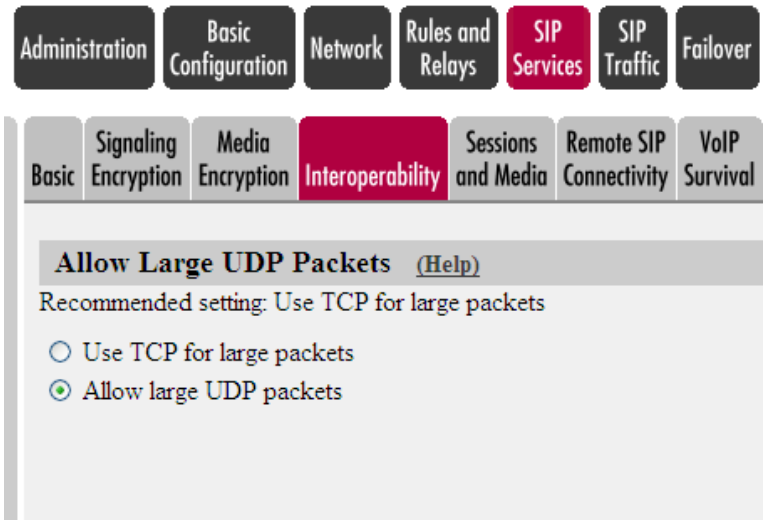
This is an example of the Network – Networks and Computers page with an Ingate SIParator in a Stand-alone configuration. The Networks and Computer page is a IP Table List or Route List, providing the Ingate knowledge of its surrounding networks and what interface they are connected too. Also, the table 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.



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

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.

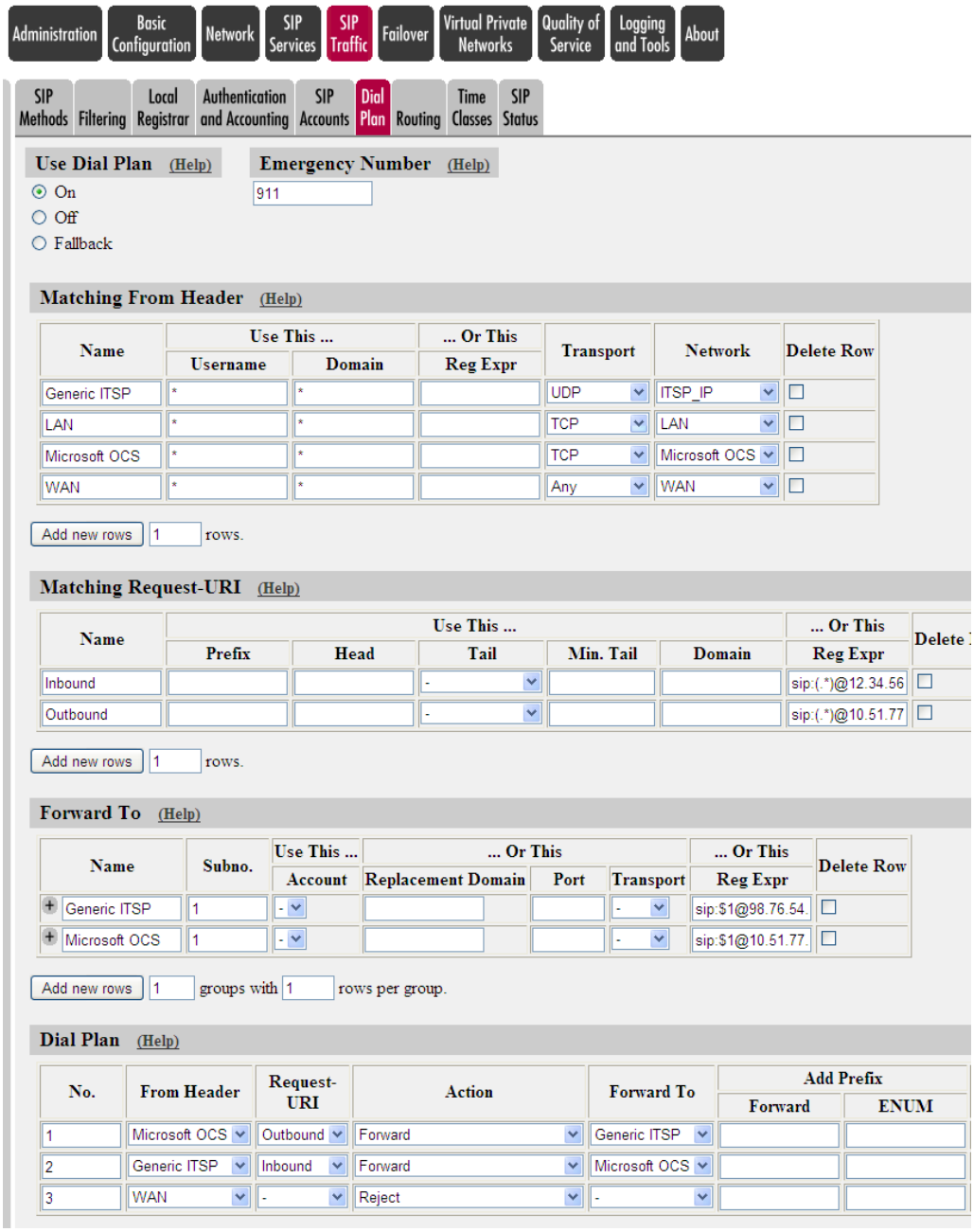


5.3.3 Dial Plan

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

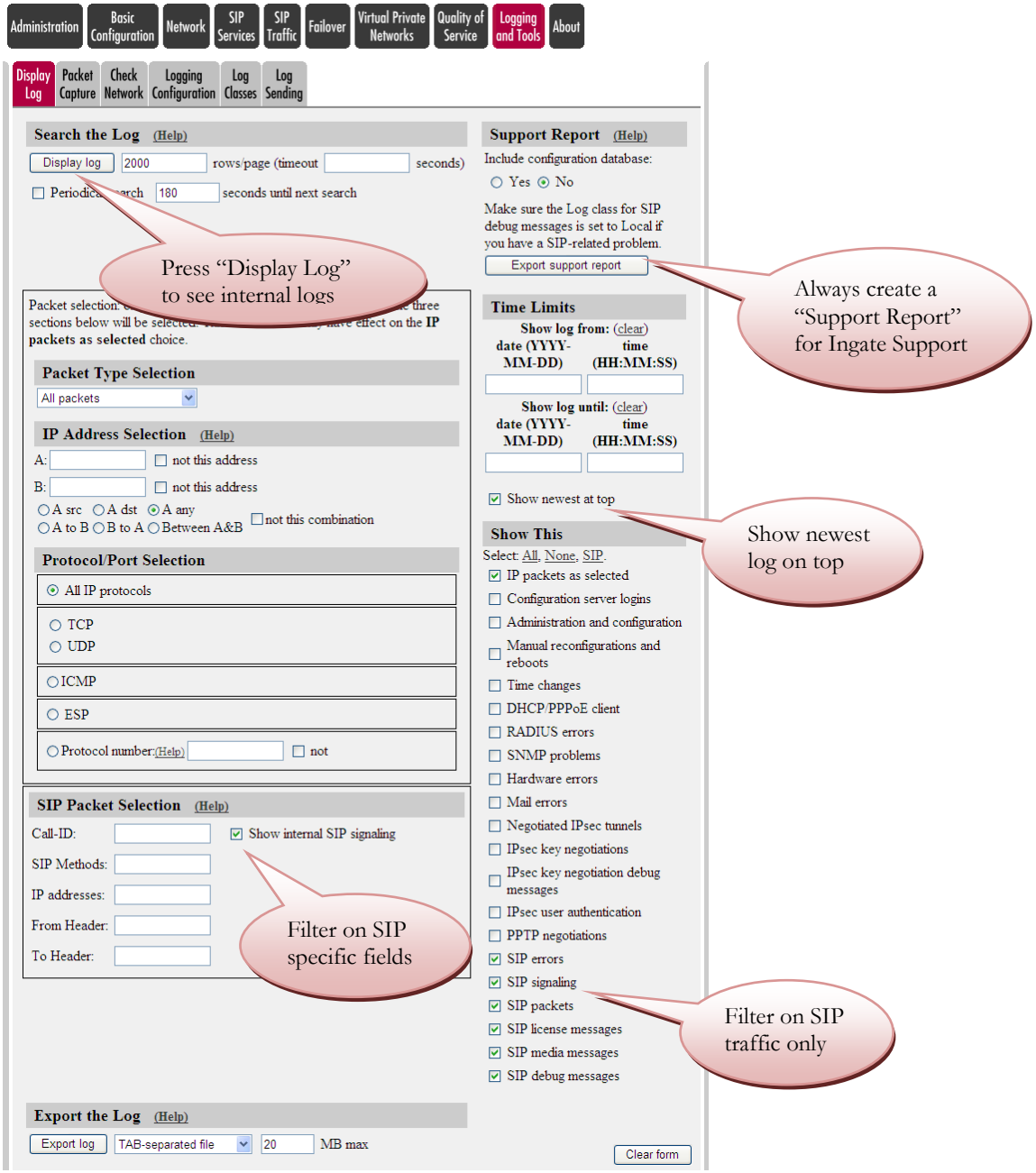
If the Service Provider does not support TCP, be sure to define the ITSP for use with the UDP transport, with a Regular Expression sip:$1@98.76.54.32;transport=udp



5.4 Ingate Troubleshooting Tools

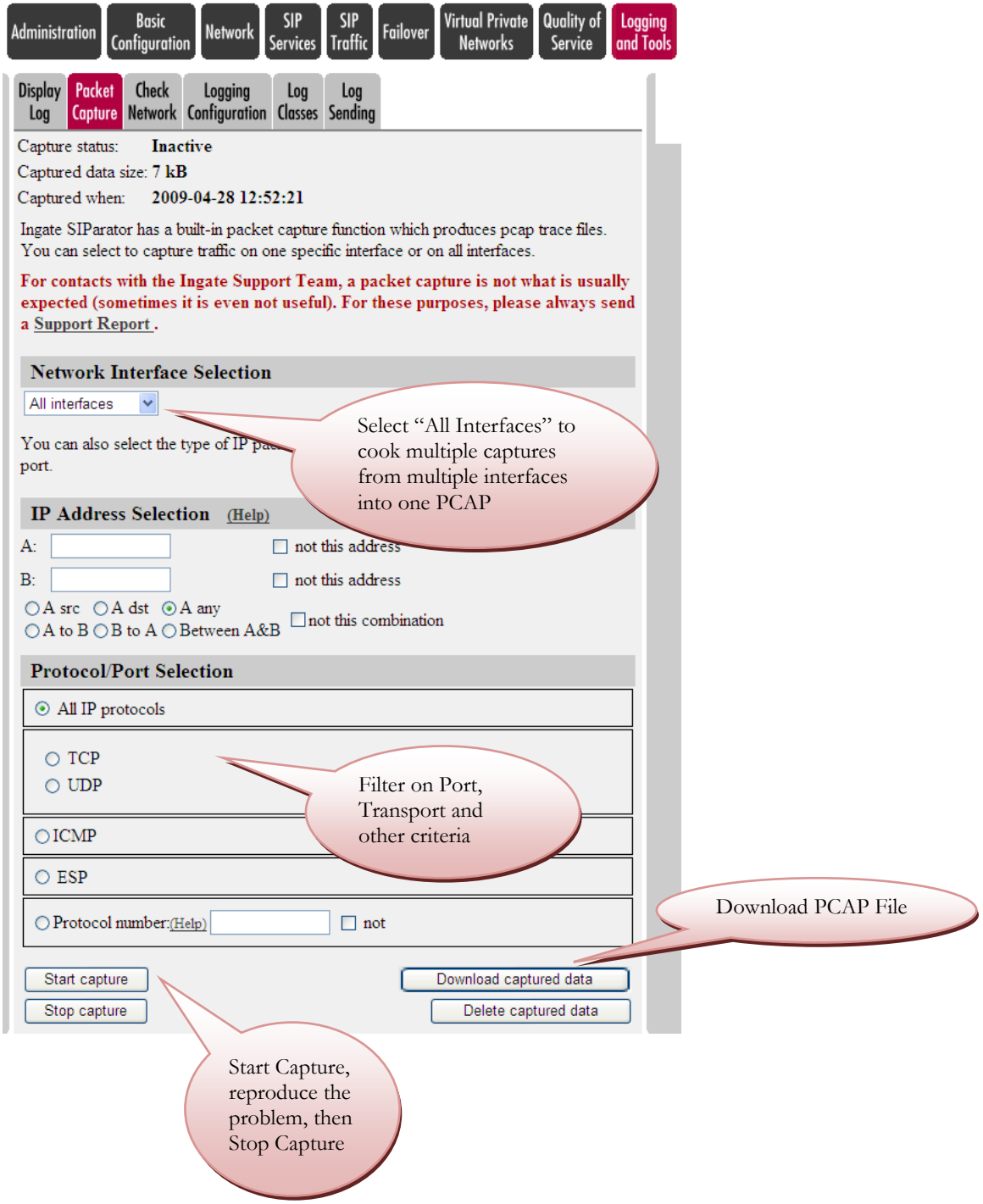
5.4.1 Display Logs

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



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.



5.4.3 Check Network

Standard PING and Trace Route feature for simple network checks.